



#### Objectif et champs d'application

La procédure « Assurer la sécurité du système d'information » a pour objectif de définir les différentes étapes intervenant dans la gestion de la sécurité du système d'information au sein de la Banque de l'Union Côte d'Ivoire (BDU-CI).

Cette procédure s'articule autour de deux (02) parties :

- Gestion des incidents ;
- Revue des accès administrateurs et mots de passe.

#### Objectifs du contrôle interne

- Garantir une gestion optimale des aspects sécuritaires du système d'information
- Garantir l'efficacité du dispositif sécuritaire relatif au système d'information au sein de la Banque de l'Union Côte d'Ivoire (BDU-CI)
- Prévenir les différents incidents émanant du système d'information de la BDU-CI
- Assurer le traitement efficace des incidents liés au système d'information de la BDU-CI

#### Rôles et responsabilités

##### Directeur Général

Sous la responsabilité du Conseil d'Administration, il a la charge de :

- Evaluer les incidents majeurs ;
- Convoquer la cellule de crise dans le cadre du traitement des incidents majeurs ;
- Participer à l'identification des plans d'actions à mener en vue du traitement des incidents majeurs.

##### Directeur de l'Audit Interne

Sous la responsabilité du Directeur Général, il a la charge de :

- Réaliser la mission d'audit relative à la revue des accès au Core Banking conformément au plan annuel d'Audit ;
- Elaborer un rapport de fin de mission et formuler des recommandations liées à la revue des accès.

##### Directeur des Systèmes d'information

Sous la responsabilité du Directeur Général, il a la charge de :

- Evaluer les incidents relatifs au système d'information ;
- Procéder au traitement des incidents relatifs au système d'information ;
- Mettre en œuvre des recommandations relatives à la revue des accès au Core Banking.



### **Agent de la DSI en charge de la Sécurité Opérationnelle**

Sous la responsabilité du Directeur des Systèmes d'Information, il a la charge de :

- Effectuer la revue des accès administrateurs ;
- Effectuer la revue des mots de passe des comptes utilisateurs ;
- Vérifier et valider la liste des administrateurs dans le système ;
- Vérifier et valider le paramétrage de mise à jour des mots de passe dans le système ;
- Effectuer la revue des accès aux salles informatiques et aux serveurs.
- Effectuer le traitement des alertes ;
- Procéder à la mise en œuvre des recommandations issues du rapport d'audit relatif à la revue des accès.

### **Sigles et Définitions**

#### ➤ Définitions

- **Antivirus** : solution informatique permettant de prévenir et traiter les menaces liées aux systèmes informatiques.
- **Compte utilisateur** : méthode d'exploitation permettant l'ouverture d'une session donnant des droits d'accès aux différents éléments du système ainsi qu'à une interface homme machine personnalisée.
- **Core Banking** : logiciel ou solution informatique mise en place par les institutions bancaires pour rassembler tous les composants requis et pertinents permettant de gérer les opérations financières des clients.
- **Incident** : évènement dont la survenance est susceptible d'impacter l'activité et la situation financière d'une entreprise.
- **Pare-feu** : logiciel ou un matériel de sécurité capable de surveiller et de contrôler le trafic réseau, tant entrant que sortant.
- **Serveur** : dispositif informatique permettant de répartir les tâches sur différents ordinateurs et les rendre accessibles à plusieurs utilisateurs finaux de manière indépendante.
- **Security Operations Center** : ensemble de personnes, de processus et de technologies responsables de la surveillance, de l'analyse et de la préservation de la sécurité des informations d'une entreprise.
- **Système d'information** : ensemble de composants interconnectés utilisé pour le fonctionnement d'une organisation et permettant de collecter, stocker, traiter et diffuser les données dans un but précis.
- **Cellule de crise** : équipe constituée de membres de différentes directions, convoquée par le Directeur Général à la suite de la survenance d'un incident majeur. La cellule de crise a pour objectif d'identifier les plans d'actions à mener dans le cadre de la gestion des incidents majeurs.



➤ **Sigles**

- BDU-CI : Banque de Développement du Mali
- DAI : Directeur de l'Audit Interne
- DG : Directeur Général
- DSI : Directeur des Systèmes d'Information
- OTP : One-Time Password (mot de passe à usage unique)
- RSSI : Responsable Sécurité des Systèmes d'Information
- SOC : Security Operations Center
- ADSISO : Agent de la DSI en charge de la Sécurité Opérationnelle
- VPN : Virtual Private Network (réseau virtuel privé)

Sommaire de la procédure

I.	Gestion des incidents.....	4
II.	Revue des accès administrateurs et mots de passe.....	4
1.	Revue des accès du Core Banking.....	4
2.	Revue des accès administrateurs.....	4
3.	Revue des mots de passe .....	5
4.	Revue des accès à la salle informatique et aux serveurs .....	5

Références / Règles de gestion

➤ **Documents de références**

- N/A

➤ **Règles de gestion**

- Au sein de la Banque de l'Union Côte d'Ivoire (BDU-CI), les incidents doivent être classés et traités en fonction de leur nature et leur impact sur les activités de l'entreprise. Il s'agit :
  - Des incidents classés mineurs : incidents non susceptibles d'engendrer des pertes financières et/ ou d'impacter l'activité de la BDU-CI. Ces incidents doivent être traités et clôturés au sein de la DSI ;
  - Des incidents classés majeurs : incidents susceptibles d'engendrer des pertes financières et de perturber l'activité de la BDU-CI. Les incidents majeurs doivent être remontés à la Direction Générale et nécessitent la tenue d'une cellule de crise.
- Les mises à jour des mots de passe des comptes utilisateurs au sein de la BDU-CI doivent se faire de manière automatique en fonction des paramétrages des différentes plateformes utilisées :
  - Active Directory : 90 jours ;
  - Microsoft 365 : authentification multi facteur (mot de passe + OTP).



Narratif de la procédure

PRO IS14 007	Assurer la sécurité du système d'information	Agent DSI, DCPC, SGGR, DAI, DG, Directeur d'entité, DSI, Membres de la cellule de crise
--------------	--	---

Acteurs	Descriptions des tâches	Documents et interfaces
<b>I. Gestion des incidents</b>		
Se référer à la procédure « gérer les risques opérationnels » du SGGR		
<b>II. Revue des accès administrateurs et mots de passe</b>		
<b>1. Revue des accès du Core Banking</b>		
DSI	<ul style="list-style-type: none"> <li>- Recevoir du Directeur de l'Audit Interne (DAI) l'email de mise à disposition des listes des comptes utilisateurs actifs et suspendus dans le cadre de la réalisation de la mission d'Audit</li> <li>- Elaborer la liste des comptes des utilisateurs et la transmettre par email au DAI</li> </ul>	Liste des comptes utilisateurs actifs/ Utilisateurs suspendus
DAI	<ul style="list-style-type: none"> <li>- Recevoir par email du DSI la liste des comptes utilisateurs actifs/utilisateurs suspendus</li> <li>- Réaliser sa mission d'audit conformément à la procédure Réaliser les activités d'audit interne (Elaborer le plan d'audit interne, réaliser les missions, suivre les recommandations)</li> </ul>	
DSI	<ul style="list-style-type: none"> <li>- Au terme de la mission d'audit, recevoir physiquement du DAI, le rapport de fin de mission d'audit interne</li> <li>- Procéder à la mise en œuvre des recommandations</li> </ul>	Rapport de fin de mission d'audit interne
<b>2. Revue des accès administrateurs</b>		
Agent de la DSI en charge de la Sécurité Opérationnelle (ADISO)	<ul style="list-style-type: none"> <li>- Se connecter aux différentes plateformes utilisées et éditer la liste des administrateurs et leurs droits</li> <li>- C2 : Vérifier que : <ul style="list-style-type: none"> <li>• Les droits des administrateurs sont conformes</li> <li>• Les droits du personnel ne faisant plus partie de la BDU-CI sont suspendus</li> </ul> </li> <li>- En cas de non-conformité des droits, procéder à leurs mises à jour conformément aux habilitations des administrateurs sous la supervision du DSI</li> </ul>	Liste des administrateurs et leurs droits



Acteurs	Descriptions des tâches	Documents et interfaces
	<ul style="list-style-type: none"> <li>- En cas de droits actifs du personnel ne faisant plus partie de la BDU-CI, procéder à la suspension immédiate de ces droits</li> <li>- En cas de conformité des droits des administrateurs, valider la liste des administrateurs dans le système</li> </ul>	
<b>3. Revue des mots de passe</b>		
ADISO	<ul style="list-style-type: none"> <li>- Se connecter aux différentes plateformes (Active Directory, Microsoft 365)</li> <li>- C3 : Vérifier que les changements de mot de passe sont correctement paramétrés sur les différentes plateformes</li> <li>- En cas de paramétrage incorrect, paramétrier de façon correcte les changements des mots de passe</li> <li>- En cas de paramétrage correct, valider le paramétrage dans le système</li> </ul>	
<b>4. Revue des accès à la salle informatique et aux serveurs</b>		
	Cette partie se déroule conformément au II.2. Revue des accès administrateurs	

#### Annexes / Enregistrements

- Liste des administrateurs et leurs droits
- Liste des comptes utilisateurs actifs/utilisateurs suspendus
- Rapport d'incident mensuel
- Rapport de mission d'audit interne
- Rapport journalier de traitement d'incident

#### Liste des ampliations

Nº	Structures	Date	Visa	Observations
01				
02				



**BDU - CI**  
LA BANQUE DE L'UNION

Processus : Gérer le système d'information

Sous-Processus : Assurer la sécurité du système d'information

Pilote et Co-pilote du processus : Direction des systèmes d'information

Référence : PRO 004  
N° de version : 1  
Date d'émission : Septembre 2024  
Page : 6 / 6

Liste des modifications

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

Rédigé par : Direction des Systèmes d'Information

Date : Septembre 2024

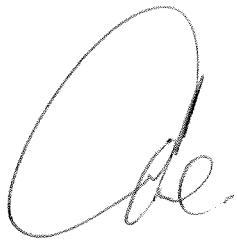
Signature :

  
20 Sept 2024

Validé par : Comité Pro

Date : 01/10/2024

Signature :



Approuvé par :

Date :

Signature :

