

**MINISTERE DE L'ECONOMIE NUMERIQUE,
DES POSTES ET DE LA
TRANSFORMATION DIGITALE** -====-

==
SECRETARIAT GENERAL

=====
**AGENCE NATIONALE DE PROMOTION
DES TIC**
=====



Burkina Faso
Unité – Progrès – Justice

Termes de référence

Recrutement d'un cabinet pour l'audit technique des plateformes.

Août 2021

Table des matières

I. Contexte et justification	3
II. Objectifs	3
1. Objectif global	3
2. Objectifs spécifiques	3
III. Résultats attendus	5
IV. Livrables attendus	5
V. Durée et déroulement de la mission	6
VI. Profil du cabinet de consultant	6
VII. Intrants fournis par le bénéficiaire	7
VIII. Financement	7

I. Contexte et justification

L'ambition du tout digital de l'administration Burkinabè pour accroître sa productivité et faciliter l'accès des services aux citoyens aux services va de pair avec une exposition de plus en plus grande des données manipulées par les plateformes qui dématérialisent les procédures si la conception, le développement et l'exploitation de celles-ci n'obéissent pas à certaines règles. De plus, les exigences des utilisateurs de plus en plus croissantes doivent être prises en compte pour mettre à disposition des plateformes performantes et qui répondent à ces exigences.

Les plateformes conçues telles que le Système Électronique de Gestion des documents (SIGED), le Circuit Intégré des Missions, le Système Intégré de Gestion des Établissements Publics de l'État (SIGEPE) et le Circuit Intégré des Missions (CIM) font face à ces contraintes et exigences.

La complétude des fonctionnalités, la correction et précision des résultats, la fiabilité, la tolérance de pannes, la facilité et la flexibilité de son utilisation, la simplicité, l'extensibilité, la compatibilité et la portabilité, la facilité de correction et de transformation, la performance, la cohérence et l'intégrité des informations qu'il contient sont tous des facteurs de qualité appréciables autour d'un logiciel.

Or, après le déploiement sur les sites pilotes, des difficultés techniques apparaissent. Elles sont entre autres, la complexité d'utilisation des solutions, la non-adéquation de certaines fonctionnalités aux attentes des utilisateurs, la lenteur constatée dans l'exécution de certaines fonctionnalités, les microcoupures fréquemment constatées, etc.

Pour mieux donc cerner le contenu de ces plateformes au niveau technique, des implications futures sur les choix techniques et technologiques, qu'est planifiée cette activité d'audit technique des plateformes majeures du e-Burkina. Cet audit portera alors une attention toute particulière sur l'architecture des applications, des codes, les technologies utilisées, les architectures de déploiement.

II. Objectifs

1. Objectif global

L'objectif global est d'effectuer un audit IT (configuration, architecture, code source, sécurité), et fonctionnel des plateformes SIGED, CIM, SIGEPE, e-Conseil des Ministres et des e-Services mais aussi du volet organisationnel de la gestion des plateformes.

2. Objectifs spécifiques

Spécifiquement, il s'agit de :

- A. Fournir une évaluation de l'état de la **résilience sécuritaire** des plateformes en :

- Effectuant une revue de code des applications ;
 - Testant la sécurité des applications à la recherche de vulnérabilités ;
 - Diagnostiquant l'intégrité des données des plateformes ;
 - Évaluant les risques sur toute la chaîne de développement, de maintenance et d'accès aux plateformes en production ;
 - Évaluant l'organisation de la gestion de la sécurité des applications et des infrastructures (matériels, réseau, locaux) ;
- B. Mettre en place, pour les plateformes, des politiques de protection et de sécurité adaptée au fonctionnement de l'Administration et à son système d'information ;
- C. Fournir une évaluation des **capacités fonctionnelle et extra-fonctionnelle** des plateformes en :
- Vérifiant que les plateformes résolvent les problèmes principaux des utilisateurs ;
 - Testant la fiabilité en termes de résistance aux erreurs des utilisateurs ou de services externes ;
 - Évaluant l'expérience utilisateur (UX), i.e., l'aisance d'utilisation à travers les éléments d'interfaces mis en place (tooltip, icônes, labels, ...) ;
 - Évaluant la performance d'exécution notamment en termes de temps de réponse au démarrage et aux actions clés essentielles aux fonctionnalités ;
- D. Fournir une évaluation de la maintenabilité des plateformes en :
- Vérifiant que le code respecte les standards et bonnes pratiques en génie logiciel (ex : documentation) et que la conception permet de maintenir les plateformes à moindre coût ;
 - Évaluant l'architecture des plateformes et des technologies utilisées ;
 - Évaluant l'adéquation de la conception et du fonctionnement des mécanismes de contrôle interne et des procédures d'exploitation ;
- E. Produire un rapport d'évaluation sur la base des cadres acceptables (par exemple, CISA) et prenant en compte :
- des propositions d'améliorations dans la stratégie de développement des plateformes;
 - une proposition d'organisation et des missions correspondantes;
 - des recommandations assorties d'un plan d'action pour corriger les vulnérabilités et réduire les risques
 - un plan d'action à court et moyen terme et des coûts y afférents.
- F. Elaborer un guide de conception et de développement de plateformes sécurisées ;
- G. Elaborer un guide de test des plateformes suivant les meilleures pratiques.

III. Résultats attendus

A l'issue de la mission, les résultats attendus sont :

- Une évaluation de l'état de la résilience sécuritaire est fournie ;
- Des politiques de protection et de sécurité adaptée au fonctionnement au fonctionnement des plateformes sont élaborées.
- Une évaluation des capacités fonctionnelle et extra-fonctionnelle des plateformes est fournie ;
- Une évaluation de la maintenabilité des plateformes est fournie ;
- Un rapport d'évaluation sur la base des cadres acceptables (par exemple, CISA) est produit ;
- Un guide de conception et de développement de plateformes sécurisées est fourni ;
- Un guide de test des plateformes est fourni ;

IV. Livrables attendus

Les rapports finaux devront inclure au minimum les sections suivantes :

- Une section relative à l'audit organisationnel et physique, fournissant l'ensemble des failles d'ordre organisationnel et physique et incluant la liste des recommandations à appliquer dans l'immédiat, en tenant compte des spécificités de l'Administration, de la classification des systèmes (criticité) et de la réalité actuelle des moyens humains et financiers.
- Une section relative aux audits techniques (test d'intrusion, audit d'architectures, audit de configuration, audit de code source), indiquant les vulnérabilités existantes, leur impact sur la pérennité des systèmes, en incluant des recommandations techniques à appliquer dans l'immédiat, concernant les moyens (réalistes) de correction des failles graves décelées.
- Une section relative à la partie analyse des risques fournissant une évaluation des risques résultant des menaces identifiées et des failles découvertes lors des phases d'audit organisationnel, physique et technique.
- Une section relative au plan d'action et stratégie de sécurité à appliquer sur le court terme, comprenant des recommandations précises quant aux mesures à prendre dans le court terme, afin de pallier les failles et insuffisances décelées, incluant tous les nécessaires organisationnels et techniques.
- Une section de synthèse, destinée aux décideurs, qui inclura d'une manière claire les importants résultats de l'estimation des risques, un résumé succinct des importantes mesures organisationnelles, physiques et techniques préconisées dans l'immédiat et sur le moyen terme, ainsi que les grandes lignes du plan d'action cadre proposé.
- Un dossier d'architecture technique et technologiques d'évolution des plateformes ;
- une présentation finale, synthétisant les points du rapport, présenté en séance ;
- un Guide de conception et de développement des plateformes sécurisées
- un Guide de test des plateformes suivant les meilleures pratiques

V. Durée et déroulement de la mission

La durée totale de la mission est de quatre (04) mois y compris les délais de réception, d'amendements et de validation des livrables.

Elle se déroulera en présentiel notamment pour toute les phases de collecte des données, de restitution et de validation des livrables.

VI. Profil du cabinet de consultant

Le cabinet de conseil devra être spécialisé dans les audits des systèmes d'information et remplir les exigences suivantes :

- Au moins cinq (05) ans d'expérience de conseil dans l'évaluation des SI similaires et des missions d'audit ;
- justifier au moins 03 marchés similaires sur les 05 dernières années en fournissant l'ensemble des justificatifs correspondants ;
- Avoir une compétence avérée dans la préparation des rapports d'audits, d'études et la capacité à les communiquer ;
- Avoir une expertise en gestion de grands projets de SI dans le Secteur Public en particulier ;

Il devra disposer du personnel minimum et qualification ci-après :

Poste	Diplôme /spécialité	Années d'expérience	Nombre de projets similaires au même poste (5 dernières années)
Un chef de mission	- BAC+5 en Informatique ou tout autre diplôme jugé équivalent, - Détenir la Certification CISA en cours de validité	10	03
Un Charge de l'audit des couches applicative	- BAC + 5 en Informatique option génie logiciel ou tout autre diplôme jugé équivalent, - Détenir l'une des certifications suivantes en cours de validité : CCNP R&S, CEH, CNA, CISM, ISO 27001, ISO 27002, ISO 27005	05	03
Un Chargé de l'audit de l'exploitation et la protection des avoirs informatiques	- BAC + 5 en sécurité des systèmes d'information ou en cyber sécurité autre diplôme jugé équivalent, - Détenir au moins l'une des certifications suivantes en cours de validité : CCNP R&S, CEH, CNA, Maitrise : ISO 27001, ISO 27002, ISO 2700, ECSA, CEI, CISSP, GCIH, GSEC,	05	03

La langue de travail est le Français. Tous les consultants devraient parler couramment la langue Française à l'orale comme à l'écrit.

VII. Intrants fournis par le bénéficiaire

Le maître d'ouvrage mettra à la disposition du soumissionnaire retenu :

- toute la documentation jugée utile par le soumissionnaire dont il dispose;
- toutes les facilités d'accès aux informations souhaitées ;
- deux agents de l'ANPTIC intégreront l'équipe du cabinet afin de suivre et participer à la réalisation de toutes les étapes de la mission ;
- un point focal pour tout besoin d'informations.

VIII. Financement

L'activité sera financée par le budget du projet e-Burkina en sa composante 2.