🏦 FinSight Bank

Politique de Gestion du Risque Opérationnel et de Continuité d'Activité (PCA)
Version 2025 – Document interne confidentiel

Préambule

La présente *Politique de Gestion du Risque Opérationnel et de Continuité d'Activité (PCA)* formalise le cadre adopté par **FinSight Bank** pour identifier, évaluer, maîtriser et atténuer les risques opérationnels susceptibles d'affecter la stabilité, la sécurité et la continuité de ses activités.
Elle s'appuie sur les dispositions de la **loi n°2016-48** relative aux établissements de crédit, sur les circulaires de la **Banque Centrale de Tunisie**, et sur la norme internationale **ISO 22301** relative au management de la continuité d'activité.

Ce dispositif vise à assurer la résilience de la Banque face aux incidents majeurs — qu'ils soient d'origine technique, humaine ou environnementale — tout en garantissant la protection des clients, la préservation des données et la disponibilité des services essentiels.

I. Objectifs et champ d'application

La politique de gestion du risque opérationnel a pour objectif de protéger les actifs de la Banque, d'assurer la fiabilité des opérations et de renforcer la confiance des parties prenantes.
Elle s'applique à l'ensemble des processus métiers, des systèmes d'information, des filiales, des partenaires externes et des prestataires critiques de FinSight Bank.

Le **Plan de Continuité d'Activité (PCA)** constitue un prolongement opérationnel de cette politique. Il définit les dispositifs, procédures et ressources nécessaires pour maintenir ou rétablir rapidement les fonctions vitales de la Banque en cas d'interruption significative.
Le PCA est activé en cas d'incident majeur, notamment catastrophe naturelle, cyberattaque, panne informatique, sinistre sur site ou indisponibilité du personnel clé.

II. Cadre de référence et principes de gouvernance

FinSight Bank s'engage à mettre en place un dispositif de gestion du risque opérationnel conforme aux exigences de la **Banque Centrale de Tunisie** et aux meilleures pratiques internationales.
Le dispositif repose sur trois principes fondamentaux : la **responsabilité**, la **prévention** et la **résilience**.

Les rôles et responsabilités sont clairement définis à travers l'organigramme fonctionnel suivant :

Niveau	Responsabilité principale	Description
Conseil d'Administration	Supervision stratégique	Valide la politique globale, le PCA et le rapport annuel de risque opérationnel.
Comité des Risques	Suivi et contrôle	Analyse les indicateurs de risque et approuve les plans de remédiation.
Direction Générale	Mise en œuvre opérationnelle	Garantit les ressources nécessaires à la gestion et à la continuité des activités.
Direction des Risques	Pilotage du dispositif	Coordonne la cartographie des risques, les contrôles et le PCA.
Audit Interne	Évaluation indépendante	Vérifie l'efficacité et la conformité du dispositif global.

Ce modèle à plusieurs niveaux garantit une surveillance constante, une répartition claire des missions et une capacité de réaction immédiate en cas d'incident majeur.

III. Définition et classification du risque opérationnel

Le **risque opérationnel** se définit comme le risque de perte résultant d'une inadéquation ou d'une défaillance des procédures, des systèmes, du personnel ou d'événements externes. Il inclut, sans s'y limiter, les risques de fraude, d'erreur humaine, de défaillance informatique, de non-conformité, de cybersécurité et de continuité d'activité.

FinSight Bank distingue plusieurs **catégories de risques opérationnels**, regroupées dans la typologie suivante :

Catégorie de risque	Description	Exemples concrets
Humain	Risques liés aux erreurs, omissions ou comportements inappropriés du personnel.	Erreurs de saisie, non-respect des procédures, fraude interne.
Processus	Risques découlant d'un défaut de conception, d'exécution ou de supervision des processus.	Retard de traitement, double validation manquante, absence de contrôle.
Systèmes	Défaillances techniques ou indisponibilité	Panne serveur, perte de

Catégorie de risque	Description	Exemples concrets
	des systèmes informatiques.	connectivité, bug logiciel.
Externe	Événements extérieurs indépendants de la Banque.	Cyberattaque, incendie, inondation, panne d'énergie, crise sanitaire.

Chaque catégorie fait l'objet d'une évaluation périodique et d'un plan d'atténuation spécifique validé par la Direction des Risques.

IV. Méthodologie de gestion et indicateurs clés

Le processus de gestion du risque opérationnel repose sur un cycle continu de **quatre étapes : identification, évaluation, maîtrise et surveillance.**

L'identification consiste à recenser les événements potentiels via des auto-évaluations de risque (RCSA), des audits et des signalements internes.
L'évaluation repose sur une méthode combinant la **probabilité d'occurrence** et l'**impact financier ou réputationnel**.
Les risques sont ensuite hiérarchisés selon une matrice d'exposition qui détermine les priorités de traitement.

Niveau de criticité	Probabilité	Impact estimé	Action prioritaire
Faible	Rare	Limité	Surveillance simple
Modéré	Occasionnel	Significatif	Plan d'atténuation local
Élevé	Fréquent	Important	Suivi mensuel par la Direction des Risques
Critique	Très fréquent	Majeur ou systémique	Escalade immédiate au Comité des Risques

La surveillance repose sur des **indicateurs clés de risque (Key Risk Indicators – KRI)** suivis mensuellement, tels que le nombre d'incidents, la durée moyenne d'interruption de service, la fréquence des alertes sécurité et le coût global des sinistres enregistrés.

V. Gestion de la continuité d'activité (PCA)

Le **Plan de Continuité d'Activité (PCA)** vise à garantir la poursuite des opérations critiques de FinSight Bank en cas de crise majeure.
Il repose sur une analyse d'impact sur les activités (*Business Impact Analysis – BIA*) permettant d'identifier les processus vitaux et de définir les délais de reprise acceptables (*Recovery Time Objectives – RTO*).

Chaque direction opérationnelle élabore un plan de continuité spécifique détaillant les procédures à suivre en cas d'indisponibilité de site, de personnel ou de système.
Des sites de repli, des sauvegardes de données et des procédures manuelles de secours sont mis en place pour assurer la reprise dans des délais optimaux.

Fonction critique	RTO cible	Mesure de secours	Responsable
Traitement des paiements	4 heures	Serveur miroir + plan de bascule automatique	Direction IT
Gestion des dépôts	8 heures	Base de données secondaire + scripts de reprise	Back-Office Financier
Relation client	12 heures	Redirection téléphonique + accès distant	Direction Réseau
Trésorerie / Marché	2 heures	Système de secours dédié	Direction Marché & Liquidité

Des tests de continuité sont réalisés au minimum une fois par an afin de valider l'efficacité du PCA. Les résultats sont consignés dans un rapport transmis au Comité d'Audit et à la Banque Centrale de Tunisie.

VI. Gestion des incidents et retour d'expérience

Tout incident opérationnel, qu'il entraîne ou non une perte financière, doit être déclaré dans un délai maximum de 24 heures à la Direction des Risques via le système interne *FinSight Risk Monitor*.
Un registre des incidents opérationnels est tenu à jour et fait l'objet d'une analyse trimestrielle. Chaque événement majeur donne lieu à un **rapport d'incident** décrivant la cause, les impacts, les mesures correctives et les enseignements tirés.

Le retour d'expérience (RETEX) constitue une composante essentielle de la politique. Il permet d'améliorer en continu les procédures internes, de renforcer la sensibilisation du personnel et d'actualiser les plans de continuité.

VII. Cybersécurité et protection des systèmes d'information

Dans un contexte de digitalisation accrue, FinSight Bank accorde une priorité absolue à la **cybersécurité**.
Le dispositif de sécurité des systèmes d'information repose sur le principe de défense en profondeur, combinant mesures techniques, organisationnelles et humaines.
Les connexions externes, les échanges de données sensibles et les accès à distance sont soumis à un contrôle renforcé.
Un **plan de réponse aux incidents cybernétiques (Cyber Response Plan)** est intégré au PCA et coordonné avec la Direction Sécurité Informatique.

Les indicateurs de performance du dispositif de sécurité sont suivis par la **Direction des Systèmes d'Information** et reportés trimestriellement au Comité des Risques et à la Direction Générale.

VIII. Formation et culture de résilience

La résilience opérationnelle repose sur la compétence et la vigilance de l'ensemble du personnel.
Des programmes de formation annuels sont organisés afin de familiariser les collaborateurs avec les procédures de gestion des incidents, les gestes à adopter en situation de crise et les protocoles de communication d'urgence.
Des exercices de simulation, à la fois techniques et organisationnels, sont menés régulièrement pour tester la coordination interservices et la réactivité des équipes face à un scénario de crise.

FinSight Bank veille à maintenir un niveau élevé de sensibilisation, de discipline et de préparation dans toutes ses structures.

IX. Révision et entrée en vigueur

La présente politique est révisée annuellement ou à la suite d'un incident majeur, d'une modification du périmètre d'activité ou d'une évolution réglementaire.
Elle entre en vigueur à compter du **1er janvier 2025**, après approbation par le **Conseil d'Administration** et le **Comité des Risques**.
Toutes les entités de FinSight Bank sont tenues d'en appliquer les principes et de participer activement à son amélioration continue.