F11 - Audit IA de l'Entreprise

Support complet d'auto-formation

Baobizz Académie

14 heures - Niveau avancé - Version juillet 2026

Mode d'emploi

Le parcours simule une mission complète. Chaque notion débouche sur une feuille de travail ou un livrable. Les textes et normes doivent être vérifiés dans leur version applicable.

Objectifs pédagogiques

• Maîtriser le cadre méthodologique de l'audit IA.

• Réaliser l'inventaire complet des usages IA.

• Évaluer les risques IA.

• Rédiger un rapport avec recommandations opérationnelles.

• Proposer un plan de remédiation et une gouvernance IA.

Cas fil rouge

SenInnov Groupe utilise la présélection de candidatures, un scoring commercial, un chatbot interne, une détection d'anomalies comptables et des outils génératifs informels.

Module 1 - Cadre méthodologique de l’audit IA

2 h - Positionner l’audit IA dans le dispositif global d’assurance, définir le périmètre de mission et bâtir un programme de travail fondé sur les risques.

1.1 - Définir l’objet de l’audit IA (20 min)

L’audit IA évalue la gouvernance, les données, les modèles, les usages, les contrôles, les fournisseurs et les impacts d’un système d’IA. Il ne se limite ni à un test technique du modèle ni à un contrôle documentaire.

Activité : À partir de quatre usages fictifs, distinguez les objectifs d’assurance, de conformité, de performance et de sécurité.
Critères : Chaque objectif doit être relié à un risque, un critère d’audit et une preuve attendue.

1.2 - Identifier les parties prenantes (20 min)

Une mission mobilise la gouvernance, les métiers, la DSI, la sécurité, la conformité, le juridique, l’audit interne, les achats et parfois des tiers. L’indépendance et les compétences de l’équipe d’audit doivent être documentées.

Activité : Construisez une matrice des parties prenantes pour l’entreprise fil rouge.
Critères : La matrice doit préciser rôle, niveau d’influence, contribution attendue et risque de conflit d’intérêts.

1.3 - Utiliser les référentiels avec discernement (25 min)

Le NIST AI RMF structure la gestion des risques autour de fonctions de gouvernance, cartographie, mesure et management. ISO/IEC 42001 traite du système de management de l’IA. L’AI Act européen impose une logique de classification et d’obligations. Les textes applicables doivent être vérifiés à la date de la mission.

Activité : Réalisez une table de correspondance entre cinq objectifs d’audit et les référentiels pertinents.
Critères : Le résultat doit distinguer obligation juridique, bonne pratique et critère interne.

1.4 - Intégrer l’IA à la cartographie des risques (20 min)

Les risques IA doivent être reliés aux processus, objectifs stratégiques, risques opérationnels, risques SI, conformité, réputation et continuité d’activité. Un même système peut générer plusieurs risques transversaux.

Activité : Positionnez les quatre systèmes de l’entreprise fictive dans une cartographie probabilité-impact.
Critères : Les justifications doivent s’appuyer sur la criticité métier, les données utilisées, l’autonomie et les populations affectées.

1.5 - Concevoir le cycle d’audit (20 min)

Le cycle comprend cadrage, compréhension, inventaire, tests, constats, contradictoire, rapport et suivi. Le niveau de profondeur dépend du risque et de la possibilité d’obtenir des preuves suffisantes.

Activité : Élaborez un calendrier de mission de six semaines.
Critères : Le calendrier doit inclure livrables, responsables, points de validation et phase contradictoire.

1.6 - Distinguer les formes d’audit (15 min)

L’audit interne vise l’amélioration du dispositif ; l’audit externe fournit une assurance indépendante selon un mandat ; l’audit réglementaire répond à une exigence précise. Les responsabilités et niveaux d’assurance ne sont pas interchangeables.

Activité : Rédigez une note expliquant quelle forme d’audit convient à trois situations.
Critères : La réponse doit préciser destinataire, indépendance, critères et limites de conclusion.

Module 2 - Inventaire et cartographie des usages IA

2 h - Détecter les usages officiels et informels, documenter les chaînes de traitement et construire un registre IA exploitable par la gouvernance.

2.1 - Préparer l'inventaire (20 min)

Un inventaire fiable combine questionnaires, entretiens, revue des contrats, analyse des flux, inventaire applicatif, dépenses fournisseurs et signaux d'usage informel. Les simples déclarations des responsables sont rarement suffisantes.

Activité : Adaptez le questionnaire d'inventaire fourni à trois directions : RH, finance et commercial.
Critères : Les questions doivent révéler aussi les usages non homologués et les outils gratuits.

2.2 - Conduire les entretiens (20 min)

Les entretiens doivent partir des décisions et tâches réellement exécutées : qui utilise l'outil, pour quoi, avec quelles données, quel contrôle humain et quelles conséquences en cas d'erreur.

Activité : Préparez un guide d'entretien de quinze questions pour le responsable RH.
Critères : Le guide doit couvrir données, modèle, décision, supervision, incidents et fournisseur.

2.3 - Analyser les traces disponibles (20 min)

Les journaux, historiques de requêtes, configurations, tickets, factures et comptes SaaS peuvent révéler des usages ignorés. L'auditeur doit toutefois respecter les droits d'accès et la confidentialité.

Activité : Identifiez dix sources de preuve permettant de confirmer l'existence d'un usage IA.
Critères : Chaque source doit être reliée à une assertion d'audit précise.

2.4 - Construire le registre IA (25 min)

Le registre décrit le système, le propriétaire, le fournisseur, le modèle, le processus, les utilisateurs, les données, les décisions, l'autonomie, les contrôles, les incidents et la date de revue.

Activité : Complétez le registre fictif pour quatre systèmes.
Critères : Aucun champ critique ne doit rester vide sans justification ni plan d'action.

2.5 - Documenter la chaîne algorithmique (20 min)

La chaîne de traitement relie collecte, préparation des données, appel du modèle, règles métier, interface, validation humaine, décision, journalisation et conservation.

Activité : Dessinez la chaîne du système de scoring commercial.
Critères : Le schéma doit faire apparaître les points de contrôle, transferts de données et dépendances externes.

2.6 - Classer les usages par criticité (15 min)

La classification doit considérer l'impact sur les personnes, les droits, la sécurité, les finances, la continuité, la réputation, l'autonomie et l'étendue du déploiement. Le schéma réglementaire applicable doit être vérifié.

Activité : Attribuez un niveau de criticité aux quatre usages et documentez votre raisonnement.
Critères : La conclusion doit être traçable, prudente et validée par la gouvernance.

Module 3 - Évaluation des risques IA

3 h - Évaluer de manière structurée les risques de biais, d'opacité, de sécurité, de souveraineté, de performance, de conformité et de dépendance.

3.1 - Construire une taxonomie des risques (25 min)

Une taxonomie utile couvre gouvernance, stratégie, données, modèle, sécurité, conformité, éthique, opérations, fournisseur, finances, réputation et continuité. Elle doit être adaptée au contexte de l'organisation.

Activité : Transformez la liste de risques fournie en univers d'audit hiérarchisé.
Critères : Chaque famille doit comporter définition, causes, événements et impacts.

3.2 - Coter risque inhérent et résiduel (25 min)

Le risque inhérent est apprécié avant les contrôles ; le risque résiduel après prise en compte de leur conception et de leur fonctionnement. La cotation ne doit pas masquer les incertitudes.

Activité : Cotez dix scénarios avec une matrice 5 x 5.
Critères : Les niveaux doivent être justifiés et les contrôles évalués séparément.

3.3 - Évaluer les données (25 min)

Les risques incluent qualité insuffisante, représentativité limitée, origine incertaine, biais historique, dérive, absence de consentement, réutilisation incompatible et conservation excessive.

Activité : Réalisez une revue de données pour le système de recrutement fictif.
Critères : Le dossier doit identifier source, qualité, population, exclusions, transformations et contrôles.

3.4 - Tester les biais (30 min)

Un test de biais compare les performances et décisions entre groupes pertinents, en tenant compte du contexte juridique et éthique. Un écart statistique n'est pas automatiquement une discrimination, mais il exige une analyse.

Activité : Calculez les taux de sélection par groupe à partir du jeu de données fourni et rédigez une conclusion prudente.
Critères : La conclusion doit distinguer constat statistique, cause possible, limite et action complémentaire.

3.5 - Évaluer l'explicabilité (20 min)

L'explicabilité doit être proportionnée à l'usage. L'auditeur vérifie si les utilisateurs comprennent les facteurs déterminants, les limites du modèle et les conditions d'escalade.

Activité : Évaluez trois explications produites par un modèle de scoring.
Critères : Une explication acceptable doit être intelligible, fidèle, stable et adaptée au destinataire.

3.6 - Auditer la cybersécurité IA (25 min)

Les risques spécifiques incluent injection de prompt, empoisonnement des données, extraction d'informations, contournement des garde-fous, modèle compromis, dépendances vulnérables et exposition de clés.

Activité : Exécutez une revue documentaire de sécurité à partir de quinze contrôles.
Critères : Les faiblesses critiques doivent mener à des tests ciblés ou à une restriction de mise en production.

3.7 - Évaluer la dépendance fournisseur (20 min)

Le verrouillage peut résulter des formats propriétaires, coûts de sortie, absence d'export, dépendance aux API, localisation des données, changements tarifaires ou disparition du service.

Activité : Complétez la grille de due diligence du fournisseur fictif.
Critères : Le dossier doit prévoir réversibilité, continuité, portabilité et alternative.

3.8 - Mesurer la performance et la dérive (20 min)

Un système peut devenir moins fiable lorsque les données, les comportements ou le contexte changent. L’auditeur vérifie indicateurs, seuils, fréquence de revue et mécanismes d’arrêt.

Activité : Définissez un tableau de surveillance pour le scoring commercial.
Critères : Chaque indicateur doit avoir un seuil, une source, un responsable et une action.

3.9 - Atelier de synthèse des risques (20 min)

Les résultats techniques doivent être traduits en risques compréhensibles par les dirigeants, sans simplification abusive.

Activité : Préparez une heatmap et les cinq risques prioritaires de l’entreprise fil rouge.
Critères : Chaque risque doit être relié à un système, un processus, une preuve et un propriétaire.

Module 4 - Gouvernance, conformité et éthique IA

2 h - Évaluer les responsabilités, politiques, comités, obligations de conformité et relations contractuelles autour de l'IA.

4.1 - Cartographier les exigences applicables (25 min)

L'auditeur commence par identifier les lois, règlements, contrats, politiques internes et exigences sectorielles réellement applicables. Au Sénégal, toute référence aux autorités ou textes doit être vérifiée dans sa version en vigueur.

Activité : Construisez une matrice d'applicabilité pour une entreprise sénégalaise exportant vers l'Europe.
Critères : Distinguez clairement exigence locale, extraterritoriale, contractuelle et volontaire.

4.2 - Évaluer la politique IA (20 min)

Une politique IA précise finalités, usages autorisés et interdits, responsabilités, données, fournisseurs, validation, sécurité, transparence, contrôle humain, incidents et sanctions internes.

Activité : Auditez la politique fictive et identifiez dix lacunes.
Critères : Les lacunes doivent être classées par risque et assorties d'une recommandation.

4.3 - Auditer la gouvernance (20 min)

La gouvernance doit attribuer des décisions à des organes identifiés : approbation des cas d'usage, acceptation des risques, incidents, changements majeurs et retrait d'un système.

Activité : Dessinez le modèle de gouvernance cible.
Critères : Le schéma doit inclure conseil ou direction, comité IA, propriétaires métier, DSI, sécurité, conformité et audit.

4.4 - Évaluer le comité éthique IA (20 min)

Un comité utile a un mandat, une composition pluridisciplinaire, des règles de saisine, une traçabilité, une gestion des conflits d'intérêts et un suivi des décisions.

Activité : Rédigez la charte du comité de l'entreprise fictive.
Critères : La charte doit éviter le rôle purement symbolique et préciser son pouvoir réel.

4.5 - Réaliser la due diligence fournisseur (20 min)

La revue couvre sécurité, confidentialité, propriété intellectuelle, sous-traitants, localisation, qualité, incidents, auditabilité, continuité, évolutions du modèle et réversibilité.

Activité : Analysez le contrat fictif et proposez dix clauses à négocier.
Critères : Les clauses doivent être opérationnelles, mesurables et cohérentes avec le risque.

4.6 - Examiner l'éthique appliquée (15 min)

L'éthique ne remplace pas le droit. Elle aide à traiter équité, dignité, autonomie, impact social, accessibilité, inclusion linguistique et effets sur l'emploi.

Activité : Rédigez une note d'arbitrage sur un outil de recrutement automatisé.
Critères : La note doit présenter bénéfices, risques, parties affectées, alternatives et conditions d'acceptabilité.

Module 5 - Rapport d’audit et plan d’action

3 h - Transformer les preuves en constats robustes, recommandations actionnables, plan de remédiation et communication adaptée aux organes de gouvernance.

5.1 - Constituer le dossier de preuves (20 min)

Chaque conclusion doit être soutenue par des éléments suffisants, pertinents, fiables et traçables. Les captures isolées ou déclarations non corroborées sont rarement suffisantes.

Activité : Classez les preuves du cas fil rouge par assertion d’audit.
Critères : Le dossier doit permettre une revue indépendante et une reconstitution du raisonnement.

5.2 - Rédiger un constat (25 min)

Un constat solide présente le critère, la situation observée, la cause, le risque ou l’effet, les preuves et la réponse du management. Il évite les jugements non étayés.

Activité : Réécrivez trois constats faibles fournis dans le pack.
Critères : Chaque constat doit être factuel, compréhensible et directement relié à une recommandation.

5.3 - Attribuer une sévérité (20 min)

La sévérité combine impact, probabilité, étendue, urgence, exposition réglementaire et efficacité des contrôles compensatoires. La terminologie doit être définie avant la mission.

Activité : Classez huit constats en critique, majeur ou mineur.
Critères : Les écarts de classement doivent être expliqués par des critères explicites.

5.4 - Formuler des recommandations actionnables (25 min)

Une recommandation précise le résultat attendu sans imposer inutilement une solution unique. Elle doit être proportionnée, réalisable, datée et attribuée.

Activité : Transformez cinq recommandations vagues en actions SMART.
Critères : Chaque recommandation doit traiter la cause et permettre une vérification ultérieure.

5.5 - Construire le plan de remédiation (25 min)

Le plan relie constat, action, responsable, échéance, ressources, dépendances, indicateur, preuve de clôture et risque accepté.

Activité : Complétez le plan d’action du cas fil rouge.
Critères : Les délais doivent refléter la criticité et les dépendances réelles.

5.6 - Préparer le contradictoire (20 min)

Le contradictoire vérifie les faits, recueille la réponse du management et clarifie les plans d’action, sans compromettre l’indépendance de l’auditeur.

Activité : Préparez la réunion de clôture avec les objections probables.
Critères : Les réponses doivent distinguer correction factuelle, divergence d’appréciation et acceptation du risque.

5.7 - Communiquer aux organes de gouvernance (20 min)

Le conseil ou la direction a besoin d’une vision synthétique : exposition globale, risques critiques, décisions attendues, limites de mission et suivi.

Activité : Préparez une synthèse exécutive d’une page.
Critères : La synthèse doit permettre une décision sans masquer les incertitudes.

5.8 - Organiser le suivi (20 min)

Le suivi vérifie la mise en œuvre et l'efficacité, pas seulement la déclaration de clôture. Les risques acceptés doivent être formalisés par l'autorité compétente.

Activité : Définissez le protocole de suivi à 30, 60 et 90 jours.
Critères : Chaque clôture doit exiger une preuve et, si nécessaire, un retest.

5.9 - Atelier final : rapport complet (25 min)

Le rapport final consolide portée, méthodologie, opinion ou conclusion, constats, recommandations, réponse du management, plan d'action et limites.

Activité : Finalisez et présentez le rapport d'audit IA de l'entreprise fictive.
Critères : La grille d'évaluation exige cohérence entre inventaire, risques, preuves, constats et plan de remédiation.

Projet final

Livrez le cadrage, le registre, le programme de travail, les feuilles de test, la cotation, les constats, la synthèse exécutive, le rapport et le plan de suivi.

Plan de transfert à 30 jours

Jalon	Action
J+1	Adapter questionnaire, risques et programme
J+7	Inventaire pilote et validation du registre
J+15	Tests d'un système et contradictoire
J+30	Présentation à la gouvernance et suivi