Édition de lecture | 2026-11-20

IA pratique pour les services financiers — Technologies de l’information

Harbour Think Tank, Caribbean AI Association, under the leadership of Adrian Dunkley | 2026-11-11

Édition de lecture abrégée du document préparé par le Harbour Think Tank de la Caribbean AI Association sous la direction d’Adrian Dunkley. Elle reprend la révision du 11 novembre 2026, les dix propositions et les limites d’intervention.

Édition de lecture abrégée du document préparé par le Harbour Think Tank de la Caribbean AI Association sous la direction d’Adrian Dunkley. Elle reprend la révision du 11 novembre 2026, les dix propositions et les limites d’intervention.

Qui décide

Les équipes d’exploitation et responsables d’applications documentent demandes et modifications avant toute intervention sur les systèmes bancaires en production. Les ingénieurs gardent la décision sur versions, accès et reprise.

Dix usages et leurs contrôles

01. Tickets d’assistance. Proposer une orientation à partir du ticket. Un analyste vérifie l’urgence et escalade les cas incertains. Niveau 1.

02. Questions d’exploitation. Retrouver les consignes avec lien et version en vigueur. Sans source autorisée et valide, transmettre la question au responsable. Niveau 0.

03. Changements de code. Repérer les lignes à vérifier et documenter le comportement attendu. L’ingénieur examine les constats et autorise toute modification. Niveau 1.

04. Tests de règles métier. Proposer cas usuels, limites et échecs attendus. Le responsable fixe le résultat attendu avant les essais contrôlés. Niveau 0.

05. Effets d’une modification. Relier le changement prévu aux services et dépendances. Les responsables vérifient la portée et les conditions de retour arrière. Niveau 1.

06. Documentation d’exploitation. Proposer des corrections à partir d’une version acceptée. Le responsable révise les modifications et conserve l’historique. Niveau 1.

07. Interfaces avant automatisation. Relier champs et systèmes et signaler les liens incertains. Les responsables des connexions vérifient compatibilité et autorisations. Niveau 0.

08. Dossiers d’accès. Comparer les autorisations existantes aux exigences du rôle et signaler les écarts. Seul le responsable autorisé modifie les droits. Niveau 0.

09. Demande de service. Comparer volumes et mesures agrégées sur des périodes équivalentes. L’analyste vérifie les causes avant de demander des capacités supplémentaires. Niveau 1.

10. Manuel de reprise. Relever étapes manquantes, prérequis et décisions sans responsable. Le responsable de continuité les teste dans un exercice autorisé. Niveau 0.

Préparer et valider un essai

Au niveau 0, l’assistant répond à une demande et une personne exécute chaque étape. Au niveau 1, il rassemble les éléments autorisés et prépare un brouillon. Il ne transmet aucun message et ne modifie aucun système. Consigner source, version de la consigne, autorisations, réviseur et critère d’arrêt.

Limiter la recherche à une collection approuvée avec versions et échéances. Tester une question documentée, une sans réponse, une couverte par un article périmé et une demandant un accès restreint. Consigner défauts manqués, suggestions nuisibles et reprises. Suspendre à la première action en production non autorisée.

Mesure et limites

Comparer des tâches équivalentes au processus courant. Consigner taille d’échantillon, temps de préparation, vérification et correction, défaillances importantes, autorisations et atteintes à la confidentialité. Inclure licence, intégration, formation, supervision et coût par exécution selon le cas. Les scores servent à choisir des essais. Le document ne rapporte aucun rendement mesuré dans un établissement. Le texte intégral présente consigne initiale, outils possibles, compétences et méthode pour chaque cas.

Références

[1] International Telecommunication Union. Global Cybersecurity Index 2024. Americas tier table, printed page 27. Jamaica appears in Tier 3, Establishing. National commitments, not firm-level operational performance.

[2] Office of the Information Commissioner, Jamaica. Data Protection Standards. Official guidance, inspected 26 October 2026; relevant sections cover purpose, minimisation, security and transfers.

[3] National Institute of Standards and Technology. Secure Software Development Framework version 1.1, Special Publication 800-218. February 2022.

[4] National Institute of Standards and Technology. Cybersecurity Framework 2.0. Official framework resource page, inspected 26 October 2026.

[5] Agent Skills. Agent Skills Overview. Accessed 10 November 2026.

Cette édition abrégée accompagne le texte intégral en anglais.

Édition en anglais (PDF)