Édition de lecture | 2026-11-20

Gestion des risques PHP dans les institutions financières

Adrian Dunkley | 2026-10-23

Le guide d’octobre 2026 demande de recenser les services dépendant de PHP, leurs responsables et les prestataires concernés. Le responsable conserve la version observée, la date, la portée de la modification et les éléments transmis par le fournisseur.

Traduction intégrale de l’édition destinée aux responsables de la surveillance et de la continuité, 20 novembre 2026. Adrian Dunkley, StarApple AI et Conseil caribéen de gestion des risques liés à l’IA. D’après la version 1.8 du 23 octobre 2026.

Recenser les services qui dépendent de PHP

Nommez un responsable métier et un responsable technique pour chaque service à la clientèle concerné. Incluez les applications gérées par des fournisseurs et les environnements de secours. Consignez la version installée, la date du constat, l’environnement et la personne responsable du constat. Un système peut dépendre d’un logiciel que l’établissement ne gère pas directement. Demandez au fournisseur des preuves portant sur le service réellement utilisé.

Distinguer exposition, interruption et compromission

Une faiblesse demande une évaluation. Un avis public ne prouve pas qu’une institution particulière a perdu des données ou subi un accès non autorisé. Un service peut aussi être interrompu lorsqu’un opérateur le suspend par précaution. Consignez séparément les faits observés, les questions en suspens et la prochaine vérification.

Vérifier le rétablissement au moyen d’un parcours client

Suivez la procédure de changement de l’établissement pour tester le correctif, confirmer qu’il est actif et consigner le résultat. Incluez une opération courante qu’un client peut mener à terme, des preuves tirées du service en fonctionnement et un contrôle de l’environnement de secours. Un ticket de changement approuvé ne suffit pas à démontrer que le service réparé fonctionne correctement.

Suivre la continuité et le risque résiduel

Consignez les interruptions, la solution de remplacement pour les clients et la personne responsable du rétablissement. Utilisez l’échelle de risque locale approuvée et demandez au responsable d’examiner l’exposition restante. Conservez les preuves ayant servi aux décisions, aux communications et à la clôture.

Portée de cette édition

Cette édition reprend les orientations de gestion. Le document original contient des annexes techniques, des fiches de travail et une mise à jour historique d’un avis. Cette édition n’évalue aucun établissement particulier. Vérifiez les informations actuelles du fournisseur avant toute décision technique. Le Conseil fait partie de l’Association caribéenne de l’IA.

Références

NIST Cybersecurity Framework

Édition en anglais (PDF)