



**Avis d'appel d'offres international**

La Banque Burundaise pour le Commerce et l'Investissement « BBCI » SM lance un avis d'appel d'offres international pour le recrutement d'un Cabinet chargé de réaliser l'audit de son système d'information.

Les Termes de Références peuvent être visités sur le site web de la Banque BBCI ou être retirés au secrétariat à la Direction Générale de la BBCI située à la l'adresse suivante : Chaussée du Peuple Murundi No 13, B.P : 2320 Bujumbura-Burundi, téléphone : (+257) 22 22 33 28 – fax : (+257) 22 22 33 39.

Les sociétés intéressées par cet avis d'appel d'offres devront soumettre leurs offres au plus tard le 27 juin 2025 à 17h00, heures de Bujumbura.

Fait à Bujumbura, le 23 Mai 2025

**Bernard KINYATA**

**Directeur de l'Administration  
et des Finances**



**Aude TOYI**

**Administrateur Directeur Général**

## TERMES DE REFERENCE POUR L'AUDIT DU SYSTEME D'INFORMATION DE LA BANQUE BURUNDAISE POUR LE COMMERCE ET L'INVESTISSEMENT (BBCI)

---

### 1. SIGLES ET ABBREVIATIONS

- SI : Système d'Information
- BBCI : Banque Burundaise pour le Commerce et l'Investissement
- COBIT: Control Objectives for Information Technologies
- ITIL : Information Technology Infrastructure Library
- ISO : International Standard Organization
- SGBD : Système de Gestion des Bases de Données
- RGPD : Règlement Général pour la Protection des Données
- API : Application Programming Interface
- ETL : Extract, Transform, Load
- LAN: Local Area Network
- WAN: Wide Area Network
- MPLS: Multi-Protocol Label Switching
- SD-WAN: Software Define Wide Area Network
- SLA : Service Level Agreement
- PCA : Plan de Continuité d'Activité
- PRA : Plan de Reprise d'Activité
- ITSM: Information Technology Service Management
- PSSI : Politique de Sécurité des Systèmes d'Information
- IAM: Identity and Access Management
- SOC : Security Operations Center
- SIEM: Security Information and Event Management
- BI: Business Intelligence
- COPIL : Comité de Pilotage
- SWOT: Strengths, Weaknesses, Opportunities and Threats

### 2. CONTEXTE

Dans un contexte de transformation digitale, la Banque Burundaise pour le Commerce et l'Investissement (BBCI) souhaite réaliser un audit complet de son Système d'Information (SI). Cet audit vise à évaluer l'adéquation, la performance, la sécurité et la gouvernance de l'ensemble des composantes du SI.

Il s'agit d'identifier les forces, les vulnérabilités, les obsolescences technologiques ainsi que les décalages par rapport aux meilleures pratiques et standards du secteur bancaire (COBIT, ITIL, ISO 27001, etc.).



Pour cela, la BCCI cherche un cabinet qualifié et disposant des ressources compétentes pour réaliser l'audit de son système d'information.

### 3. OBJECTIFS DE L'AUDIT

Les objectifs de l'audit du système d'information incluent :

- Auditer le système d'information dans sa globalité (Infrastructure, Systèmes, Core Banking et Applications métiers, Gouvernance, Organisation, etc.) ;
- Fournir une cartographie précise des risques du SI ;
- Apprécier le niveau de maturité IT et de digitalisation ;
- Vérifier la conformité avec les réglementations locales et internationales (RGPD, etc.)
- Evaluer le niveau de performance et de disponibilité de l'infrastructure informatique, y compris les ressources hébergées à l'extérieur ;
- Identifier les besoins en optimisation, rationalisation ou modernisation ;
- Analyser la capacité du système d'information à soutenir l'innovation, notamment sur le plan de la digitalisation ;
- Proposer un plan de mise à niveau et de transformation réaliste.

### 4. PORTÉE GÉNÉRALE DE LA MISSION

La mission d'audit couvre l'ensemble des Systèmes d'Information de la Banque, incluant les composantes suivantes :

- Les infrastructures physiques et logiques (réseaux, serveurs, systèmes, data centers) ;
- Le Core banking et autres applicatifs métiers (compensation, crédit, trésorerie, contrôle des opérations, reporting, logistique, etc.) ainsi que leurs bases de données ;
- La gouvernance, l'organisation, les compétences et les ressources humaines, les processus et procédures de gestion ;
- La sécurité de l'information et la gestion des risques informatiques ;
- La gestion et la valorisation des données.

La mission s'effectuera en présentiel et à distance.

### 5. PORTEE DETAILLEE DE LA MISSION

Afin d'assurer une évaluation complète et détaillée, l'audit sera organisé autour de plusieurs chantiers thématiques dont chacun correspond à un domaine critique du Système d'Information :

#### 5.1. Audit du Core Banking

Ce chantier a pour objectif d'évaluer l'efficacité, la robustesse, l'évolutivité et l'adéquation du système Core banking en place vis-à-vis des besoins fonctionnels actuels et futurs de la Banque.

Il devra aussi permettre d'identifier les forces, les faiblesses, les risques et les pistes d'amélioration du système Core banking. Cet audit portera notamment les aspects suivants :

- **Cartographie fonctionnelle du Core Banking** : recenser les modules installés (comptes, crédits, épargne, reporting, trésorerie, etc.), leur usage effectif, leur pertinence et leur couverture fonctionnelle.
- **Performance et fiabilité** : analyser les performances (temps de réponse, disponibilité, taux d'incidents), la capacité de traitement des opérations, les goulots d'étranglement et les limites techniques.
- **Interopérabilité et intégration** : évaluer les interfaces avec les autres systèmes (paiements, canaux digitaux, reporting réglementaire, comptabilité, etc.) ainsi que la qualité des échanges inter-systèmes.
- **Sécurité et traçabilité** : examiner les dispositifs de sécurité intégrés au Core Banking (profils utilisateurs, traçabilité des actions, gestion des accès) et leur conformité aux bonnes pratiques et normes en vigueur.
- **Support éditeur et maintenance** : vérifier la relation avec l'éditeur, les contrats de maintenance, la fréquence des mises à jour, le niveau d'autonomie interne et l'existence de compétences clés.
- **Évolutivité et alignement stratégique** : apprécier la capacité du système à évoluer avec les besoins métiers, l'ouverture à de nouveaux produits ou filiales, et la compatibilité avec les futures orientations stratégiques (digitalisation, ouverture multicanale, expansion régionale).

## 5.2. Autres applications et bases de données

Ce chantier concerne les autres logiciels utilisés par la Banque pour ses opérations métiers, supports et fonctions transverses. Il inclut :

- L'inventaire des applications (métiers, support, transverses) ;
- Les systèmes de gestion des bases de données (SGBD), de sauvegarde et de récupération, des données ;
- L'analyse des versions, de la couverture fonctionnelle et du cycle de vie ;
- L'interfaçage, les API, ETL, intégration avec le Core Banking ;
- Le taux de défaillance, la disponibilité, la gestion des incidents et le support éditeur ;
- Les coûts directs et indirects liés à l'exploitation et à la maintenance ;

## 5.3. Réseaux et Sécurité

Ce chantier vise à évaluer la qualité, la performance et la sécurité des infrastructures réseau de la Banque, sur les sites centraux et distants :

- La cartographie des interconnexions (LAN, WAN, MPLS, SD-WAN, etc.) ;
- L'analyse de la redondance, des points de défaillance et des débits ;
- La sécurité du réseau (firewalls, filtrage, segmentation, audits) ;
- La conformité avec les SLA opérateurs et l'optimisation des coûts ;
- La conformité aux bonnes pratiques de sécurité informatique ;

1 B

- L'analyse du plan de réponse aux incidents réseau et du plan d'évolutivité ;
- La vérification de l'adéquation des équipements et des configurations réseau.

#### 5.4. Infrastructures matérielles et systèmes

Il s'agit ici d'évaluer la robustesse, la performance et la maintenabilité des équipements informatiques et des environnements d'exploitation :

- Le parc des serveurs, les environnements de virtualisation, les systèmes d'exploitation ;
- La gestion du stockage, des sauvegardes, des restaurations, le Plan de continuité d'activité/Plan de reprise d'activité (PCA/PRA) ;
- La supervision et le monitoring, l'administration et la planification de la capacité ;
- L'analyse de la maintenance.

#### 5.5. Data centers

Ce chantier porte sur l'analyse des centres de données hébergeant les ressources critiques de la Banque. Il comprend :

- La visite des sites primaires et secondaires ;
- L'évaluation des conditions physiques (climatisation, alimentation, accès) ;
- La vérification de la certification (Tier, ISO), de la disponibilité, de la documentation ;
- L'examen des modalités de réplication et des tests de basculement ;
- La conformité des systèmes de détection et de réponse aux incidents (incendie, inondation, poussières).

#### 5.6. Gouvernance et organisation IT

L'objectif est d'évaluer comment la Direction des Systèmes d'Information (DSI) est structurée, pilotée et alignée avec la stratégie globale de la Banque. Ce chantier inclut :

- Les rôles, responsabilités, comités, schéma directeur ;
- Les processus ITSM (gestion des incidents, changements, mises en production) ;
- Les outils de pilotage, le reporting et l'alignement stratégique ;
- L'analyse des compétences, des formations et de la documentation interne.

#### 5.7. Cybersécurité et gestion des risques

Ce volet évalue la capacité de la Banque à prévenir, détecter, répondre et se rétablir face aux menaces numériques :

- Les politiques de sécurité des systèmes d'information (PSSI), les dispositifs de gestion des identités et accès (IAM) ;
- L'analyse des vulnérabilités, les tests d'intrusion, SOC/SIEM ;
- L'efficacité des outils de cybersécurité en place face aux différentes menaces actuelles ;
- L'étendue et le niveau d'exposition du système de la Banque aux cybermenaces ;
- La conformité et le réalisme du plan de reprise après sinistre ;

- La résilience du système, le niveau de préparation proactive de l'équipe IT, la gestion de crise et la sensibilisation du personnel.

#### 5.8. Gestion des données et Business Intelligence (BI)

Enfin, ce chantier porte sur la capacité de la Banque à maîtriser, structurer et valoriser ses données pour améliorer la prise de décision :

- La gouvernance, les propriétaires de données, la qualité et la traçabilité ;
- L'architecture des entrepôts de données, les outils de BI ;
- L'exploitabilité des données pour les décisions stratégiques.

### 6. DÉMARCHE MÉTHODOLOGIQUE ATTENDUE

Le soumissionnaire devrait suivre une méthode structurée en 5 phases :

- **Phase 0 : Cadrage de la mission**
  - Kick-off, identification des interlocuteurs
  - Collecte des documents de référence
- **Phase 1 : Diagnostic et collecte d'informations**
  - Entretiens ciblés avec les responsables IT et métiers
  - Relevés techniques, tests préliminaires
- **Phase 2 : Analyse des risques et benchmarking**
  - Évaluation comparative avec les standards internationaux
  - Identification des vulnérabilités, lacunes et risques critiques
- **Phase 3 : Recommandations et feuille de route**
  - Propositions concrètes d'amélioration et de mise en conformité
  - Estimation budgétaire et priorités
- **Phase 4 : Restitution et transfert de compétences**
  - Rapport final, synthèse exécutive et présentation au COPIL
  - Remise des livrables et support à la mise en œuvre

### 7. PROPOSITION DE PLANNING INDICATIF

Le soumissionnaire proposera un planning indicatif avec les phases ci-après :

| Phase                     | Durée |
|---------------------------|-------|
| Phase 0 : Cadrage         |       |
| Phase 1 : Diagnostic      |       |
| Phase 2 : Analyse         |       |
| Phase 3 : Recommandations |       |
| Phase 4 : Restitution     |       |

La durée maximale attendue est de deux (2) mois.

## 8. COMPOSITION DE L'ÉQUIPE PROJET ATTENDUE

La composition de l'équipe projet attendue du soumissionnaire est la suivante :

| Position                              | Rôles                                                                               | Niveau d'étude et Expérience                                                                             |
|---------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Chef de mission                       | Coordination globale, supervision, reporting, interlocuteur principal               | <ul style="list-style-type: none"> <li>Ingénieur ou BAC+5</li> <li>Plus de 8 ans d'expérience</li> </ul> |
| Expert infrastructures & systèmes     | Audit serveurs, stockage, virtualisation, PCA/PRA                                   | <ul style="list-style-type: none"> <li>Ingénieur ou BAC+5</li> <li>Plus de 8 ans d'expérience</li> </ul> |
| Expert réseaux et sécurité            | Audit LAN/WAN/SD-WAN, architecture réseau, firewalls, vulnérabilités, cybersécurité | <ul style="list-style-type: none"> <li>Ingénieur ou BAC+5</li> <li>Plus de 8 ans d'expérience</li> </ul> |
| Expert Core banking                   | Audit du Core Banking et d'autres applications métiers, interfaçage, cycle de vie   | <ul style="list-style-type: none"> <li>Ingénieur ou BAC+5</li> <li>Plus de 8 ans d'expérience</li> </ul> |
| Expert gouvernance IT / conformité    | Audit processus IT, alignement stratégique SI                                       | <ul style="list-style-type: none"> <li>Ingénieur ou BAC+5</li> <li>Plus de 8 ans d'expérience</li> </ul> |
| Expert data /BI /gestion de la donnée | Évaluation de la qualité, gouvernance et valorisation des données                   | <ul style="list-style-type: none"> <li>Ingénieur ou BAC+5</li> <li>Plus de 8 ans d'expérience</li> </ul> |

## 9. LIVRABLES ATTENDUS

Les livrables attendus sont :

- Un Rapport d'audit global et structuré du SI avec une vue particulière sur le Core banking ;
- Une Cartographie des risques IT et une matrice SWOT ;
- Un Plan des recommandations opérationnel et hiérarchisé (actions à court, moyen et long terme) ;
- Une Feuille de route de transformation du SI ;
- Un Support de présentation pour le COPIL.

## 10. PROFIL DU PRESTATAIRE RECHERCHÉ

Le cabinet retenu devra justifier des qualifications suivantes :

- Des références en audit SI bancaire, en particulier dans le contexte africain ;
- Une maîtrise des standards et cadres de référence internationaux (COBIT, ITIL, ISO 27001) ;
- Des compétences en conduite de projet avec une approche orientée résultats ;
- Une disponibilité d'une équipe pluridisciplinaire et expérimentée dans les métiers d'une banque.

### 11. VALIDITE ET DEPOT DES OFFRES

Les soumissionnaires seront engagés par leurs offres pour une durée de validité de soixante jours (60 jours) à compter de la date limite de dépôt des offres.

Les soumissionnaires doivent déposer une offre technique et une offre financière. L'offre technique devra comporter au moins les documents suivants :

- Une lettre de soumission signée ;
- La présentation de la société ;
- La méthodologie de travail ;
- Le planning indicatif des activités ;
- La composition de l'équipe alignée avec les CVs de chaque membre ;
- Les références des missions similaires avec description des travaux réalisés.

Les offres seront déposées électroniquement à l'adresse [joseph.ndayishimiye@bbcibank.com](mailto:joseph.ndayishimiye@bbcibank.com) au plus tard le 27/06/2025 à 17h00, heures de Bujumbura.

Pour toute information complémentaire, vous pouvez contacter M. Joseph NDAYISHIMIYE, tel +25771220598.

### 12. EVALUATION DES OFFRES

Les offres seront évaluées sur la base d'une pondération de l'offre technique à 60% et de l'offre financière à 40%.

