Objet et champs d'application

Cette procédure décrit le déroulement et toutes les dispositions pratiques permettant d'assurer une gestion efficace des risques liés à la sécurité de l'information liés aux projets et aux livrables tout au long du cycle de vie du projet. Elle s'appuie sur la procédure **<<Manager les projets>>** de la BDU-CI.

Cette procédure s'applique à l'ensemble des projets de la banque liés ou faisant intervenir les actifs suivantes de la banque:

- Les données de la banque ;
- Les données à caractère personnel ;
- Les biens incorporels (la propriété intellectuelle, la marque et la réputation) ;
- Le personnel (employés, personnel temporaire, contractants, bénévoles) ;
- Matériel, logiciel et services (serveurs, poste de travail, équipements réseaux et de sécurité, appareil mobiles, logiciel acheté ou conçu en interne) ;
- Sites et bâtiments (Sites, bâtiments, bureaux) ;
- Les archives physiques.

Il s'agit notamment de :

- Projets informatiques (nouveaux systèmes, migrations, applications web/mobile, etc.)
- Projets organisationnels (réorganisation des processus métier)
- Projets liés à la conformité réglementaire
- Projets d'infrastructure et de sécurité
- Nouveau produits
- Transformation disgitale

Objectifs de la procédure

Garantir que tous les projets bancaires intègrent la sécurité de l'information dès la phase de conception, afin de protéger les données, respecter les réglementations, réduire les risques et assurer la confiance des clients

Rôles et responsabilités

- **Chef de l'équipe projet**
  - Intégrer la sécurité dans le plan du projet ;
- **Comité de validation des Projets :**
  - Arbitrer les décisions de sécurité ayant un impact sur les délais et budgets
- **Le RSSI**

Chargé de :

- Evaluer les risques de sécurité liée à chaque projet de la banque
- Identifier les exigences de sécurité de l'information à prendre en compte dans les projets de la banque
- Identifier les exigences de conformité à prendre en compte dans les projets de la banque

Comité de demarrage et validation de projet

- **Le Chef de Service Organisation**

Sous la responsabilité du Directeur Général, il a en chargé de :

- Collecter et identifier les problématiques de sécurité débouchant sur des projets fonctionnels ;
- Vérifier et valider le Procès-Verbal (PV) de séance de validation des livrables de lancement des projets ;
- Examiner et valider le fonctionnement correct des outils informatiques implémentés par le prestataire
- Elaborer le compte-rendu (CR) de séance d'évaluation de projet ;
- Veiller à la présence du Responsable du RSSI au sein du Comité projet;
- s'assurer que les dossiers à soumettre au RSSI sont correctement constitués.

Sigles et Définitions

➢ Définitions

- **La gestion de la sécurité dans les projets** consiste à identifier, évaluer et atténuer les risques de sécurité, qu'ils soient informatiques, physiques ou liés à l'exploitation. Cette gestion comprend la planification, la mise en œuvre et le suivi des exigences de sécurité tout au long du cycle de vie du projet. En résumé, la gestion de la sécurité dans les projets est un processus continu qui vise à protéger les actifs du projet et à garantir la sécurité des personnes et des biens.
- **L'évaluation des risques de sécurité de l'information dans un projet** consiste à identifier, analyser et évaluer les risques potentiels qui pourraient compromettre la confidentialité, l'intégrité et la disponibilité des informations utilisées dans le projet.

➢ Sigles

RSSI : Responsable de la Sécurité du Système d'Information ;
BDU-CI : Banque de l'Union de Cote d'Ivoire ;
CSO : Chef de Service Organisation ;
CEP : Chef de l'Equipe Projet
PV : Procès-Verbal

Sommaire de la procédure

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
- Procédure interne **<< Manager les projets>>**
- **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

- Les risques liés à la sécurité de l'information doivent être évalués et traités dès le début et périodiquement tout au long de son cycle de vie;
- La délivrance d'un avis préalable du RSSI est subordonnée à une analyse des risques formalisée qui identifie de manière structurée les différents risques auxquels BDU-CI est exposée dans le cadre de la mise en service de tous nouveaux produits, services ou applications informatiques par rapport aux risques liées à la sécurité des informations de la Banque.
- Les avis du RSSI doivent être écrits, clairs et motivés. Ces avis sont généralement de 3 natures :
  - avis favorable sans réserve ;
  - avis favorable avec réserve(s);
  - avis défavorable en l'état.

Lorsque des réserves sont formulées, celle-ci doivent être précises et applicables.

Le RSSI doit s'assurer que ses avis sont appliqués en veillant à ce que :

- un avis négatif soit respecté ;

- les réserves éventuellement exprimées par Le RSSI soient levées avant le lancement du produit ou la réalisation du projet.

Le RSSI fait partie intégrante du comité de démarrage et de validation des projets

L'avis du RSSI est obligatoire mais consultatif, il ne saurait être décisionnaire. Cependant, lorsque le RSSI émet un avis défavorable, celui-ci ne peut rester lettre morte de la part du "Comité Projet" ou du Chef de Projet qui doivent en tenir compte en corrigeant les insuffisances qui ont motivé cet avis.

Aussi, en cas d'avis défavorable, le DG pourra décider de l'avis finale pour le lancement du projet e auprès de la Direction Générale peut être recherché qui appréciera les motifs de l'avis du RSSI et décidera de la conduite à tenir.. Tout doit en effet être mis en œuvre pour corriger les faiblesses identifiées par le RSSI.

Narratif de la procédure		
PRO-RSSI-SSI-02	Gestion de la sécurité dans les projets	

Acteurs	Descriptions des tâches	Documents et interfaces
I. Phase de conception et validation des projets		
I.1. Identification et analyse des risques (Collecte des problématiques)		
RSSI	– Identifier les actifs, menaces et vulnérabilités – Evaluer les risques (probabilité x impact) – Définir les mesures de traitement	Rapport évaluation des risques
I.2. Définition des exigences de sécurité (élaboration des livrables de lancement)		
RSSI	– Définir les exigences de sécurité à prendre en compte dans le cadre du projet – Transmettre le rapport au Responsable Organisation par mail ou physiquement	Rapport d'exigence
CSO	– Préparer la documentation pour la tenue du comité de démarrage et de validation du projet	
I.3. Validation des exigences de sécurité (validation des livrables de lancement des projets)		
CSO	– Convier par mail les membres du CVP à une séance de validation des exigences de sécurité	
Membres du CVP	– Valider les exigences de sécurité en mettre ne œuvre dans le cadre du projet	PV de séance
CSO	– Au terme de la réunion, élaborer le PV de séance de la rencontre du comité su de validation des exigences de sécurité – Soumission du PV au membre du comité pour signature	PV de séance
Membre du CVP	– Signature du PV	PV de séance
Phase de supervision de la mise en œuvre des projets		
I.4. Mise œuvre des exigences de sécurité validées		
Prestataire/équipe interne projet	– Mettre en œuvre les exigences de sécurité validées	
I.5. Suivi de la mise œuvre des exigences de sécurité		

Acteurs	Descriptions des tâches	Documents et interfaces
RSSI	– Effectuer des tests d'intrusion internes et externes – Effectuer des scans de vulnérabilités – Effectuer des tests de résilience – Définir le plan de reprise de la solution	
Prestataire	– Corriger les défaillances – Fournir les plans de reprise et de secours	
RSSI	– Donne son accord pour la mise en production de la solution	
RSSI	– Vérifier la conformité – S'assurer du fonctionnement des controles – Documenter le dossier sécurité	

Liste des modifications

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

Rédigé par : RESPONSABLE SECURITE SYSTEME D'INFORMATION	Validé par : COMITE PROCEDURES	Approuvé par : DIRECTION GENERALE
Date : 05/11/2025	Date : 05/11/2025	Date :
Signature :	Signature :	Signature :