

TERMES DE REFERENCE

AFD CBJ 1280 02 F

MISSION D’EXPERTISE COURT TERME

**PENTEST**

Décembre 2025



# Informations générales

|  |  |
| --- | --- |
| Intitulé de la mission | Prestation de service pour le diagnostic de la sécurité (pentest) de SIGIBé et SyGMEF au profit de la Direction Générale des Impôts (DGI) |
| Bénéficiaire(s) | Direction Générale des Impôts |
| Pays | Bénin |
| Budget estimé | 30 000€, hors frais de déplacements et missions, pris en charge en supplément |

# Contexte et justification du besoin

Pour améliorer la mobilisation des ressources internes, le gouvernement du Bénin a mis en place, avec l’appui de l’Agence Française de Développement (AFD), le Projet d’Appui à la Modernisation du Système d’Information (PAMSI) au bénéfice de la Direction Générale des Impôts (DGI).

Le projet PAMSI vise à moderniser les systèmes d’information de la Direction Générale des Impôts (DGI) en vue d’accroître les performances de l’administration fiscale et améliorer la mobilisation des ressources intérieures. Il vise l’atteinte des objectifs spécifiques suivants :

* Amélioration des échanges et de l’analyse des données dans le SI (Composante 1) ;
* Renforcement de la dématérialisation des procédures et services (Composante 2) ;
* Amélioration des performances, de la fiabilité et de la sécurité du système d’information (Composante 3).

Afin d’assurer un accès fiable et sécurisé à ses services en ligne et de répondre au mieux aux attentes des contribuables, la DGI accorde une importance particulière à la sécurité et à la disponibilité de son système d’information. Compte tenu du contexte de menaces persistantes et de l’évolution constante des risques, toute faille de sécurité pourrait avoir des conséquences majeures sur l’atteinte des objectifs stratégiques de l’institution ainsi que sur le respect de ses obligations et engagements.

Dans une démarche d’amélioration continue, la DGI souhaite évaluer l’efficacité de ses dispositifs de sécurité et leur conformité aux référentiels en vigueur (politiques, standards, bonnes pratiques, etc.). Cette évaluation vise à identifier et à mettre en œuvre, le cas échéant, des mesures préventives, détectives et correctives complémentaires permettant de maintenir un niveau de risque maîtrisé et de renforcer la résilience globale du système d’information.

# Objectifs et résultats attendus

## Objectif général

L'objectif principal de la mission est de diagnostiquer la sécurité des applications SIGIBé et SyGMEF, et d’évaluer la conformité et l’efficacité des mesures de sécurité mises en œuvre au regard des standards et normes du domaine.

## Objectifs spécifiques

1. Réaliser les tests de pénétration internes, externes et applicatifs de SIGIBé et SYGMeF selon des scénarios de compromission réalistes : attaques externes depuis internet (adresses IP publiques, serveurs exposés, VPN, etc.), attaques par un invité ou un utilisateur connecté au réseau interne (postes utilisateurs, serveurs internes, contrôles d’accès, annuaire, etc.), tests applicatifs (injections, failles XSS, CSRF, etc.), en vue d’identifier les failles exploitables de l’infrastructure technique, des applications, des interfaces exposées et des environnements critiques ;
2. Évaluer la robustesse des mécanismes de contrôle d'accès, de segmentation réseau, de surveillance des journaux, de chiffrement des données, ainsi que les mesures de résilience (sauvegardes, continuité d’activité, etc.) mises en place pour atténuer les impacts d’une cyberattaque ;
3. Évaluer l’alignement du dispositif de sécurité aux normes et cadres de référence reconnus : ISO/IEC 27001, COBIT, CIS Benchmark, etc.
4. Examiner les processus de gestion des incidents, des habilitations et des accès à privilèges ;
5. Formuler des mesures de sécurisation et un plan d’action hiérarchisé pour corriger les failles de sécurité et prendre en charge les risques identifiés selon la criticité.

## Résultats à atteindre

Au terme de la mission du consultant, les résultats suivants sont attendus :

1. Le rapport d’audit est élaboré ;
2. Les mesures de sécurisation et le plan d’actions sont proposés pour corriger les failles de sécurité et prendre en charge les risques identifiés, hiérarchisées selon la criticité.

# Description de la mission

## Méthodologie

L’approche méthodologique à adopter pour la réalisation de la présente mission s’appuiera sur les normes, standards et référentiels reconnus en matière de tests d’intrusion, d’audit de la sécurité des systèmes d’information et de la gestion des risques de sécurité informatique :

* NIST SP 800-115 : Guide technique pour la planification et l’exécution de tests de sécurité
* CIS Benchmark : Guide de bonnes pratiques en matière de configurations sécurisées de composants technologiques ;
* ISO/IEC 27001 : Système de management de la sécurité de l'information (SMSI) ;
* ISO/IEC 27002 : Contrôles de la Sécurité de l’Information.

La démarche sera structurée en quatre (04) grandes étapes, chacune comportant des livrables spécifiques, des parties prenantes définies et un mode de communication adapté.

#### Phase I : cadrage

Le cabinet doit conduire une réunion de cadrage avec les parties prenantes de la mission. L’objectif de la phase de cadrage est de :

* S’accorder sur les objectifs de la mission, délimiter le périmètre et clarifier le mandat du consultant : ce qui est inclus / exclus, résultats attendus, etc.
* Identifier les parties prenantes ;
* Présenter l’approche méthodologique de conduite de la mission ;
* Noter les contraintes liées à la mission et évaluer les risques (par exemple la non-disponibilité de certaines parties prenantes), et estimer les ressources indispensables au succès de la mission (ressources humaines, matérielles, etc.) ;
* Préparer un check-list de la documentation nécessaire à la conduite de la mission : la structure organisationnelle de la DGI, les processus, la gouvernance de la sécurité, les aspects déontologiques et contractuels, etc. ;
* Elaborer un planning prévisionnel de la mission.

Une note de cadrage formalise les informations nécessaires pour cette phase.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Livrables |  | Parties prenantes |  | Modes de communication |
| 1. Note de cadrage | * Équipe projet DGI * RSSI * Cabinet d’audit * Equipe projet PAMSI | Réunion en présentiel |

#### Phase II : Planification

* Recueil d’informations :
* Préparer une check-list des éléments clés à auditer prioritairement ;
* Constituer une liste de contrôles à réaliser pour évaluer les pratiques de la DGI par rapport à la règlementation et aux meilleures pratiques ;
* Collecter la documentation nécessaire à la conduite de la mission ;
* Collecter un maximum d’information sur le SI (adresses IP, noms de domaine, services exposés, etc.) à l’aide des techniques appropriées.

* Définition du plan d’audit :
* Définir les ponts de contrôles à réaliser et leurs objectifs ;
* Définir les tests à réaliser et les ressources nécessaires.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Livrables |  | Parties prenantes |  | Modes de communication |
| 1. Liste exhaustive des éléments clés à auditer ; 2. Plan de tests détaillé. | * Équipe projet DGI * RSSI * Cabinet d’audit SSI * Equipe projet PAMSI | * Courriels * Échanges téléphoniques * Réunion de validation du plan en ligne * Accès aux systèmes pour la collecte d’information (adresses IP, noms de domaine, services exposés, etc.) à l’aide des techniques appropriées. |

#### Phase III : Réalisation

* Effectuer les Pentests et identifier les vecteurs d’attaque (ports ouverts, services actifs, versions logicielles, etc.), les vulnérabilités et les défauts de contrôle ou de configuration pouvant compromettre la sécurité des informations et des données ;
* Simuler l’exploitation des vulnérabilités identifiées ;
* Collecter les preuves et rédiger les constats dans un Tableau des Points d’Attention;
* Analyser la documentation et réaliser des entretiens stratégiques avec les acteurs clés ;
* Evaluer la conformité et l’efficacité des mesures de sécurité existantes au regard des référentiels et des normes des systèmes d'information par utilisation des différents outils de collecte pour recueillir les informations.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Eléments d'entrée |  | Livrables |  | Parties prenantes |  | Modes de communication |
| 1. Liste des éléments clés à auditer ; 2. Plan de tests détaillé | 1. Relevés des Constats d'audit 2. Journal de tests d’intrusion 3. Tableau des Points d’Attention | * Équipe projet DGI * RSSI * Cabinet d’audit SSI * Equipe projet PAMSI | * Entretien individuels en présentiel * Accès aux systèmes |

#### Phase IV : Elaboration du rapport provisoire

* Consolider l’ensemble des constats ;
* Hiérarchiser les risques ;
* Elaborer les différents rapports d’audit ;
* Proposer des recommandations ;
* Finaliser les rapports d’audit ainsi qu’un plan d’action de la mise en œuvre des recommandations.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Eléments d'entrée |  | Livrables |  | Parties prenantes |  | Modes de communication |
| 1. Relevés des Constats d'audit 2. Journal de tests d’intrusion 3. Tableau des Points d’Attention | 1. Rapport provisoire d’audit avec recommandations et plan d‘actions 2. Support de présentation | * Équipe projet DGI * RSSI * Cabinet d’audit SSI * Equipe projet PAMSI | * Courriels * Échanges téléphoniques * Réunion de validation du rapport en ligne |

#### Phase V : Validation du rapport provisoire

Une rencontre de validation du rapport d’audit provisoire sera organisée deux (02) semaines après sa soumission à la DGI. Le cabinet devra prendre en compte les observations faites lors de cette rencontre afin de finaliser et soumettre un rapport définitif.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Eléments d'entrée |  | Livrables |  | Parties prenantes |  | Modes de communication |
| Rapport provisoire d’audit | Rapport définitif d’audit avec recommandations et plan d‘actions | * Équipe projet DGI * RSSI * Cabinet d’audit SSI * Equipe projet PAMSI | * Courriels * Échanges téléphoniques * Réunion de validation du rapport en ligne |

# Durée et calendrier des livrables

La mission devra être conduite dans un délais de 2 mois. Les délais de production des livrables sont donnés ci-dessous à partir de T0, la date de démarrage de la mission.

Le démarrage de la mission sera prévu entre décembre 2025 et janvier 2026

|  |  |  |
| --- | --- | --- |
| Livrables | Homme/jours | Date d’achèvement |
| 1. Note de cadrage | 5 | T0 + 4 Jours |
| 1. Liste exhaustive des éléments clés à auditer 2. Plan de tests détaillé. | 2 | T0 + 10 jours |
| 1. Relevés des Constats d'audit 2. Journal de tests d’intrusion 3. Tableau des Points d’Attention | 30 | T0 + 48 jours |
| 1. Rapport provisoire d’audit avec recommandations et plan d‘actions 2. Support de présentation | 5 | T0 + 55 jours |
| 1. Rapport final | 3 | T0 + 60 jours |

# Profil du cabinet et personnel

## Expérience requise pour le cabinet

Le cabinet à recruter doit satisfaire les exigences suivantes :

* Être spécialisé dans la conduite de missions d’audit de sécurité des systèmes d’informations ;
* Avoir réalisé au moins deux (02) missions de test d’intrusion (Pentest) au cours des trois dernières années (2023, 2024, 2025) ;
* Avoir réalisé des missions d’audit de la sécurité des systèmes d’information et de la gestion des risques de sécurité informatique suivant les standards et les référentiels reconnus dans ce domaine ;
* Avoir une bonne expérience dans les outils spécialisés d’analyse de vulnérabilités, de diagnostic réseau, de détection d’intrusion et d’exploitation de failles (Nessus, Nmap, Burp Suite, Metasploit, Wireshark, etc.) serait un atout.

## Personnel requis

Le cabinet devra être composé de professionnels qualifiés disposant des compétences suivantes :

* **Expert senior en sécurité des systèmes d'information (Chef de mission) :**
  + **Rôle** : analyse de la stratégie de cybersécurité et de la gouvernance de la sécurité de l'information.
  + **Compétences** : Maîtrise des normes et réglementations: ISO 27001, RGPD, Certifications : PMP , PSPO et ITIL Gestion des risques cyber et conformité (PSSI, ISMS, gestion des menaces), Expertise des Framework de gouvernance IT
  + **Expérience** : 10 ans en cybersécurité et gouvernance IT.
* **Expert Pentesteur / Ethical Hacker :**
  + **Rôle** : Mène les tests d'intrusion et les simulations d'attaques.
  + **Compétences** : Exploitation des vulnérabilités et tests d'intrusion avancés, Tests de sécurité liés aux API et aux hyperviseurs.
  + **Expérience** : 3 à 5 ans en cybersécurité offensive.
  + **Certifications**: le pentesteur devra justifier d'une des certifications suivantes: OSCP, Red Team Operator, OSEP, OSWE.

# Confidentialité

Le cabinet doit respecter le caractère confidentiel des informations qui pourraient se retrouver en sa possession au cours de la mission. De plus, les données collectées ne seront strictement utilisées par le cabinet que pour les besoins de la mission d’audit pour la DGI.

# Organisation de la mission

Les candidats préciseront dans leurs offres la méthodologie de conduite de la mission qu’ils comptent suivre pour l’atteinte des objectifs. Cette méthodologie fera ressortir clairement les tâches qui seront exécutées sur le terrain à Cotonou et celles qui pourront s’exécuter à distance.

La méthodologie doit comprendre le planning opérationnel de la mission avec les étapes clés, le calendrier des livrables, un plan d'affectation du personnel et le chronogramme de leur mobilisation (sur le terrain et à distance).

Les dates des missions terrain seront convenues conjointement entre Expertise France, la DGI, et l’expert. Elles seront organisées par l’équipe projet d’Expertise France.

Si l’expert est international, l’ensemble des frais relatifs aux missions seront couverts par le projet. L’expert sera en charge de la réservation de son hôtel, de l’obtention de son visa, ainsi que des déplacements à Cotonou. L’équipe projet réservera le vol aller-retour. Les frais (hébergement, frais de bouche, transport sur place, téléphonie) seront couverts par des per diem au taux DGFiP (145€ par nuitée). Le visa est remboursé au réel. Les billets d’avion sont directement pris en charge par Expertise France.

# Budget

Le budget estimé est de 30000€, hors frais de déplacements et missions, pris en charge en supplément. La facturation s’effectuera par homme/jour travaillé, sur présentation d’une feuille de temps.

# Dossier à soumettre

Il sera attendu en réponse à la publication :

* Les CV des experts à mobiliser ;
* Les preuves des prestations réalisées par le cabinet répondant aux exigences mentionnées ci-dessus ;
* La méthodologie de conduite de la mission telle que décrite plus haut ;
* Une offre financière.