Opportunité – Business – Responsabilité

OBR Partner

Formation – Conseil – Ingénierie

Trajectoire SI & SSI

Stratégie, diagnostic et feuille de route

Formation · Conseil · AMOA · Audit · Architecture d'Entreprise

PME & ETI EN FRANCE | BANQUE-FINANCE-ASSURANCE EN AFRIQUE

Mission de conseil & AMOA

10 à 14 semaines · 20 à 38 jours-homme selon le périmètre

Deux profils seniors : direction de mission, expert cyber

26 000 € HT le socle · 37 500 € la configuration standard

Notre bilan à date : 2 missions conduites, 100 jours-homme livrés depuis 2025

Agenda

Du cap stratégique à la feuille de route chiffrée

1. **L'offre en un coup d'œil**
   Marché, nature, public, durée, charge et bilan à date
2. **Le besoin, le cadrage & le périmètre**
   À qui s'adresse la mission, et la ligne de partage assumée
3. **La démarche en cinq phases**
   Approche, méthodes et livrables, phase par phase
4. **Les artefacts de la méthode**
   Matrice OKR, performance des chaînes de valeur, EBIOS, priorisation
5. **Ce que la mission produit**
   Livrables outillés, résultats et impact attendus
6. **Offre financière, prolongements & équipe**
   Chiffrage, jalons, conditions et profils mobilisés

L'offre en un coup d'œil

Ce qu'il faut retenir avant d'entrer dans le détail

MARCHÉ	NATURE	PUBLIC	DURÉE	CHARGE	À PARTIR DE
PME & ETI · France, puis BFA · Afrique	Conseil & AMOA, en co-construction	Direction générale, DSI, RSSI	10 à 14 semaines · 20 à 38 JH	1 300 € · 1 000 € l'expert cyber	26 000 € HT le socle

POUR QUOI FAIRE

Les situations qui appellent cette mission

- Une feuille de route SI ou une politique de sécurité à actualiser, voire inexistante
- Des investissements nombreux, sans critère d'arbitrage homogène entre projets
- Une recommandation d'audit ou une observation du régulateur à traiter
- Un besoin de regard indépendant avant un engagement lourd — core banking, cloud

CE QUE NOUS FAISONS

Cinq phases, cinq jalons de décision

- Stratégie métier & numérique : objectifs et résultats clés, contribution du numérique
- Capacités et chaînes de valeur · diagnostic de maturité et de performance
- Sécurité des SI : analyse de risques, politique actualisée, plan de sécurisation
- Portefeuille priorisé et feuille de route chiffrée sur 12 à 36 mois

CE QUE VOUS RÉCUPÉREZ

Des livrables outillés et réutilisables

- Le référentiel d'objectifs et de résultats clés, et la matrice de contribution numérique
- Les cartographies de capacités et de chaînes de valeur, les grilles de maturité
- La politique et la stratégie de sécurité actualisées, le plan et son RACI
- Le portefeuille priorisé, les fiches projets et la feuille de route chiffrée

NOTRE BILAN À DATE

2 MISSIONS

100 JOURS-H.

Cette fiche reprend, à l'identique, la page O8 de la présentation du cabinet. Les pages qui suivent la détaillent.

Le besoin

À qui s'adresse cette mission, et ce qui indique qu'elle est pertinente maintenant

DÉCIDEURS & ACHETEURS

Qui prescrit, qui arbitre, qui signe

- Direction générale et directeurs généraux adjoints
- DSI, RSSI et direction de la production informatique
- Direction des risques, conformité, audit interne et contrôle permanent
- Direction de la transformation, organisation et PMO
- Direction financière, pour l'arbitrage du portefeuille d'investissement

SIGNAUX DE DÉCLENCHEMENT

Ce qui indique que l'offre est pertinente maintenant

- Feuille de route SI ou politique de sécurité à actualiser, voire inexistante
- Investissements nombreux, sans critère d'arbitrage homogène entre projets
- Décalage entre priorités métier, exigences de résilience et de conformité
- Recommandation d'audit ou observation du régulateur à traiter
- Stratégie d'entreprise adoptée mais non déclinée fonction par fonction

Deux signaux ou plus cochés : la mission est adressable. Un entretien de cadrage, sans frais et sans engagement, choisit la configuration.

Contexte & enjeux

Un système d'information au cœur d'un moment stratégique

1

Une ambition de transformation

Digitalisation, excellence client, performance commerciale : le SI érigé en levier d'exécution de la stratégie.

2

Une stratégie à décliner

Des ambitions définies, mais pas encore traduites en stratégie métier ni numérique, fonction par fonction.

3

Un cap SI & SSI à poser

Une stratégie SI alignée au métier et une politique de sécurité actualisées, là où elles font défaut.

4

Un cadre réglementaire exigeant

Régulateur bancaire, maîtrise des risques, conformité et contrôle interne : un socle de confiance à outiller.

5

Le numérique comme levier de valeur

Digitalisation, monétique, paiements mobiles, données et IA : traduire les objectifs en usages concrets.

6

La confiance à ancrer

Analyse de risques, exigences du régulateur, sécurité des paiements, protection des données.

Cadrage conceptuel & périmètre

Informatique, numérique, système d'information : trois notions emboîtées

LE SYSTÈME D'INFORMATION

Le périmètre traité

- Hommes, processus automatisés et manuels, données et informatique
- L'ensemble organisé qui produit et fait circuler l'information au service de l'activité et de la décision
- Le SI englobe l'informatique et intègre le numérique — il inclut aussi la part non informatisée : organisation, processus manuels, gouvernance de l'information

CE QUE COUVRE LA MISSION

La couche stratégique

- Couche stratégie, métier et capacités de l'architecture d'entreprise
- Stratégie numérique déduite des objectifs métier
- Volet SSI : gouvernance, politique de sécurité, analyse de risques, conformité, plan de sécurisation des processus
- Portefeuille priorisé et feuille de route SI & SSI chiffrée

HORS PÉRIMÈTRE

Traité ailleurs, articulé par un RACI

- Couches technique, applicative et données : architecture cible détaillée et plan de migration — relèvent d'un schéma directeur SI complet
- Sécurisation des actifs : infrastructure, hébergement et supervision — relèvent de la production et de la DSI

Une même ligne de partage, appliquée aux deux volets : couche stratégique contre couche technique, sécurité des processus contre sécurité des actifs. C'est ce qui évite les malentendus de périmètre en cours de mission.

Ce qui distingue cette mission

Une logique « business-pull », un périmètre assumé, un diagnostic mesuré

	Une mission de schéma directeur classique	La mission OBR Partner
Le point de départ	Le parc applicatif et les projets en cours	Les objectifs et résultats clés de chaque fonction métier
La logique	« Tech-push » : partir de la technologie disponible	« Business-pull » : chaque initiative découle d'un résultat clé métier
Le périmètre	Tout le SI, sans ligne de partage explicite	Couche stratégique assumée, couches technique et applicative traitées ailleurs
La sécurité	Un chapitre en fin de rapport	Une phase entière, conduite par un expert certifié, avec un RACI de responsabilités
Le diagnostic	Une appréciation qualitative	Maturité de 0 à 5, indicateurs et niveaux de service mesurés, neuf critères par activité
Ce qui reste	Un rapport	Des référentiels outillés, réutilisables pour les cycles suivants

> Les méthodes des grands cabinets — Balanced Scorecard, OKR, capacités et chaînes de valeur, EBIOS Risk Manager, TOGAF — appliquées au réel, sur des référentiels sectoriels déjà outillés. C'est ce qui rend une mission complète accessible à un coût contenu.

Objectifs & démarche générale

Quatre objectifs, un même aboutissement : une trajectoire actionnable

1

Décliner l'ambition en stratégie

Traduire les ambitions en objectifs et résultats clés par fonction, et en déduire la stratégie numérique.

2

Diagnostiquer l'existant prioritaire

Évaluer capacités, chaînes de valeur et processus prioritaires : maturité, performance, irritants et risques.

3

Actualiser la sécurité des SI

Mettre à jour la politique et la stratégie de sécurité, avec une analyse de risques et un plan de sécurisation des processus.

4

Outiller la décision

Doter l'établissement d'un portefeuille priorisé et d'une feuille de route SI & SSI séquencée et chiffrée.

La signature de la méthode — la stratégie numérique est déduite de la contribution attendue du numérique aux objectifs de chaque fonction clé. Une logique « business-pull », jamais « tech-push ».

Vue d'ensemble de la mission

Cinq phases, un cadrage et un pilotage transverse — configuration standard : 30 jours-homme

Bloc	Objet	Charge
Cadrage & mobilisation	Mobilisation des acteurs, collecte documentaire et référentiels de travail	2 JH
Phase 1 — Stratégie métier & numérique	Déclinaison en objectifs et résultats clés par fonction, puis en stratégie numérique	5 JH
Phase 2 — Capacités & chaînes de valeur	Cartographie des capacités et des chaînes de valeur, analyse de couverture	3 JH
Phase 3 — Diagnostic des chaînes prioritaires	Maturité, performance, analyse multicritère des activités, entretiens opérationnels	4,5 JH
Phase 4 — Sécurité des systèmes d'information	Analyse de risques, politique et stratégie de sécurité, conformité, plan de sécurisation	9,5 JH
Phase 5 — Portefeuille & feuille de route	Priorisation, structuration du portefeuille, feuille de route séquencée et chiffrée	4 JH
Transverse — Pilotage & restitutions	Coordination, assurance qualité, restitution intermédiaire et comité de pilotage final	2 JH

Durée : 10 à 14 semaines selon le périmètre. La phase de sécurité est le poste le plus dense et le plus variable : elle mobilise l'expert cybersécurité et s'ajuste à l'existant de l'établissement.

Démarche détaillée — phases 1 à 3

Du cap stratégique à la photographie objectivée de l'existant

PHASE 1
Stratégie métier & numérique

- Appropriation de la stratégie et alignement aux ambitions de l'établissement
- Déclinaison en objectifs et résultats clés par fonction — Balanced Scorecard puis OKR
- Contribution attendue du numérique aux objectifs de chaque fonction
- Formulation conjointe des stratégies métier et numérique
- Livrables : référentiel OKR par fonction, matrice de contribution numérique, note de stratégie

PHASE 2
Capacités & chaînes de valeur

- Cartographie des capacités de niveaux 1 et 2, à partir d'un référentiel sectoriel
- Analyse de couverture, forces et faiblesses des capacités
- Cartographie des sept chaînes de valeur, revue et adaptée au contexte
- Approfondissement sélectif sur les chaînes prioritaires
- Livrables : cartographie des capacités, cartographie des chaînes de valeur

PHASE 3
Diagnostic des chaînes prioritaires

- Diagnostic de maturité sur une échelle de 0 à 5
- Diagnostic de performance : indicateur clé et niveau de service cible par chaîne
- Analyse multicritère des activités sur neuf critères
- Entretiens opérationnels : métiers, risques, conformité, SI, monétique
- Livrables : grilles de maturité en radar, grilles d'analyse multicritère, rapport de diagnostic

Phase 1 en pratique

La matrice OKR × contribution numérique — la stratégie numérique déduite, fonction par fonction

Fonction	Objectif	Résultat clé cible	Contribution attendue du numérique
Crédit	Accélérer l'octroi	Délai − 30 %	Workflow digitalisé et moteur de scoring
Clientèle	Bancariser	+ 15 % de comptes	Entrée en relation en ligne, connaissance client dématérialisée
Opérations	Fiabiliser les traitements	− 40 % d'incidents	Automatisation et contrôles intégrés
Recouvrement	Améliorer le taux à 90 jours	+ 12 points	Relance automatisée et priorisation par le risque
Conformité	Réduire le délai de traitement des alertes	− 50 %	Filtrage outillé et traçabilité de bout en bout

Illustration. Chaque initiative de la feuille de route se rattache à un résultat clé métier et peut être remontée jusqu'à lui. C'est ce qui la rend défendable devant une direction générale.

Phase 3 en pratique

Les sept chaînes de valeur, mesurées : indicateur clé, niveau de service cible et écart au réalisé

Chaîne de valeur	Indicateur clé	Cible	Réalisé	Statut
1 · Entrer en relation	Délai moyen d'entrée en relation	≤ 24 h	3,2 j	Critique
2 · Financer	Délai d'octroi d'un crédit	≤ 5 j	9 j	Critique
3 · Opérations & paiements	Taux d'incidents sur paiements	≤ 0,5 %	1,3 %	Critique
4 · Épargne & placements	Taux de souscription digitale	≥ 30 %	12 %	Critique
5 · Commerce international	Délai de traitement d'un dossier	≤ 48 h	60 h	À surveiller
6 · Servir & fidéliser	Taux de résolution au premier contact	≥ 80 %	63 %	Critique
7 · Recouvrer	Taux de recouvrement à 90 jours	≥ 70 %	58 %	À surveiller

Illustration. Les indicateurs et les cibles sont arrêtés en atelier avec le contrôle de gestion et les métiers. L'analyse multicritère complète la mesure activité par activité, sur neuf critères.

Démarche détaillée — phases 4 et 5

De la sécurisation des processus à la feuille de route gouvernée

PHASE 4

Sécurité des systèmes d'information

- Analyse des risques sur les processus et le SI prioritaires, selon EBIOS Risk Manager
- Actualisation de la politique de sécurité des SI et de la stratégie de sécurité
- Analyse de conformité au regard du cadre applicable : régulateur bancaire, sécurité des paiements, protection des données
- Plan de sécurisation des processus et RACI d'articulation avec la production et la DSI
- Livrables : cartographie des risques, politique et stratégie actualisées, rapport de conformité, plan de sécurisation et RACI

PHASE 5

Portefeuille & feuille de route

- Évaluation de l'existant : schéma directeur en vigueur et projets déjà engagés
- Priorisation des initiatives selon un scoring valeur × faisabilité × risque
- Structuration du portefeuille : programmes, projets et fiches
- Feuille de route séquencée sur 12 à 36 mois, chiffrage et gouvernance
- Livrables : note d'évaluation du portefeuille, matrice de priorisation, portefeuille et fiches projets, feuille de route chiffrée

Phase 4 en pratique

EBIOS Risk Manager en cinq étapes, et un partage de responsabilités écrit

1 Cadrage & socle de sécurité

- Périmètre, valeurs métier et événements redoutés
- Socle de sécurité existant et écarts

2 Sources de risque

- Qui pourrait attaquer, avec quelle motivation
- Objectifs visés et couples source / objectif retenus

3 Scénarios stratégiques

- Chemins d'attaque par les parties prenantes de l'écosystème
- Prestataires, partenaires, correspondants

4 Scénarios opérationnels

- Modes opératoires techniques sur les processus et le SI prioritaires
- Vraisemblance et gravité

5 Traitement du risque

- Mesures de sécurité et plan de sécurisation
- Risques résiduels explicitement acceptés

Le partage des responsabilités est écrit : l'établissement porte la sécurité des processus, la production et la DSI portent la sécurité des actifs. C'est ce RACI qui évite qu'une politique de sécurité reste sans propriétaire.

Phase 5 en pratique

Priorisation valeur × faisabilité — quatre quadrants, une feuille de route séquencée

1

Gains rapides

Valeur haute, faisabilité haute. Ils ouvrent la feuille de route et installent la crédibilité de la démarche auprès des métiers.

2

Chantiers structurants

Valeur haute, faisabilité basse. Programmes de fond, séquencés sur 12 à 36 mois, avec leurs dépendances et leurs jalons.

3

Optionnels

Valeur basse, faisabilité haute. À lancer si la capacité le permet, jamais au détriment des deux premiers quadrants.

4

À challenger

Valeur basse, faisabilité basse. À arrêter, à reformuler ou à reporter — mais explicitement, et devant le comité de pilotage.

Chaque initiative est notée sur trois axes : valeur, faisabilité et risque. Le portefeuille en résulte ; la feuille de route le séquence sur 12 à 36 mois, en tenant compte de la capacité d'exécution réelle des équipes.

Synthèse des livrables

Des livrables outillés, réutilisables et prêts à décider

Cadrage

Note de cadrage · outils et référentiels de travail · classeur de collecte

Phase 1 — Stratégie

Référentiel OKR par fonction · matrice de contribution numérique · note de stratégie métier & numérique

Phase 2 — Capacités

Cartographie des capacités (N1/N2) · cartographie des chaînes de valeur

Phase 3 — Diagnostic

Grilles de maturité · grilles d'analyse multicritère · rapport de diagnostic opérationnel

Phase 4 — Sécurité

Cartographie des risques · politique & stratégie de sécurité · rapport de conformité · plan de sécurisation & RACI

Phase 5 — Trajectoire

Matrice de priorisation · portefeuille & fiches projets · feuille de route séquencée et chiffrée

Tous les référentiels sont remis outillés, en licence d'usage interne illimitée, et réutilisables pour les cycles suivants.

Ce que la mission produit

Des activités aux livrables, des livrables aux résultats, des résultats à l'impact

ACTIVITÉS
Ce que fait OBR Partner

- Entretiens dirigeants et ateliers avec les directions métier
- Cartographies des capacités et des chaînes de valeur
- Diagnostic de maturité, de performance et analyse multicritère
- Analyse des risques de sécurité et analyse de conformité
- Restitution intermédiaire d'arbitrage et comité de pilotage final

LIVRABLES
Ce que vous recevez

- Référentiel d'objectifs et de résultats clés, note de stratégie métier et numérique
- Cartographies capacités et chaînes de valeur, grilles de maturité
- Rapport de diagnostic opérationnel objectivé
- Politique et stratégie de sécurité actualisées, rapport de conformité, plan de sécurisation
- Portefeuille priorisé, fiches projets et feuille de route chiffrée sur 12 à 36 mois

RÉSULTATS
Ce que vous pouvez décider ou améliorer

- La direction générale arbitre sur une base objectivée, non sur des convictions
- Les écarts de conformité sont connus, hiérarchisés et planifiés
- Le portefeuille est priorisé et doté d'une gouvernance qui tient dans la durée
- Les équipes disposent de référentiels réutilisables pour les cycles suivants

IMPACT
La valeur mesurable visée

- Conformité sécurisée vis-à-vis du régulateur et des recommandations d'audit
- Investissements SI alignés sur les objectifs métier, doublons éliminés
- Résilience opérationnelle et exposition aux risques majeurs réduite
- Décisions d'engagement documentées et défendables devant le Conseil

Conditions de réussite & gouvernance

Ce que la réussite suppose de part et d'autre, et qui fait quoi

FACTEURS CLÉS DE SUCCÈS

Six conditions qui déterminent la valeur produite

- Un sponsor au niveau de la direction générale, et un comité de projet constitué dès le cadrage
- Accès aux dirigeants des fonctions clés : deux à trois entretiens par fonction, planifiés en amont
- Transmission du plan stratégique, des cartographies, du schéma directeur en vigueur et des politiques de sécurité
- Disponibilité des interlocuteurs métier, risques, conformité, SI et monétique pour les ateliers
- Décisions prises aux jalons : sans arbitrage à la restitution intermédiaire, le diagnostic part dans toutes les directions
- Un correspondant unique côté établissement pour la logistique et la relance documentaire

GOUVERNANCE

Trois acteurs, des rôles distincts

- L'établissement — désigne le sponsor et le comité de projet, ouvre l'accès aux dirigeants et aux documents, arbitre aux jalons, valide les livrables
- OBR Partner — conduit la mission, anime les ateliers, produit les livrables, assure la coordination et l'assurance qualité, restitue au comité de pilotage
- DSI, risques & conformité — apportent l'existant technique, les politiques et les exigences du régulateur ; valident le partage de responsabilités du plan de sécurisation

Ces conditions sont rappelées dans la proposition. Aucune n'est une formalité : chacune a déjà fait la différence entre une mission utile et un rapport rangé.

Planning & gouvernance de la mission

Un déroulé sur 10 à 14 semaines, jalonné par cinq points de décision

Jalon	Semaine	Objet	Instance
Cadrage validé	S1 – S2	Périmètre, acteurs, calendrier et référentiels de travail arrêtés	Comité de projet
Restitution intermédiaire	S5 – S6	Stratégie métier & numérique, capacités et chaînes de valeur — arbitrage	Direction générale
Diagnostic partagé	S7 – S8	Photographie objectivée de l'existant et priorités confirmées	Comité de projet
Politique & stratégie de sécurité	S9 – S11	Analyse de risques, conformité et plan de sécurisation validés	Risques & DSI
Restitution finale	S12 – S14	Portefeuille priorisé et feuille de route chiffrée — décision d'engagement	Comité de pilotage

> La mission est conduite en co-construction : ateliers avec les métiers, entretiens dirigeants et validations intermédiaires. Aucun livrable n'est produit hors du regard de l'établissement.

Offre financière

Trois configurations, des taux journaliers publiés, une facturation au réel

DURÉE
10 à 14 semaines selon le périmètre

ÉQUIPE
Directeur de mission et expert cybersécurité

FACTURATION
Au réel, sur les jours effectivement réalisés

FRAIS ANNEXES
En sus, ~20 % en mission hors zone

Configuration	Périmètre	Charge	Montant HT
Trajectoire SI — socle	Phases 1, 2, 3 et 5, sans volet sécurité. Cadrage et pilotage inclus.	20 JH	26 000 €
Trajectoire SI & SSI — standard	Les cinq phases, volet sécurité dimensionné à l'existant.	30 JH	37 500 €
Trajectoire SI & SSI — étendue	Analyse de risques approfondie et conformité renforcée.	38 JH	46 400 €

Taux journaliers publiés, sans remise : directeur de mission 1 300 € HT, expert cybersécurité et conformité 1 000 € HT. Configuration standard : 25 JH et 5 JH. Règlement adossé aux jalons : 30 % à la commande, 30 % à la restitution intermédiaire, 40 % à la restitution finale. Validité 30 jours.

Après la feuille de route

Quatre prolongements chiffrés — la trajectoire est un début, pas une fin

1

AMOA à la journée — 1 300 €

Appui ponctuel : cadrage d'un chantier, rédaction d'un cahier des charges, dépouillement d'un appel d'offres, arbitrage technique.

2

Revue trimestrielle — 2 500 €

Une demi-journée par trimestre : avancement du portefeuille, réajustement de la feuille de route, alerte sur les dérives.

3

Lancement des chantiers — 13 000 à 19 500 €

10 à 15 JH : structuration du programme, mise en place de la gouvernance et du dispositif de pilotage, démarrage des gains rapides.

4

Schéma directeur SI complet — dès 25 JH

Couches applicative, données et technique : architecture cible détaillée et plan de migration, en prolongement de la couche stratégique.

Déclinaison Groupe — une fois la trajectoire posée sur une première entité, les référentiels sont capitalisés : chaque filiale suivante mobilise une charge réduite, sur un socle commun et une trajectoire qui lui est propre.

Frais de déplacement

Trois modalités alternatives, à convenir avant le lancement

1

Prise en charge directe

Le client organise et règle directement le transport, l'hébergement et les frais associés. La modalité la plus simple, et celle que nous recommandons.

2

Refacturation au réel

OBR Partner avance les frais, puis les refacture au réel sur présentation des justificatifs. Aucune marge n'est appliquée sur ces frais.

3

Forfaits convenus

Indemnité de séjour et enveloppe de transport aérien, arrêtées à l'avance : 250 € par jour et par intervenant, 2 000 € par vol aller-retour.

Une part significative de la mission se conduit à distance. Les déplacements sont concentrés sur les ateliers et les restitutions, ce qui contient ce poste autour de 20 % des prestations.

Conditions contractuelles

Confidentialité, données, propriété des livrables et modalités de règlement

Rubrique	Engagement
Confidentialité	Accord de confidentialité réciproque signé avant toute transmission de document. Les informations reçues restent internes à la mission ; elles ne sont ni citées ni réutilisées sans accord écrit de l'établissement.
Données à caractère personnel	La mission ne requiert aucune donnée client. Les échantillons éventuellement nécessaires au diagnostic sont anonymisés par l'établissement avant transmission.
Propriété des livrables	Les livrables produits pour la mission — diagnostics, stratégie, portefeuille, feuille de route, plan de sécurisation — sont la propriété pleine et entière de l'établissement.
Propriété des référentiels	Les référentiels et grilles outillés — OKR, capacités, chaînes de valeur, maturité, analyse multicritère, trame de politique de sécurité, classeur de collecte — restent la propriété d'OBR Partner et sont concédés en licence d'usage interne illimitée.
Équipe & sous-traitance	L'expert cybersécurité intervient sous la responsabilité d'OBR Partner. Aucune sous-traitance non déclarée. Tout changement d'intervenant est soumis à l'accord de l'établissement.
Assurance	Responsabilité civile professionnelle en cours de validité ; attestation communiquée sur demande.
Règlement	30 % à la commande, 30 % à la restitution intermédiaire, 40 % à la restitution finale. Paiement à 30 jours date de facture. Montants hors taxes.
Validité de la proposition	30 jours à compter de sa date de remise.

Variantes & personnalisation

Trois curseurs pour décliner cette mission sur un autre établissement ou un autre marché

AXE 1
Secteur & métier

- Banque de détail — particuliers et professionnels
- Banque des entreprises et institutionnels
- Assurance et bancassurance
- Microfinance et institutions de financement
- Services financiers spécialisés, monétique et paiements
- Hors BFA : secteur public, télécoms, industrie

AXE 2
Zone & cadre applicable

- UMOA — BCEAO et Commission Bancaire
- CEMAC — COBAC et BEAC
- Maroc — Bank Al-Maghrib
- France et Union européenne — ACPR, EBA, DORA, AI Act
- Paiements et données — PCI-DSS, RGPD, autorités nationales

AXE 3
Périmètre & profondeur

- Socle SI seul, sans volet sécurité — 20 JH
- Standard SI & SSI — la présente offre, 30 JH
- Étendue, analyse de risques approfondie — 38 JH
- Option : schéma directeur SI complet
- Déclinaison Groupe : socle commun, trajectoire par filiale

Ce qui change : références réglementaires, cas d'usage, vocabulaire. Ce qui ne change pas : la structure, la méthode et les outils remis.

L'équipe

Trois profils seniors : la stratégie SI, la conduite de grands programmes, la sécurité certifiée

ZSO
Directeur de mission

- Stratégie et schéma directeur métier & SI ; architecture d'entreprise et urbanisation — TOGAF L1 & L2
- Gouvernance SI, contrôle de gestion du SI, direction de programmes de transformation
- Intégration de core banking, diagnostic données et IA, analyse de risques
- Missions OBR Partner attestées : SDSI de BGFI Services ; état des lieux SI et vision cible du SIGFI pour le ministère des Finances du Gabon

MSY
Direction de programme & grands SI

- 36 ans dans les systèmes d'information : audit, schémas directeurs, direction de grands programmes
- Direction de centres de services de 60 à 200 personnes, multi-sites et multi-pays
- Assurance, prévoyance et protection sociale : systèmes de gestion conçus et livrés de bout en bout
- Ingénieur EPITA. Intervenant OBR Partner sur le SDSI de BGFI Services

HOL
Expert cybersécurité & conformité

- Analyse et gestion des risques cyber ; architecture de sécurité — SOC, gestion des identités et des accès
- Audit ISO 27001, NIST, PCI-DSS, COBIT ; continuité d'activité et résilience — ISO 22301
- Plus de dix ans en sécurité des SI d'institutions financières et d'organismes publics en Afrique de l'Ouest
- CISSP, CISM, CISA, ISO 27001 Lead Auditor et Implementer, ISO 22301, ISO/IEC 42001 Lead Implementer. Formateur certifié PECB

Architecture d'entreprise, direction de grands programmes et sécurité certifiée dans une même équipe — et rien que des seniors. Les références de nos intervenants ont été acquises à titre individuel ; elles ne constituent pas des missions du cabinet.

Choisissons ensemble votre trajectoire SI & SSI

Prochaine étape : un entretien de cadrage, sans frais et sans engagement, pour arrêter le périmètre, la configuration et le calendrier de la mission.

Zouber Sotbar — Fondateur

zouber.sotbar@obr-partner.com · +33 7 81 02 87 96 · www.obr-partner.com

OBR PARTNER — FORMATION · CONSEIL · INGÉNIERIE | BANQUE · FINANCE · ASSURANCE

Opportunité – Business – Responsabilité

OBR Partner

Formation – Conseil – Ingénierie