

Management des risques de cybersécurité dans le secteur financier africain (mobile money, fintech, néo-banques)

Lien : https://maroc-performance.com/formation/management-des-risques-de-cybersecurite-dans-le-secteur-financier-africain-mobile-money-fintech-neo-banques

DURÉE
8 jours (56h)

RÉFÉRENCE
MRL293

CATÉGORIE
Management des Risques Sectoriels et Grands Projets

Maroc Performance

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principaux risques et menaces cyber affectant le secteur financier africain.
- Construire une cartographie complète des risques de cybersécurité et des actifs critiques.
- Identifier les vulnérabilités spécifiques aux banques digitales, fintechs, Mobile Money et néo-banques.
- Renforcer la sécurité des plateformes de paiement, applications mobiles, API et infrastructures Cloud.
- Maîtriser les dispositifs IAM, authentification forte et contrôle des accès.
- Mettre en place des capacités efficaces de détection, Security Monitoring et Threat Intelligence.
- Structurer un dispositif d’Incident Response, de gestion de crise et de résilience opérationnelle.
- Maîtriser les risques cyber liés aux fournisseurs, partenaires technologiques et écosystèmes financiers.
- Renforcer la gouvernance, la protection des données et la conformité en matière de cybersécurité.
- Quantifier et piloter financièrement l’exposition au cyberrisque à travers des KPI, KRI et scénarios de pertes.
- Intégrer les risques cyber dans le dispositif global de Risk Management et de gouvernance de l’institution.
- Élaborer une stratégie et une feuille de route de cybersécurité adaptées aux nouveaux modèles financiers digitaux africains.

Maroc Performance

👥 POUR QUI ?

- Chief Information Security Officers (CISO) et responsables cybersécurité des institutions financières.
- Chief Risk Officers (CRO), responsables Risk Management et gestionnaires des risques opérationnels.
- Directeurs IT, CIO, CTO et responsables des infrastructures technologiques.
- Responsables sécurité des systèmes d’information, SOC et Cyber Threat Intelligence.
- Responsables Mobile Money, paiements digitaux et plateformes financières.
- Dirigeants et responsables de fintechs, néo-banques et banques digitales.
- Responsables fraude, LCB-FT, conformité et contrôle interne.
- Responsables Data, Cloud, API et architectures digitales.
- Auditeurs internes, consultants et professionnels de la gouvernance des risques technologiques.
- Responsables résilience opérationnelle, continuité d’activité et gestion de crise.
- Responsables Risk & Compliance des opérateurs télécoms et écosystèmes Mobile Money.
- Cadres dirigeants souhaitant renforcer la résilience cyber et la sécurité des services financiers numériques en Afrique.

Maroc Performance



Programme détaillé

1 / Fondamentaux des risques cyber dans le secteur financier africain

- Comprendre les spécificités des cyberrisques affectant banques, fintechs, opérateurs Mobile Money et néo-banques.
- Identifier les principales menaces pesant sur les infrastructures, données, applications et services financiers digitaux.
- Évaluer les impacts financiers, opérationnels, réglementaires et réputationnels des cyberattaques.

2 / Cartographie et évaluation des risques de cybersécurité

- Construire une cartographie des actifs, processus critiques, menaces et vulnérabilités.
- Évaluer la probabilité, l'impact et la criticité des scénarios de risque cyber.
- Définir les priorités de traitement selon l'exposition et l'appétit au risque de l'institution.

3 / Menaces cyber et typologies d'attaques financières

- Identifier les attaques par phishing, malware, ransomware, ingénierie sociale et compromission de comptes.
- Analyser les risques liés aux API, applications mobiles, plateformes de paiement et infrastructures Cloud.
- Comprendre les mécanismes de fraude numérique, Account Takeover et attaques ciblant les transactions financières.

4 / Cybersécurité du Mobile Money et des paiements digitaux

- Identifier les vulnérabilités propres aux plateformes Mobile Money et aux réseaux d'agents.
- Sécuriser les transactions, comptes clients, wallets, interfaces USSD, applications et API.
- Mettre en place des contrôles contre la fraude, le SIM Swap, le vol d'identifiants et les transactions non autorisées.

Maroc Performance

5 / Cybersécurité des fintechs et néo-banques

- Évaluer les risques liés aux architectures digitales, Cloud, microservices et API ouvertes.
- Sécuriser les parcours d'onboarding, d'authentification, de paiement et de gestion des comptes.
- Intégrer la cybersécurité dès la conception des produits et services financiers numériques.

6 / Gestion des identités, accès et authentification

- Mettre en place des dispositifs robustes d'Identity and Access Management (IAM).
- Renforcer l'authentification multifacteur, la gestion des privilèges et le contrôle des accès.
- Prévenir les compromissions de comptes, usurpations d'identité et accès internes non autorisés.

7 / Détection des incidents, SOC et Threat Intelligence

- Mettre en place des mécanismes de Security Monitoring adaptés aux institutions financières.
- Exploiter la Cyber Threat Intelligence pour anticiper les menaces et enrichir les capacités de détection.
- Définir des scénarios de détection et indicateurs permettant d'identifier rapidement les incidents.

8 / Incident Response, gestion de crise et résilience opérationnelle

- Structurer un dispositif de réponse aux incidents cyber et définir les rôles des équipes.
- Élaborer des plans de gestion de crise, continuité d'activité et reprise après incident.
- Organiser des simulations et exercices permettant de tester la résilience des infrastructures financières.

9 / Risques liés aux tiers, fournisseurs et écosystèmes fintech

- Identifier les risques cyber liés aux prestataires Cloud, processeurs de paiement, agrégateurs et partenaires technologiques.
- Mettre en place des processus de due diligence, contractualisation et surveillance des fournisseurs critiques.
- Intégrer les risques de Supply Chain Cyber dans le dispositif global de gestion des risques.

Maroc Performance

10 / Protection des données, conformité et gouvernance cyber

- Identifier les risques liés aux données personnelles, financières et transactionnelles.
- Mettre en place des politiques de sécurité, contrôle interne, conformité et gouvernance des données.
- Aligner le dispositif cyber sur les exigences réglementaires et les bonnes pratiques internationales applicables.

11 / Cyber Risk Quantification, assurance et pilotage financier du risque

- Quantifier les pertes potentielles liées aux scénarios de cyberattaque.
- Définir des KPI, KRI, seuils d’alerte et tableaux de bord pour piloter le cyberrisque.
- Évaluer les stratégies de réduction, transfert et couverture financière des risques cyber.

12 / Stratégie de cybersécurité et Cyber Risk Management intégré

- Construire un dispositif global de Cyber Risk Management adapté aux institutions financières africaines.
- Intégrer cybersécurité, fraude, risque opérationnel, résilience et gouvernance dans une approche cohérente.
- Élaborer une feuille de route permettant de renforcer durablement la sécurité des banques digitales, fintechs, Mobile Money et néo-banques.

Maroc Performance

⚗ Approche pédagogique

- ✔ Support Ecrit et Projection
- ✔ Exposés Interactifs, Podcasts et Vidéos
- ✔ Brainstorming et Jeux de Rôle
- ✔ Mises en Situation pour faciliter l'assimilation
- ✔ Cas Pratiques et Labs inclus pour leur impact opérationnel
- ✔ Test de Validation des Acquis des Connaissances

Prochaines dates programmées

18 au 27 Jan. 2027	Présentiel - Casablanca
15 au 24 Mars 2027	Présentiel - Casablanca
10 au 19 Mai 2027	Présentiel - Casablanca
05 au 14 Juil. 2027	Présentiel - Casablanca
30 Août au 08 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@maroc-performance.com
Web : https//www.maroc-performance.com

Document généré le 18/11/2026 — Réf : MRL293
Maroc Performance — Tous droits réservés

Maroc Performance