BANQUE DE LA REPUBLIQUE DU BURUNDI
SERVICE SUPERVISION DES ETABLISSEMENTS BANCAIRES
ET STABILITE FINANCIERE

INSTITUTION:
DATE DE CONTROLE:
SUPERVISEUR :
PERSONNES INTERROGEES :

RESUME DES CONCLUSIONS SUR LE RISQUE OPERATIONNEL

No	Objet	**Remarques et Conclusions du superviseur**	**Observations après un entretien**
1	**Contrôle effectué par le Conseil d'Administration et la Direction** • Efficacité des comités du C.A • Contrôle de la Direction		
2	**Politiques, Procédures et Limites** • Pertinence des politiques • Mise en place des procédures et limites		
3	**Identification adéquate du risque, mesure, contrôle et gestion du système d'information** • Identification des risques • Mesure et contrôle de la gestion du système d'information		
4	**Procédures adéquates du contrôle interne et d'audits** • Adéquation des contrôles internes • Efficacité de l'audit interne et externe		

PROCEDURES DE CONTROLE DU RISQUE OPERATIONNEL

Rappel:

Le risque opérationnel est un risque de pertes directes ou indirectes dues à une inadéquation ou à une défaillance des procédures (analyse ou contrôle absent ou incomplet, procédure non sécurisée), du personnel (erreur, malveillance ou fraude), des systèmes internes (panne informatique,...) ou à des risques externes (inondation, incendie,...).

No	Objet	
A	**Le contrôle effectué par le Conseil dôAdministration et la Direction** • Evaluer la politique des risques opérationnels et les tests de conformité utilisés pour cette politique. Les domaines concernés sont : - L'informatique - Les caisses - Les dépôts et le blanchiment des capitaux - Les immobilisations : revoir la politique de contrôle des immobilisations de la banque, s'assurer de l'adéquation des procédures de leur acquisition, de leur dépréciation, de leur cession et de leur valorisation. Revoir la politique de l'institution sur les comptes dormants • Stratégie informatique Obtenir la stratégie informatique de la banque et apprécier son adéquation. Vérifier que cette stratégie a été approuvée par le Conseil dôAdministration et est régulièrement mise à jour. Revoir les minutes du directeur informatique ou d'un autre comité ayant la responsabilité globale pour des questions informatiques de l'établissement. Confirmer la pertinence du projet.	
B		

No	Objet	
	Politiques, Procédures & Limites • Politique informatique S'enquérir de la politique de sécurité de la banque et s'assurer qu'elle est approuvée par le Conseil d'Administration et mise à jour. • Revoir les procédures et limites a) Généralités Obtenir une compréhension du système informatique de la banque et en particulier décrire : ➢ Le système central de la banque ➢ Le système d'exploitation ➢ Le matériel informatique ➢ Les autres logiciels d'application en cours d'utilisation b) Politique de sécurité Revoir la politique de la sécurité informatique de la banque et s'assurer qu'elle traite les questions suivantes : ➢ importance de la sécurité de l'information dans l'institution ➢ classification des actifs ➢ sécurité du personnel ➢ sécurité logique et physique et environnementale ➢ sécurité des télécommunications ➢ exigences réglementaires et contractuelles, sensibilisation à la sécurité, à la formation et à l'éducation ➢ détection des zones d'insécurité et les renseigner ➢ renforcement des dispositions applicables en cas de violation. ➢ Evaluer la pertinence des procédures de l'institution pour l'autorisation et le suivi des modifications du système. c) Plan de Continuité d'Activité (PCA) Obtenir une copie du plan de continuité des activités de l'institution et vérifier son adéquation. Au minimum, le plan devrait contenir : ➢ La classification des systèmes par ordre d'importance en	

No	Objet	
	fonction de leur sensibilité aux événements ➢ Inventaire des décisions importantes relatives au personnel, au matériel et aux fournisseurs de logiciels ➢ Organisation et l'attribution des responsabilités en cas de catastrophe. ➢ Alternative de sauvegarde hors site c'est-à-dire un back up externe. • Gestion des fournitures (matériel et logiciel) Evaluer les activités importantes de la Direction avant la sélection des fournisseurs. S'assurer que la Direction participe aux activités de sélection. Au minimum, elle devrait considérer : ➢ Réputation du vendeur ➢ La situation financière du vendeur ➢ Service chargé du suivi des contrats ➢ Le coût du développement, de la maintenance et de l'approvisionnement. • Nouveaux développements technologiques Pour les systèmes bancaires par téléphone et internet : ➢ Acquérir une compréhension des systèmes bancaires par téléphone et internet en examinant le site web ainsi que les informations montrant comment ces systèmes fonctionnent ➢ Examiner la documentation et mener des discussions avec la Direction afin de déterminer comment sont effectués les contrôles de sécurité pour les modules bancaires par téléphone et internet • Revue du logiciel bancaire ➢ Revoir la liste de tous les logiciels d'application standard utilisés sous licence ➢ Veiller à ce que la banque dispose des procédures pour se prémunir contre l'utilisation non autorisée de logiciels ➢ Examiner les contrôles mis en place pour suivre les modifications des programmes et données ➢ S'assurer que le personnel informatique n'initie et n'approuve pas les opérations	

No	Objet	
	➢ Obtenir une liste de tous les principaux rapports produits par le système en indiquant leur fréquence et leur distribution ➢ Examiner et commenter les opérations d'ouverture et de clôture de la journée ➢ S'assurer que le logiciel bancaire intègre un système permanent pour le renouvellement des ordres (exemple : les dépôts, crédits, découverts…) ➢ S'assurer que le logiciel antivirus est régulièrement mis à jour. • Contrôle physique et environnemental a) l'accès à la salle de serveur est-il limité au personnel autorisé ? b) les disques et bandes informatiques sont-ils stockés dans une armoire anti-feux ? c) y a-t-il un contrôle adéquat sur le mouvement des disquettes et des cassettes ? d) veiller à ce que la banque conserve au moins trois générations de sauvegarde. e) veiller à ce que les copies de sauvegarde soient conservées en dehors du site d'exploitation. f) la salle des serveurs est-elle protégée contre la poussière, la fumée et l'humidité ? g) veiller à ce que la banque dispose d'extincteurs. h) veiller à ce que la banque dispose d'un onduleur et d'un groupe électrogène de secours. i) contrôler l'armoire de câblage LAN (Local Area Network) et vérifier qu'il est physiquement sécurisé. j) veiller à ce que le serveur de logiciel bancaire soit séparé du serveur de messagerie internet pour éviter le risque d'accès non autorisé par des tiers. k) veiller à ce que la banque dispose d'un inventaire à jour du matériel. • Le système de contrôle du réseau informatique (a) Obtenir un schéma du réseau local de la banque montrant comment les interfaces du réseau local sont connectés avec d'autres	

No	Objet	
	réseaux et faire des commentaires. (b) S'assurer que tous les utilisateurs du système ont des mots de passe uniques et ceux-ci sont changés fréquemment. (c) s'assurer que l'accès au réseau local et l'accès à un logiciel bancaire est une nécessité pour démarrer le travail. (d) s'assurer que la connexion au réseau est désactivée après une courte période d'inactivité. (e) S'assurer que l'accès au poste de contrôle du système est limité. Toutes les tentatives de connexion au poste de contrôle doivent être enregistrées. (f) S'assurer qu'il n'y a pas d'utilisateurs temporaires ou non protégés dans le système. Ces comptes sont généralement ciblés par les pirates. • Assistance au système Pour les banques qui ont de grandes opérations informatiques complexes, s'assurer que la banque a mis en place un service d'assistance avec un système de suivi des plaintes pour résoudre rapidement les problèmes que les utilisateurs peuvent avoir avec leurs systèmes. • Dépôts 1) Revoir la composition du total des dépôts à la date de contrôle et faire des commentaires appropriés sur sa solidité / stabilité (c à d profil de maturité, type de compte, la source). 2) Revoir le guide des tarifs de l'institution. 3) Evaluer le coût moyen des dépôts et le comparer au coût des dépôts du secteur. Lorsque les deux coûts diffèrent sensiblement, obtenir des explications de la différence. 4) Vérifiez que l'institution a une politique exigeant que les clients envoient régulièrement leurs états financiers. 5) Prendre un échantillon de dépôts sur lesquels les intérêts ont été payés et vérifier que l'institution a calculé le montant exact des	

No	Objet	
	intérêts à payer 6) Sélectionnez les bons d'épargne et les comptes courants et vérifier que: ➢ Le chèque a été dûment autorisé; ➢ Le timbre approprié a été utilisé sur le bon; ➢ L'entrée est enregistré dans le compte du grand livre respectif ; 7) Pour les comptes classés comme dormants, vérifiez que : -Le système identifie les comptes dormants. -La personne habilitée a approuvé tous les débits / crédits à ces comptes. -Vérifiez que les transferts des comptes dormants vers les comptes normaux sont approuvés par un agent autre que celui qui a approuvé les opérations sur les comptes dormants. 8) Obtenir le registre de clôture de comptes. En utilisant un échantillon approprié, s'assurer que les comptes fermés ne sont pas sur la liste des comptes normaux. 9) Vérifier que les soldes des comptes fermés ont été versés aux bénéficiaires légitimes. 10) Lorsque l'institution a des coffres-forts, évaluer la pertinence des contrôles. **12 .Connaître son Client (KYC)** 1) Obtenir la politique anti-blanchiment d'argent de la banque et évaluer sa pertinence. Déterminer si les tests de conformité sont réalisés sur une base annuelle. 2) Vérifier si le questionnaire de lutte contre le blanchiment d'argent est rempli. 3) A partir des nouveaux dépôts reçus (compte ouvert depuis la date du précédent contrôle ou précédente date de clôture), vérifier que : ➢ La clientèle a obtenu le mandat pour l'ouverture du compte avant qu'il ne soit opérationnel ➢ Le formulaire d'ouverture de compte doit renfermer la	

No	Objet	
C	signature du client dûment vérifiée et approuvée par un responsable habilité. ➢ L'ouverture de compte est appuyée par des documents d'identification, notamment la carte nationale d'identité, le passeport, le permis de conduire, certificat de naissance pour les mineurs, des factures des services publics, le certificat d'enregistrement des entreprises, registre de commerce, numéros d'identification fiscale, les articles et protocole d'association, les statuts, l'agrément etc… ➢ Vérifier que les fonds ont été effectivement reçus en se référant aux pièces justificatives 4) Consulter la dernière liste de l'ONU établissant les personnes soupçonnées être liées au terrorisme et les sites Web américains : http:/www.un.org/Docs/sc/committees/1267/ pdflist.pdf et http :/ www.treas.gov/offices/ enforcement/ofac/sdn/t11sdn.pdf. Vérifiez si les individus / entités énumérés dans la Liste des Nations Unies et États-Unis ont des actifs / dépôts dans la banque **13. Immobilisations** 1) Vérifier les titres de propriété détenus par l'institution (par exemple les certificats fonciers, fonds de commerce etc…) 2) Obtenir un registre des immobilisations et si nécessaire et possible, vérifier leur existence physique. 3) Vérifiez si les immobilisations sont assurées. 4) Vérifier si les primes payées pour les biens donnés en bail, ainsi que pour les bâtiments, sont amortis sur une période n'excédant pas la durée du bail, et que des dispositions ont été prises pour le bon entretien, conformément aux termes du bail. 5) Vérifiez si les loyers, rentes foncières, tarifs et taxes foncières sont régulièrement payées.	

No	Objet	
F	**13. Fraudes et Contrefaçons** Se renseigner sur les fraudes et les fichiers de contrefaçons / rapports / données et les examiner par rapport au dernier contrôle. Souligner les défaillances spécifiques dans les contrôles internes et évaluer l'efficacité des processus de gestion de la fraude.	
G	**14. Caisse et Avoirs en banque** ➢ Revoir les encaisses et s'assurer qu'elles ont été vérifiées et examinées par un responsable. ➢ S'assurer que les contrôles ponctuels sont effectués régulièrement. ➢ S'assurer que les limites d'encaisse mises en place sont respectées. ➢ S'assurer que l'encaisse a une couverture d'assurance adéquate. ➢ S'assurer qu'il y a une double intervention au trésor. ➢ Revoir les comptes excédentaires et déficitaires et vérifier si l'institution dispose des procédures adéquates pour leur suivi. ➢ Réviser les rapprochements de tous les comptes bancaires des correspondants (nostro) et s'assurer que les questions en suspens sont rapidement traitées. ➢ S'assurer que les comptes de liaison sont régulièrement rapprochés et n'ont pas de points en suspens **15. Distributeur Automatique de Billets (DAB)** a) Garantir que l'argent distribué par le DAB est réconcilié avec les bordereaux de retrait d'espèces en temps opportun (au minimum chaque jour). b) S'assurer qu'un représentant de la banque est chaque fois présent lors de l'entretien ou maintenance du DAB. c) demander les journaux de transaction qui retracent chaque	

No	Objet	
	opération financière effectuée par le DAB. d) contrôler la disponibilité de la liste des opérations et les commentaires sur le DAB en cas d'arrêt le cas échéant. e) contrôler les procédures de rapprochement des soldes de trésorerie du DAB et la liquidité réelle dans le coffre. **16. Transfert électronique de fonds (Swift, Télex,)** a) Évaluer les contrôles sur l'interface automatique avec les systèmes comptables de la banque. b) évaluer la sécurité en cas modification de clés authentificatrices. c) Evaluer les procédures en cas d'urgence. d) Evaluer les procédures de correction et de nouvelle présentation de messages sortants rejetés. e) Évaluer les contrôles sur le traitement des messages entrants. Les messages qui ne sont pas authentifiés ou qui sont marqués, autant que possible les doublons doit être correctement contrôlée. f) Veiller à ce qu'il y ait une séparation des tâches au sein du service de transfert électronique.	

CONTROLE RISQUE OPERATIONNEL QUESTIONNAIRE

	OUI/NO	Références	Remarque
RISQUE OPÉRATIONNEL INTERNE (Questionnaire de contrôle) oui ou non a) Le système de contrôle interne est-il approprié pour le type et le niveau des risques au regard de la nature et de la portée des activités de l'institution? b. Est-ce que la structure de l'institution permet d'établir clairement les pouvoirs et la responsabilité de surveiller le respect des politiques, des procédures et des limites? c. Les lignes de reporting (système de transmission) délimitent-elles suffisamment les zones de contrôle des lignes de métier et la séparation adéquate des tâches pour toute l'organisation? d. Les structures officielles de l'organisation reflètent-elle le fonctionnement réel ? e. Y a t-il des procédures adéquates pour assurer la conformité aux lois et règlements applicables? f. Est-ce que l'audit interne est indépendant et objectif? g. Les contrôles internes et les systèmes d'information sont-ils suffisamment testés et examinés; une attention est portée sur une			

documentation adéquate et les faiblesses constatées. h. Est-ce que le comité d'audit ou le conseil d'administration s'est assuré de l'efficacité des audits internes sur une base régulière?			

RÉVISÉ PAR:

NOM:

SIGNATURE/DATE: