ASH INSTITUTE

Building Skills

coaching & training

PCA : PILIER STRATÉGIQUE DE GESTION DES RISQUES

Cas Pratique : PRA de l'environnement Swift des banques en Tunisie"

Lieu

Hôtel Novotel,
Avenue Mohamed V, Tunis

Coût

Le prix par participant
est fixé à **2.290 Dinars** Hors Taxes.

Dates

2 , 3 et 4 décembre 2026

Pièces Jointes :

Planning et programme du workshop

Bulletin d'inscription (retour par e-mail)

FORMATEUR : Jalel ZAGRANI

Ex directeur général de Système d'informations à la Banque Centrale de Tunisie

Intérêt de la formation

La continuité d'activité est devenue une composante essentielle de la maîtrise du risque opérationnel. Une panne informatique, une cyberattaque, l'indisponibilité d'un site, la défaillance d'un prestataire critique, une rupture de télécommunication ou une indisponibilité de ressources clés peuvent interrompre des services financiers essentiels et produire des effets en chaîne sur les clients, les partenaires et les infrastructures de place.

Dans le contexte tunisien, la continuité et la résilience sont directement liées aux attentes de gouvernance et de gestion des risques de la Banque Centrale de Tunisie. La circulaire BCT n°2024-05, applicable aux gestionnaires des systèmes de paiement et de règlement-livraison de titres, formalise notamment des exigences précises en matière de PCA, d'objectifs de reprise, de durée maximale d'interruption admissible, de site secondaire, de communication et de tests.

La formation permettra d'aborder la continuité d'activité avec une approche méthodologique et organisationnelle mais sera également appuyée par un cas pratique concret, directement lié aux problématiques opérationnelles et techniques rencontrées par les établissements bancaires tunisiennes. A cet effet elle sera couronnée par la mise en œuvre d'un PRA 'Plan de Reprise d'Activité' de l'environnement Swift des banques en Tunisie.

Objectifs de la formation

Au terme de ce workshop les participants devraient être en mesure de :

- Positionner le PCA dans le dispositif global de gestion des risques et de gouvernance d'un établissement financier
- **Comprendre les attentes du cadre tunisien en matière de continuité, de risque opérationnel, de cybersécurité et de résilience des services critiques**
- **Réaliser un Business Impact Analysis (BIA) et identifier les activités, ressources, systèmes et prestataires critiques**
- **Définir de manière cohérente la DMIA/MTPD, le RTO et le RPO selon la criticité des activités**

- Construire des stratégies de continuité adaptées : site de secours, télétravail de crise, redondance, solutions de repli et procédures manuelles
- Articuler PCA, PRA informatique, gestion de crise, cybersécurité et gestion des prestataires externes
- Élaborer un programme de tests réaliste et exploiter les résultats pour améliorer le dispositif
- Mettre en place des indicateurs et un reporting permettant aux organes de gouvernance de piloter la résilience opérationnelle

Public cible

Cette formation s'adresse à un public large. Elle concerne notamment :

- Responsables gestion des risques, risque opérationnel, continuité d'activité
- Sécurité des systèmes d'information, DSI,
- Conformité, contrôle interne, audit interne, opérations, moyens de paiement
- Trésorerie, organisation
- Responsables de sites et managers impliqués dans la gestion de crise ou la résilience

Lieux

Hôtel Novotel, Avenue Mohamed V, Tunis, Tunisie

Toutes les commodités propices à une formation de haut niveau seront de mise : salle de conférences polyvalente, équipement audiovisuel, écran et flip chart, vidéo-projecteur, régie sonorisation, connexion internet WIFI, etc

Supports

Une documentation riche sur support magnétique servira de base pédagogique et sera remise aux participants au premier jour de la formation

Date

2 au 4 décembre 2026

Coût

Le prix par participant est fixé à **2.290 Dinars** Hors Taxes. Ce montant couvre les frais d'inscription, les supports pédagogiques, les pauses café et les repas-déjeuners.

Programme de formation

1ère Journée : GOUVERNANCE DU PCA ET ANALYSE D'IMPACT

SÉQUENCE 1 : Le PCA comme composante du dispositif de gestion des risques

- Définitions : continuité d'activité, résilience opérationnelle, gestion de crise, reprise informatique et plan de secours
- Positionnement du PCA dans la gouvernance des risques : conseil, direction générale, risques, métiers, DSI et audit
- Lien entre risque opérationnel, risque cyber, risque fournisseur, risque de concentration et continuité

- Principes de proportionnalité : calibrer le PCA selon la taille, la complexité et la criticité des activités
- Passer d'un PCA documentaire à un dispositif piloté, testé et mesurable

SÉQUENCE 2 : Cadre tunisien et attentes de la BCT

- Lecture opérationnelle des exigences tunisiennes relatives à la continuité et à la gestion des risques
- Circulaire BCT n°2024-05 : menaces internes et externes, objectifs de reprise, DMIA, site secondaire, communication et participation des prestataires critiques aux tests
- Exigences de traçabilité, d'intégrité, de disponibilité et de gestion des incidents pour les systèmes critiques
- Articulation avec les obligations de cybersécurité et les dispositifs de contrôle interne
- Documentation attendue : politique, BIA, scénarios, plans, résultats de tests, plans d'actions et reporting

SÉQUENCE 3 : Business Impact Analysis (BIA) et cartographie des dépendances

- Identifier les produits, services et processus critiques
- Évaluer les impacts d'une interruption : financier, client, réglementaire, juridique, réputationnel et systémique
- Définir la durée maximale d'interruption admissible (DMIA/MTPD)
- Déterminer les objectifs de reprise : RTO et RPO
- Identifier les ressources indispensables : personnel, applications, données, locaux, télécoms, fournisseurs et infrastructures externes
- Cartographier les interdépendances entre front-office, back-office, paiements, trésorerie, canaux digitaux et fonctions support

2ème Journée : STRATÉGIES DE CONTINUITÉ, BIA ET PRA

SÉQUENCE 4 : Scénarios de rupture et stratégies de continuité

- Indisponibilité du siège ou d'un site critique
- Panne majeure du système d'information ou perte d'un centre de données
- Cyberattaque, ransomware, corruption ou indisponibilité des données
- Rupture de télécommunications ou d'alimentation électrique
- Indisponibilité de ressources humaines clés
- Défaillance d'un prestataire ou d'un fournisseur technologique critique
- Choisir les stratégies : redondance, site de repli, PRA, télétravail de crise, solutions alternatives et procédures dégradées

SÉQUENCE 5 : Du PCA au PRA informatique et au site de secours

- Différence et complémentarité entre PCA et PRA
- Architecture de secours : site primaire, site secondaire, réplication, sauvegardes et basculement
- Cohérence entre RPO/RTO métiers et capacités techniques de reprise
- Protection de l'intégrité et de la disponibilité des données pendant la bascule et la reprise
- Organisation du retour au site nominal et contrôle post-reprise
- Points de vigilance sur les dépendances télécoms, cloud, fournisseurs et solutions mutualisées

SÉQUENCE 6 : Gestion de crise et communication

- Critères d'activation du PCA et niveaux de crise
- Cellule de crise : composition, rôles, chaîne de décision et délégations
- Main courante, journal de crise et traçabilité des décisions
- Communication interne : collaborateurs, métiers, agences et fonctions support
- Communication externe : clients, prestataires, infrastructures de place et autorités compétentes selon le cas

- Préparation de messages et circuits d'escalade pour éviter les délais et contradictions

SÉQUENCE 7 : Tests du PCA et exercices de crise

- Typologie des tests : documentaire, table-top, technique, basculement partiel basculement complet et exercice de crise
- Construire un scénario réaliste et des injects successifs
- Tester les métiers, les systèmes, les communications, les prestataires et le site secondaire
- Mesurer les temps réels de reprise et les comparer aux objectifs fixés
- Formaliser les écarts, responsabilités, délais de correction et retests
- Intégrer les leçons tirées des incidents réels et des changements significatifs

3ème Journée : Cas Pratique : PRA de l'environnement Swift des banques en Tunisie"

- **Principes de ' Disaster Recovery ' pour les applications SWIFT Net**
  - Les composantes de SWIFT Net
  - Les configurations types
  - Les risques majeurs pour les différentes interfaces utilisées (Alliance Access, Alliance Gateway, Alliance Web,...)
  - Cartographie des flux, des dépendances réseau et des points critiques pour continuité des paiements.
- **Résilience typique d'Alliance Access**
  - Résilience avec l'option ' DB Recovery'
  - Résilience sans l'option ' DB Recovery'
  - Problème de connectivité
  - Problème Hardware (carte mère, disque, carte contrôleur, mémoire,...)
- **Résilience typique d'Alliance Gateway**
- **Résilience HSM et gestion des certificats**
- **Résilience réseau**

- **Autres dispositifs et alternatives**
  - Procédures de récupération pour 'Alliance Web Platform'
  - Solutions de repli : recours à une connexion indirecte via un « Service Bureau » ou à une solution mutualisée.
  - Analyse de la faisabilité des modes de repli, leurs responsabilités et leurs limites contractuelles.