GUIDE PRATIQUE – ÉDITION NOVEMBRE 2026 – SUISSE

IA DANS L'ENTREPRISE

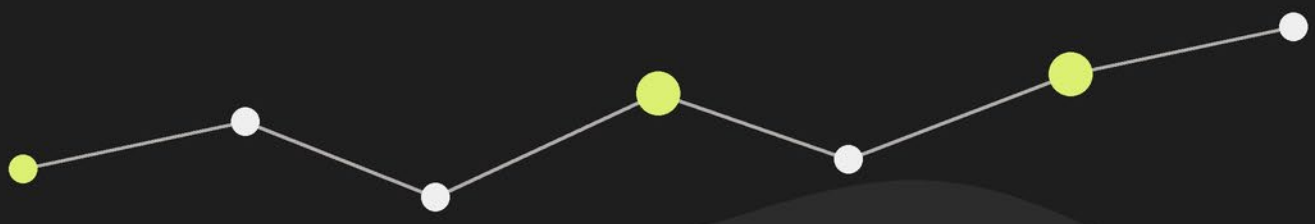
Transformer l'IA en valeur, sans perdre le contrôle

Le guide pratique pour une adoption utile, sécurisée et maîtrisée

Édition novembre 2026 • Suisse

VALEUR MÉTIER · DONNÉES · SÉCURITÉ · GOUVERNANCE

awsmtech.ch | +41 (0) 22 552 60 70 | mail@awsmtech.ch



NOTE AU LECTEUR

Ce livre blanc s'adresse aux dirigeantes et dirigeants, responsables métiers, responsables informatiques, responsables de la sécurité et fonctions de conformité des organisations suisses. Il propose un cadre de décision : il ne constitue ni un avis juridique, ni une certification de conformité, ni une promesse de performance.

L'intelligence artificielle évolue vite. Les fonctionnalités, contrats, lieux de traitement, sous-traitants, modèles et obligations doivent être revérifiés au moment d'un choix ou d'un déploiement. Les exemples proposés sont volontairement simplifiés et doivent être adaptés au contexte, au secteur et à l'appétence au risque de chaque organisation.

LE POINT DE VUE AWSMTECH

L'enjeu n'est plus simplement de donner accès à l'IA. Il est d'organiser son utilisation autour des données, des processus, de la sécurité, de la responsabilité humaine et de la valeur mesurable.

Comment utiliser ce guide

1. Commencez par le résumé exécutif et les dix décisions de direction.
2. Utilisez la matrice des données et la checklist comme outils opérationnels.
3. Appliquez la méthode AWSMTECH 6D à un cas d'usage réel, limité et mesurable.
4. Faites valider les points juridiques, contractuels et sectoriels pertinents avant mise en production.

À propos de cette édition

Cette version intègre un cadrage suisse renforcé, une distinction claire entre conformité, cybersécurité et gouvernance, un traitement approfondi du Shadow AI, un chapitre consacré à Microsoft 365 Copilot et aux IA professionnelles, un cadre spécifique pour les agents, une méthode de déploiement en six étapes et une feuille de route de 90 jours.

RÉSUMÉ EXÉCUTIF

L'IA n'est plus un projet futur. Elle est déjà utilisée pour rédiger, rechercher, résumer, traduire, analyser, préparer des réunions, produire du code ou automatiser des tâches. Cette diffusion crée des gains rapides, mais aussi un écart entre les usages réels et la capacité de l'entreprise à les gouverner.

01 — Valeur
Partir d'un problème métier, pas d'un outil. Définir un résultat observable avant de choisir une technologie.

02 — Données
Savoir quelles informations entrent, sortent, sont conservées et deviennent accessibles à l'IA.

03 — Sécurité
Protéger identités, permissions, terminaux, connecteurs, journaux et actions disponibles aux agents.

04 — Gouvernance
Attribuer un responsable, fixer les usages autorisés et prévoir validation humaine, mesure et arrêt.

Les dix décisions de direction

1. Nommer un sponsor métier et un responsable opérationnel de l'IA.
2. Cartographier les usages déjà présents, y compris les comptes personnels et outils non approuvés.
3. Définir une politique simple : autorisé, autorisé sous conditions, interdit.
4. Classer les données et relier chaque classe aux environnements IA autorisés.
5. Sélectionner les cas d'usage selon valeur, faisabilité, risque et effort.
6. Assainir les identités, droits d'accès et pratiques de partage avant une IA connectée.
7. Séparer assistance, recommandation et action autonome ; augmenter les contrôles avec le pouvoir d'agir.
8. Mesurer la situation de départ puis la qualité, le temps, le coût et le risque après déploiement.
9. Former les collaborateurs aux usages, aux limites et à la responsabilité de vérification.
10. Industrialiser seulement les usages dont la valeur nette et la maîtrise du risque sont démontrées.

LA QUESTION À POSER DÈS MAINTENANT
Savez-vous où l'IA est utilisée dans votre entreprise, avec quelles données, pour quelle valeur et sous quel contrôle ?

SOMMAIRE

01 De l'expérimentation à la maîtrise

02 Comprendre l'IA sans jargon inutile

03 Trouver la valeur : cas d'usage et priorités

04 Shadow AI : rendre visible l'invisible

05 Données : décider ce que l'on peut confier à une IA

06 IA professionnelle et Microsoft 365 Copilot

07 Architecture : choisir le bon niveau d'intégration

08 Cybersécurité : protéger le système complet

09 Cadre suisse, LPD et portée européenne

10 Gouvernance : règles, rôles et preuves

11 Agents IA : quand le logiciel peut agir

12 La méthode AWSMTECH 6D

13 Feuille de route des 90 premiers jours

14 ROI, adoption et conduite du changement

15 Sobriété numérique et horizon 2027-2030

16 Checklist, charte et outils pratiques

17 Conclusion et accompagnement AWSMTECH (Switzerland) SA

CHAPITRE 01

DE L'EXPÉRIMENTATION À LA MAÎTRISE

L'IA devient un sujet de direction lorsqu'elle touche aux données, aux décisions et aux processus.

L'intelligence artificielle n'est plus réservée aux équipes techniques ou aux grandes entreprises. Elle est déjà présente dans les logiciels bureautiques, la relation client, les outils de sécurité, les plateformes métier et les services accessibles depuis un navigateur. Pour un dirigeant, la question n'est donc plus de savoir s'il faut s'y intéresser, mais comment l'utiliser de manière utile, maîtrisée et responsable.

Derrière la simplicité apparente d'une conversation avec un assistant se trouvent des décisions structurantes : quelles données peut-on lui confier ? Où sont-elles traitées ? Quels droits utilise-t-il ? Qui vérifie la réponse ? Que se passe-t-il si le système agit ? Comment calcule-t-on le coût complet ? Et comment s'assure-t-on que le temps libéré crée réellement de la valeur ?

Quatre piliers indissociables

Pilier	Question de direction	Signal d'alerte
Valeur métier	Quel résultat doit s'améliorer et comment le mesurer ?	Un achat de licences sans cas d'usage ni référence de départ.
Données	Quelles informations sont utilisées, avec quels droits et quelle qualité ?	Des partages historiques trop larges ou des sources non fiables.
Sécurité	Comment protéger l'accès, le traitement, les connecteurs et les actions ?	Un agent ou une extension dispose de plus de droits que nécessaire.
Gouvernance	Qui décide, contrôle, documente et répond en cas d'erreur ?	Personne ne peut arrêter l'usage ou expliquer sa finalité.

De l'outil à la capacité d'entreprise

Un chatbot isolé produit des réponses. Une capacité d'entreprise relie l'IA à un processus, à des données autorisées, à des identités, à des règles, à des indicateurs et à une responsabilité humaine. La différence entre les deux ne se joue pas seulement sur le modèle : elle se joue sur l'intégration et l'exploitation.

À RETENIR POUR LE DIRIGEANT

L'IA accélère ce qui existe. Sur un processus clair et maîtrisé, elle peut créer un avantage. Sur un processus confus, elle accélère les incohérences.

CHAPITRE 02

COMPRENDRE L'IA SANS JARGON INUTILE

Un système puissant reste probabiliste : la fluidité de la réponse ne garantit ni la vérité ni l'adéquation au contexte.

Ce qu'est une IA générative

Un modèle de langage calcule une réponse probable à partir d'instructions et de contexte. Il ne raisonne pas comme une personne, ne connaît pas spontanément la politique interne de l'entreprise et ne distingue pas toujours un fait d'une formulation plausible. Sa performance dépend de l'entraînement du modèle, du contexte fourni, des outils auxquels il a accès et des contrôles qui entourent son usage.

Les cinq limites à garder en tête

Limite	Conséquence	Réponse organisationnelle
Erreur factuelle	Une réponse crédible peut être fausse ou datée.	Exiger des sources, définir les contrôles et garder une validation humaine.
Contexte incomplet	Le système ignore une exception métier ou une règle locale.	Fournir une base documentaire maîtrisée et tester les exceptions.
Biais	Le résultat peut reproduire des déséquilibres des données ou du processus.	Évaluer par groupes et scénarios ; documenter les décisions sensibles.
Variabilité	Deux formulations proches peuvent produire des résultats différents.	Utiliser gabarits, règles, évaluations et seuils d'acceptation.
Confidentialité	Une donnée transmise peut sortir du périmètre attendu.	Limiter les données, approuver les outils et encadrer les connecteurs.

Le système compte davantage que le modèle

Dans un usage professionnel, la qualité vient rarement d'un modèle seul. Elle résulte d'un ensemble : identité de l'utilisateur, interface, consigne, documents de référence, règles métier, calculs déterministes, filtres, journalisation, supervision et procédure de recours. Remplacer un modèle sans revoir cet ensemble améliore parfois peu le résultat.

RAG, règles et calculs

Une architecture de recherche augmentée par génération (RAG) sélectionne des documents autorisés avant de demander au modèle de répondre. Elle peut améliorer la pertinence et la traçabilité, à condition que les sources soient à jour, bien classées et accessibles aux bonnes personnes. Les calculs critiques, règles tarifaires et conditions d'éligibilité doivent autant que possible rester déterministes : l'IA explique ou assiste, mais une règle contrôlée décide.

PRINCIPE DE CONCEPTION

Ne demandez pas à une consigne de compenser une architecture faible. Les droits, les règles, les tests et la supervision sont des contrôles plus solides qu'un simple « sois prudent ».

CHAPITRE 03

TROUVER LA VALEUR : CAS D'USAGE & PRIORITÉS

Le bon projet n'est pas le plus spectaculaire. C'est celui qui améliore un travail réel avec un risque maîtrisable.

Quatre familles de valeur

Accélérer
Recherche, synthèse, préparation, rédaction de première version, classement et extraction.

Améliorer
Contrôles de cohérence, couverture documentaire, standardisation et qualité de service.

Augmenter
Assistance contextuelle, analyse de scénarios et accès à l'expertise au moment du besoin.

Transformer
Reconfiguration d'un processus de bout en bout, avec orchestration, règles et actions contrôlées.

Exemples adaptés aux métiers sensibles

Secteur	Cas d'usage à faible exposition	Cas d'usage à encadrer fortement
Études d'avocats	Synthèse de sources publiques, préparation de trames, recherche dans une base validée.	Analyse de dossiers clients, secret professionnel, génération de conclusions ou décisions.
Fiduciaires	Préparation de listes de pièces, explication de procédures, classification.	Analyse de salaires, fiscalité personnalisée, rapprochements et écritures automatiques.
Cliniques privées	Documentation interne, préparation de supports, aide administrative.	Données de santé, triage, recommandation clinique ou communication patient.
Banques privées	Veille publique, préparation de rendez-vous, synthèse documentaire.	Profilage, crédit, conseil, transaction ou décision affectant un client.
Notaires	Modèles de courriers, recherche de clauses approuvées, contrôle de complétude.	Actes, identités, successions, transfert automatique vers des systèmes métier.
ONG / institutions	Traduction, capitalisation, synthèse de rapports publics.	Données de bénéficiaires, localisation sensible, décisions d'allocation.

La matrice de priorité

Évaluez chaque idée sur quatre axes : valeur, faisabilité, risque et effort. Un gain rapide combine valeur visible, données disponibles, faible droit d'action et validation simple. Un projet structurant justifie un pilote plus long. Une idée séduisante mais sans données fiables, sans propriétaire ou avec un risque disproportionné doit être différée ou abandonnée.

UNE ALTERNATIVE PEUT ÊTRE MEILLEURE

Comparez toujours l'IA avec une règle, un formulaire, une amélioration de processus, un moteur de recherche, une automatisation classique ou une meilleure formation. La solution la plus simple est souvent la plus robuste.

CHAPITRE 04

SHADOW AI : RENDRE VISIBLE L'INVISIBLE

Le principal risque n'est pas toujours l'IA que l'entreprise déploie, mais celle que ses collaborateurs utilisent déjà sans cadre commun.

Le premier projet IA d'une entreprise n'est pas nécessairement lancé par la direction. Il peut commencer lorsqu'un collaborateur colle un e-mail client dans un service public pour améliorer sa formulation, importe un tableau afin de l'analyser, active un assistant de réunion, installe une extension de navigateur ou connecte un agent à sa boîte aux lettres.

Ces usages peuvent apporter une valeur immédiate. Mais lorsqu'ils échappent à l'inventaire, au contrat, aux règles d'accès et au support, ils forment un Shadow AI : une couche d'outils, de comptes et de flux que l'organisation ne sait ni piloter ni arrêter.

Les six questions de la cartographie

1. Quels outils et fonctions IA sont réellement utilisés, y compris dans les logiciels déjà sous licence ?
2. Les utilisateurs se connectent-ils avec un compte professionnel ou personnel ?
3. Quelles données sont saisies, téléversées, enregistrées, transcrites ou synchronisées ?
4. Quels assistants, extensions, connecteurs et agents ont accès à la messagerie, aux fichiers ou aux applications ?
5. Quelles conditions contractuelles, options de réutilisation et politiques de conservation s'appliquent ?
6. Quels usages influencent une décision, une communication externe ou une action dans le système d'information ?

Interdire ne suffit pas

Une interdiction générale peut déplacer l'usage vers des comptes personnels, réduire la visibilité et freiner les usages légitimes. Une réponse plus efficace combine un environnement autorisé, une politique courte, des alternatives pratiques, une formation ciblée et des mécanismes de détection. L'objectif est de rendre le bon comportement plus simple que le contournement.

MESSAGE CLÉ
Avant d'interdire ou d'autoriser, il faut savoir ce qui existe. La cartographie du Shadow AI est le point de départ d'une gouvernance crédible.

Livrable minimal

Élément	Contenu attendu
Registre des outils	Nom, fournisseur, version/offre, propriétaires, populations utilisatrices.
Flux de données	Types de données, sources, destinations, conservation, sous-traitants.
Niveau de risque	Sensibilité, portée, automatisation, impact sur les personnes et opérations.
Décision	Autorisé, autorisé sous conditions, pilote, suspendu, interdit.
Plan d'action	Responsable, mesure corrective, date et preuve de clôture.

CHAPITRE 05

DONNÉES : DÉCIDER CE QUE L'ON PEUT CONFIER À UNE IA

Une politique utile transforme la classification de l'information en décision concrète pour l'utilisateur.

Les trois questions avant chaque usage

1. Quelle est la sensibilité de l'information : publique, interne, confidentielle, personnelle, soumise au secret ou critique ?
2. L'outil et le compte sont-ils approuvés pour cette catégorie de données et cette finalité ?
3. La quantité d'information transmise est-elle strictement nécessaire au résultat recherché ?

Matrice opérationnelle

Catégorie	Exemples	Règle par défaut	Contrôles minimums
Public	Site web, brochures, offres publiées.	Possible dans un outil autorisé.	Vérifier droits d'auteur, exactitude et communication de marque.
Interne	Procédures, comptes rendus, plans non sensibles.	Compte professionnel et environnement approuvé.	Identité, journalisation, conservation et validation du résultat.
Confidentiel	Contrats, prix, stratégie, informations client.	Analyse préalable du cas et de l'outil.	Minimisation, droits, chiffrement, clauses contractuelles, tests.
Personnel / sensible	RH, santé, finance, données de tiers.	Uniquement si finalité, base et garanties sont validées.	AIPD si risque élevé, transparence, contrôle humain, limitation stricte.
Secret / critique	Secret professionnel, secrets d'affaires, identifiants, clés.	Environnement spécifiquement approuvé ; sinon interdit.	Isolation, moindre privilège, supervision, traçabilité et procédure d'incident.

Minimiser avant de transmettre

La meilleure donnée à protéger est souvent celle que le système n'a pas besoin de recevoir. Supprimez les identifiants inutiles, réduisez le document au passage pertinent, remplacez les exemples réels par des cas synthétiques et évitez de joindre un dossier complet pour obtenir une réponse sur une seule clause.

Qualité et permissions

Connecter une IA à une base documentaire ne rend pas cette base fiable. L'entreprise doit définir les sources de référence, supprimer les doublons, identifier les versions obsolètes, corriger les partages trop larges et attribuer un propriétaire. Une IA de recherche rend les permissions historiques plus visibles ; elle ne les corrige pas à elle seule.

RÈGLE SIMPLE
Une IA ne devrait jamais recevoir plus de données ni plus de droits que ceux nécessaires à la tâche, pendant la durée nécessaire à la tâche.

CHAPITRE 06

IA PROFESSIONNELLE & MICROSOFT 365 COPILOT

La différence ne tient pas seulement au modèle : identité, droits, données, contrat et administration déterminent le niveau de maîtrise.

Quatre niveaux à distinguer

Niveau	Description	Point de vigilance
Service public	Outil accessible en ligne, parfois avec un compte personnel.	Conditions d'usage, réutilisation des données, absence d'administration centrale.
Compte professionnel	Offre contractuelle administrée pour une équipe ou une organisation.	Configuration, conservation, rôles administratifs et usages autorisés.
Copilot intégré	Assistant relié aux applications et aux données accessibles dans Microsoft 365.	La qualité des permissions, du partage et de la classification devient déterminante.
Agent métier	Système relié à des sources, outils ou workflows internes.	Droits d'action, connecteurs, données tierces, journalisation et révocation.

Ce que change Microsoft 365 Copilot

Microsoft indique que Copilot s'appuie sur les modèles, Microsoft Graph et les applications Microsoft 365, et qu'il ne présente à un utilisateur que le contenu auquel celui-ci dispose déjà d'au moins un droit de lecture. Les invites, réponses et données récupérées via Microsoft Graph ne sont pas utilisées pour entraîner les modèles fondamentaux de Copilot. Ces garanties ne dispensent pas l'entreprise de corriger les accès existants, de décider des fonctions activées et de gouverner la conservation des interactions.

Avant le déploiement

1. Vérifier les comptes, l'authentification multifacteur, les rôles privilégiés et les appareils.
2. Analyser les sites SharePoint, équipes Teams, liens anonymes, groupes et partages externes.
3. Définir les informations sensibles et appliquer des labels, règles de prévention de fuite et politiques de conservation adaptées.
4. Choisir un groupe pilote, des cas d'usage, des critères de succès et un dispositif de support.
5. Contrôler les agents et applications intégrées, leurs permissions, leurs conditions et leurs sources.
6. Former les utilisateurs à citer, vérifier, minimiser et signaler les résultats problématiques.

POINT D'ATTENTION

L'IA n'invente pas nécessairement un problème de gouvernance des données. Elle peut révéler, amplifier ou accélérer un problème de permissions qui existait déjà.

Ne pas confondre protection et pertinence

Un environnement professionnel peut offrir de solides engagements de sécurité et de confidentialité tout en produisant une réponse inexacte. La protection des données traite du cadre de traitement ; la validation métier traite de la qualité et de la décision. Les deux contrôles sont nécessaires.

CHAPITRE 07

ARCHITECTURE : CHOISIR LE BON NIVEAU D'INTÉGRATION

Du chatbot isolé à l'agent connecté, l'utilité augmente avec l'accès au contexte — et l'exigence de contrôle augmente avec elle.

Trois voies de déploiement

Voie	Quand l'utiliser	Avantages	Contraintes
Service géré	Usages bureautiques standard, démarrage rapide.	Administration, mises à jour, intégration et support fournisseur.	Dépendance contractuelle, périmètre fonctionnel, résidence et sous-traitants à vérifier.
Plateforme cloud / API	Cas métier sur mesure, intégration à plusieurs systèmes.	Contrôle de l'interface, des règles, des sources et des évaluations.	Architecture, sécurité, exploitation, coûts variables et compétences.
Déploiement dédié	Données ou contraintes justifiant isolation et contrôle renforcés.	Maîtrise accrue de l'hébergement et de certains flux.	Coût, performance, maintenance, mises à jour, supervision et compétences rares.

Architecture de référence



Les contrôles doivent suivre tout le flux : authentification, autorisation, filtrage des données, recherche documentaire, appel du modèle, exécution d'outils, génération de la réponse et conservation des traces. Une revue limitée au fournisseur du modèle laisse de côté la majorité du risque opérationnel.

Sept questions d'architecture

1. Quel résultat et quel niveau de service sont attendus ?
2. Quelles données entrent, sortent, sont conservées ou réutilisées ?
3. Le système propose-t-il, recommande-t-il ou agit-il ?
4. Quels volumes, latences, disponibilités et coûts faut-il garantir ?
5. Qui exploite, supervise, met à jour et répond en cas d'incident ?
6. Comment changer de modèle, de fournisseur ou d'hébergement ?
7. Comment tester la qualité après chaque évolution du système ?

RÉVERSIBILITÉ
Évitez d'enfermer le processus dans un modèle unique. Séparez autant que possible les données, les règles, l'orchestration et le fournisseur du modèle.

CHAPITRE 08

CYBERSÉCURITÉ : PROTÉGER LE SYSTÈME COMPLET

La sécurité commence avant le premier prompt et continue après la réponse, jusque dans les actions déclenchées.

Menaces principales

Menace	Exemple	Contrôle prioritaire
Fuite de données	Document client copié dans un outil non autorisé.	Outils approuvés, minimisation, DLP, formation et surveillance.
Sur-partage	L'IA retrouve un fichier auquel l'utilisateur avait un accès trop large.	Revue des permissions, gouvernance SharePoint/Teams, labels.
Prompt injection	Une instruction cachée dans un document détourne l'agent.	Isoler les contenus non fiables, limiter les outils, valider les actions.
Compromission de compte	Un attaquant utilise un assistant connecté avec les droits de la victime.	MFA résistante au phishing, accès conditionnel, détection et révocation.
Chaîne de fournisseurs	Un connecteur ou sous-traitant traite des données inattendues.	Due diligence, clauses, inventaire, contrôle des intégrations.
Coût ou boucle	Un agent répète des appels ou exécute une action à grande échelle.	Quotas, limites, budgets, temporisation, kill switch.

Conforme ne signifie pas automatiquement sécurisé

La conformité détermine le cadre dans lequel des données et traitements peuvent être utilisés. La cybersécurité protège identités, systèmes et informations contre les accès, modifications ou pertes non autorisés. La gouvernance définit les usages, rôles et responsabilités. Un outil peut satisfaire des engagements contractuels et être mal configuré ; une architecture robuste peut soutenir un traitement inapproprié. Les trois dimensions doivent être traitées ensemble.

Contrôles de base

- Inventaire des systèmes, modèles, agents, extensions, sources et sous-traitants.
- Identité professionnelle, authentification forte, moindre privilège et revues régulières.
- Classification de l'information, prévention de fuite et chiffrement selon le risque.
- Environnements séparés pour développement, test et production ; données synthétiques lorsque possible.
- Journaux exploitables, alertes, gestion des secrets, sauvegardes et procédure de réponse.
- Évaluations de sécurité incluant injection, exfiltration, contenu malveillant et abus des outils.

DÉFENSE EN PROFONDEUR
Aucun filtre de contenu ne remplace l'authentification, les permissions, l'isolation, la limitation des actions et la supervision.

CHAPITRE 09

CADRE SUISSE, LPD & PORTÉE EUROPÉENNE

Pour une entreprise suisse, le point de départ est la LPD ; d'autres cadres peuvent s'ajouter selon les activités, les personnes et les marchés concernés.

Le principe suisse

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) rappelle que la LPD s'applique directement aux traitements de données recourant à l'IA. L'organisation doit notamment examiner la transparence, la finalité, la proportionnalité, la sécurité, les droits des personnes, les décisions automatisées et, lorsque le risque est élevé, la nécessité d'une analyse d'impact relative à la protection des données.

Questions de conformité à documenter

1. Quelle est la finalité et pourquoi l'IA est-elle nécessaire ou proportionnée ?
2. Quelles catégories de données et de personnes sont concernées ?
3. Qui agit comme responsable, sous-traitant ou sous-traitant ultérieur ?
4. Où les données sont-elles traitées et quelles garanties encadrent les transferts ?
5. Quelle information est fournie aux personnes et comment exercer leurs droits ?
6. Le résultat produit une décision automatisée ou influence fortement une personne ?
7. Quels risques élevés imposent une analyse d'impact, une consultation ou des mesures renforcées ?
8. Quelle durée de conservation, quelle traçabilité et quelle procédure d'incident sont prévues ?

Quand le RGPD ou l'AI Act peuvent compter

Le RGPD peut s'appliquer à une entreprise suisse selon ses établissements, son offre de biens ou services et le suivi de personnes dans l'Union européenne. L'AI Act suit une logique fondée sur le risque et peut concerner des acteurs établis hors de l'Union lorsque les conditions territoriales du règlement sont réunies. Son application est progressive : certaines interdictions et obligations de culture IA sont applicables depuis 2025 ; le règlement est devenu largement applicable en août 2026, tandis que certaines obligations relatives aux systèmes à haut risque bénéficient de délais ultérieurs. Une analyse juridique spécifique reste nécessaire.

Responsabilités sectorielles

Le secret professionnel, le droit du travail, les obligations de santé, la réglementation financière, les règles de conservation, les exigences contractuelles et les engagements envers des bailleurs ou bénéficiaires peuvent imposer des limites supplémentaires. L'absence d'une loi sectorielle dédiée à l'IA ne supprime pas les obligations existantes.

PRINCIPE DIRECTEUR

L'utilisation de l'IA ne supprime aucune responsabilité existante de l'entreprise concernant ses données, ses décisions et ses obligations professionnelles.

CHAPITRE 10

GOUVERNANCE : RÈGLES, RÔLES & PREUVES

Une gouvernance légère mais explicite vaut mieux qu'une politique ambitieuse impossible à appliquer.

Le modèle de décision

Rôle	Responsabilité
Direction / sponsor	Fixer l'ambition, l'appétence au risque, les priorités et les moyens.
Propriétaire métier	Définir le résultat, le processus, les exceptions et la validation.
IT / architecture	Choisir l'intégration, exploiter le service, assurer réversibilité et performance.
Sécurité	Évaluer menaces, identités, droits, connecteurs, journaux et incidents.
Protection des données / juridique	Qualifier les rôles, finalités, garanties, contrats, droits et impacts.
RH / formation	Définir compétences, accompagnement, règles d'usage et effets sur le travail.
Utilisateurs	Respecter le cadre, vérifier les résultats, signaler erreurs et incidents.

Le registre IA

Chaque usage significatif doit avoir une fiche : finalité, propriétaire, utilisateurs, données, fournisseurs, modèle ou service, sources, connecteurs, niveau d'autonomie, contrôles, métriques, risques, base contractuelle, dates de revue et décision de maintien. Le registre n'est pas un inventaire figé : il soutient les audits, les changements de modèle et les réponses aux incidents.

Trois niveaux de contrôle humain

Niveau	Application	Exigence
Human in the loop	La décision ou l'action attend une validation humaine.	Pertinent pour communications externes, données sensibles et actions à impact.
Human on the loop	Le système agit dans des limites et l'humain supervise.	Seuils, alertes, échantillonnage, possibilité d'arrêt et revues.
Human out of the loop	Le système agit sans validation opérationnelle.	À réserver aux actions faibles, réversibles, très testées et plafonnées.

Les preuves à conserver

- Décision d'autorisation et responsable nommé.
- Analyse des données, contrats, risques et mesures compensatoires.
- Jeux de tests, résultats, seuils et traitement des exceptions.
- Versions du système, modifications, incidents et actions correctives.
- Formation, communication et acceptation des règles par les populations concernées.

GOUVERNANCE PROPORTIONNÉE

Plus un usage traite de données sensibles, influence une personne ou peut agir dans le système, plus l'exigence de preuve et de contrôle doit être élevée.

CHAPITRE 11

AGENTS IA : QUAND LE LOGICIEL PEUT AGIR

Une réponse erronée est un contenu à corriger ; une action erronée peut modifier un système, engager l'entreprise ou affecter un tiers.

Un assistant fournit une proposition. Un agent peut utiliser des outils, interroger plusieurs sources, enchaîner des étapes et réaliser une action : créer un ticket, mettre à jour un CRM, envoyer un message, produire un document, déclencher un workflow ou appeler une API. Le changement essentiel n'est pas l'autonomie affichée, mais la capacité d'agir avec des droits réels.

Le périmètre minimal à définir

1. Objectif autorisé et critères de réussite.
2. Sources accessibles et niveau de confiance de chaque source.
3. Outils et actions disponibles, avec paramètres et limites.
4. Identité utilisée par l'agent et privilèges associés.
5. Validations humaines obligatoires et seuils d'escalade.
6. Journaux, alertes, conservation et capacité de reconstitution.
7. Quotas, budgets, horaires, environnements et mécanisme d'arrêt.
8. Procédure de révocation, de correction et de retour arrière.

Classer les actions

Classe	Exemples	Politique
Lecture	Rechercher, résumer, comparer.	Accès selon les droits de l'utilisateur ; sources citées et vérification.
Préparation	Préremplir, rédiger un brouillon, proposer une mise à jour.	Validation humaine avant publication ou écriture.
Écriture réversible	Créer un ticket, classer un document, mettre à jour un champ.	Périmètre limité, journal, test, seuil et possibilité d'annuler.
Action engageante	Envoyer, approuver, payer, supprimer, modifier un droit.	Validation forte, séparation des tâches ; souvent interdite par défaut.

Tests spécifiques

- Instructions malveillantes dans les documents ou pages consultées.
- Conflit entre les instructions système, utilisateur et contenu externe.
- Échec d'un outil, réponse partielle, doublon, boucle ou reprise après interruption.
- Tentative d'accès à une source ou une action hors périmètre.
- Dégradation silencieuse après changement de modèle, de connecteur ou de données.

RÈGLE D'OR

Plus une IA obtient la capacité d'agir, plus les principes de moindre privilège, traçabilité, réversibilité et validation humaine deviennent essentiels.

CHAPITRE 12

LA MÉTHODE AWSMTECH 6D

Six étapes pour passer d'usages dispersés à une capacité utile, sûre et industrialisable.

1. Découvrir
Inventorier usages, attentes, outils et Shadow AI.

2. Diagnostiquer
Évaluer processus, données, identités, sécurité et gouvernance.

3. Définir
Prioriser les cas d'usage et concevoir les contrôles.

4. Déployer
Piloter sur un périmètre réel mais maîtrisé.

5. Démontrer
Mesurer valeur, qualité, adoption, coût et risque.

6. Développer
Industrialiser, étendre, corriger ou arrêter.

1 — Découvrir

Entretiens courts, observation du travail et inventaire technique permettent de faire apparaître les irritants, ressaisies, recherches longues, documents parallèles, usages déjà présents et attentes des équipes. Le livrable est une carte des opportunités et des risques, pas une liste de produits.

2 — Diagnostiquer

L'analyse porte sur la maturité du processus, la qualité et la propriété des données, les identités, les permissions, l'architecture, les obligations, les compétences et la capacité d'exploitation. Un processus instable ou non mesuré est d'abord simplifié ; l'IA intervient ensuite si elle ajoute une valeur nette.

3 — Définir

Les cas sont classés selon valeur, faisabilité, risque et effort. Pour chacun, AWSMTECH formalise la finalité, le niveau d'autonomie, les données, l'architecture cible, les contrôles, les critères de succès et la décision de sortie. Le choix technologique vient après le besoin métier.

4 — Déployer

Le pilote utilise des cas représentatifs, inclut les exceptions et se déroule avec des utilisateurs désignés. Les accès sont limités, les journaux activés, les procédures de support et d'incident testées. Un pilote n'est pas une démonstration : il doit reproduire les contraintes réelles sans exposer l'entreprise à un risque non maîtrisé.

5 — Démontrer

Le résultat est comparé à une référence : temps, délai, qualité, taux de correction, satisfaction, erreurs, coût et incidents. Les échecs sont documentés. Le bénéfice est calculé après intégration, accompagnement et contrôle, et non uniquement sur la vitesse apparente de génération.

6 — Développer

Les usages prouvés sont industrialisés avec un propriétaire, un budget, une supervision, des revues et un plan de réversibilité. Les usages insuffisants sont corrigés ou arrêtés. Développer signifie aussi former, ajuster la politique et enrichir progressivement les sources et contrôles.

LA LOGIQUE 6D
Découvrir → Diagnostiquer → Définir → Déployer → Démontrer → Développer. Une boucle de décision, pas une course au déploiement.

CHAPITRE 13

FEUILLE DE ROUTE DES 90 PREMIERS JOURS

Un premier cycle court doit produire de la visibilité, un cadre praticable et une preuve de valeur — pas une transformation totale.

Jours 1 à 30 — Voir et cadrer

Action	Livrable
Nommer sponsor, pilote et groupe de travail.	Mandat, rôles et cadence de décision.
Cartographier outils, usages et données.	Registre initial du Shadow AI et des intégrations.
Définir une politique provisoire.	Règles « autorisé / sous conditions / interdit ».
Identifier 5 à 10 opportunités.	Fiches cas d'usage avec valeur et risques.
Contrôler les fondations.	État des identités, permissions, partages et appareils.

Jours 31 à 60 — Prioriser et préparer

Action	Livrable
Noter les cas selon valeur, faisabilité, risque, effort.	Portefeuille priorisé et décisions motivées.
Choisir un à trois pilotes.	Périmètre, utilisateurs, données, architecture et contrôles.
Mesurer la référence.	Temps, qualité, coûts, erreurs et satisfaction avant changement.
Former les pilotes.	Règles, méthodes, scénarios et procédure de signalement.
Tester sécurité et exploitation.	Journaux, accès, support, arrêt et incident.

Jours 61 à 90 — Tester et décider

Action	Livrable
Exécuter sur des cas réels.	Résultats, exceptions, retours et incidents.
Comparer à la référence.	Tableau de valeur, coût, qualité et risque.
Corriger ou réduire le périmètre.	Nouvelle version du processus et des contrôles.
Décider.	Industrialiser, prolonger, repositionner ou arrêter.
Mettre à jour la gouvernance.	Registre, politique, formation et plan trimestriel.

CRITÈRE DE RÉUSSITE À 90 JOURS

L'entreprise sait ce qui est utilisé, a posé des règles compréhensibles et peut démontrer objectivement la valeur — ou l'absence de valeur — d'au moins un cas d'usage.

CHAPITRE 14

ROI, ADOPTION & CONDUITE DU CHANGEMENT

Le nombre de licences mesure une dépense. La valeur se mesure dans le travail réel, après contrôle de la qualité et des risques.

Mesurer autre chose que l'utilisation

Un processus auparavant réalisé en 45 minutes et réduit à 15 minutes économise théoriquement 30 minutes par occurrence. Répété 20 fois par mois par cinq personnes, il représente 50 heures mensuelles potentielles. Mais ce calcul n'est utile que si le résultat reste de qualité, si les corrections ne consomment pas le gain, si le temps libéré est réinvesti et si le coût complet reste inférieur à la valeur créée.

Tableau de mesure

Dimension	Indicateurs possibles
Productivité	Temps par dossier, délai, volume, files d'attente, capacité.
Qualité	Taux d'erreur, complétude, cohérence, reprise, satisfaction client.
Adoption	Utilisateurs actifs, fréquence utile, diversité des cas, autonomie.
Risque	Incidents, données exposées, sorties non vérifiées, actions annulées.
Économie	Licences, intégration, exploitation, support, formation, coût de sortie.
Humain	Charge cognitive, satisfaction, compétences, qualité du contrôle.

Une formule simple

VALEUR NETTE MENSUELLE

(heures réellement libérées × valeur d'une heure utile) + gains de qualité + risques évités − coût complet mensuel.

Les gains de qualité et les risques évités doivent être estimés avec prudence. Les hypothèses sont documentées et révisées après le pilote. Une présentation transparente distingue la capacité théorique, le gain observé et la valeur effectivement captée.

Conduire le changement

- Commencer par les tâches pénibles et répétitives, sans promettre la disparition du travail.
- Impliquer les experts métier dans les tests, les règles et les critères de qualité.
- Former à la vérification et à l'escalade, pas seulement à la formulation de prompts.
- Créer une communauté de pratique et des exemples approuvés par métier.
- Reconnaître les échecs et retirer les cas qui déplacent la charge au lieu de la réduire.
- Suivre les effets sur les rôles, l'apprentissage, la responsabilité et la relation client.

SIGNAL DE MATURITÉ

Une organisation mature sait arrêter un usage populaire mais non rentable, et investir dans un usage discret qui améliore durablement un processus.

CHAPITRE 15

SOBRIÉTÉ NUMÉRIQUE & HORIZON 2027-2030

L'IA doit être dimensionnée pour l'utilité : le plus grand modèle, le contexte le plus long et l'agent le plus autonome ne sont pas toujours les meilleurs choix.

Principes de sobriété

1. Ne lancer que les usages associés à un bénéfice métier mesurable.
2. Choisir le plus petit modèle suffisant et limiter la longueur des contextes et réponses.
3. Mettre en cache, mutualiser et éviter les boucles d'agents sans limite.
4. Réduire les données transférées et la fréquence des appels inutiles.
5. Intégrer infrastructure, durée de vie, localisation et mix électrique dans les décisions.
6. Mesurer un impact par unité utile : dossier traité, erreur évitée, heure réellement libérée.

Trois scénarios de préparation

Scénario	Ce qui change	Préparation utile dès maintenant
IA intégrée partout	Les fonctions d'assistance deviennent standard dans les logiciels.	Gouverner les fonctions activées, les permissions et l'adoption.
Agents spécialisés	Des agents exécutent des séquences limitées et contrôlées.	Modulariser les processus, définir les actions et renforcer les journaux.
Exigence de preuve	Clients, régulateurs et directions demandent plus de documentation.	Tenir un registre, conserver tests, décisions, versions et responsables.

Ce qui changera moins vite

La responsabilité, la qualité des données, la compréhension du métier, la confiance du client, la sécurité des identités et la nécessité de mesurer resteront déterminantes. Les modèles évolueront rapidement ; les fondations organisationnelles progresseront au rythme de l'entreprise. C'est pourquoi l'investissement le plus durable porte souvent sur les données, les processus, les droits et les compétences.

NE PAS PARIER SUR UNE PRÉDICTION

Une entreprise préparée teste, mesure, apprend et change de solution lorsque les résultats le justifient. Elle n'a pas besoin de prédire exactement 2030.

CHAPITRE 16

CHECKLIST, CHARTE & OUTILS PRATIQUES

Des outils simples pour transformer les principes en décisions vérifiables.

Checklist avant mise en production

✓	Domaine	Critère
☐	Finalité	Le résultat attendu et le propriétaire métier sont définis.
☐	Alternative	Une solution sans IA a été comparée.
☐	Données	Sources, catégories, qualité, droits et conservation sont documentés.
☐	Fournisseurs	Contrats, sous-traitants, lieux de traitement et sortie sont examinés.
☐	Sécurité	Identité, moindre privilège, secrets, journaux, tests et incident sont prêts.
☐	Qualité	Jeux de test, seuils, sources et traitement des exceptions sont définis.
☐	Humain	Validation, supervision, recours et responsabilités sont explicites.
☐	Agents	Actions, quotas, validations, révocation et retour arrière sont testés.
☐	Conformité	LPD, exigences sectorielles et éventuelle portée UE sont analysées.
☐	Valeur	Référence, indicateurs, coût complet et date de décision sont fixés.
☐	Adoption	Formation, support, communication et mécanisme de retour existent.
☐	Réversibilité	Export, remplacement, archivage et arrêt sont praticables.

Charte IA — clauses essentielles

Une charte concise doit être comprise en moins de dix minutes. Elle précise :

- les outils et comptes autorisés ;
- les catégories de données interdites ou soumises à validation ;
- l'obligation de minimiser, vérifier et citer les sources lorsque pertinent ;
- l'interdiction de présenter une sortie IA comme validée sans contrôle ;
- les règles pour les communications externes, décisions et actions automatisées ;
- le canal de signalement des erreurs, fuites, contenus problématiques et usages inconnus ;
- les conséquences d'un non-respect et le processus d'exception.

FORMULATION RECOMMANDÉE

L'IA peut aider à préparer, rechercher, résumer et proposer. Elle ne transfère pas la responsabilité de l'utilisateur ni de l'entreprise. Toute utilisation doit respecter la classification de l'information, les outils approuvés et le niveau de validation prévu.

Fiche de cas d'usage

Champ	À renseigner
Problème / résultat	Processus concerné, irritant, indicateur et cible.
Utilisateurs	Population, compétences, volume et contexte.
Données	Sources, catégories, qualité, droits, conservation.
Solution	Service, modèle, architecture, outils, agent, fournisseur.
Contrôles	Règles, tests, validation, journaux, sécurité, incident.
Décision	Pilote, date, budget, responsable, critères de poursuite ou arrêt.

GLOSSAIRE

Terme	Définition
Agent IA	Système capable de poursuivre un objectif sur plusieurs étapes et d'utiliser des outils pour agir.
AIPD	Analyse d'impact relative à la protection des données personnelles, requise dans certains cas à risque élevé.
API	Interface permettant à des applications d'échanger des demandes et des résultats.
Hallucination	Réponse fausse ou inventée, formulée de manière plausible par un modèle.
IA générative	Système produisant un contenu nouveau : texte, image, son, vidéo, code ou combinaison de formats.
LLM	Grand modèle de langage entraîné à traiter et générer du texte.
Moindre privilège	Principe consistant à n'accorder que les droits nécessaires, pour la durée nécessaire.
Prompt	Instruction, question ou contexte transmis à une IA.
Prompt injection	Instruction malveillante, parfois cachée dans un contenu, visant à détourner un système.
RAG	Méthode recherchant des documents avant de les fournir au modèle pour appuyer une réponse.
Shadow AI	Utilisation d'outils ou fonctions IA sans visibilité, validation ou gouvernance suffisante.
Traçabilité	Capacité à reconstituer les données, versions, décisions et actions d'un système.

RÉFÉRENCES & MÉTHODE

Les références ci-dessous privilégient les sources officielles et les cadres pratiques. Les contenus fournisseurs et calendriers réglementaires évoluent ; ils doivent être revérifiés avant toute décision. Dernière revue éditoriale : 11 novembre 2026.

1. PFPDT — IA et protection des données — Application directe de la LPD, transparence et risques élevés.

2. PFPDT / OFCS — IA générative au travail — Sensibilisation aux risques de données et de sécurité en milieu professionnel.

3. Commission européenne — AI Act — Cadre fondé sur le risque et calendrier d'application.

4. Microsoft Learn — Data, Privacy and Security for Microsoft Copilot — Données organisationnelles, permissions, entraînement, conservation et agents.

5. Microsoft Learn — How data is protected and audited — Labels, chiffrement, SharePoint, OneDrive, audit et rétention.

6. NIST — AI Risk Management Framework 1.0 — Cadre de gestion des risques IA.

7. OWASP — GenAI Security Project — Risques de sécurité des applications basées sur des modèles de langage.

8. Organisation internationale du Travail — Generative AI and Jobs — Exposition des tâches et transformation du travail.

9. Agence internationale de l'énergie — Energy and AI — Énergie, centres de données et usages de l'IA.

Méthode éditoriale

Le contenu synthétise des principes de gouvernance, sécurité, protection des données et conduite du changement. Il distingue les engagements publiés par les fournisseurs des contrôles qui restent à la charge du client. Les exemples sont génériques et ne garantissent pas un résultat identique dans une autre organisation.

CHAPITRE 17

REPRENDRE LE CONTRÔLE AVANT D'ACCÉLÉRER

L'objectif n'est pas de déployer plus d'IA. Il est d'utiliser l'IA là où elle crée de la valeur, sous un contrôle adapté.

Votre entreprise utilise probablement déjà l'intelligence artificielle. La vraie question est : savez-vous où elle est utilisée, avec quelles données, pour quelle valeur et sous quel contrôle ?

L'IA peut accélérer l'accès à l'information, améliorer la productivité et transformer certains processus. Mais sa valeur ne vient pas uniquement du modèle choisi. Elle dépend de la qualité des données, de la sécurité de l'environnement, de la pertinence des cas d'usage, de l'adhésion des collaborateurs et de la gouvernance mise en place.

L'APPROCHE AWSMTECH

Cartographier. Prioriser. Sécuriser. Expérimenter. Mesurer. Industrialiser.

De l'IT managé à la Managed Intelligence

AWSMTECH accompagne les métiers sensibles en Suisse romande avec des services d'infogérance, de cybersécurité, de cloud, de poste de travail et de direction IT externalisée. La Managed Intelligence prolonge cette mission : transformer les technologies, les données et l'intelligence artificielle en capacités métier durables et maîtrisées.

Formats d'accompagnement

Intervention	Résultat attendu
Diagnostic IA & Shadow AI	Inventaire, carte des risques, règles prioritaires et portefeuille de cas d'usage.
Readiness Microsoft 365 Copilot	Revue des identités, permissions, partage, données, sécurité et pilote.
Atelier de priorisation	Matrice valeur / faisabilité / risque / effort et décisions de lancement.
Pilote 6D	Conception, déploiement contrôlé, mesure du ROI et décision d'industrialisation.
Gouvernance & sécurité	Charte, registre, contrôles, agents, journalisation et dispositif d'incident.

Parlons de votre premier cas d'usage

L'INFOGÉRANCE IT DE CONFIANCE POUR LES MÉTIERS SENSIBLES

awsmtech.ch | +41 (0) 22 552 60 70 | mail@awsmtech.ch

Genève • Martigny

© 2026 AWSMTECH (Switzerland) LTD. Tous droits réservés.