I. Objectif et champs d'application

Cette procédure a pour objet de définir les règles, responsabilités et modalités pratiques de classification des **applications critiques** utilisées par la Banque de l'Union – Côte d'Ivoire (BDU-CI). Elle vise à garantir que chaque application, en fonction de sa sensibilité et de son rôle dans les processus métiers, soit correctement classifiée afin d'assurer :

- La disponibilité des services essentiels ;
- La confidentialité et l'intégrité des données traitées ;
- La conformité réglementaire ;
- La continuité des activités en cas d'incident.

Elle s'applique à toutes les applications internes et externes utilisées par la BDU-CI (core banking, ERP, solutions de messagerie, GED, bases de données, applications métiers, cloud SaaS, etc.).

II. Objectifs de la procédure

- Définir un niveau de criticité pour chaque application de la Banque.
- Adapter les mesures de sécurité et de résilience selon la classification.
- Réduire les risques d'indisponibilité, de compromission ou de perte de données ;
- Permettre une gestion efficace des plans de continuité et de reprise d'activité ;
- Renforcer la traçabilité, le suivi et la gouvernance applicative.

III. Rôles et responsabilités

RÔLE	RESPONSABILITÉ
Direction Générale	Assurer les moyens nécessaires à la gestion sécurisée des applications critiques.
RSSI	Définir les règles de classification applicative, superviser la mise en œuvre, assurer la sensibilisation. Le RSSI est responsable du registre de la classification des applications de la Banque.

DSI	Appliquer les mesures techniques (segmentation, durcissement, sauvegardes, supervision, PRA/PCA).
Managers et Directeurs métiers	Identifier les applications utilisées dans leur périmètre, proposer la classification adéquate.
USER	Utiliser les applications conformément à leur classification, signaler toute anomalie.
Direction de l'Audit Interne	Contrôler périodiquement l'application de cette procédure.

IV. Sigles et Définitions

- **Définitions**

Classification des applications : Processus consistant à catégoriser les applications de la Banque (Publique, Interne, Confidentielle, Critique/Secrète) selon leur importance, leur sensibilité et l'impact potentiel de leur compromission ou indisponibilité.

Application critique (sensible ou stratégique) : Application dont l'indisponibilité, la compromission ou la perte d'intégrité aurait un impact majeur sur les opérations, la conformité réglementaire ou la réputation de la Banque (ex. : Core Banking, systèmes de paiement, cryptographie, etc.).

Inventaire central des applications (CMDB) : Base de données centralisée qui recense toutes les applications utilisées par la Banque, avec leurs caractéristiques (description, responsables, dépendances, niveau de classification).

Métadonnées de classification : Informations techniques associées à chaque application (niveau de classification, responsables, dépendances critiques, exigences de sécurité, etc.) permettant la traçabilité et la gestion dans les outils de supervision.

Sigles

CMDB : Configuration Management DataBase (base de gestion des applications et actifs technologiques).

GED : Gestion Électronique des Documents (outil transverse).

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 classification des actifs informationnels et technologiques de la BDU-CI

❖ Règles de gestion (Processus de classification des applications de la BANQUE)

➢ Identification des applications

Chaque direction métier, en collaboration avec la DSI, dresse la liste des applications utilisées dans son périmètre. Les applications identifiées doivent inclure :

- ➢ Applications métiers critiques (Core Banking, paiements, crédits, etc.) ;
- ➢ Applications de support (RH, finance, comptabilité, etc.) ;
- ➢ Outils transverses (messagerie, GED, collaboration, sécurité, etc.).

Les informations à collecter comprennent : nom de l'application, description, usage métier, données traitées, dépendances techniques et critiques, responsables applicatifs (métier & technique), éventuellement d'autres informations que l'équipe trouvera pertinentes.

➢ **Attribution du niveau de classification**

Chaque application est classifiée selon les critères définis dans la politique de classification de la BDU-CI :

- **Confidentialité des données traitées** (ex. données clients, financières, réglementaires, etc.).
- **Disponibilité requise** (24/7, heures ouvrées, tolérance à l'interruption).
- **Intégrité des informations** (impact d'une altération des données).
- **Dépendance métier** (impact direct sur les processus métiers critiques).
- **Conformité réglementaire** (ex. BCEAO, lois locales, RGPD, LCB-FT).

Le niveau attribué (Non critique, Importante, Sensible et Stratégique) est attribué par le Responsable Métier et la DSI, puis consigné dans le registre de classification des applications.

➢ **Marquage et traçabilité**

Chaque application doit être documentée dans l'inventaire central des applications de la Banque avec son niveau de classification.

Les métadonnées de classification doivent être intégrées dans les outils de gestion (CMDB / ITSM, etc.).

Les applications critiques (niveau **sensible** et **stratégique**) doivent faire l'objet de mesures de sécurité renforcées et validées par le RSSI : journalisation obligatoire, suivi d'accès, documentation des flux et dépendances, MFA, flux cryptés, surveillance SIEM, sauvegarde, inclus dans le dispositif PCA/PRA etc.

Ces mesures de sécurité renforcées concernant les applications critiques doivent faire l'objet d'audit de la part du service sécurité du système d'information au moins chaque année.

➢ **Révision périodique**

Les niveaux de classification sont revus au moins une fois par an ou en cas d'évolution majeure : changement d'usage, mise à jour fonctionnelle, migration technologique, nouvelle réglementation.

Toute nouvelle application doit être évaluée et classifiée **avant sa mise en production**.
Les résultats des revues sont transmis au RSSI et intégrés au plan d'audit interne.

- **Surveillance et contrôle**

Surveillance technique

Les contrôles d'accès aux applications sont basés sur le niveau de classification.
Vérification périodique du respect des exigences de sécurité (authentification, chiffrement, sauvegarde, PRA/PCA, etc.).
Tests réguliers de résilience des applications sensibles et stratégiques (ex. core banking, paiement, etc.).

Surveillance organisationnelle

Revue périodique des classifications par les responsables métiers et la DSI.
Audits internes chaque année pilotés par le RSSI pour vérifier la cohérence entre classification et mesures de sécurité appliquées.

- **Niveaux de classification des applications**

- **Niveau 1 – Application Non critique** : impact minimal sur les opérations en cas d'indisponibilité (ex. : Outils bureautiques standards, applications de formation, outil e-learning interne, etc.). Tout le monde peut y avoir accès sans problème et ne traite pas de données interne à la BDU-CI.
- **Niveau 2 – Application Importante** : Impact modéré en cas d'indisponibilité, mais activité globale non paralysée (ex. : reporting interne, etc.). Seuls les employés autorisés y ont accès et traitent des données internes de la BDU-CI.
- **Niveau 3 – Application Sensible** : Impact significatif en cas d'indisponibilité, pouvant affecter la productivité ou la relation client (ex. : Messagerie, GED, applications de gestion clients, etc.). Seuls les employés autorisés y ont accès et traitent des données confidentielles de la BDU-CI.
- **Niveau 4 – Application Stratégique** : Impact majeur sur la Banque en cas d'indisponibilité, compromission ou perte de données (ex. : Core Banking System,

système de paiement, systèmes de gestion cryptographique, etc.). Seuls les employés autorisés y ont accès et traitent des données confidentielles voire secrètes.

- **Signalement des anomalies de classification**

Tout collaborateur, prestataire ou administrateur constatant une **erreur de classification** ou une application critique (niveau **sensible** et **stratégique**) mal protégée doit :

1. Informer immédiatement le RSSI et la DSI.
2. Consigner l'anomalie dans l'outil ITSM ou registre des non-conformités.

- **Analyse et catégorisation des écarts de classification**

Écart de niveau 1 (mineur) : Une erreur de classification a été identifiée sur une application non critique, sans impact opérationnel. Cet écart devra être corrigé par le responsable applicatif.

Écart de niveau 2 (modéré) : Une application importante a été classifiée comme non critique. Le risque associé existe, mais reste limité. Cet écart doit être corrigé rapidement par le responsable applicatif, sous le suivi du RSSI.

Écart de niveau 3 (majeur) : Une application sensible a été classifiée à un niveau inférieur à celui requis, ce qui peut entraîner un impact significatif. Le traitement de cet écart doit être prioritaire et faire l'objet d'un rapport au Comité Sécurité.

Écart de niveau 4 (critique) : Une application stratégique (paiement, Core Banking) a été classifiée à un niveau inférieur ou n'est pas protégée conformément à son niveau requis. Cet écart doit faire l'objet d'une **escalade immédiate au Comité Sécurité** afin de définir un plan d'action et les mesures d'urgence appropriées.

- **Traitement des écarts de classification**

Mesures immédiates possibles : Les mesures immédiates pouvant être mises en œuvre (sans s'y limiter) incluent la restriction des accès, la suspension temporaire de l'application, ainsi que le confinement des usages sensibles.

Investigation : le Responsable Applicatif en charge de l'application, la DSI et le RSSI procèdent à une analyse conjointe afin d'identifier la cause de l'écart.

Mesures correctives : Les mesures correctives envisageables (sans s'y limiter), selon les cas, incluent le reclassement de l'application, le renforcement des habilitations, le durcissement des contrôles, ainsi que la mise à jour des plans de reprise et de continuité d'activité (PRA/PCA).

Suivi post-incident : mise à jour du registre des applications, capitalisation des retours d'expérience et sensibilisation des responsables métiers.

NB : Un écart de niveau 3 ou 4 sur une application critique doit être traité comme un **incident de sécurité majeur** conformément à la procédure de gestion des incidents.

VI. Narratif de la procédure		
PRO-RSSI-SSI-06	Procédure de gestion de la classification des applications critiques	RSSI, DSI, Direction audit interne, Managers, users, Direction générale.

Acteurs	Descriptions des tâches	Outils et interfaces
I. <u>Identification et classification initiale des applications</u>		
Directions métiers / Responsables applicatifs	– Identifier les applications utilisées dans leur périmètre (métiers, support, transverses). – Collecter les informations : nom, description, usage métier, données traitées, dépendances, responsables métier & technique. – Proposer un niveau de classification (non critique, Importante, Sensible, Stratégique). – Soumettre la proposition de classification à validation conjointe avec la DSI et le RSSI.	Registre de classification des applications, Inventaire central (CMDB), Fiches d'applications, Outil ITSM
DSI / RSSI	– Valider la classification attribuée selon les critères de confidentialité, disponibilité, intégrité, dépendance métier et conformité. – Documenter le niveau retenu dans l'inventaire central des applications. – Assurer la cohérence entre classification et contrôles sécurités.	Outil ITSM, CMDB, Documentation technique
II. <u>Marquage et traçabilité</u>		
Responsables applicatifs / DSI	– Documenter la classification dans l'inventaire central des applications. – Intégrer les métadonnées de classification dans la CMDB et les outils de suivi. – Mettre en place des journaux de traçabilité pour les applications critiques (sensibles et stratégiques). – Définir les flux applicatifs et dépendances critiques.	CMDB, ITSM, Outils de monitoring, Journaux applicatifs
III. <u>Révision périodique</u>		
Responsables métiers / DSI	– Réaliser une revue annuelle des classifications.	Registre de classification, Rapports

	– Réévaluer la classification en cas de changement majeur (migration, mise à jour, réglementation, etc). – Transmettre les résultats au RSSI pour consolidation et suivi.	d'audit interne, ITSM
IV. Surveillance et contrôle		
DSI / RSSI	– Mettre en place des contrôles techniques en fonction de la classification (authentification, chiffrement, PRA/PCA, sauvegarde, etc.). – Réaliser des tests réguliers de résilience sur les applications critiques. – Vérifier le respect des règles via audits et contrôles automatiques. – Suivre les incidents et les non-conformités.	Outils de supervision applicative, SIEM, DLP, Rapports d'audit, ITSM
V. Signalement et traitement des écarts		
Utilisateurs / Administrateurs	– Signaler toute erreur de classification ou protection insuffisante. – Documenter le cas dans l'outil ITSM et informer immédiatement la DSI/RSSI. – Appliquer les mesures correctives rapides sous supervision.	ITSM, Email professionnel, Registre des non-conformités
RSSI / DSI / Comité Sécurité	– Analyser et catégoriser les écarts (Niveau 1 à 4). – Définir et appliquer les mesures correctives : restriction d'accès, reclassement, PRA/PCA, sensibilisation, etc. – En cas d'écart de niveau 3 ou 4, escalade immédiate au Comité Sécurité et mise en œuvre du plan de remédiation.	ITSM, Procédures internes, Réunions de crise, Rapports d'incident
VI. Suivi et amélioration continue		
Direction Audit Interne	– Vérifier périodiquement la bonne application des règles de classification. – Identifier les écarts et proposer des actions correctives. – Suivre la mise en œuvre des recommandations. – Garantir la conformité aux normes ISO 27001 et à la politique SSI.	Rapports d'audit, Grilles de contrôle, Documentation interne

Annexes / Enregistrements

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 PROCEDURE	Approuvé par : DIRECTION GENERALE
Date : 05/11/2025	Date : 05/11/2025	Date :
Signature :	Signature :	Signature :