Objet et champs d'application

Cette procédure décrit le déroulement et toutes les dispositions pratiques permettant d'assurer une gestion efficace des changements intervenus dans le système d'information de la banque afin de limiter les risques pour la disponibilité, l'intégrité et la confidentialité des systèmes bancaires.

Elle s'applique à l'ensemble des changements de la banque faisant intervenir les actifs suivants de la banque:

- Les systèmes critiques bancaires (Core Banking System, moyens de paiement, e-banking, etc.).
- Les infrastructures (serveurs, bases de données, réseaux, sécurité, cloud).
- Les postes de travail et outils bureautiques.

Objectifs de la procédure

Les objectifs associés à cette procédure sont de permettre de répondre aux exigences suivantes :

- Réduire le nombre de défauts et de retraitements touchant la fourniture de solutions et de services ;
- S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'a qu'un impact minimum sur l'activité ;
- Maintenir l'intégrité de l'information et de l'infrastructure de traitement.

Rôles et responsabilités

➢ **La Direction des Systèmes d'Information**

Chargé de :

- Mettre en œuvre les changements informatiques selon la procédure de gestion des changements informatiques
- Implémenter et tester le changement.

2. Le RSSI

chargé de :

- Evaluer les risques, valider ou rejeter la demande ;
- valider la conformité sécurité ;
- Contrôler la bonne application de la mise en œuvre de la procédure de gestion des changements informatiques.

3. La Direction de l'Audit Interne

chargé de :

- Effectuer un contrôle annuel de niveau 3 pour identifier les écarts dans le contrôle de la mise en œuvre de la procédure.

Sigles et Définitions

➢ **Définitions**

Changement : toute modification, création, suppression apportée à l'environnement IT (applications, configurations, infrastructures).

Il existe trois (3) catégories de changements informatiques :

➢ **Changement standard**

Un changement standard est une modification préapprouvée, répétitive et à faible risque, dont la procédure de mise en œuvre est documentée, testée et validée.

Ces changements ne nécessitent pas d'approbation spécifique du comité de changement (CAB), car ils suivent un processus automatisé ou prédéfini

Ex :

- Création d'un compte utilisateur avec profil standard sur Active Directory.
- Application d'un patch mineur Windows ou antivirus sur poste utilisateur.
- Ajout d'une imprimante réseau dans une agence.
- Mise à jour de signatures de sécurité sur un antivirus ou firewall
- Etc.…

➢ **Les Changements normaux**

Un changement normal est une modification planifiée dont le risque ou l'impact potentiel doit être évalué avant exécution.

Il nécessite une analyse de risque, une validation formelle, et un plan de déploiement détaillé.

Exemple :

- Migration d'un serveur Core Banking ou d'un composant applicatif.
- Mise à jour d'une base de données de production.
- Modification des règles d'un pare-feu entre zones sécurisées.
- Changement de version d'un outil métier.
- Refonte d'un lien réseau entre agences

Les changements normaux peuvent avoir lieu à différents niveaux, notamment :

➢ **Au niveau réseau :**

- Ajout d'une interconnexion ou d'un nouveau segment réseau ;
- Modification massive des règles de filtrages ;
- Ajout d'un nouvel équipement d'infrastructure ;
- Modification de l'architecture réseau, extension vers des services Cloud, etc ;

➢ **Au niveau système :**

- Ajout d'un nouveau serveur ;
- Utilisation d'un nouveau système d'exploitation d'un serveur ;
- Changement de l'infrastructure de sauvegarde, etc ;

➢ **Au niveau applicatif :**

- Mise en production d'une nouvelle application ou version dans le périmètre ;
- Exposition d'une application sur internet ;
- Utilisation d'une nouvelle bibliothèque applicative, etc ;

➢ **Au niveau métier :**

- Stockage des informations de cartes bancaires ;
- Modification des flux de réception ou d'envoi de cartes ;

➢ **Les Changements urgents**

Un changement urgent est une modification non planifiée, à réaliser immédiatement pour corriger une panne critique, une faille de sécurité, ou un incident majeur ayant un impact sur les opérations bancaires. Ce type de changement est exceptionnel, nécessitant une action immédiate, avec validation et documentation a posteriori

Exemple :

- Application immédiate d'un patch de sécurité critique pour corriger une vulnérabilité exploitée.
- Modification d'une règle de firewall pour rétablir un service essentiel (paiements SWIFT, Core Banking).
- Redémarrage ou remplacement d'un serveur en panne affectant un service critique.
- Action d'urgence suite à cyberattaque ou incident de sécurité majeur.
- Etc…

➢ **Sigles**

RSSI : Responsable de la Sécurité du Système d'Information ;
BDU-CI : Banque de l'Union de Cote d'Ivoire ;
RE : Responsable de l'Entité demandeur du Changement (supérieur hiérarchique direct)
PCI DSS: Payment Card Industry Data Security Standard

Sommaire de la procédure

Table des matières

Références / Règles de gestion

➢ Documents de références réglementaires

- **Normes ISO/IEC 27001 : 2022 et ISO/IEC 27002:2022** exigences et mesures de sécurité relatives au système de management de la sécurité de l'information;
- **PCI-DSS v4.0 :** exigences de sécurité applicables aux environnements traitant des données de cartes bancaires
- **Politique de Sécurité des Système d'Information**
- **BCEAO / UEMOA** : directives sur la sécurité des systèmes d'information bancaires
- **Loi locale sur la protection des données personnelles** (Loi ivoirienne n° 2013-450)

➢ Règles de gestion

Tout changement doit être motivé.

- Les changements standards sont pré approuvés par le Directeur des Systèmes d'Information
- Les changements normaux sont approuvés par le RSSI, la Direction du Contrôle Permanent, conformément à la procédure de gestion des changements
- Les changements urgents sont approuvés en urgence par le DSI et le RSSI avec validation postérieure.

Les demandes de changements normaux doivent être clairement décrites, justifiées par le demandeur et validées par sa hiérarchie. Cette étape doit être clairement consignée dans un memo ou dans un cahier des charges validé par la hiérarchie du demandeur..

Narratif de la procédure		
PRO-RSSI-SSI-05	Gestion des changements informatiques	

Acteurs	Descriptions des tâches	Documents et interfaces
I.1. Soumission d'une demande de changement normal		
Demandeur	– Faire un mémo d'approbation du changement motivant le changement. Le mémo doit comporter les éléments suivants : o Description du changement o Justification / objectif o Impact attendu (systèmes, sécurité, utilisateurs) o Ressources nécessaires o Planning proposé o Planification dans le calendrier des changements. o Plan de retour arrière (rollback) – Transmettre le memo au RE pour validation	Mémo d'approbation du changement
RE	– Réceptionner le mémo – Valider le mémo – Transmettre le mémo au RSSI pour approbation	Mémo d'approbation du changement
I.2. Analyse et évaluation du changement normal		
RSSI/Membre de la Direction Contrôle Permanent	– Réception du mémo – Convoquer une réunion de changement au besoin. Les acteurs concernés sont : les acteurs métiers concerné par l'applicatifs, le RSSI, un membre de la Direction du Contrôle Permanent – Analyser l'impact (sécurité, opérationnel, financier, réglementaire) – Elaborer un rapport d'analyse d'impact – Faire un PV office de GO ou non GO	Mémo d'approbation du changement Rapport d'analyse d'impact PV de réunion

Acteurs	Descriptions des tâches	Documents et interfaces
	- Signer le memo - Transmettre le memo au Directeur du contrôle permanent	
I.3. Approbation du changement normal		
Directeur Contrôle permanent	- Valider ou rejeter le changement sur la base du rapport d'analyse d'impact, du PV de réunion et de la signature de mémo par le RSSI - Transmettre le mémo validé à l'équipe technique	Mémo d'approbation du changement
I.4. Test et préparation de la mise en œuvre du changement normal		
Equipe technique	Sur la base du mémo validé, - Elaborer le plan de test - Déterminer une procédure de retour en arrière - Documenter les solutions aux incidents connus qui surviendront - Prévoir un plan de restauration pour le cas où les changements ne réussiraient pas - Tester le changement dans un environnement de pré-production ; - Une fois les tests effectués et lorsque les résultats sont concluants, rédiger un memo soumis à la Direction Générale pour autoriser le déploiement. - Elaborer une procédure de déploiement - Informer toutes les parties prenantes du changement;	Mémo d'approbation du changement Document et plan de test
Direction Générale	- Validation du mémo d'autorisation de déploiement	Memo d'autorisation du déploiement du changement
I.5. Mise en Œuvre du changement normal		
Equipe technique	- Sauvegarder les systèmes avant changement. - Déployer le changement - Journaliser les opérations de changement	

Acteurs	Descriptions des tâches	Documents et interfaces
I.6. Vérification et examen du changement mis en œuvre		
❖ **Le changement concerne l'architecture réseau**		
Equipe technique	– Mettre à jour le schéma réseau ; – Mettre à jour la matrice justifiant les flux réseau; – Modifier les règles de filtrage réseau en fonction du changement ;	Rapport de déploiement
RSSI	– Réaliser des tests d'intrusion des éléments de segmentation.	Rapport de test
❖ **Le changement concerne l'installation d'un nouveau système**		
Equipe technique	– Appliquer les standards de configuration – Mettre à jour l'inventaire du périmètre PCI DSS	Rapport de déploiement
RSSI	– Inclure le nouveau système dans le périmètre des scans internes ; – S'il s'agit d'un nouveau type de serveur, réaliser des tests d'intrusion à l'encontre de celui-ci.	Rapport de déploiement
❖ **Le changement concerne un système, une base de données ou un média qui stocke des données de carte**		
Equipe technique	– Mettre à jour la politique de rétention et suppression des données de carte; – Si l'équipement concerné est mis hors service, supprimer les données de carte de manière sécurisée conformément à la procédure définie.	Rapport de déploiement
I.7. Clôture et documentation de la mise en œuvre du changement		
Equipe technique	– Rédiger le rapport de déploiement du changement. – Transmettre le rapport de déploiement du changement au Directeur du Système d'information pour validation	Rapport de déploiement

Acteurs	Descriptions des tâches	Documents et interfaces
Directeur du système d'information	- Valider le rapport de déploiement du changement - Archiver le rapport de déploiement du changement	Rapport de déploiement

Annexes / Enregistrements

- Mémo d'approbation du changement
- PV de réunion
- Document et plan de test
- Memo d'autorisation du déploiement du changement
- Rapport de déploiement

Liste des modifications

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

Rédigé par : RESPONSABLE SECURITE DES SYSTEMES D'INFORMATIONS	Validé par : COMITE DES PROCEDURES	Approuvé par : DIRECTION GENERALE
Date : 05/11/2025	Date : 05/11/2025	Date :
Signature :	Signature :	Signature :