

Résilience opérationnelle et BCPDRP pour institutions financières

Lien : https://maroc-performance.com/formation/resilience-operationnelle-et-bcpdrp-pour-institutions-financieres

DURÉE
5 jours (35h)

RÉFÉRENCE
FA176

CATÉGORIE
Gestion des Risques et Gestion Actif/Passif

Maroc Performance

OBJECTIFS DE LA FORMATION

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

- Maîtriser les principes fondamentaux de la résilience opérationnelle dans les institutions financières.
- Comprendre et distinguer BCP, DRP, gestion de crise et Disaster Recovery.
- Réaliser une Business Impact Analysis complète des activités critiques.
- Définir les RTO, RPO et niveaux de tolérance aux interruptions.
- Concevoir et déployer un Business Continuity Plan adapté aux activités financières.
- Construire un Disaster Recovery Plan couvrant les systèmes et infrastructures critiques.
- Intégrer les risques cyber, technologiques, Cloud et liés aux prestataires critiques.
- Mettre en place une organisation efficace de gestion des incidents et des crises majeures.
- Concevoir des tests, exercices et simulations permettant de mesurer la capacité réelle de reprise.
- Piloter un dispositif intégré de résilience opérationnelle conforme aux exigences de gouvernance, de risque et de supervision.

👥 POUR QUI ?

- Directeurs des risques, Chief Risk Officers et responsables Enterprise Risk Management.
- Responsables Business Continuity Management, BCP et Operational Resilience.
- Directeurs des systèmes d’information, CIO, CTO et responsables infrastructures IT.
- Responsables cybersécurité, sécurité des systèmes d’information et gestion des incidents.
- Responsables Disaster Recovery, IT Service Continuity et infrastructure.
- Responsables risques opérationnels, contrôle interne et conformité.
- Responsables métiers des banques, assurances, sociétés de financement et institutions financières.
- Auditeurs internes, auditeurs IT et responsables de la qualité et du contrôle des dispositifs de résilience.
- Responsables fournisseurs, outsourcing, Cloud et gestion des risques liés aux tiers.
- Dirigeants, responsables de crise et cadres impliqués dans la gouvernance et le pilotage de la résilience opérationnelle.

Maroc Performance



Programme détaillé

1 / FONDAMENTAUX DE LA RÉSILIENCE OPÉRATIONNELLE FINANCIÈRE

- Comprendre les principes, objectifs et composantes de la résilience opérationnelle appliquée aux banques, assurances et institutions financières.
- Distinguer continuité d'activité, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), gestion de crise et résilience opérationnelle.
- Identifier les exigences prudentielles et les bonnes pratiques internationales applicables à la résilience des institutions financières.

2 / GOUVERNANCE ET CADRE DE MANAGEMENT DE LA RÉSILIENCE

- Définir les responsabilités du Conseil, de la Direction Générale, des fonctions risques, IT, sécurité et métiers.
- Mettre en place une gouvernance intégrée permettant de piloter les risques de continuité et de résilience.
- Définir les politiques, procédures, comités, indicateurs et mécanismes d'escalade nécessaires.

3 / BUSINESS IMPACT ANALYSIS (BIA) ET CARTOGRAPHIE DES RISQUES

- Réaliser une Business Impact Analysis permettant d'identifier les processus, activités et services critiques.
- Évaluer les impacts financiers, réglementaires, opérationnels, réputationnels et clients liés aux interruptions.
- Déterminer les Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) et niveaux de tolérance aux interruptions.

4 / BUSINESS CONTINUITY PLAN (BCP)

- Concevoir un Business Continuity Plan couvrant les processus critiques et les scénarios d'interruption majeurs.
- Définir les stratégies de continuité : solutions de secours, redondance, sites alternatifs, procédures manuelles et ressources de remplacement.

Maroc Performance

- Organiser les plans de continuité par métiers, fonctions critiques, filiales et entités du groupe.

5 / DISASTER RECOVERY PLAN (DRP) ET RÉSILIENCE IT

- Concevoir un Disaster Recovery Plan permettant la restauration rapide des systèmes et infrastructures critiques.
- Définir les architectures de sauvegarde, réplication, haute disponibilité, sites de reprise et solutions de restauration.
- Tester les capacités de récupération des applications, bases de données, réseaux et infrastructures technologiques.

6 / CYBERSÉCURITÉ, DONNÉES ET RISQUES TECHNOLOGIQUES

- Intégrer les cyberattaques, ransomware, compromissions de données et indisponibilités IT dans les scénarios de résilience.
- Mettre en place des mécanismes de sauvegarde, restauration, segmentation et protection des données critiques.
- Articuler cybersécurité, continuité d'activité, Disaster Recovery et gestion des incidents technologiques.

7 / GESTION DE CRISE ET INCIDENTS MAJEURS

- Définir une organisation de crise permettant une prise de décision rapide lors d'événements majeurs.
- Élaborer les procédures d'alerte, d'escalade, de communication et de coordination avec les parties prenantes.
- Organiser la communication de crise avec les collaborateurs, clients, autorités, fournisseurs et partenaires stratégiques.

8 / TIERS CRITIQUES, CLOUD ET SOUS-TRAITANCE

- Identifier et évaluer les prestataires, fournisseurs et partenaires dont la défaillance pourrait compromettre la continuité des services.
- Intégrer les risques liés au Cloud, aux FinTechs, aux fournisseurs IT et aux services externalisés dans le dispositif de résilience.
- Définir les exigences contractuelles, SLA, plans de secours et mécanismes de réversibilité applicables aux tiers critiques.

9 / TESTS, EXERCICES ET AMÉLIORATION DES PLANS

Maroc Performance

- Concevoir et exécuter des tests BCP/DRP : simulations de crise, tests de bascule, restauration, cyber-résilience et exercices de crise.
- Mesurer les performances de récupération par rapport aux RTO, RPO et niveaux de service définis.
- Identifier les écarts, formaliser les plans d'actions et améliorer continuellement les dispositifs de résilience.

10 / PILOTAGE DE LA RÉSILIENCE ET CONFORMITÉ PRUDENTIELLE

- Mettre en place des indicateurs de résilience, tableaux de bord, reporting et mécanismes de surveillance continue.
- Intégrer la résilience opérationnelle dans le Risk Management, l'audit interne, le contrôle interne et le dispositif de gouvernance.
- Élaborer une feuille de route permettant d'assurer la conformité, la robustesse opérationnelle et la capacité de reprise de l'institution.

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

04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca
16 au 20 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

Maroc Performance — Tous droits réservés

Maroc Performance