I. Objectif et champs d'application

Cette procédure a pour objet de définir les règles, responsabilités et modalités pratiques relatives aux opérations de sauvegarde et de restauration des données, systèmes et infrastructures critiques de la Banque de l'Union – Côte d'Ivoire (BDU-CI).

Elle vise à garantir :

- La disponibilité, l'intégrité et la confidentialité des données sauvegardées ;
- La capacité de restauration rapide et fiable en cas d'incident, cyberattaque ou sinistre ;
- Le respect des exigences réglementaires (BCEAO, PCI DSS, ISO 27001) et contractuelles.

Cette procédure s'applique à :

- Tous les environnements (production, préproduction, test, développement) ;
- Tous les collaborateurs, administrateurs, prestataires et partenaires impliqués dans les opérations de sauvegarde ou restauration ;
- Tous les sites de la BDU-CI (siège, agences, sites distants).

II. Objectifs de la procédure

- Définir un cadre rigoureux pour la planification, l'exécution et le suivi des sauvegardes.
- Assurer la traçabilité et la sécurisation des sauvegardes et des restaurations.
- Garantir le respect des RPO (Recovery Point Objective) et RTO (Recovery Time Objective).
- Réduire les risques de perte de données, de corruption ou de compromission.
- Assurer une amélioration continue par le biais de tests réguliers et de contrôles périodiques.

III. Rôles et responsabilités

RÔLE	RESPONSABILITÉ

Direction Générale	Allouer les ressources nécessaires (humaines, techniques, financières).
RSSI	Valider les exigences de sécurité (chiffrement, isolation, traçabilité) ; Superviser la conformité et évaluer les risques ; Déclencher la gestion d'incident en cas d'anomalie critique.
DSI	Définir et mettre en œuvre les plans de sauvegarde/restauration ; Maintenir l'infrastructure de sauvegarde ; Piloter les opérations et documenter les dispositifs.
Responsables métiers / applicatifs	Identifier les données critiques et exigences RPO/RTO ; Valider les tests de restauration pour leur périmètre ; Signaler toute évolution impactant le dispositif.
Administrateurs systèmes, réseaux et sauvegardes	Exécuter les sauvegardes et restaurations ; Configurer et maintenir les solutions ; Surveiller les journaux et traiter les anomalies.
Utilisateurs	Stocker les fichiers professionnels uniquement dans les répertoires sauvegardés ; Signaler les besoins ou incidents liés à la perte de données.
Direction de l'Audit Interne	Réaliser des contrôles annuels de conformité et formuler des recommandations.

IV. Sigles et Définitions

➢ Définitions

Sauvegarde complète : copie intégrale des données d'un système.

Sauvegarde différentielle : copie des données modifiées depuis la dernière complète.

Sauvegarde incrémentielle : copie des données modifiées depuis la dernière sauvegarde (complète ou incrémentielle).

Règle 3-2-1 : Bonnes pratiques de sauvegarde consistant à conserver 3 copies des données, sur 2 supports différents, dont 1 hors ligne ou externalisée.

Test de restauration : Simulation contrôlée d'une opération de récupération des données pour vérifier l'efficacité, la rapidité et la conformité du processus.

➢ Sigles

RPO : durée maximale acceptable de perte de données.

RTO : délai maximal pour restaurer un service après incident.

ART (Actual Recovery Time) : Temps réellement constaté pour la restauration d'un service après un incident.

CDE (Cardholder Data Environment) : Environnement où sont stockées, traitées ou transmises les données de cartes de paiement (PCI DSS).

DEX : Dossier d'Exploitation regroupant la documentation technique et opérationnelle liée aux systèmes sauvegardés.

WORM (Write Once, Read Many) : Technologie garantissant qu'une donnée ne peut être modifiée ni supprimée après son enregistrement initial.

Sommaire de la procédure

V. Références / Règles de gestion

❖ Documents de références

- Norme ISO/IEC 27001 : 2022 ;
- Politique de sécurité des systèmes d'information de la BDU-CI ;
- Politique de sauvegarde et de restauration BDU-CI – V01 ;
- PCA et PRA de la BDU-CI.

❖ Liste des éléments concernés par la présente procédure de sauvegarde.

- Bases de données applicatives ;
- Les configurations réseaux critiques ;
- Les VM(s) critiques ;
- Logs critiques.

❖ **Règles de gestion (Processus opérationnels des sauvegardes de la Banque)**

➢ **Planification et classification des sauvegardes**

- Définir les fréquences : quotidienne, hebdomadaire, mensuelle, annuelle.
- Respecter la règle **3-2-1** : 3 copies, sur 2 supports différents, dont 1 hors ligne.
- Appliquer les durées de rétention définies (14 jours, 5 semaines, 12 mois, archivage annuel).
- Documenter les périmètres sauvegardés (DEX, fiches de sauvegarde).

➢ **Exécution des sauvegardes**

- Automatiser les sauvegardes via un logiciel centralisé.
- Chiffrer systématiquement les données sensibles (AES 256 minimum).
- Journaliser toutes les opérations (horodatage, logs d'erreur, etc.).
- En cas d'échec, analyser, corriger, relancer et documenter.

➢ **Surveillance et contrôle**

- Contrôles de 1er niveau : DSI → Suivi quotidien, hebdomadaire et mensuel.
- Contrôles de 2e niveau : RSSI → Audits de conformité et sécurité (conformément aux DEX, fiches de sauvegarde établies et au plan de contrôle).
- Contrôles de 3e niveau : Audit interne → vérification annuelle.
- Supervision automatisée (SIEM, alertes DLP, etc.).

➢ **Gestion des restaurations**

- La demande de restauration est formalisée (formulaire, justification, périmètre, etc.).
- La DSI sélectionne la sauvegarde valide (contrôle des hash, journaux, etc.).
- L'opération est réalisée par un administrateur autorisé, via un poste et réseau dédiés.
- Vérification post-restauration : intégrité des données + validation métier.
- Rapport de restauration rédigé et archivé.

➢ **Tests de restauration**

- Core Banking : tous les 3 mois en test + tous les 5 ans en production.
- Applications métiers sensibles : 1 test complet/2an + restaurations ciblées/trimestriel.
- Infrastructure technique : restauration des configurations réseau et serveurs (6 mois).
- Postes de travail sensibles : restauration sur demande + restaurations ciblées/trimestriel + sensibilisation des utilisateurs.

➢ **Gestion des anomalies et incidents**

- Échec mineur : relance immédiate, correction par DSI.
- Incident majeur (ex. ransomware) : isolement immédiat de l'infrastructure de sauvegarde, alerte au RSSI, déclenchement du PCA/PRA.
- Tout incident documenté dans le registre ITSM.

➢ **Amélioration continue**

- Revues semestrielles du périmètre de sauvegarde.
- Mises à jour des procédures après tout incident ou évolution majeure.
- Sensibilisation régulière des collaborateurs.

❖ **Règles de gestion (Liste des tâches des Administrateurs Systèmes & Sauvegarde)**

➢ **Rappel du plan de reprise informatique (PRI) de la BDU-CI :**

Une procédure de restauration détaillé est donnée par niveau de priorité à la page 43 du **PRI** :

- Il faut d'abord restaurer les infrastructures réseau **(niveau 4) ;**
- Il faut ensuite restaurer les hôtes/cluster/VM qui constitut le **(niveau 3)** ;
- Il faut ensuite restaurer les bases de données et les applications **(niveau 2)** ;
- Et en dernière position restaurer les applications de connexion utilisateurs **(niveau 1).**

La remise en service du réseau constitue un prérequis indispensable à toute autre opération. Ce paramètre doit être intégré et pris en compte dans la procédure de sauvegarde et de restauration.

Priorité de restauration des serveurs : une fois la connectivité rétablie, procéder d'abord à la restauration des services essentiels (Active Directory, DNS, serveurs de fichiers, messagerie Exchange, etc.), puis des applications métiers, et enfin des bases de données ainsi que des serveurs de fichiers associés.

Les tableaux relatifs aux RTO, RPO et ART sont déjà établis, Il faut absolument en tenir compte. À titre d'exemple, pour l'application **AMPLITUDE** (Core Banking), les valeurs sont les suivantes : **RTO 0–4h**, **ART 1h** et **RPO 24h**. Le plan de reprise informatique recense également d'autres applications, assorties de leurs exigences spécifiques, qui doivent être prises en compte.

➢ **Actions quotidiennes des Administrateurs Systèmes & Sauvegarde :**

- **Contrôler l'intégrité des jobs de sauvegarde** : Les échecs et exécutions partielles doivent être recensés. Les jobs critiques, en particulier ceux liés au Core Banking, et/ou aux autres applications critiques de la Banque doivent faire l'objet d'une reprise immédiate, avec réexécution manuelle en cas d'absence d'auto-correction.

- **Vérification de l'atteinte du RPO :** pour chaque périmètre (**surtout pour les applications sensibles et stratégiques**), s'assurer que l'horodatage de la dernière copie récupérable est conforme au RPO défini (exemple : AMPLITUDE ≤ 24h). En cas de dérive, procéder à une escalade immédiate.

- **Supervision et journalisation :** analyser les alertes, anomalies et indicateurs de capacité (tampons disques, files d'attente, déduplication, bandes, etc.). Toutes les observations doivent être consignées, avec horodatage, dans le journal d'exploitation des sauvegardes.

- **Contrôle du chiffrement :** s'assurer que l'ensemble des jeux de sauvegarde classés comme **confidentiels** et **secrets** sont transmis et stockés en AES-256 (minimum), sans anomalie liée aux clés ou certificats.

- **Vérification de la réplication et des copies hors site :** contrôler l'état des répliques vers le site de repli et/ou vers le cloud (si utilisé), ainsi que la fraîcheur de la copie hors ligne du jour, lorsqu'elle est prévue.

- **Sécurisation de l'infrastructure de sauvegarde :** les connexions administratives doivent être effectuées exclusivement depuis un poste dédié et via le VLAN d'administration. Aucun compte Active Directory de production ne doit être utilisé dans l'environnement de sauvegarde.

- Lorsque la sauvegarde automatique n'est pas possible, l'administrateur de sauvegarde doit quotidiennement déconnecter les serveurs concernés afin de préparer l'opération de sauvegarde manuelle. La Division Exploitation exécute ensuite la commande prévue, après quoi l'administrateur se connecte au serveur de sauvegarde pour transférer les données. Trois copies distinctes sont systématiquement réalisées : une copie locale conservée sur le serveur d'origine, une seconde sur le site de sauvegarde (serveur backup du GOS) et une troisième transférée vers le site de Bamako pour assurer la redondance géographique. La copie originale n'est toutefois jamais supprimée, garantissant ainsi la disponibilité et l'intégrité des données sources.

➢ **Actions Hebdomadaire des Administrateurs Systèmes & Sauvegarde :**

- **Sauvegarde complète hebdomadaire :** exécuter les sauvegardes complètes planifiées pour les applications concernées ainsi que pour les configurations des équipements réseau (pare-feux, routeurs, switches).

- **Rotation et inventaire des supports :** gérer l'entrée et la sortie des bandes ou seaux, mettre à jour l'inventaire, contrôler l'intégrité des scellés et la traçabilité des mouvements, et vérifier l'état du coffre ainsi que du site externe.

- **Revue des exclusions :** s'assurer que tous les nouveaux répertoires et serveurs applicatifs sont correctement inclus dans la sauvegarde, sans omission d'agent ni de volume.

- **Capacité et rétention :** s'assurer que les durées de rétention définies (14 jours / 5 semaines / 12 mois) sont respectées sans purge anticipée. Ajuster les fenêtres de sauvegarde ou les capacités de stockage si nécessaire.

- **PCI/CDE :** effectuer un test ciblé de restauration d'un jeu de données PAN dans un environnement de test afin de valider l'absence de corrélation avec les données réelles et le respect des contrôles d'accès. Consigner les résultats dans le journal d'exploitation.

➢ **Actions mensuelles des Administrateurs Systèmes & Sauvegarde :**

Test de restauration scénarisé par niveau de priorité (PRI) :

- **N4 (réseau) :** restaurer une configuration de pare-feu et un switch dans un environnement laboratoire, dans leur format d'origine, afin de vérifier leur intégrité et leur conformité aux configurations prévues (**Chaque 6 mois**).
- **N3 (hôte/cluster/VM)** : restaurer une machine virtuelle non critique depuis la sauvegarde, en incluant la clé de déchiffrement. La restauration peut être effectuée en mode bare-metal pour les VM si nécessaire. Vérifier l'intégrité des données et mesurer le temps de restauration, puis comparer aux valeurs ART/RTO définies. Consigner l'ensemble des résultats dans la documentation appropriée (**Chaque 6 mois**).
- **N2 (base de données ou application) :** effectuer la restauration d'un fichier utilisateur sur un partage ainsi que d'un élément applicatif (ex. courriel ou objet de base de données non critique) dans un environnement bac à sable. Vérifier la lisibilité et l'intégrité des données restaurées, puis consigner le résultat du test (**Chaque 6 mois**).
- **Revue des RTO/RPO :** comparer les temps de restauration réels (ART observé) aux RTO cibles. Tout écart doit être signalé et accompagné d'un plan d'action correctif. Les tableaux PRI comportant des champs incomplets doivent être finalisés en collaboration avec les métiers concernés.

- **Audit du chiffrement et de la gestion des clés :** vérifier l'application des politiques de chiffrement AES-256 en transit et au repos, ainsi que la rotation et le stockage sécurisé des clés. Réaliser un test de restauration intégrant un déchiffrement de bout en bout afin de valider la conformité et l'intégrité du processus.

- **Revue de la sécurité de l'infrastructure de sauvegarde :** vérifier que l'authentification des systèmes de sauvegarde n'est pas liée à l'Active Directory de production. Réaliser des tests d'isolement d'urgence conformément au document opérationnel détaillé, simulant la coupure complète de l'infrastructure pour valider les procédures de confinement.

- **Rapport mensuel de sauvegarde :** inclure le taux de succès des jobs, les écarts constatés par rapport aux RPO, l'âge de la dernière copie hors ligne, les temps de restauration comparés aux RTO/ART, ainsi que les incidents et correctifs appliqués. Le rapport doit être diffusé à la DSI, au RSSI et aux métiers concernés.

➢ **Actions annuelles des Administrateurs Systèmes & Sauvegarde :**

- **Exercice de reprise complet « bout-en-bout » :** réaliser un exercice combinant simulation de scénario réalisée en salle de réunion (table-top) et tests techniques, couvrant les quatre niveaux de priorité (PRI) : réseau, hôtes/VM, bases de données et connexions utilisateurs. Mesurer formellement les temps de restauration et les RPO, et valider les résultats avec les métiers concernés.

- **Revue annuelle du périmètre de sauvegarde après évolutions du SI :** identifier les nouvelles applications, volumes et montées en charge, puis mettre à jour la documentation associée (DEX, fiches d'inventaire, procédures de restauration).

- **Contrôle des sites de stockage physique :** inspecter la sécurité des coffres et salles de bandes, vérifier les conditions environnementales et s'assurer du respect des procédures de transport des supports.

- **Archivage annuel et gestion de la rétention :** effectuer la purge et la rotation des archives conformément aux durées prévues (12 mois/annuelles), et réaliser un test de lisibilité sur un échantillon représentatif des archives.

- **CDE/PCI :** réaliser la revue de la cartographie des flux de données PAN et de la segmentation du CDE. Effectuer des tests de restauration afin de confirmer l'absence

de corrélation avec les données réelles (données tronquées, hachées, tokenisées ou chiffrées), et vérifier le respect des mécanismes WORM ainsi que la journalisation associée.

- **Mise à jour du PRI (sections 6.4.3/6.4.4) :** intégrer les retours d'expérience et assurer la complétude des tableaux RTO, RPO et ART.

➢ **Instructions opérationnelles détaillées :**

1. Reprise rapide d'un job en échec (quotidien)

- Pour tout job de sauvegarde échoué, identifier le job KO dans le tableau de bord, consulter les journaux d'exécution associés et qualifier l'incident en déterminant s'il s'agit d'un problème réseau, d'un agent défaillant ou d'un manque d'espace de stockage.

- Corriger la cause (par exemple : redémarrer l'agent, libérer de l'espace ou ajuster la fenêtre de sauvegarde) puis relancer le job.

- Si un deuxième échec survient pour une application sensible et/ou critique, procéder à une escalade immédiate auprès de la DSI et du RSSI conformément au niveau de priorité (PRI), en consignant l'horodatage et la cause de l'incident dans le journal d'exploitation.

2. Demande de restauration validée (à la demande)

- Enregistrer un ticket en précisant qui l'a émis, quel service ou application est concerné, où et quand l'incident ou la demande est survenu, ainsi que le motif, et obtenir la validation (approuver) correspondante.

- Effectuer la restauration dans un environnement contrôlé, de préférence en test d'abord, avec un accès strictement restreint et une journalisation complète de toutes les actions effectuées.

- Pour les données sensibles ou situées dans le CDE, seules les personnes autorisées doivent intervenir. Vérifier l'absence de corrélation avec les données réelles et effectuer un scan anti-malware avant toute réintégration dans l'environnement de production.

- En cas d'indisponibilité du logiciel de sauvegarde pour la restauration automatique, l'administrateur de sauvegarde se connecte au serveur concerné pour procéder à la restauration des données. Il commence par décompresser le fichier de sauvegarde nécessaire, puis lance le processus de restauration conformément aux procédures établies, afin de rétablir l'intégrité et la disponibilité des données sur le système cible.

3. **Sortie bande hors-ligne du jour (quotidien/hebdo)**
   - Étiqueter et chiffrer les supports (AES-256), les sceller et consigner toutes les opérations. Assurer le transport vers le site sécurisé en maintenant une traçabilité complète, puis mettre à jour l'inventaire logique et physique des supports.

4. **Test mensuel PRI par niveau**
   - **N4 (réseau) :** restaurer la configuration de sauvegarde des équipements Fortinet et des switches dans un environnement maîtrisé, puis valider la connectivité réseau.
   - **N3 (hôte/VM) :** restaurer une machine virtuelle depuis son image système et vérifier que le démarrage (boot) s'effectue correctement.
   - **N2 (base) :** restaurer une base de données et vérifier son intégrité en comparant les checksums et la volumétrie avec les valeurs attendues.

5. **Indicateurs simples à suivre**

   - **Suivi du taux de succès des jobs de sauvegarde**, en distinguant le taux global et celui des applications de classification sensible et stratégique.

- **Suivi des écarts de RPO** : contrôler la dérive maximale constatée pour chaque application afin de s'assurer du respect des objectifs de continuité définis.

- **Vérification de l'âge de la dernière copie hors-ligne** pour s'assurer que les sauvegardes déconnectées sont à jour et conformes aux exigences de rétention.

- **Suivi du pourcentage de tests de restauration réussis** afin d'évaluer l'efficacité et la fiabilité des procédures de reprise.

- **Analyse des écarts entre les RTO définis et les ART réellement observés** lors des restaurations, afin d'identifier les points d'amélioration du processus.

- **Vérification de l'inventaire des supports**, en s'assurant qu'il est conforme aux exigences liées aux tests, à la journalisation et à la rétention définies.

6. Écarts et améliorations

- Compléter les tableaux RTO, RPO et ART pour les équipements, bases et serveurs d'applications manquants, puis les faire valider par les métiers, étape indispensable pour piloter le respect des RPO et la planification des tests de restauration.

- Documenter la procédure d'isolement d'urgence de l'infrastructure de sauvegarde et la tester via une checklist et un exercice pratique afin de valider son efficacité.

- Formaliser le plan de sauvegarde (section 6.4.4) sous forme de matrice associant chaque application ou système au type de sauvegarde (complète, différentielle, incrémentielle), à la fréquence, à la rétention, au chiffrement, à l'emplacement (site, DR, cloud, hors-ligne) et aux tests associés.

Exemple de plan de sauvegarde pour l'application **Commandes Informix** avec les données suivantes (issues du plan de reprise informatique de la BDU-CI) :

- **Description de l'application :** Sauvegarde et restauration d'Amplitude ;
- **RTO :** 0 - 4 Heures ;
- **ART :** instantanée ;
- **RPO :** instantanée ;
- Application pris en charge par la DSI.

7. Plan de sauvegarde de Commandes Informix

Éléments	Type de sauvegarde	Fréquence	Rétention	Emplacement	test mensuel
BD Amplitude	Sauvegarde complète	Quotidienne	30 jours	Site principale + DR	6 mois
BD Amplitude	Sauvegarde/incrémentielle	Tous les 1h	48h	Site principale + DR	N/A
Fichier de config	Sauvegarde complète	Quotidienne	30 jours	Site principale + DR	6 mois
Logs Critiques	Sauvegarde complète	Quotidienne	30 jours	Site principale + DR	6 mois
Snapshots VM	Snapshot applicatif / base	Tous les 1h	24h	Site principale + DR	6 mois
Cloud optionnel	Sauvegarde complète	Quotidienne	30 jours	Cloud (optionnel)	6 mois
Cloud optionnel	Sauvegarde/incrémentielle	Tous les 1h	48h	Cloud (optionnel)	6 mois

NB : Un plan de sauvegarde officiel et validé doit être systématiquement élaboré pour chaque application classée comme sensible ou stratégique. Ce plan doit intégrer les paramètres RTO, RPO et ART définis dans le Plan de Reprise Informatique, validé conjointement par la DSI et les métiers. Il doit également être mis à jour régulièrement, conformément aux politiques et procédures en vigueur, ainsi qu'aux évolutions ou changements intervenant dans l'activité de la Banque.

VI. Narratif de la procédure		
PRO-RSSI-SSI-08	Procédure de gestion des sauvegardes et des restaurations	RSSI, DSI, Direction audit interne, Managers, users, Direction générale.

Acteurs	Descriptions des tâches	Outils et interfaces
I. <u>Procédure de gestion des sauvegardes et restaurations</u>		
Responsables métiers / applicatifs	– Identifier les données critiques de leur périmètre. – Définir les RPO/RTO avec la DSI. – Valider les tests de restauration. – Signaler les évolutions applicatives impactant les sauvegardes.	Registres métiers, PRI/PCA, DEX (dossiers d'exploitation), Formulaires de demande
Utilisateurs	– Stocker leurs données uniquement dans les répertoires sauvegardés (OneDrive Pro, serveurs dédiés, etc.). – Signaler tout besoin de restauration via le canal officiel. – Ne pas manipuler directement les supports de sauvegarde.	OneDrive Pro, Serveurs fichiers BDU-CI, Formulaire ITSM, Email pro
Administrateurs systèmes & sauvegarde	– Configurer et exécuter les sauvegardes automatiques (complètes, différentielles, incrémentielles). – Surveiller les journaux d'exécution et corriger les anomalies. – Chiffrer toutes les sauvegardes sensibles (AES 256). – Gérer les supports (bande, disque, cloud, hors ligne). – Réaliser les restaurations sur demande validée.	Logiciels de sauvegarde centralisés, Consoles d'administration, SIEM, Solutions de chiffrement, Réseau d'administration isolé
DSI	– Définir et maintenir la stratégie de sauvegarde (3-2-1). – Valider les plans de sauvegarde/restauration. – Piloter la gestion des incidents liés aux sauvegardes. – Assurer la documentation et la traçabilité (DEX, fiches de sauvegarde, inventaire).	Outil ITSM, Rapports périodiques, DEX, Catalogue de sauvegardes, PRI/PCA

Acteurs	Descriptions des tâches	Outils et interfaces
	– Lancer les tests périodiques de restauration. – Assurer la conformité réglementaire (BCEAO, PCI DSS).	
RSSI	– Valider les mesures de sécurité associées (isolement, chiffrement, traçabilité). – Contrôler la conformité et superviser la gestion des incidents. – Déclencher des audits SSI spécifiques après anomalies critiques. – Superviser les tests de restauration CDE (PCI DSS).	SIEM, Rapports de conformité, Outil ITSM, Journal d'incidents
Direction de l'Audit Interne	– Réaliser les contrôles de niveau 3 sur les dispositifs de sauvegarde/restauration. – Vérifier la traçabilité, la conformité et l'efficacité des mesures. – Formuler des recommandations et assurer le suivi correctif.	Rapports d'audit, Checklists de conformité, Documentation interne

Annexes / Enregistrements

Plan de sauvegarde des applications sensibles et des configurations à caractère critique

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