



BEXTIO
AUGMENTED ENTERPRISE

TOME III — AUGMENTE

VOLUME 6 SUR 7

GOUVERNER L'ENTREPRISE AUGMENTÉE

Définis ce que l'IA peut faire, mesure ce qu'elle change et garde la
responsabilité humaine.

Toussaint Kadio N'GUESSAN

BEXTIO ÉDITIONS

L'IA T'AIDE À ALLER PLUS LOIN. TU RESTES RESPONSABLE.



BEXTIO
AUGMENTED ENTERPRISE

GOUVERNER L'ENTREPRISE AUGMENTÉE

TOME III — AUGMENTE

Volume 6 sur 7

**Définis ce que l'IA peut faire, mesure ce qu'elle change
et garde la responsabilité humaine.**

Toussaint Kadio N'GUESSAN

© 2026 Toussaint Kadio N'GUESSAN. Tous droits réservés.

Publié sous la marque BEXTIO Éditions par Toussaint Kadio N'GUESSAN.

ÉDITION FRANÇAISE V1.2 — LOCKED — 15 SEPTEMBRE 2026.

Aucune partie de cet ouvrage ne peut être reproduite, stockée ou transmise
par quelque moyen que ce soit sans autorisation, hors exceptions prévues
par la loi.

SOMMAIRE

PARTIE VI — GARDE LE CONTRÔLE À MESURE QUE L'IA AGIT	4
CHAPITRE 28 — GARDE LA MAÎTRISE DE TES SYSTÈMES D'IA	5
CHAPITRE 29 — AUTOMATISE SANS ABANDONNER LA RESPONSABILITÉ HUMAINE	27
CHAPITRE 30 — MESURE CE QUE L'IA CHANGE RÉELLEMENT	48
CHAPITRE 31 — EMPÊCHE UNE ERREUR DE S'AMPLIFIER	70
CHAPITRE 32 — TRANSFORME LE TRAVAIL SANS CONFONDRE AUTOMATISATION ET REMPLACEMENT	93

**PARTIE VI — GARDE LE CONTRÔLE À MESURE QUE
L’IA AGIT**

CHAPITRE 28 — GARDE LA MAÎTRISE DE TES SYSTÈMES D'IA

CAS PRATIQUE — IBM

Plus l'IA peut voir, recommander et agir, plus ton entreprise doit savoir exactement quels systèmes existent, ce qu'ils ont le droit de faire et qui répond de leurs conséquences. IBM sert ici de cas pratique pour comprendre comment transformer la gouvernance en discipline opérationnelle, sans confondre outil de gouvernance et conformité garantie.

28.1 — PLUS L'IA PEUT AGIR, PLUS TU DOIS SAVOIR CE QUE TU AUTORISES

Nous venons de franchir une frontière. L'IA peut désormais : chercher; analyser; recommander; générer; utiliser des outils; modifier des systèmes; déclencher des workflows; accomplir certaines missions.

La question n'est donc plus seulement : « Que peut-on faire avec l'intelligence artificielle ? »

Elle devient : « Comment savons-nous quelles intelligences artificielles fonctionnent dans l'entreprise, pourquoi elles existent, ce qu'elles peuvent faire, quels risques elles créent et qui en reste responsable ? »

C'est la gouvernance.

28.2 — LA GOUVERNANCE DOIT COMMENCER AVANT LE DÉPLOIEMENT

Une erreur fréquente consiste à penser d'abord innovation. Puis déploiement.

Puis, si nécessaire, la gouvernance. Cette séquence devient dangereuse dès que les modèles ou les agents touchent des clients, des collaborateurs, des paiements, des décisions, des données personnelles ou des systèmes critiques.

La gouvernance doit donc commencer avant le déploiement et continuer pendant toute la vie du système.

28.3 — COMMENCE PAR SAVOIR QUELLES IA EXISTENT DANS TON ENTREPRISE

Imaginons une entreprise utilisant : un assistant marketing; trois modèles prédictifs; deux outils de recrutement; un chatbot client; un agent de support; une IA financière; plusieurs API de modèles externes.

Question simple : qui possède l'inventaire complet ? Pour chaque système quelle équipe ?

quel fournisseur ? quel modèle ?

quelle version ? quelles données ?

quelle finalité ? quels utilisateurs ?

quel niveau de risque ? Sans inventaire pas de véritable gouvernance.

28.4 — SI TU NE VOIS PAS TES IA, TU NE PEUX PAS LES GOUVERNER

Au chapitre 23, Uber nous a montré pourquoi une entreprise doit voir ce qui se passe réellement avant de demander à l'IA de prédire ou d'agir.

La même exigence s'applique à son intelligence artificielle.

L'organisation doit pouvoir observer

SES PROPRES SYSTÈMES D'IA.

Quels modèles ? Quels agents ?

Quels prompts critiques ? Quels déploiements ?

Quels cas d'usage ? Quels incidents ?

Quels propriétaires ? La gouvernance commence par rendre l'intelligence artificielle visible.

28.5 — IBM TRAITE PRÉCISÉMENT CETTE PROBLÉMATIQUE

watsonx.governance permet de : enregistrer; documenter; évaluer; surveiller des actifs d'intelligence artificielle.

Cela inclut : des modèles de machine learning; des modèles génératifs; des templates de prompts; et désormais des agents et applications agentiques dans certaines composantes de gouvernance.

Le système cherche donc à construire

UN REGISTRE GOUVERNÉ DE L'INTELLIGENCE ARTIFICIELLE.

28.6 — NE GOUVERNE PAS SEULEMENT LE MODÈLE : GOUVERNE LE CAS D'USAGE

C'est une évolution importante. Une entreprise ne déploie jamais seulement : « un modèle ».

Elle déploie un cas d'usage. Par exemple classer les réclamations.

Le système peut comprendre : un modèle; des données; un prompt; un workflows; des règles; une interface; des humains; des décisions.

Ainsi l'unité de gouvernance doit souvent être

LE SYSTÈME DANS SON CONTEXTE D'USAGE.

28.7 — UN MÊME MODÈLE PEUT AVOIR DEUX RISQUES TRÈS DIFFÉRENTS

Prends le même modèle génératif dans deux usages. Dans le premier, il résume des notes internes. Dans le second, il contribue à une décision de crédit.

La technologie peut être identique, mais la finalité, les données, les personnes affectées, l'autorité accordée au système et les conséquences d'une erreur changent complètement.

LE RISQUE D'UNE IA DÉPEND DE SON USAGE, DE SON AUTORITÉ ET DE SES CONSÉQUENCES.

28.8 — C'EST POURQUOI IBM RELIE MODÈLES ET CAS D'USAGE

Dans l'architecture de gouvernance, le cas d'usage peut être documenté, révisé et relié à des responsables, des évaluations, des risques et des validations.

Le modèle n'est donc pas un objet technique flottant. Il appartient à un contexte organisationnel.

28.9 — GARDE LES FAITS QUI PERMETTENT DE RECONSTRUIRE UNE DÉCISION

Comment le modèle a-t-il été construit ? Avec quelles données ?

Quelle version ? Qui l'a validé ?

Quelles métriques ? Quelles limites ?

Quand a-t-il été déployé ? A-t-il changé ?

IBM utilise notamment des AI Factsheets pour documenter une partie de ces éléments.

L'idée est fondamentale.

UNE IA GOUVERNABLE DOIT LAISSER UNE TRACE DOCUMENTAIRE.

28.10 — LA BONNE DOCUMENTATION T'AIDE À COMPRENDRE QUI A DÉCIDÉ QUOI ET POURQUOI

Six mois après un incident, l'organisation doit pouvoir demander : « Pourquoi avons-nous autorisé ce système ? »

Qui avait validé ? Sur quelles preuves ?

Avec quelles limites connues ?

Quelle version était en production ? Une mémoire de gouvernance permet de répondre.

28.11 — LE CYCLE DE VIE DE L'IA DOIT ÊTRE GOUVERNÉ DE BOUT EN BOUT

Gouverner une IA ne consiste pas à l'approuver une fois puis à l'oublier. La gouvernance accompagne tout son cycle de vie.

IDÉE → CAS D'USAGE → ÉVALUATION DU RISQUE → DÉVELOPPEMENT OU SÉLECTION → TEST → APPROBATION → DÉPLOIEMENT → SURVEILLANCE → INCIDENT OU DÉRIVE → CORRECTION → RETRAIT OU ÉVOLUTION.

À chaque étape, l'entreprise doit pouvoir dire qui décide, sur quelles preuves et avec quelle possibilité de revenir en arrière.

28.12 — UN SYSTÈME APPROUVÉ HIER PEUT DEVENIR MAUVAIS DEMAIN

Pourquoi ? Les données changent.

Les utilisateurs changent.

Le monde change. La distribution des entrées change.

Le modèle peut dériver. Une nouvelle population peut l'utiliser.

Un fournisseur peut mettre à jour son système. Ainsi

APPROBATION ≠ VALIDITÉ PERMANENTE.

28.13 — IBM PERMET DE SURVEILLER CERTAINES MÉTRIQUES APRÈS DÉPLOIEMENT

watsonx.governance peut notamment surveiller : qualité; équité; dérive; métriques propres aux applications génératives; seuils configurés.

Lorsqu'un seuil n'est plus respecté une alerte peut être déclenchée.

Nous passons de gouvernance documentaire à

GOVERNANCE OBSERVABLE.

28.14 — TRANSFORME TES INTENTIONS EN SEUILS DE CONTRÔLE

Dire : « Notre modèle doit rester fiable » est une intention.

Dire : « Si cette métrique descend sous le seuil défini, une revue est déclenchée »

commence à devenir un contrôle opérationnel. La gouvernance mature transforme principes en mécanismes.

28.15 — MAIS UNE MÉTRIQUE NE PEUT PAS RÉSUMER TOUTE LA CONFIANCE

Une excellente moyenne peut cacher un problème grave. Un modèle peut être précis globalement et échouer sur un sous-groupe. Un agent peut réussir la plupart de ses tâches et rester dangereux dans quelques situations critiques.

Pour gouverner, tu dois donc regarder la distribution des erreurs, les cas extrêmes, les populations affectées et le coût des échecs, pas seulement un score moyen.

UNE BONNE MÉTRIQUE AGRÉGÉE NE RÉSUME PAS TOUT LE RISQUE.

28.16 — IL FAUT MESURER SELON LE TYPE DE SYSTÈME

Modèle prédictif : précision; recall; faux positifs; faux négatifs; calibration, c'est-à-dire l'écart entre la confiance du modèle et ce qui se produit réellement; dérive; équité.

IA générative : exactitude; fidélité; toxicité; pertinence; hallucination; groundedness; respect des instructions.

Agent : taux de mission réussie; actions incorrectes; outils utilisés; violations de permissions; escalades; incidents; capacité de récupération.

La gouvernance doit évoluer avec la nature de l'intelligence.

28.17 — LE PASSAGE AUX AGENTS CHANGE ENCORE LE PROBLÈME

Un modèle produit une sortie. Un agent peut produire une conséquence.

La gouvernance doit donc ajouter : permissions; outils; actions; limites; identité; journalisation; responsabilité.

Dans le volume précédent, le cas Block a montré pourquoi l'autorité d'un agent doit rester limitée. Ici, l'enjeu est de gouverner cette autorité dans la durée.

28.18 — IBM COMMENCE DÉSORMAIS À INTÉGRER LES AGENTS À SON PÉRIMÈTRE DE GOUVERNANCE

Dans les versions récentes de son système de Model Risk Governance, IBM définit un objet Agent permettant de documenter les agents IA et les applications agentiques.

Cette évolution est importante. Elle reconnaît implicitement que la gouvernance centrée uniquement sur les modèles n'est plus suffisante.

28.19 — L'AGENT DOIT AVOIR UNE IDENTITÉ GOUVERNABLE

Toute action importante doit pouvoir être rattachée à un acteur identifiable : humain, service ou agent. Pour un agent, documente au minimum son identité, sa version, sa mission, son propriétaire et ses permissions.

Si une action ne peut pas être attribuée, l'entreprise perd sa capacité à enquêter, corriger, retirer une autorisation et demander des comptes.

IDENTITÉ → RESPONSABILITÉ → TRAÇABILITÉ.

28.20 — LES PERMISSIONS COMPTENT AUTANT QUE LE MODÈLE

Un excellent modèle doté de permissions excessives peut être dangereux.

Un modèle imparfait doté de permissions étroites peut rester confiné.

La gouvernance doit donc demander : « Que peut-il faire si son raisonnement est faux ? »

Pas seulement : « Son raisonnement est-il généralement bon ? »

28.21 — LE RISQUE DÉPEND DU SYSTÈME, DE SON USAGE ET DE SON AUTORITÉ

Le risque d'une IA ne vient pas seulement de son taux d'erreur. Il dépend aussi de ce qu'elle peut faire et de l'ampleur de ses conséquences.

RISQUE OPÉRATIONNEL $\approx$ PROBABILITÉ D'ERREUR $\times$ IMPACT $\times$ AUTORITÉ DU SYSTÈME $\times$ PORTÉE DU DÉPLOIEMENT $\times$ DIFFICULTÉ DE RÉCUPÉRATION.

Ce n'est pas une loi scientifique. C'est un cadre simple pour raisonner : une erreur rare peut devenir critique si le système agit à grande échelle et si la reprise est difficile.

28.22 — UN MODÈLE PEU FIABLE N'EST PAS TOUJOURS INUTILISABLE

Imagine un assistant interne de brainstorming. Même si certaines propositions sont mauvaises, le risque peut rester limité si l'humain vérifie.

Le même niveau de fiabilité serait inacceptable pour un système autonome pilotant une décision critique.

La gouvernance doit donc être

PROPORTIONNÉE.

28.23 — GOUVERNANCE FAIBLE RISQUE

Exemple générer une première structure de présentation interne.

Contrôles possibles : outils approuvés; pas de données sensibles non autorisées; validation de l'utilisateur.

Pas besoin d'un comité de dix personnes pour chaque prompt.

28.24 — GOUVERNANCE RISQUE MOYEN

Exemple préparer une réponse client. Le système peut rédiger.

Mais certaines catégories nécessitent validation. Les données doivent être autorisées.

Les communications peuvent être journalisées.

28.25 — GOUVERNANCE RISQUE ÉLEVÉ

Exemple recommander une décision financière importante.

Il faut potentiellement : tests plus rigoureux; données gouvernées; validation; explicabilité; journaux d'actions; contrôle humain; procédure d'appel; surveillance continu.

28.26 — GOUVERNANCE RISQUE CRITIQUE

Lorsque erreur et action peuvent provoquer un dommage majeur, certaines actions peuvent simplement être

INTERDITES À L'AUTONOMIE.

La maturité ne consiste pas à automatiser tout ce qui est techniquement possible.

Elle consiste aussi à savoir ce qui ne doit pas l'être.

28.27 — GOUVERNER SIGNIFIE AUSSI CARTOGRAPHIER LES RISQUES

Risque de : biais; erreur; confidentialité; sécurité; fraude; hallucination; mauvaise décision; dépendance; dérive; atteinte aux droits; non-conformité; perte de compétence; action non autorisée.

Une entreprise mature ne demande pas seulement : « Est-ce risqué ? »

Elle demande : « Quel risque précisément, pour qui, dans quelle situation et avec quelle conséquence ? »

28.28 — IBM A CONSTRUIT UN AI RISK ATLAS

IBM maintient également un référentiel de risques liés à l'IA.

L'intérêt n'est pas de transformer une liste de risques en checklist aveugle.

Il est d'aider les équipes à développer un vocabulaire commun. Une organisation qui ne nomme pas un risque a davantage de difficulté à le gouverner.

28.29 — UTILISE UN VOCABULAIRE COMMUN POUR PARLER DES RISQUES

Le juriste peut parler de « risque de conformité », le data scientist de « dérive », le responsable sécurité d'« exfiltration » et le métier de « mauvaise réponse ». Ils parlent peut-être du même système sans partager la même représentation.

La gouvernance doit permettre un langage transversal.

28.30 — C'EST POURQUOI LA GOUVERNANCE EST ORGANISATIONNELLE, PAS SEULEMENT TECHNIQUE

Elle mobilise : direction; métiers; data; IT; cybersécurité; juridique; conformité; risques; RH; audit.

Un modèle ne devient pas gouverné parce qu'un data scientist l'a testé.

Il devient gouverné lorsque les responsabilités nécessaires sont organisées.

28.31 — NOMME UN PROPRIÉTAIRE MÉTIER

Chaque cas d'usage devrait avoir une personne ou fonction responsable de sa finalité.

Pourquoi ce système existe-t-il ? Quelle décision sert-il ?

Quelle valeur doit-il créer ? Quels utilisateurs affecte-t-il ?

La gouvernance ne doit pas rester dans le département informatique.

28.32 — LE RESPONSABLE TECHNIQUE NE PORTE PAS SEUL LE RISQUE MÉTIER

Une équipe technique peut savoir comment le système fonctionne.

Mais le métier doit savoir ce que signifie une erreur. Un faux positif dans un filtre anti-spam n'a pas la même conséquence qu'un faux positif dans un système antifraude bloquant des transactions.

Le contexte métier détermine une partie du risque.