Objectif et champs d'application

La procédure « Gérer les risques opérationnels » a pour objectif de décrire les modalités d'identification, d'évaluation, de suivi et maîtrise en temps opportun de tous les risques opérationnels inhérents à l'activité Banque de l'Union Côte d'Ivoire (BDU-CI). Le but étant de :

- Contribuer à la mise en place effective, au sein de l'établissement, d'un dispositif de gestion intégrée des risques ;
- Mettre en œuvre et renforcer le dispositif de gestion des risques.

Cette procédure s'applique à toutes les activités, à toutes les entités opérationnelles et au Service Gestion Globale des Risques.

Objectifs du contrôle interne

- S'assurer que les risques opérationnels auxquels est confrontée la Banque de l'Union Côte d'Ivoire (BDU-CI) sont effectivement maitrisés
- S'assurer que les politiques et procédures de BDU-CI sont respectées
- S'assurer que les contrôles de premier niveau sont appropriés et effectifs
- Suivre la mise en œuvre, par les entités opérationnelles des plans d'actions correctifs définis dans le cadre des différentes missions de contrôle et d'investigations

Rôles et responsabilités

Chef du Service Gestion Globale des Risques

Sous la responsabilité du Directeur Général, il a la charge de vérifier et valider le rapport de déclaration d'incident.

Analyste Risques

Sous la responsabilité du Chef de Service Gestion Globale des Risques, il a la charge de :

- Constituer un dossier de déclaration d'incident ;
- Rédiger un rapport de déclaration d'incident en se munissant d'une « Fiche de déclaration des incidents »
- Proposer des solutions en vue de la correction de l'incident ;
- Identifier le Responsable de Traitement des incidents.
- Faire le suivi de toutes les recommandations mises en place.

Sigles et Définitions

Définitions

- **Gestions des risques** : l'ensemble des stratégies, politiques et procédures mises en place afin que tout risque significatif et toute concentration de risques associée soient détectés, mesurés, limités, maîtrisés et atténués, et qu'il en soit rendu compte, de façon précoce et exhaustive.

- **Risque opérationnel** : le risque de pertes résultant de carences ou de défaillances attribuables à des processus, des personnes, des systèmes internes ou à des événements externes. Cette notion inclut le risque juridique mais exclut les risques stratégiques et de réputation.

Sigles

- AR : Analyste Risques
- CSGGR : Responsable Service Gestion Globale des Risques
- DG : Directeur Général

Sommaire de la procédure

Références / Règles de gestion

- Documents de références

- Politique de Gestion des risques
- Circulaire n°04-2017 /CB/C relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA

- Règles de gestion

- Les équipes du Service Gestion Globale des Risques doivent disposer des connaissances et du savoir-faire nécessaires à l'exercice de leur fonction et leur permettant d'identifier, évaluer, atténuer et maitriser les risques inhérents aux activités de la Banque.

- Le SGGR effectue un comité des risques composé de quatre (04) administrateurs qui est effectué avant la tenue des différents conseils.

- Les activités des fonctions de contrôle des filiales des compagnies financières et des établissements de crédit maisons-mères peuvent être partiellement externalisées auprès de la maison-mère ou d'une autre entité du groupe implantée dans l'UMOA. Toutefois, l'externalisation n'exonère pas l'établissement de l'obligation de rendre compte de l'efficacité et de la conformité de ses fonctions de contrôle aux dispositions légales et réglementaires.

- Les événements de pertes opérationnelles ou incidents opérationnels doivent être classés dans l'une des sept catégories ci-après définies, afin d'assurer la cohérence au niveau de l'identification, de l'évaluation et de la fixation des objectifs de gestion des risques opérationnels à l'échelle de l'établissement :
- Fraude interne : risque de pertes dues à des actes intentionnels, impliquant au moins une partie interne à l'établissement, visant à frauder, détourner des biens appartenant à l'établissement ou à sa clientèle, manipuler des informations, contourner les règlements, la législation ou la politique de l'établissement ;
- Fraude externe : risque de pertes résultant des actes, de la part d'un tiers, visant à frauder, détourner des biens appartenant à l'établissement ou à sa clientèle, manipuler des informations ou contourner la législation ;
- Pratiques en matière d'emploi et de sécurité sur le lieu de travail : risque de pertes découlant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, y compris les litiges ou différends entre l'établissement et ses employés ;
- Pratiques concernant les clients, les produits et l'activité commerciale : risque de pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients ou d'un manquement imputable à la nature ou à la conception d'un produit donné ;
- Dommages occasionnés aux actifs physiques : risque de pertes lié à des destructions ou dommages résultant d'une catastrophe naturelle ou des causes externes ;
- Interruptions d'activités et défaillances des systèmes : risque de pertes résultant d'interruptions de l'activité ou de dysfonctionnements des systèmes technologiques ;

- Exécution des opérations, livraison et gestion des processus : risque de pertes lié à une défaillance dans le traitement d'une transaction ou dans la gestion des processus et les pertes subies dans le cadre des relations avec les contreparties commerciales et les fournisseurs.

- L'établissement doit collecter les données relatives aux événements de pertes opérationnelles. Le processus y relatif doit être documenté et mis à jour périodiquement.

- La gestion du risque opérationnel doit couvrir l'ensemble des sept catégories d'événements de pertes opérationnelles citées à l'article 28 de la Circulaire N°04-2017/CB/C relative à la gestion des risques dans les établissements de crédit et les compagnies financières de L'UMOA. Pour identifier et évaluer le risque opérationnel, l'établissement peut recourir notamment aux outils de gestion ci-après :
- Les autoévaluations du risque opérationnel ;
- La cartographie des processus opérationnels ;
- Les indicateurs de risque et de performance en matière de surveillance du risque opérationnel et les indicateurs d'efficacité du système de contrôle interne ;
- Les analyses des événements de pertes opérationnelles tant à l'intérieur qu'à l'extérieur de l'établissement ;
- Les analyses de risques spécifiques à chaque produit, processus et système en place ;
- Les analyses de scénarios.

Narratif de la procédure		
PRO CI 08 003	Gérer le risque opérationnel	AR, Déclarant, CSGGR, Responsable en charge du traitement de l'incident

Acteurs	Descriptions des tâches	Documents et interfaces
I. Collecte des données de pertes opérationnelles		
I.1. Déclaration de l'incident de perte opérationnelle		
Déclarant (Opérationnel qui constate l'incident)	- Constater la survenance de l'incident - Renseigner immédiatement la fiche de déclaration d'incident (Fichier Excel) - Transmettre immédiatement la fiche de déclaration d'incident à sa hiérarchie	Fiche de déclaration de l'incident
Hiérarchie	- Prendre connaissance de l'incident et apporter des corrections éventuelles à la fiche de déclaration d'incident - Déclarer l'incident dans un délai de 48h via la messagerie (Outlook) à l'AR. - Suivre la déclaration de l'incident jusqu'à l'obtention d'un numéro d'incident de l'AR	Fiche de déclaration de l'incident

Acteurs	Descriptions des tâches	Documents et interfaces
	NB : Les informations renseignées dans la fiche de déclaration sont les suivantes : *- Les dates de survenance et de remontée de l'incident* *- La description succincte de l'incident* *- La qualification de l'incident* *- Les conséquences* *- Les propositions de solutions* *- Les porteurs des recommandations*	
I.2. <u>Rédaction du rapport de déclaration d'incident</u>		
AR	- Réceptionner le mail relatif à l'objet de l'incident - Réceptionner par mail la fiche de déclaration d'incident - Enregistrer les informations nécessaires, relatives à la déclaration d'incident dans un fichier Excel - Attribuer un numéro d'incident - Constituer un dossier de déclaration d'incident en menant les actions suivantes : • Collecte d'élément de preuve • Analyse des documents collectés • Établissement d'un rapprochement entre l'incident et les documents afin d'identifier la pertinence de chaque document collecté et faire ressortir une preuve probante permettant de déterminer le caractère frauduleux ou non de l'incident • Proposer des solutions en vue de la correction de l'incident - Rédiger un rapport de déclaration d'incident en se munissant d'une « Fiche de déclaration des incidents » - Identifier le Responsable de Traitement des incidents ou celui de la mise en œuvre les recommandations formulées dans le rapport - Transmettre par mail ou physiquement le rapport d'incident (document Word) pour validation au Chef de Service Gestion des Risques	Base de remontée d'incidents de perte opérationnelle Rapport de déclaration d'incident
CSGGR	- Recevoir par email ou physiquement le rapport de déclaration d'incident - C7 : Vérifier la pertinence et la cohérence des informations - En cas de non-conformité, mentionner ses observations par email ou physiquement puis retourner le fichier à l'AR pour prise en charge	Rapport de déclaration d'incident

Acteurs	Descriptions des tâches	Documents et interfaces
	– En cas de conformité ou après corrections éventuelles, valider le rapport de déclaration et le transmettre par mail au Responsable en charge du traitement de l'incident et aux Responsables des Directions ou services concernés par l'incident pour leurs observations	
Les responsables des entités concernées par l'incident	– Recevoir le rapport d'incident – Formuler ses observations sur le contenu du rapport – Transmettre les observations au CSGGR.	Rapport de déclaration d'incident
CSGGR	– Recevoir le rapport d'incident avec les observations des entités concernées par l'incident – Organiser une rencontre pour des d'échanges afin de la levée des points de désaccord – Apporter des corrections éventuelles au rapport d'incident – Transmettre le rapport d'incident au DG	Rapport de déclaration d'incident
I.3. Validation du rapport d'incident par la DG		
DG	– Recevoir et prendre connaissance du rapport de déclaration d'incident – Donner par écrit des instructions pour la mise ouvre des recommandations – Transmettre le rapport validé au CSGGR	Rapport de déclaration d'incident
I.4. Mise en œuvre et suivi des recommandations		
CSGGR/AR	– Transmettre aux Responsables des entités concernées par l'incident pour mise en œuvre des recommandations – Faire un suivi minutieux de toutes les recommandations mises en place – Produire un rapport trimestriel sur les risques opérationnels qui sera transmis au Directeur Général	Rapport de déclaration d'incident Rapport trimestriel
II. Contrôle et atténuation du risque opérationnel		
	– *Cf Pro PP4 004 : Assurer le contrôle permanent*	

Annexes / Enregistrements

- Fiche de déclaration de l'incident
- Rapport de déclaration d'incident
- Rapport trimestriel sur les risques

Liste des ampliations

N°	Structures	Date	Visa	Observations
01				
02				

Liste des modifications

N°	Nature de la modification	Date	Chapitre ou page concerné (e)	Observations
01				
02				

Rédigé par : SGGR	Validé par : Comité Procédures	Approuvé par :
Date : Mai 2024	Date : 25/06/2024	Date :
Signature :	Signature :	Signature :