

Audit IT et cybersécurité pour institutions financières

Lien :
https://maroc-performance.com/formation/audit-it-et-cybersecurite-pour-institutions-financieres

DURÉE
5 jours (35h)

RÉFÉRENCE
FA165

CATÉGORIE
Contrôle Interne Bancaire et Conformité

Maroc Performance

🎯 OBJECTIFS DE LA FORMATION

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

- Maîtriser les principes, méthodes et techniques de l’audit des systèmes d’information des institutions financières.
- Identifier et évaluer les principaux risques informatiques, technologiques et cyber.
- Savoir construire une cartographie des risques IT et apprécier l’efficacité des dispositifs de contrôle.
- Maîtriser les principes de gouvernance IT, de contrôle interne et de gestion des accès.
- Être capable d’auditer les dispositifs de cybersécurité des infrastructures, applications et réseaux financiers.
- Savoir évaluer la sécurité des données, API, applications digitales et systèmes de paiement.
- Maîtriser l’audit des environnements cloud et la gestion des risques liés aux prestataires technologiques.
- Évaluer la continuité d’activité, la résilience informatique et la capacité de réponse aux incidents cyber.
- Savoir conduire une mission complète d’audit IT, documenter les constats et construire des plans de remédiation.
- Être capable de produire un reporting stratégique permettant à la Direction et aux organes de gouvernance de piloter les risques IT et cybersécurité.

👥 POUR QUI ?

- Directeurs des systèmes d’information (DSI), CIO et responsables IT des institutions financières.
- Chief Information Security Officers (CISO) et responsables cybersécurité.
- Auditeurs IT, responsables audit informatique et spécialistes de l’audit des systèmes d’information.
- Auditeurs internes, responsables contrôle interne et responsables conformité.
- Risk Managers spécialisés en risques IT, cyber, opérationnels et technologiques.
- Responsables infrastructure, réseaux, cloud, applications et architecture des systèmes d’information.
- Responsables sécurité des données, IAM, SOC, gestion des vulnérabilités et réponse aux incidents.
- Responsables paiements, digital banking, API et plateformes technologiques financières.
- Responsables continuité d’activité, résilience opérationnelle et plans de reprise informatique.
- Responsables gestion des fournisseurs IT, externalisation, fintechs et Third-Party Risk Management.
- Consultants, experts en cybersécurité, auditeurs externes et professionnels du conseil en risques technologiques.
- Dirigeants, membres des Comités d’Audit et des Comités des Risques de banques, compagnies d’assurance, fintechs et autres institutions financières.

Maroc Performance



Programme détaillé

1 / Fondamentaux de l’audit IT dans les institutions financières

- Comprendre les objectifs, principes et méthodologies de l’audit des systèmes d’information financiers.
- Identifier les principaux risques IT affectant les banques, assurances, fintechs et institutions financières.
- Évaluer la gouvernance, l’organisation et le niveau de maturité du dispositif de contrôle informatique.

2 / Gouvernance IT et cadre de contrôle interne

- Évaluer la gouvernance des systèmes d’information et l’alignement de l’IT avec la stratégie de l’institution.
- Maîtriser les principes de séparation des fonctions, gestion des responsabilités et contrôle des accès.
- Identifier les faiblesses de contrôle interne susceptibles d’affecter la sécurité, l’intégrité et la disponibilité des données.

3 / Gestion des risques IT et cartographie des risques

- Identifier et évaluer les risques liés aux infrastructures, applications, réseaux, données et prestataires IT.
- Construire une cartographie des risques IT intégrant probabilité, impact, criticité et dispositifs de maîtrise.
- Définir des plans de traitement, indicateurs de risque et mécanismes de suivi des risques technologiques.

4 / Cybersécurité et protection des infrastructures financières

- Identifier les principales menaces cyber : phishing, ransomware, malware, attaques DDoS, compromission d’identifiants et fraude.

Maroc Performance

- Évaluer les dispositifs de protection des réseaux, serveurs, endpoints, applications et infrastructures cloud.
- Contrôler l’efficacité des mesures de détection, prévention, réponse et remédiation face aux incidents cyber.

5 / Gestion des identités, accès et privilèges

- Auditer les mécanismes d’authentification, autorisation et gestion du cycle de vie des utilisateurs.
- Évaluer les accès privilégiés, comptes administrateurs, séparation des tâches et mécanismes MFA.
- Identifier les accès excessifs, orphelins ou incompatibles avec les responsabilités des collaborateurs.

6 / Sécurité des données, applications et paiements

- Évaluer les dispositifs de protection des données sensibles, financières et personnelles.
- Auditer la sécurité des applications bancaires, plateformes digitales, API et systèmes de paiement.
- Vérifier les mécanismes de chiffrement, journalisation, traçabilité, intégrité et prévention des fuites de données.

7 / Audit du cloud, des infrastructures et des tiers IT

- Évaluer les risques liés à l’externalisation, au cloud computing et aux services technologiques critiques.
- Auditer les contrôles de sécurité des fournisseurs, fintechs, prestataires cloud et sous-traitants informatiques.
- Mettre en place une approche de Third-Party Risk Management intégrant due diligence, contractualisation et surveillance continue.

8 / Continuité d’activité, résilience et gestion des incidents

- Évaluer les plans de continuité informatique, plans de reprise d’activité et dispositifs de résilience opérationnelle.
- Tester les capacités de sauvegarde, restauration, redondance et reprise des systèmes critiques.
- Auditer les processus de détection, qualification, escalade, réponse et retour d’expérience après incident cyber.

9 / Méthodologie, techniques et outils d’audit IT

Maroc Performance

- Maîtriser les différentes étapes d’une mission d’audit IT : planification, collecte des preuves, tests, analyse et restitution.
- Utiliser les techniques d’échantillonnage, analyse des logs, tests de contrôles, data analytics et revues de configuration.
- Formaliser les constats, niveaux de criticité, recommandations et plans de remédiation de manière auditable.

10 / Reporting, conformité et pilotage de la cybersécurité

- Évaluer la conformité des dispositifs IT aux exigences réglementaires, prudentielles et aux référentiels de cybersécurité applicables.
- Construire des tableaux de bord permettant de suivre les vulnérabilités, incidents, contrôles et plans d’action.
- Produire des rapports d’audit exploitables par la Direction Générale, le Comité d’Audit, le Comité des Risques et les fonctions de supervision.

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

23 au 27 Nov. 2026	Présentiel - Casablanca
22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca

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

Maroc Performance

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 : FA165
Maroc Performance — Tous droits réservés

Maroc Performance