Édition de lecture | 2026-11-20

Comment l’IA peut contribuer à la faillite d’une banque

Adrian Dunkley | 2026-11-18

Huit scénarios examinent la liquidité, la fraude, la concentration du crédit et les dépendances communes. L’étude relie des incidents documentés à des enchaînements possibles de pertes. Elle ne chiffre pas la probabilité de faillite.

Adrian Dunkley · 18 novembre 2026. Revue des éléments disponibles et scénarios de crise. Traduction du texte public repris dans l’édition imprimée du 20 novembre 2026.

Une banque suffisamment capitalisée peut manquer de liquidités

Une banque peut respecter ses exigences de fonds propres et épuiser ses liquidités. Un projet de rapport produit par IA et non vérifié peut retarder la réponse à un déficit de trésorerie. Un faux message du directeur général peut accélérer les retraits. Cette revue n’a trouvé aucune conclusion publique d’une autorité de surveillance qui désigne l’IA comme cause principale de la faillite d’une banque de dépôt agréée. Les incidents documentés servent à examiner comment l’IA peut amplifier les pertes ou fragiliser une banque déjà sous pression. [17, 22, 3] Le registre complémentaire recense 100 risques.

Les éléments disponibles au 18 novembre 2026

La revue porte sur des rapports de surveillance, des dossiers publics et des études sur le crédit et le travail de bureau disponibles à cette date. La liste américaine des faillites couvre uniquement les banques des États-Unis. [22]

Dans l’enquête de la Banque d’Angleterre et de la Financial Conduct Authority, des tiers fournissaient 39 % des systèmes d’IA déclarés en 2026, contre 33 % en 2024. Pour les systèmes jugés très importants, la part est passée de 35 % à 53 %. Il s’agit du Royaume-Uni. Les répondants et les méthodes de déclaration ont changé. Le dénominateur correspond aux cas d’usage déclarés en 2024 et aux systèmes déclarés en 2026. Ces chiffres mesurent l’exposition aux fournisseurs. Figure : ensemble des usages ou systèmes, 33 % en 2024 et 39 % en 2026. Usages ou systèmes de grande importance, 35 % en 2024 et 53 % en 2026. [1, 2]

Le Conseil de stabilité financière distingue quatre voies de propagation. Les banques peuvent dépendre des mêmes fournisseurs ou réagir aux mêmes signaux de marché. Les incidents informatiques et les erreurs de modèles peuvent aussi se répercuter entre établissements. En 2025, le Conseil a appelé à améliorer le suivi. Le FMI relève que l’IA pourrait accroître la liquidité des marchés en temps normal, facilitant les échanges entre acheteurs et vendeurs. En période de tension, des signaux similaires et des ordres plus rapides peuvent compliquer les échanges. [3, 4, 5]

Gains de travail et nouvelles erreurs

Une étude auprès de consultants a constaté de meilleures performances avec l’IA sur les tâches à la portée de l’outil. Sur une tâche qui dépassait ses capacités, les utilisateurs donnaient moins souvent la bonne réponse. Dans une autre enquête américaine, des employés de bureau ont décrit des résultats d’IA soignés en apparence qui obligeaient des collègues à reprendre le travail. Les auteurs parlent de « workslop ». Ces déclarations couvrent plusieurs secteurs et ne donnent aucun taux d’erreur bancaire. [13, 14]

Dans une banque, un projet peut paraître complet tout en utilisant la mauvaise période ou en omettant un solde important. Le responsable de la relecture doit rapprocher les montants significatifs du grand livre et vérifier la date de déclaration. Un spécialiste juridique, du crédit ou de la trésorerie doit contrôler les conclusions qui dépendent de règles ou d'un jugement expert.

Une étude américaine évaluée par les pairs sur les prêts hypothécaires a trouvé des écarts de prix entre emprunteurs au risque comparable. La comparaison des prêteurs fintech aux autres prêteurs variait selon le type de prêt. Les banques ont donc intérêt à tester les décisions par groupe d'emprunteurs. Ces résultats américains ne mesurent pas les performances pour les microentreprises jamaïcaines ou les bénéficiaires d'envois de fonds. [15]

Dans sa déclaration de novembre 2026, la Banque de Jamaïque signale des risques de fraude et de cyberincident liés à l'IA. Ses tests de résistance publiés ne chiffrent pas le risque de faillite bancaire associé à l'IA. [24]

Six incidents et la portée de la comparaison

Hong Kong, 2024. Usage documenté de l'IA. Une fausse visioconférence a conduit à des virements vers cinq comptes locaux. L'entreprise victime a perdu environ 200 millions de dollars de Hong Kong. [18]

Banco Popular Dominicano, 2025. Usurpation de l'identité d'une banque. Celle-ci a dénoncé une fausse vidéo de son directeur général faisant la promotion d'un placement frauduleux. Son avis ne chiffre pas les pertes des clients. [23]

Infrastructure de paiement jamaïcaine, 2026. La Banque de Jamaïque a signalé un cyberincident chez Jamaica Electronic Transfer Services Limited. MultiLink et la chambre de compensation automatisée sont restés en service. La déclaration n'attribue pas l'incident à l'IA. [25]

Knight Capital, 2012. Comparaison avec une erreur logicielle. Une erreur a généré des ordres que le courtier-négociant n'entendait pas transmettre. La SEC américaine a relevé une perte de plus de 460 millions USD. [19]

CrowdStrike, 2024. Comparaison entre fournisseurs communs. Une mise à jour logicielle de sécurité a perturbé les systèmes Windows concernés. La dépendance commune a étendu la portée de la panne. [21]

Silicon Valley Bank, 2023. Comparaison avec une faillite bancaire. Le 9 mars, les clients ont retiré plus de 40 milliards USD. La Réserve fédérale a relevé des défaillances de gestion et de supervision ainsi que des lacunes dans la gestion des risques de liquidité et de taux d'intérêt. [20]

Les deux premiers cas illustrent un usage frauduleux de l'IA. Les quatre autres montrent comment peut se propager une défaillance comparable.

Huit scénarios pour 2027–2029. Banque et méthode

La banque de référence est un établissement de dépôt caribéen de taille moyenne. Elle détient 2 milliards USD d'actifs et 1,6 milliard USD de dépôts. Elle peut mobiliser 260 millions USD d'actifs liquides le jour même. Ses fonds propres admissibles dépassent le minimum applicable de 60 millions USD. Ces soldes sont des hypothèses. Le coussin de fonds propres désigne la partie admissible au-delà du minimum.

La banque utilise des services d’IA de tiers dans certaines activités et peut exploiter un nombre limité de modèles localement. Le personnel et des règles fixes assurent encore de nombreuses décisions. Chaque scénario suppose l’exposition décrite dans son déclencheur. Les huit déclencheurs décrivent des événements possibles sur une année pour une banque, selon les conditions de déploiement ou du marché.

Pour chaque ligne, on multiplie la probabilité supposée du déclencheur par la probabilité supposée d’une conséquence grave s’il survient. Les deux bornes basses et les deux bornes hautes donnent une fourchette de sensibilité. La projection à trois ans répète le taux annuel bas ou haut et suppose une exposition équivalente et l’indépendance des années. Une panne prolongée, des fraudes répétées ou une faiblesse persistante invalident cette hypothèse.

Les sources éclairent le choix des scénarios et des contrôles. L’auteur a fixé les probabilités pour les besoins de l’exercice, sans les ajuster à des données d’incidents bancaires. Les conséquences diffèrent et peuvent se recouper. Additionner les lignes ne donne pas une probabilité de faillite.

Déclencheurs, probabilités et seuils de gravité

Chaque ligne donne successivement la probabilité du déclencheur en un an, celle de la conséquence grave si le déclencheur survient, puis celle de la conséquence grave en un an et en trois ans. Chaque ligne a son seuil. Les plages chiffrées conservent le point décimal du tableau original.

Un agent d’IA modifie les paiements. Voie directe. Un agent doté d’un droit d’écriture effectue une modification non autorisée dans le système de paiement. 2–6% · 5–20% · 0.10–1.20% · 0.30–3.56%. Seuil : interruption supérieure à quatre heures ou perte directe d’au moins 5 millions USD. [3, 10, 19]

Fraude au paiement par hypertrucage. Voie indirecte. Le personnel reçoit une usurpation crédible liée à un paiement important. 8–20% · 5–15% · 0.40–3.00% · 1.20–8.73%. Seuil : pertes frauduleuses non recouvrées d’au moins 5 millions USD. [18, 17]

Intrusion assistée par IA. Voie indirecte. Une compromission importante touche la banque ou un prestataire. Une enquête en attribue une partie à l’IA. 3–10% · 10–25% · 0.30–2.50% · 0.90–7.31%. Seuil : un service critique est indisponible pendant un jour ouvré. [6, 17, 10]

Panne d’un fournisseur d’IA commun. Voie indirecte. Un incident du fournisseur touche deux services bancaires critiques simultanément. 4–12% · 10–30% · 0.40–3.60% · 1.20–10.42%. Seuil : un service critique est indisponible pendant un jour ouvré. [21, 2, 4]

Rapport erroné et ruée sur les dépôts. Voie combinée. Une erreur importante dans un rapport de liquidité coïncide avec une crise publique de confiance. 1–4% · 5–20% · 0.05–0.80% · 0.15–2.38%. Seuil : les liquidités mobilisables dans la journée ne couvrent pas les obligations avant financement d’urgence. [20, 14, 9]

Chute des investissements en IA. Voie indirecte. Un repli du secteur frappe une banque dont les expositions de crédit ou de marché sont concentrées. 5–15% · 5–20% · 0.25–3.00% · 0.75–8.73%. Seuil : pertes supérieures au coussin de 60 millions USD. [8, 7]

Migration imposée vers un modèle local. Voie indirecte. Une obligation d’usage local touche un processus critique avant que la banque ait fini de tester la solution de secours. 2–8% · 10–30% · 0.20–2.40% · 0.60–7.03%. Seuil : un service critique est indisponible pendant un jour ouvré. [12, 11, 10]

Biais du crédit à grande échelle. Voie directe. Après son lancement, le modèle échoue au test de taux d’erreur de la banque pour un groupe d’emprunteurs. 8–20% · 5–15% · 0.40–3.00% · 1.20–8.73%. Seuil : une revue identifie au moins 1 000 décisions à réexaminer. [15, 9]

Lecture de la figure annuelle

Les barres présentent les estimations basses et hautes d’une conséquence grave en un an. Dans l’ordre de la figure : fournisseur commun 0,40–3,60 %, fraude par hypertrucage 0,40–3,00 %, chute des investissements 0,25–3,00 %, biais du crédit 0,40–3,00 %, intrusion 0,30–2,50 %, migration locale 0,20–2,40 %, agent de paiement 0,10–1,20 %, rapport erroné et ruée 0,05–0,80 %. Les seuils de gravité varient selon la ligne.

Une insuffisance de liquidités signifie que les disponibilités ne couvrent pas tous les paiements exigibles. Le non-respect du minimum de fonds propres survient lorsque les fonds admissibles passent sous le seuil applicable. Dans les deux cas, la banque ou le superviseur peut agir. Le superviseur décide d’intervenir ou de fermer l’établissement selon le droit local. Le modèle n’estime ni fermeture ni résolution.

Exemple chiffré. Rapport erroné et vague de retraits

Un rapport de trésorerie rédigé par IA omet un groupe important de déposants. La trésorerie utilise ce projet pour fixer sa réserve de la journée. Un faux message sur la santé de la banque circule tandis que des clients peinent à se connecter. L’équipe de crise reçoit pour consigne de traiter l’erreur et le message public comme un seul événement.

Dans l’exercice, 18 % des dépôts sortent en un jour, soit 288 millions USD. Les 260 millions USD disponibles le jour même laissent un déficit de 28 millions avant financement d’urgence. À 12 % de retraits, il reste 68 millions. Si la banque perd ce jour-là l’accès à 50 millions de garanties, les liquidités s’épuisent vers 13,1 % des dépôts. Un financement d’urgence peut changer ces résultats s’il arrive à temps.

Supposons qu’un rapport matinal exact permette à la trésorerie de mobiliser 30 millions USD de plus à temps. Avec les mêmes retraits de 288 millions, le déficit devient un excédent de 2 millions. La séquence va de l’omission de dépôts à la réserve réduite, puis de la fausse affirmation aux retraits accélérés et à l’insuffisance des liquidités. Valeurs de la figure, en millions USD : trésorerie initiale 260, retraits à 18 % 288, trésorerie avec les fonds supplémentaires 290.

Exemple chiffré. Perte sur les prêts aux infrastructures d’IA

Supposons 120 millions USD de prêts aux centres de données et projets connexes. Avant le choc, les emprunteurs tirent encore 40 millions sur des engagements. Une perte de 30 % de cet encours coûte 48 millions. Une autre perte de 15 millions sur des actifs négociés porte le total à 63 millions.

Le total dépasse de 3 millions USD le coussin de 60 millions avant effets fiscaux ou évolution des actifs pondérés par les risques. Sans perte sur les actifs négociés, une perte sur prêts de 37,5 % épuise le coussin. Ce calcul est un test de sensibilité simplifié. Les banques peuvent appliquer leurs règles actuelles de fonds propres et compter chaque exposition une seule fois. [8, 7]

Stratégie. Le contrôle local dépasse la question du serveur

La souveraineté en matière d'IA consiste à conserver la maîtrise de la destination des données et des personnes qui peuvent exploiter ou modifier un service. Une politique peut imposer le stockage local, le traitement local ou limiter le choix des fournisseurs. Les exigences opérationnelles diffèrent. Le passage obligatoire à un modèle local est ici un choc de politique hypothétique.

L'hébergement local peut renforcer la maîtrise des dossiers sensibles et des journaux d'accès, mais placer deux sites de reprise sur le même réseau électrique ou télécom. Un modèle hébergé localement peut dépendre d'un fournisseur étranger pour ses mises à jour ou la validation de licences. Les données d'apprentissage peuvent manquer pour certains crédits. Avant la migration, testez le service avec le personnel, les données et les produits locaux.

La Banque mondiale relève des lacunes dans la puissance de calcul, la connectivité, les données locales et les compétences. La banque peut mutualiser formation et tests avec des partenaires régionaux tout en gardant ses règles de décision. Pour un service critique, demandez à deux équipes désignées de démontrer leur capacité à l'exploiter et à le rétablir. Testez le secours en conditions d'ouragan ou en l'absence d'une personne clé. La consultation de juillet 2026 de la Banque de Jamaïque sur l'externalisation constitue une référence régionale pour la continuité et la surveillance. Vérifiez les règles locales en vigueur avant de signer. [12, 11, 26, 10]

Neuf décisions stratégiques. Améliorations, défaillances et mesures

Croissance et entrée sur le marché. Comparez les demandes des clients et les lacunes des agences. Des estimations erronées peuvent faire financer une offre sans demande suffisante. Mesurez demande payante en essai, usage répété et coût réel.

Crédit et tarification. Orientez les cas simples et repérez les pièces manquantes. Les revenus locaux peuvent conduire à de mauvaises décisions ou à des prix inégaux. Mesurez arriérés, écarts de prix et décisions révisées par produit et groupe.

Coûts et effectifs. Réduisez le temps de rédaction et de tri des dossiers. Les reprises peuvent augmenter ou les réviseurs expérimentés partir. Mesurez le délai jusqu'à l'approbation, le coût des corrections et les effectifs de contrôle par poste.

Trésorerie et capital. Comparez les prévisions de liquidités et signalez les besoins de financement. Un modèle commun peut manquer un mouvement de taux ou un rapport omettre un solde élevé. Mesurez erreur de prévision, marge disponible le jour même et pertes sous choc commun.

Service client. Répondez aux questions courantes en plusieurs langues. Un outil peut donner une mauvaise échéance ou empêcher le contact avec un humain. Mesurez litiges hors délai, appels répétés et erreurs par langue.

Fraude et cyberdéfense. Regroupez les alertes et rapprochez les dossiers. Masquer des alertes faibles peut laisser passer une fraude. Un agent trop privilégié peut exposer des données. Mesurez pertes non détectées, délai de réponse et actes dépassant les autorisations.

Partenariats et externalisation. Achetez un service long à développer. Plusieurs fournisseurs peuvent partager le même hébergeur ou la même équipe. Mesurez le délai de reprise sur un service indépendant et le coût de sortie.

Crédits aux infrastructures. Financez des projets à locataires confirmés et contrats durables. Plusieurs prêts peuvent dépendre d'un acheteur, d'un réseau ou d'une technologie. Une nouvelle IA peut réduire la demande d'équipements existants. Mesurez l'exposition par locataire commun, les tirages et la valeur recouvrable sous tension.

Politique des données et capacité locale. Gardez la maîtrise des dossiers et testez les produits locaux. Une échéance peut imposer un service faible avec un secours partageant le même point de panne. Mesurez les taux de réussite par produit et pays, le rétablissement indépendant et les effectifs formés par poste.

Demandes que peut formuler le conseil d'administration

Utilisez le registre pour désigner des responsables et choisir les tests. Commencez par les fournisseurs communs, les services qui déplacent des fonds et les rapports fixant la trésorerie ou les fonds propres. Chaque équipe doit savoir qui peut arrêter l'IA et quel service prend le relais.

Faites répéter à la trésorerie une ruée alors que la banque mobile est indisponible. Demandez aux paiements de démontrer qu'un virement urgent exige toujours deux personnes autorisées. Demandez au crédit de comparer ses décisions entre groupes d'emprunteurs. Consignez les tests échoués et la date du prochain exercice. [10, 4, 9]

Remplacez les hypothèses par les données internes. Conservez le nombre de dossiers examinés, le nombre d'erreurs ayant passé les contrôles et le coût de reprise. Consignez les incidents évités de peu impliquant une panne ou un fournisseur partagé. Mesurez le temps de propagation des dommages aux équipes, aux clients et aux autres banques. Réestimez après toute modification du volume, de l'autonomie, du fournisseur ou du contrôle. Conservez l'estimation précédente et sa date.

L'auteur

Adrian Dunkley est spécialiste de l'IA, dirigeant bancaire expérimenté et investisseur.

Références

[1] Bank of England and Financial Conduct Authority (2024). Artificial intelligence in UK financial services.

[2] Bank of England and Financial Conduct Authority (2026). Artificial intelligence in UK financial services.

[3] Financial Stability Board (2024). The financial stability implications of artificial intelligence.

[4] Financial Stability Board (2025). Monitoring adoption of artificial intelligence and related vulnerabilities in the financial sector.

[5] International Monetary Fund (2024). Global Financial Stability Report, October, chapter 3. AI in capital markets.

[6] International Monetary Fund (2024). Global Financial Stability Report, April, chapter 3. Cyber risk and financial stability.

[7] International Monetary Fund (2026). Global Financial Stability Report, October.

[8] Bank of England (2026). Financial Stability Report, July.

[9] Federal Reserve, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation (2026). Revised guidance on model risk management.

[10] Basel Committee on Banking Supervision. Consolidated banking guidelines on operational resilience.

[11] Bank of Jamaica (2026). Consultation draft on outsourcing and third-party risk management.

[12] World Bank (2025). Digital Progress and Trends Report. Strengthening AI Foundations.

[13] Dell’Acqua et al. (2023). Navigating the Jagged Technological Frontier. Working paper.

[14] BetterUp Labs and Stanford Social Media Lab (2025). US desk-worker survey on workslop.

[15] Bartlett, Morse, Stanton and Wallace (2022). Consumer-lending discrimination in the FinTech Era. Journal of Financial Economics.

[16] Consumer Financial Protection Bureau (2023). Chatbots in consumer finance.

[17] Financial Crimes Enforcement Network (2024). Alert on deepfake fraud targeting financial institutions.

[18] Hong Kong Government (2024). Legislative Council reply on fraud involving deepfakes.

[19] US Securities and Exchange Commission (2013). Administrative order concerning Knight Capital Americas.

[20] Federal Reserve (2023). Review of the Federal Reserve’s supervision and regulation of Silicon Valley Bank.

[21] CrowdStrike (2024). Form 8-K on the 19 July update and outages.

[22] Federal Deposit Insurance Corporation. Failed bank list for the United States.

[23] Banco Popular Dominicano (2025). Notice on a fake video of its chief executive.

[24] Bank of Jamaica (2026). Financial Policy Committee statement, November.

[25] Bank of Jamaica (2026). Statement on the cyber incident at JETS Limited.

[26] UNESCO. Caribbean Artificial Intelligence Policy Roadmap.

CAIA · 100 risks

CAIA · How AI can contribute to bank failure

Édition en anglais (PDF)