Déployer l'IA en toute sécurité

Le guide des leaders pour transformer les investissements en IA en valeur

Un leader mondial des services technologiques

Experis
ManpowerGroup



©Experis 2026 Déployer l'IA en toute sécurité

Table des matières

1 Introduction 3-4

Sommaire 3
Avant-propos : l'innovation à la croisée des chemins 4

2 Transformation des entreprises par le déploiement 5-9

L'illusion d'une IA prête à l'emploi 5-7
La nouvelle surface d'attaque de l'entreprise 7
La gouvernance devient un avantage concurrentiel 8-9

3 Créer une différenciation concurrentielle 10-13

Repenser les organisations pour l'ère des agents 10-12
Pleins feux : ExcelerateWorkflow propulsé par IBM® watsonx Orchestrate™ 11
La dimension humaine de la transformation par l'IA 12-13

4 Guide des leaders technologiques 14-16

Cinq mesures que les leaders technologiques devraient prendre dès maintenant 14-15
L'expertise mondiale d'Experis 16

Introduction



Résumé

Les investissements en IA s'accélèrent, mais de nombreuses organisations peinent encore à transformer l'expérimentation en valeur d'affaires mesurable : Les investissements en IA s'accélèrent, mais de nombreuses organisations peinent encore à transformer l'expérimentation en valeur d'affaires mesurable : l'écart n'est pas uniquement technologique. Il repose sur l'alignement avec les objectifs d'affaires, à la préparation des données, à la cybersécurité, à la gouvernance, aux capacités de la main-d'œuvre et à la capacité d'intégrer l'IA à la façon dont le travail s'effectue réellement.

L'idée d'une transformation des entreprises par une IA prête à l'emploi est un mythe : les projets qui obtiennent de bons résultats dans des environnements pilotes stagnent souvent lorsqu'ils se heurtent aux systèmes existants, à des données fragmentées, à des responsabilités floues, à des exigences de sécurité et à des flux de travail réels. La technologie seule ne peut pas surmonter ces obstacles.

À mesure que l'IA s'intègre davantage à l'entreprise, chaque nouveau modèle, nouvel agent, nouvel ensemble de données et nouvelle intégration crée à la fois des occasions et des risques. Les entreprises doivent sécuriser une surface d'attaque grandissante, établir des responsabilités claires, repenser les flux de travail et développer les compétences nécessaires pour que les gens utilisent et supervisent l'IA efficacement. Sans ces fondations, les projets pilotes prometteurs peinent à prendre de l'expansion et les investissements ne génèrent pas leur plein rendement.

La prochaine phase d'adoption de l'IA exige un changement de perspective. La question n'est plus de savoir si les organisations devraient investir dans l'IA, mais comment les leaders peuvent dé -ployer l'IA de façon sécuritaire, responsable et efficace. Les recherches d'Experis soulignent ce défi. Alors que 66 % des professionnels des TI affirment que leur organisation augmente ses investisse -ments en IA, seuls 9 % indiquent que l'IA est pleinement intégrée aux activités et à la stratégie.[1]

Avant-propos : l'innovation à la croisée des chemins

Lors de nos récentes discussions avec nos clients, il est devenu évident que l'IA est passée au-delà de l'expérimentation. Tous secteurs confondus, les organisations investissent massivement dans l'IA, l'automatisation, les infrastructures infonuagiques et des systèmes de plus en plus autonomes. **Pour bon nombre d'équipes de direction, la question n'est plus de savoir s'il faut investir, mais comment transformer cet investissement en résultats.**

C'est là que l'ambition devance souvent l'exécution. Les modèles et les outils s'améliorent rapidement, mais leur déploiement en entreprise demeure difficile. Les résultats opérationnels sont inégaux, tandis que la sécurité, la gouvernance et la préparation de la main-d'œuvre accusent souvent un retard par rapport à la technologie.

Un projet pilote réussi n'est pas la même chose qu'une solution évolutive. Dans les activités quotidiennes, l'IA doit fonctionner avec des données irrégulières, des systèmes existants, des mécanismes de contrôle établis, une adoption inégale et un contexte où les menaces changent vite. **Les principaux obstacles proviennent de plus en plus des systèmes qui entourent la technologie, et non de la technologie ellemême.**

Ce défi prendra de l'ampleur à mesure que l'IA gagnera en autonomie. Les systèmes ne se contenteront pas de générer du contenu ou de répondre à des questions, ils prendront aussi des décisions, coordonneront des tâches, interagiront avec les systèmes opérationnels et poseront des gestes autrefois réalisés par des personnes. Les leaders ont besoin d'une surveillance accrue, de responsabilités plus claires et d'une main-d'œuvre formée pour utiliser ces outils de façon responsable.

Les organisations qui progressent traitent l'IA comme une transformation de l'entreprise, et non comme un autre déploiement technologique. Elles lient les initiatives aux priorités opérationnelles, établissent une gouvernance dès le départ, intègrent la sécurité à la résilience opérationnelle, repensent les flux de travail plutôt que d'automatiser ceux qui sont défaillants, et investissent dans les personnes autant que dans la technologie.

Ce rapport examine comment les organisations peuvent aborder la prochaine phase de la transformation par l'IA. En nous appuyant sur les recherches menées auprès de leaders technologiques du monde entier, ainsi que sur des perspectives plus larges du marché sur l'adoption de l'IA, la cybersécurité, la gouvernance et le changement organisationnel, nous analysons les décisions de leadership qui détermineront si les investissements en IA deviennent des avantages concurrentiels durables ou des expérimentations coûteuses.

L'avenir de l'IA n'appartiendra pas aux organisations disposant des modèles les plus avancés. Il appartiendra aux entreprises capables d'intégrer ces modèles aux flux de travail, de les encadrer de manière responsable, de les protéger efficacement et de permettre aux personnes de les utiliser avec confiance.



Kye Mitchell

Kye Mitchell
Experis US Brand Leader



James Hallahan

James Hallahan
Experis Europe Brand Leader

Transformation des entreprises par le déploiement de l'IA à grande échelle



L'illusion de l'IA prête à l'emploi

Les outils d'IA peuvent produire des résultats impressionnants dans un environnement contrôlé, mais les activités d'entreprise sont moins indulgentes. **Un système de production doit fonctionner avec de vraies données, des applications existantes, des mécanismes de contrôle établis, des comportements d'utilisation inégaux et des processus opérationnels qui ont rarement été conçus pour l'IA. La difficulté ne consiste pas à prouver qu'un modèle peut accomplir une tâche. Elle consiste à bâtir le système environnant qui permet au modèle de fonctionner de façon fiable, répétée et à un niveau de risque acceptable.**

Cette distinction aide à expliquer l'écart grandissant entre l'activité liée à l'IA et sa valeur. Une récente étude mondiale a révélé que seulement 5 % des entreprises généraient de la valeur grâce à l'IA à grande échelle. Un autre groupe de 35 %déployait l'IA à grande échelle et commençait à générer de la valeur, tandis que 60 % ont déclaré obtenir peu de valeur concrète malgré des investissements substantiels.[2] Le groupe de tête ne s'est pas contenté d'automatiser davantage de tâches. Il a développé la stratégie, le modèle opérationnel, les talents, la technologie et les capacités en matière de données nécessaires pour transformer le travail fondamental.

A Le point de vue des responsables des TI sur l'état actuel de la mise en œuvre mondiale de l'IA[1]

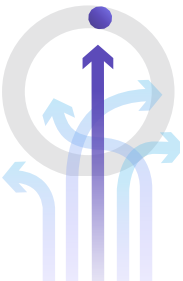
Mise en œuvre
Nous intégrons activement l'IA dans certains secteurs
32 %

Exploration
Nous faisons de la recherche et menons des projets pilotes
30 %

Déploiement à grande échelle
L'IA est déployée dans l'ensemble de l'entreprise
19 %

Pas commencé
Nous n'avons pas encore commencé à explorer l'intégration de l'IA
10 %

Pleinement intégrée
L'IA est intégrée à nos activités et à notre stratégie
9 %



Seulement 5 % des entreprises généraient de la valeur grâce à l'IA à grande échelle.

Nos propres recherches révèlent la même tension du point de vue des leaders technologiques. La plupart des leaders technologiques de la haute direction indiquent que leur entreprise augmente ses investissements en IA, et 60 % affirment que leur organisation met en oeuvre l'IA dans au moins certains secteurs. Pourtant, seuls 9 % disent que l'IA est pleinement intégrée aux activités et à la stratégie.[1] Plus de la moitié signalent un rendement positif de leurs investissements en IA, mais les écarts entre les tailles d'entreprise, les secteurs et les marchés suggèrent que les premiers rendements ne se traduisent pas toujours par un déploiement à grande échelle dans l'entreprise.

Commencez par l'entreprise, pas par le modèle

Un cas d'utilisation techniquement viable peut tout de même représenter un faible investissement opérationnel. Les leaders doivent savoir quel flux de travail changera, qui est responsable du résultat, quel risque l'organisation accepte et comment la valeur sera mesurée. Sans ces décisions, les projets pilotes tendent à s'accumuler autour de l'enthousiasme local plutôt qu'autour des priorités de l'entreprise.

Le besoin d'un meilleur alignement est clair. **Près de la moitié des leaders technologiques, soit 48 %, classent maintenant l'alignement de la stratégie des TI avec les objectifs opérationnels parmi les responsabilités les plus importantes des responsables des TI, comparativement à 34 % en 2025.** Malgré cela, l'alignement déclaré entre les stratégies opérationnelle et technologique est demeuré statistiquement inchangé à 77 %, comparativement à 80 % l'année précédente. Entre-temps, 44 % citent le rythme rapide des changements technologiques comme un obstacle majeur, et 61 % des responsables des TI affirment que les cadres supérieurs n'en savent pas assez sur leur rôle et ses exigences.[1]

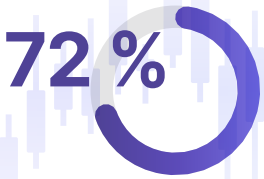
Priorités mondiales des responsables des TI en 2026[1]

1. Aligner les TI avec la stratégie opérationnelle
2. Renforcer la cybersécurité
3. Transformation numérique
4. Réduction des coûts
5. Talents technologiques
6. Conformité réglementaire

Ces conclusions révèlent un enjeu de leadership. **L'IA ne peut pas relever uniquement des TI lorsque son impact s'étend aux activités, aux finances, aux risques, aux affaires juridiques, à l'expérience client et à la main-d'oeuvre. Les leaders doivent partager la responsabilité du choix des problèmes, de la refonte des flux de travail et de la mesure des résultats.** Les leaders technologiques doivent traduire les possibilités techniques en décisions sur lesquelles le reste de l'entreprise peut agir.

Moderniser les fondations pour permettre l'expansion

Les données et l'architecture déterminent aussi si les cas d'utilisation prometteurs survivent la production. L'étude d'IBM auprès des PDG en 2025 a révélé que 68 % des PDG sondés considéraient une architecture de données intégrée à l'échelle de l'entreprise comme essentielle à la collaboration interfonctionnelle, tandis que 72 % considéraient les données exclusives comme essentielles pour libérer la valeur de l'IA générative.3 Parallèlement, la moitié a déclaré que des investissements rapides avaient laissé leur organisation avec une technologie fragmentée et déconnectée. Seulement 16 % des initiatives d'IA avaient été déployées à l'échelle de l'entreprise.



des PDG affirment que les données exclusives sont la clé pour libérer la valeur de l'IA générative.[3]

Pour les leaders, cela fait de la modernisation un élément de la stratégie d'IA plutôt qu'un programme d'infrastructure distinct. Les questions pratiques consistent notamment à savoir si les données sont accessibles avec les bonnes autorisations, si les modèles peuvent se connecter de façon sécuritaire aux systèmes de base, si les résultats peuvent être surveillés et si l'organisation peut modifier ou retirer une plateforme sans perturber les activités essentielles.

La nouvelle surface d'attaque de l'entreprise

À mesure que l'IA s'intègre aux activités fondamentales, la cybersécurité s'étend au-delà des réseaux, des appareils et des applications. **Les organisations doivent également protéger les modèles, les données d'entraînement et de récupération, les requêtes, les identités des agents, les actions automatisées, les intégrations et les environnements infonuagiques qui les relient entre eux. Une faiblesse à n'importe quel niveau peut compromettre la fiabilité de l'ensemble du flux de travail.**

C'est pourquoi la cybersécurité doit être considérée comme une condition de la croissance de l'IA. Selon nos propres recherches, 78 % des leaders technologiques principaux ont indiqué que leur entreprise augmente ses investissements en cybersécurité. La cybersécurité est aussi la compétence technologique la plus importante, citée par 46 %, devant l'IA et l'apprentissage automatique à 37 % et l'informatique infonuagique à 31 %. Pourtant, le niveau de préparation n'avance pas au même rythme. Seuls 72 % affirment que leur stratégie de gestion des risques est alignée sur leur préparation en cybersécurité, comparativement à 77 % en 2025. La même proportion offre régulièrement de la formation en cybersécurité, soit peu de changement par rapport aux 74 % de l'année précédente.[1]

Un regain d'attention des responsables des TI envers la cybersécurité



78 % augmentent leur budget de cybersécurité



La cybersécurité est la compétence la plus recherchée chez les talents technologiques



La cybersécurité demeure la principale préoccupation qui empêche les responsables des TI de dormir

Les agents font monter les enjeux

Le virage vers l'IA agentique ajoute une nouvelle catégorie d'exposition aux risques, car les agents peuvent se déplacer entre les systèmes et agir. **Le risque principal ne se limite plus à l'inexactitude d'une réponse. Les leaders doivent se demander ce que le système est autorisé à faire, aux données auxquelles il peut accéder, comment son identité est gérée et ce qui se produit lorsqu'une action est inattendue.**

Les contrôles d'accès doivent donc refléter la tâche, et non simplement l'utilisateur ou l'application. Les agents ne devraient pas hériter d'autorisations étendues uniquement parce que cela facilite la mise en oeuvre. Les organisations doivent également pouvoir tracer les requêtes, les sources de données, les décisions, les actions et les exceptions afin que les équipes de sécurité puissent comprendre ce qui s'est passé et intervenir au besoin.

L'IA est à la fois un outil de sécurité et un défi de sécurité

Les équipes de sécurité utilisent également l'IA pour accroître la rapidité et l'efficacité de la défense. **Une étude récente a révélé que 91 % des répondants utilisaient ou expérimentaient des solutions de cybersécurité alimentées par l'IA, et 84 % ont indiqué que les outils de sécurité améliorés par l'IA aidaient les équipes à devenir plus efficaces et performantes.** Parallèlement, 86 % ont signalé au moins une atteinte à la sécurité au cours des 12 derniers mois, et 56 % ont cité le manque de compétences en cybersécurité comme une cause importante des failles à la sécurité.[4]



56 %

des leaders technologiques affirment que les lacunes en compétences de cybersécurité sont la principale cause des brèches de sécurité.[4]

La leçon n'est pas de ralentir l'adoption de l'IA, mais les leaders technologiques doivent la relier à une ingénierie sécurisée dès le départg. **Les leaders de la sécurité devraient participer à la sélection des cas d'utilisation, à la conception des chemins de données, à l'évaluation des fournisseurs et à la modification des flux de travail.** Les contrôles ajoutés après le déploiement sont plus susceptibles de créer des retards, des solutions de contournement et de la méfiance.

Faire de la sécurité une discipline opérationnelle partagée

La sécurité de l'IA ne relève pas uniquement du responsable de la sécurité de l'information (RSI). Les directeurs d'entreprises doivent définir les résultats et les exceptions acceptables. Les équipes technologiques doivent bâtir et maintenir l'architecture. Les équipes juridiques et de gestion des risques doivent traduire les obligations en contrôles utilisables. Les responsables de la main-d'oeuvre doivent soutenir la formation et l'adoption. Les employés doivent savoir quand et comment remettre en question, escalader ou annuler les décisions soutenues par l'IA.

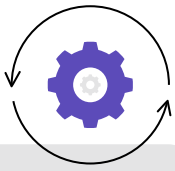
La gouvernance devient un avantage concurrentiel

La gouvernance est souvent décrite comme une contrainte à l'innovation. En pratique, une gouvernance faible crée de l'incertitude, des retards, des répétitions d'examens et des décisions incohérentes. **Une solide gouvernance donne aux équipes un parcours reproductible, de l'idée à la production. Elle précise quels risques exigent une escalade, qui a le pouvoir d'approuver ou d'arrêter un déploiement et comment les systèmes seront surveillés après leur lancement.**

Une récente étude auprès d'entreprises a révélé que la réglementation et le risque étaient devenus les principaux obstacles au développement et au déploiement de l'IA générative. La plupart des entreprises sondées prévoyaient que moins de 30 % de leurs expériences atteindraient le déploiement complet dans les six mois, tandis que 69 % s'attendaient à ce qu'il faille au moins un an pour mettre en oeuvre une stratégie de gouvernance complète.[5]

Une gouvernance efficace est le plus grand obstacle

50 % des cadres de la haute direction affirment que la traduction des principes d'IA responsable en processus opérationnels constitue leur principal obstacle au progrès.[5]





Une autre récente enquête sur l'IA responsable a établi un lien direct entre la gouvernance et la valeur. 58 % des cadres ont affirmé que les initiatives d'IA responsable améliorent le rendement du capital investi et l'efficacité organisationnelle, 55 % ont signalé des avantages pour l'expérience client et l'innovation, et 51 % ont cité une cybersécurité et une protection des données renforcées. Le défi était la concrétisation, 50 % ayant identifié le passage des principes aux processus évolutifs comme leur principal obstacle.[5]

La gouvernance doit se poursuivre après le lancement

Les contrôles traditionnels mettent souvent l'accent sur l'approbation avant le déploiement. L'IA exige une attention égale après le déploiement, car les modèles, les données, les utilisateurs et les conditions d'exploitation changent. La gouvernance devrait inclure une surveillance continue, des boucles de rétroaction, une réponse aux incidents, de la documentation, des examens périodiques et des normes claires pour la modification ou le retrait.

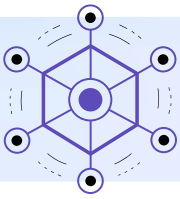
Les systèmes agentiques rendent cet enjeu particulièrement important. Plus un système est autonome, plus les leaders doivent définir précisément sa portée, ses points d'escalade et la supervision humaine. **La gouvernance devrait préciser qui est responsable du résultat, qui peut inspecter le système, qui peut le suspendre et quelles preuves sont requises avant que le système puisse reprendre ses activités.**

Tension croissante liée à la souveraineté

La souveraineté des données ajoute une autre couche de complexité. **La plupart des leaders technologiques (81 %) décrivent la souveraineté numérique comme une priorité élevée ou critique. Parallèlement, 67 % s'attendent à ce que leur organisation augmente ses investissements dans la prestation de services de TI à l'étranger et dans des pays voisins.**[1] Cette tension est compréhensible lorsque les leaders opérationnels souhaitent exercer un plus grand contrôle sur les données et l'infrastructure tout en tirant parti de la technologie, des compétences et de la capacité de prestation mondiales.

La réponse n'est pas l'indépendance technologique complète. Il faut plutôt clarifier ce qui doit demeurer sous un contrôle direct, ce qui peut être confié à des partenaires, où les données peuvent être stockées ou traitées, et comment l'organisation peut maintenir la continuité si un fournisseur, une plateforme, une réglementation ou une situation géopolitique change.

La souveraineté prend de l'ampleur



81 % des responsables des TI et des leaders technologiques principaux affirment que la souveraineté numérique est une priorité élevée ou critique.[1]

Traiter la réglementation comme une exigence de conception

La Loi sur l'IA de l'Union européenne illustre pourquoi la gouvernance doit être intégrée aux activités. Cette réglementation adopte une approche fondée sur les risques et comprend des exigences précises qui touchent l'IA liée au milieu de travail et à l'emploi. Son cadre de sanctions peut atteindre 35 millions d'euros ou 7 % du roulement annuel mondial pour les infractions les plus graves, avec d'autres niveaux pour les autres obligations et les renseignements inexacts.[6]

Pour les organisations multinationales, la conformité ne peut se réduire à un examen juridique ponctuel. Les équipes ont besoin d'une façon pratique de relier les obligations locales aux inventaires de systèmes, aux classifications des risques, aux pratiques de données, à la supervision humaine, à la documentation et à la gestion des fournisseurs.

Créer une différenciation concurrentielle



Repenser les organisations pour l'ère des agents

L'IA peut accélérer le travail, mais la rapidité n'améliore pas un processus fragmenté, dupliqué ou mal pris en charge. Les organisations qui superposent des agents aux inefficacités existantes risquent de créer de la confusion plus rapidement. La première étape consiste à comprendre comment le travail circule actuellement entre les services, les systèmes et les points de décision.

Des recherches plus récentes montrent pourquoi la refonte des flux de travail est importante. **Les entreprises conçues pour l'avenir vont au-delà de l'automatisation isolée et transforment leurs fonctions fondamentales. Elles poursuivent des ambitions pluriannuelles en IA, adoptent des modèles opérationnels axés d'abord sur l'IA, obtiennent les talents nécessaires et utilisent une technologie et des données adaptées à leurs besoins.** Une étude estime que 70 % de la valeur potentielle de l'IA est concentrée dans les fonctions opérationnelles fondamentales plutôt que dans les activités de soutien.[2]

70 % de la valeur potentielle de l'IA est concentrée dans les fonctions opérationnelles fondamentales plutôt que dans les activités de soutien.



Passer de l'automatisation des tâches à leur orchestration

L'IA agentique fait passer la discussion de l'automatisation de tâches individuelles à la coordination du travail entre les personnes et les systèmes numériques. Cela exige un niveau d'orchestration capable de rendre le travail visible, de l'acheminer adéquatement, d'appliquer des contrôles et de mesurer les résultats. Cela exige également une responsabilité humaine explicite.

Les leaders devraient définir quelles décisions demeurent entre les mains des personnes, lesquelles sont soutenues par l'IA et lesquelles peuvent être exécutées par un agent dans les limites établies. Ils devraient aussi déterminer comment les exceptions sont renvoyées aux personnes, comment le rendement est évalué et comment les leçons tirées de l'utilisation réelle améliorent le flux de travail au fil du temps.

En vedette

ExcelerateWorkflow propulsé par IBM® watsonx Orchestrate™

Aujourd'hui, la plupart des organisations ne peinent pas à repérer les occasions liées à l'IA. Le défi consiste à rendre l'IA opérationnel à grande échelle. Bon nombre d'initiatives d'IA démontrent un potentiel lors des phases pilotes, mais stagnent avant de générer unevaleur opérationnelle durable. Le défi est rarement la technologie elle-même. Plus souvent, les entreprises se heurtent à des flux de travail fragmentés, des systèmes déconnectés, des responsabilités floues, des exigences de gouvernance et des obstacles à l'adoption par la main-d'oeuvre qui empêchent l'IA de faire partie des activités quotidiennes.

La prochaine phase de la transformation par l'IA exige plus que le déploiement de nouveaux outils. Elle exige de relier l'IA à la façon dont le travail est accompli. **Pour aider les organisations à combler cet écart, et à passer de l'expérimentation à l'exécution, Experis a développé ExcelerateWorkflow, propulsé par IBM® watsonx Orchestrate.**

Conçu pour soutenir l'orchestration des flux de travail entre les fonctions opérationnelles et technologiques, ExcelerateWorkflow aide les organisations à intégrer les agents d'IA dans leurs environnements opérationnels existants avec une meilleure visibilité, une meilleure gouvernance et une supervision humaine accrue. Plutôt que de se concentrer sur des occasions d'automatisation isolées, la solution réunit les personnes, les systèmes et les agents d'IA afin de coordonner le travail, de réduire les frictions opérationnelles et de favoriser une exécution plus efficace et responsable.

IBM® watsonx Orchestrate™ offre une plateforme de gestion et d'orchestration des agents qui permet aux entreprises de découvrir, gérer et orchestrer des agents d'IA natifs et conçus à l'externe, avec des capacités intégrées de gouvernance, de contrôle et de sécurité. Experis complète cette technologie par son expertise de mise en oeuvre, de transformation des flux de travail, de services d'intégration et d'habilitation de la main-d'oeuvre, et un soutien à la gestion du changement. Ensemble, ces capacités aident les clients à concrétiser l'IA de façon sécuritaire et à grande échelle, en harmonie avec les objectifs opérationnels et les exigences du monde réel.

Cette approche reflète un changement plus large qui se produit dans tous les secteurs. Les organisations vont au-delà des cas d'utilisation isolés de l'IA et se demandent comment l'IA peut améliorer le rendement opérationnel dans toutes les fonctions et tous les flux de travail. Le succès dépend de plus en plus de l'intégration de la technologie, de la gouvernance, des personnes et des processus dans un modèle opérationnel unifié.

En combinant une expertise technologique, des capacités de transformation de la main-d'oeuvre et des modèles de prestation évolutifs, **Experis aide les entreprises à accélérer l'adoption de l'IA, à établir des responsabilités claires, à renforcer la confiance envers les flux de travail soutenus par l'IA et à obtenir des résultats opérationnels mesurables provenant de leurs investissements.**

L'IA crée du potentiel. La valeur pour l'entreprise découle de l'intégration réussie de ce potentiel aux flux de travail.

IBM
Gold Partner

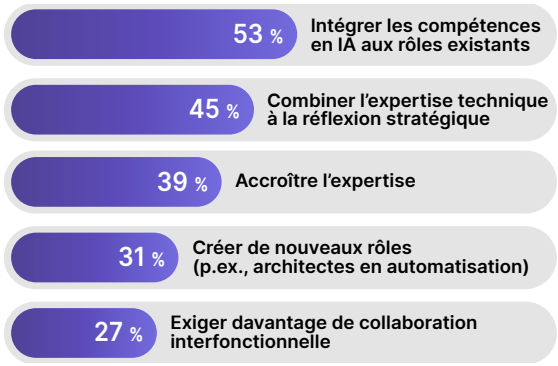
IBM, le logo IBM, watsonx et watsonx Orchestrate sont des marques de commerce ou des marques de commerce déposées d'International Business Machines Corporation.



Repenser les rôles en fonction des flux de travail

La transformation du modèle opérationnel redéfinit déjà le travail technologique. Notre recherche révèle que 53 % des organisations intègrent les compétences en IA à des rôles existants, 45 % combinent l'expertise technique à la réflexion stratégique, et 39 % augmentent la polyvalence des rôles dans plusieurs domaines. Près du tiers créent de nouveaux rôles, comme ceux d'éthicien des données et d'architecte en automatisation. Beaucoup moins indiquent éliminer des rôles afin de réaffecter les effectifs ou de réduire les coûts.[1]

Principales approches des responsables des TI pour les talents technologiques augmentés par l'IA[1]



Cette tendance laisse entendre que le déploiement de l'IA à grande échelle dépend moins de la mise à pied des personnes que de la redéfinition des responsabilités. Les employés doivent comprendre clairement comment l'IA modifie les décisions, les transferts, la responsabilisation et les attentes en matière de service. Les gestionnaires doivent savoir comment évaluer le rendement lorsque les résultats sont produits par une combinaison de personnes et de systèmes.

Principales compétences recherchées par les responsables des TI[1]

1. Cybersécurité
2. IA et apprentissage automatique
3. Informatique infonuagique
4. Développement logiciel
5. Collaboration et travail d'équipe

La dimension humaine de la transformation par l'IA

La question des talents va au-delà de la capacité d'une entreprise à recruter suffisamment de spécialistes de l'IA. Un déploiement sécuritaire à grande échelle exige un portefeuille cohérent de capacités techniques, de gouvernance, de leadership et de main-d'oeuvre. Ces capacités doivent être accessibles là où les décisions sont prises, et non isolées dans un petit centre d'excellence.

Notre récente recherche auprès des responsables des TI illustre le large éventail de compétences dont les équipes de TI du monde entier ont besoin. **La cybersécurité est la compétence technologique la plus souvent citée, à 46 %, suivie de l'IA et de l'apprentissage automatique à 37 %, puis de l'informatique infonuagique à 31 %.** La collaboration, le développement logiciel (DevOps), l'adaptabilité, la résolution de problèmes, la communication et le leadership figurent aussi parmi les priorités. Cette combinaison reflète la réalité selon laquelle l'IA en entreprise est à la fois un système technique et un programme de transformation organisationnelle.

Développer quatre dimensions de capacité

1

Capacité technique :

IA, données, infonuagique, cybersécurité, ingénierie logicielle, architecture, tests et intégration de plateformes.

2

Capacité de gouvernance:

Classification des risques, politiques, surveillance, conformité, audit, évaluation des fournisseurs et IA responsable.

3

Capacité de leadership :

Alignement avec les activités, décisions d'investissement, responsabilisation, communication et direction du changement.

4

Capacité de la main-d'oeuvre :

Connaissances en IA, adoption, confiance, collaboration, apprentissage continuet supervision humaine.

Combler l'écart de l'adoption

Un système peut être déployé techniquement sans être adopté de façon significative. Experis a constaté que l'alignement entre la mise en oeuvre de nouvelles technologies et l'adoption par les employés a diminué en 2026. **Lorsque les équipes ne comprennent pas comment un outil s'intègre à leur travail, de quoi elles demeurent responsables ou à quel moment elles doivent remettre en question les résultats obtenus, l'adoption devient inégale et le risque augmente.**

La formation devrait donc aller au-delà des démonstrations de fonctionnalités. Les employés doivent s'exercer à utiliser l'IA dans de véritables flux de travail, évaluer les résultats, reconnaître les limites, protéger les données et signaler les préoccupations. Les gestionnaires ont besoin de soutien pour repenser les rôles et les mesures. Les dirigeants ont besoin d'un langage commun pour parler de valeur, de risque et de supervision humaine.

Développer les leaders avec autant d'intention que les spécialistes

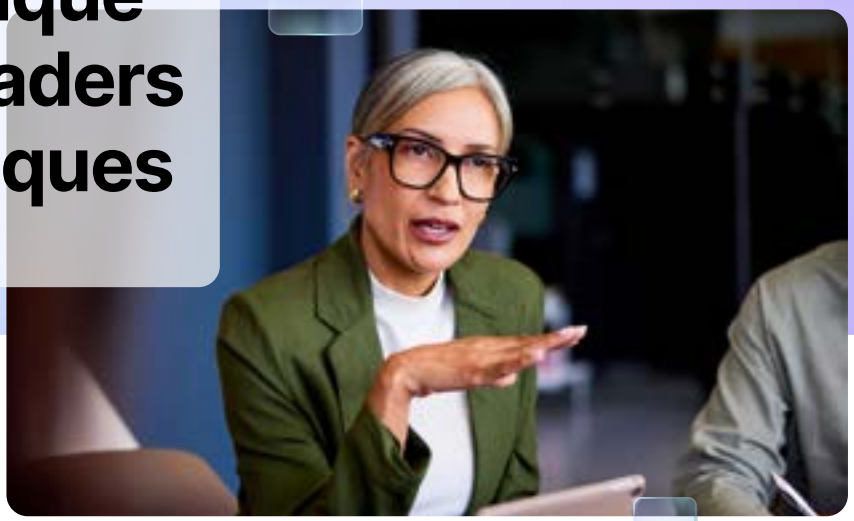
Le bassin de relève en leadership mérite la même attention. Seuls 58 % des organisations de l'étude Experis mettent régulièrement en oeuvre des programmes pour développer les futurs dirigeants technologiques, une baisse par rapport aux 63 % de 2025.1 Cette baisse survient alors que les rôles de leadership exigent une combinaison plus complexe de jugement technique, de compréhension des affaires, de communication, de gouvernance et de capacité à gérer le changement.



Seuls 58 % des organisations développent régulièrement de futurs dirigeants technologiques, par rapport à 63 % en 2025.

Les entreprises doivent combiner le développement interne, le recrutement ciblé, les partenaires spécialistes et les modèles de prestation flexibles. **L'objectif n'est pas de doter chaque capacité d'un poste permanent. Il consiste à veiller à ce que l'entreprise puisse accéder à la bonne expertise, maintenir la responsabilisation et transférer les connaissances à mesure que la technologie et les risques évoluent.**

Guide pratique pour les leaders technologiques



Cinq mesures que les leaders technologiques devraient prendre dès maintenant

Passer de l'expérimentation en IA à la création de valeur pour l'entreprise exige des mesures ciblées. **Ces cinq priorités donnent aux leaders technologiques une feuille de route pratique pour aligner les investissements avec les résultats d'affaires, renforcer la sécurité et la gouvernance, repenser le travail en fonction de l'IA et développer les capacités nécessaires pour passer à l'échelle en toute confiance.**

Ensemble, ces mesures créent un système d'entreprise pour déployer l'IA à grande échelle en toute sécurité. Elles relient les investissements aux résultats, l'innovation au contrôle, l'automatisation à la responsabilisation et la technologie aux personnes qui lui donnent de la valeur.

1. Aligner les investissements en IA avec les résultats d'affaires

2. Faire de la cybersécurité une priorité d'affaires essentielle

3. Mettre en place la gouvernance avant de passer à l'expansion

4. Repenser les flux de travail avant de déployer des agents

5. Investir dans les capacités, pas seulement dans la technologie

« Dire que nous allons plus vite ou que la qualité est meilleure ne constitue pas un RCI. Si nous gagnons du temps grâce à l'IA, la véritable question est : qu'allons-nous en faire? La valeur d'un projet doit être mesurée en fonction des revenus ou de la rentabilité. »

– Responsable des TI, secteur des produits de luxe, France



1. Aligner les investissements en IA avec les résultats d'affaires :

Exiger que chaque initiative importante détermine le responsable des activités, le flux de travail, le résultat, la mesure d'adoption, le responsable des risques et l'indicateur de valeur avant de passer à l'échelle.

Quel résultat d'affaires changera?

Qui sera responsable du résultat après le déploiement?

Quelles preuves justifieront la poursuite de l'investissement?



2. Faire de la cybersécurité une priorité d'affaires essentielle :

Étendre la conception de la sécurité aux modèles, aux données, aux agents, aux identités, aux intégrations, aux fournisseurs et aux actions automatisées.

À quoi le système peut-il accéder et que peut-il faire?

Comment les comportements inattendus seront-ils détectés?

Qui a l'autorité d'intervenir?



3. Mettre en place la gouvernance avant de passer à l'expansion :

Créer un processus reproductible de classification, d'approbation, de surveillance, d'escalade et de retrait.

Quelles décisions exigent une révision humaine?

Quelle documentation et quels tests sont requis?

Comment les contrôles s'adapteront-ils après le lancement?



4. Repenser les flux de travail avant de déployer des agents :

Cartographier le travail de bout en bout et éliminer la fragmentation avant d'ajouter de l'autonomie.

À quels endroits le travail se bloque-t-il aujourd'hui?

Quelles activités devraient être dirigées par des personnes, assistées par l'IA ou exécutées par des agents?

Comment les exceptions retournerontelles aux personnes?



5. Investir dans les capacités, pas seulement dans la technologie

Développer un portefeuille de capacités techniques, de gouvernance, de leadership et de main-d'oeuvre en misant sur le développement interne et l'expertise externe.

Quelles capacités est-il stratégique de posséder?

Où les partenaires peuvent-ils accélérer les progrès?

Comment le transfert des connaissances et l'apprentissage continu se déroulerontils?

Expertise mondiale d'Experis

Alors que l'IA transforme le paysage de la cybersécurité, les organisations font face à un défi à deux volets : exploiter la puissance des technologies émergentes tout en gérant un environnement de risque de plus en plus complexe. Qu'il s'agisse de sécuriser les systèmes alimentés par l'IA et de protéger les actifs de données essentiels, de moderniser l'infrastructure ou de renforcer la gouvernance, le succès exige plus que de simples investissements technologiques. Il exige la bonne combinaison de stratégie, d'expertise spécialisée et d'exécution. C'est là qu'Experis aide les entreprises à passer de l'expérimentation à l'impact.

Expertise en IA et en données

Transformez les données en renseignements exploitables grâce à des services de modernisation des données, de modélisation de l'IA, d'automatisation, d'analytique avancée et de gouvernance. Les organisations obtiennent une meilleure visibilité, une prise de décision renforcée et une adoption plus responsable de l'IA.

DevSecOps et ingénierie sécurisée

Intégrez la sécurité à l'ensemble du cycle de vie technologique en combinant les pratiques de développement, d'exploitation et de sécurité. Cela contribue à accélérer l'innovation tout en réduisant les risques et en renforçant la résilience.

Modernisation de l'infonuagique et des applications

Modernisez les systèmes existants, migrez vers des environnements infonuagiques et concevez des architectures évolutives pour soutenir les exigences émergentes en matière d'IA et de cybersécurité. Les organisations bénéficient d'une plus grande agilité et d'une base technologique conçue pour la croissance future.

Gouvernance, qualité et conformité

Renforcez la confiance envers les initiatives numériques grâce à l'ingénierie de la qualité, aux tests automatisés, à la validation du rendement et aux tests de sécurité. Le résultat : une fiabilité accrue, un risque opérationnel réduit et une plus grande confiance dans les investissements technologiques.

Délai de création de valeur accéléré

Tirez parti de méthodologies éprouvées, d'une expertise spécialisée et de modèles de prestation agiles pour passer plus rapidement de la stratégie à des résultats mesurables. Experis met l'accent sur des résultats plus rapides et un impact concret sur les affaires.

[1] Perspectives 2026 des responsables des TI d'Experis [2] BCG [3] IBM Institute for Business Value [4] Fortinet [5] Deloitte [6] Union européenne

Restons en contact

Ressources mondiales d'Experis pour les leaders technologiques

Accédez à des talents et à des services technologiques spécialisés appuyés par un réseau mondial qui accompagne les clients de divers secteurs et marchés. Une expertise approfondie des domaines aide les organisations à relever avec confiance des défis complexes de transformation.

Passer de l'expérimentation en IA à un impact d'affaires mesurable exige plus que de nouveaux outils. Cela exige la bonne combinaison d'expertise technologique, de stratégie de main-d'oeuvre et de soutien à l'exécution. À titre de leader mondial des services technologiques, Experis® aide les entreprises à transformer le potentiel technologique en impact d'affaires grâce à l'IA, aux données, à l'infonuagique, à la modernisation des applications, à l'ingénierie de la qualité et à des solutions de talents spécialisés.

Pour en savoir plus, visitez *experis.ca*, ou suivez-nous sur *LinkedIn*.

Méthodologie de recherche

Experis a commandé un sondage auprès de 1 930 hauts dirigeants technologiques dans 12 pays, du 28 janvier au 4 mars 2026. Les répondants comprenaient des responsables des TI, des directeurs de la technologie, des responsables de la sécurité de l'information et d'autres hauts dirigeants technologiques ayant le pouvoir de décision concernant les budgets de TI et l'embauche. De plus, des entrevues qualitatives approfondies ont été menées dans chaque marché.