BCEAO

BANQUE CENTRALE DES ÉTATS
DE L'AFRIQUE DE L'OUEST

DOSSIER D'APPEL D'OFFRES - AO/Z00/DBA/040/2023

FOURNITURE ET DEPLOIEMENT D'UNE INFRASTRUCTURE RESILIENTE DE TRAITEMENT DE DONNÉES À LA BANQUE CENTRALE DES ETATS DE L'AFRIQUE DE L'OUEST

AOÛT 2023

Avenue Abdoulaye FADIGA
BP 3108 – Dakar - Sénégal

Tél. (221) 33 839 05 00 / Fax. (221) 33 823 93 35
courrier.bceao@bceao.int - www.bceao.int

PREMIERE PARTIE : DISPOSITIONS GÉNÉRALES

I.1. Introduction

La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) est l'Institut d'émission commun aux huit (8) Etats membres de l'Union Monétaire Ouest Africaine (UMOA), à savoir le Bénin, le Burkina, la Côte d'Ivoire, la Guinée-Bissau, le Mali, le Niger, le Sénégal et le Togo.

La BCEAO exerce ses activités à travers :

- son Siège à Dakar ;
- une Direction Nationale dans chacun des États membres, comprenant une Agence Principale et une ou plusieurs Agences Auxiliaires ;
- le Secrétariat Général de la Commission Bancaire (SGCB) de l'UMOA sis à Abidjan ;
- le Centre de Traitement Fiduciaire (CTF) basé à Yamoussoukro ;
- la Représentation auprès des Institutions Européennes de Coopération (RIEC) sise à Paris.

La BCEAO envisage, au titre de son plan stratégique, de consolider les leviers devant permettre de favoriser l'absorption des technologies innovantes.

A cet égard, elle lance cet appel d'offres afin de sélectionner un prestataire pour la fourniture et le déploiement d'une infrastructure résiliente de traitement de données à l'effet de mettre en place un cloud privé, évolutif, sécurisé, hautement disponible et facile à exploiter.

I.2. Objet

Le présent dossier d'appel d'offres concerne la fourniture des matériels, logiciels et licences associées, ainsi que des services requis pour faire évoluer les centres de données existant au sein de la Banque. Ces centres de données reposent sur une architecture trois tiers, composée de serveurs de traitement, de réseaux de stockage et de baies de disques avec une architecture hyper-convergée, répondant aux exigences spécifiées en termes de sécurité, de haute disponibilité, de scalabilité, de simplicité d'exploitation, de facilité de gestion et de contrôle unifié.

I.3. Allotissement

Le marché est constitué d'un lot unique et indivisible.

Les soumissionnaires sont invités à présenter une offre forfaitaire et globale du marché.

I.4. Conditions de participation à l'appel d'offres

La participation au présent appel d'offres est ouverte à toutes les entreprises éligibles, disposant de qualifications techniques et financières correspondant aux exigences des termes de référence.

Toutefois, les entreprises impliquées dans des activités illégales, notamment le blanchiment des capitaux, le financement du terrorisme, la corruption ainsi que toute pratique collusoire, frauduleuse ou coercitive, ne sont pas autorisées à prendre part au présent appel à concurrence.

En outre, tout candidat en situation de conflit d'intérêt devra en informer la Banque dans sa lettre de soumission, en précisant les termes dudit conflit.

I.5. Groupement

Les groupements sont autorisés dans le cadre du présent appel d'offres. Toutefois, la seule forme acceptée est le groupement solidaire. A ce titre, les entreprises concernées devront présenter, dans leur soumission, l'acte constitutif du groupement signé par les parties. Ce document devra en outre indiquer le chef de file dudit groupement.

I.6. Sous-traitance

La sous-traitance est subordonnée à l'accord préalable écrit de la Banque Centrale. Si elle est autorisée, la sous-traitance ne pourra excéder 30% de la valeur du contrat de base.

I.7. Période de validité des offres

La validité des offres devra être d'au moins cent vingt (120) jours à compter de la date de dépôt.

I.8. Langue de soumission

Les offres et tous les documents concernant la soumission, échangés entre le soumissionnaire et la Banque Centrale, devront être rédigés en langue française.

Les notices des équipements pourront être rédigées dans une autre langue, à condition d'être accompagnées d'une traduction certifiée desdites notices en français.

I.9. Frais de soumission

Le soumissionnaire supportera tous les frais afférents à la préparation et à la présentation de son offre. La Banque Centrale ne sera en aucun cas responsable de ces frais ni tenue de les régler, quels que soient le déroulement et l'issue de la procédure d'appel d'offres.

I.10. Monnaie de soumission

La monnaie utilisée est le franc CFA. Toutefois, les soumissions valorisées en euros seront acceptées pour les fournisseurs établis hors de la zone UMOA. Pour des besoins de comparaison, toutes les offres seront converties en francs CFA.

I.11. Régime fiscal

En vertu des dispositions des articles 28 du Traité de l'Union Monétaire Ouest Africaine (UMOA), en date du 20 janvier 2007, 7 des Statuts de la BCEAO, 10, paragraphe 10-1 du Protocole relatif aux privilèges et immunités de la BCEAO, annexés audit Traité, et 8 de l'Accord de Siège conclu le 21 mars 1977 entre le Gouvernement de la République du Sénégal et la BCEAO, la Banque Centrale bénéficie, dans le cadre du présent appel d'offres, du régime de l'exonération de tous impôts, droits, taxes et prélèvements d'effet équivalent dus dans les Etats membres de l'UMOA.

I.12. Propriété des documents et droits d'auteur

Les documents et les livrables fournis par le Prestataire retenu dans le cadre de l'exécution de ses missions resteront la propriété de la Banque.

Les droits d'auteur pour tous les documents préparés par le Prestataire demeureront sa propriété. Cependant, il autorisera la Banque, sans préalable, à utiliser ces documents pour la réalisation d'autres prestations similaires ou supplémentaires, sans qu'il puisse prétendre à quelque indemnité que ce soit.

Le Prestataire retenu sera censé avoir reçu l'autorisation écrite des détenteurs des procédés brevetés ou protégés, des droits de licences et autres, utilisés par lui dans le cadre du présent marché. La responsabilité de la Banque ne saurait en aucun cas être engagée à l'occasion d'un litige à ce sujet.

I.13. Modalités de paiement

En cas d'attribution, les modalités de règlement proposées sont les suivantes :

- une avance de trente pour cent (30 %) à la signature du contrat contre la fourniture d'une lettre de garantie à première demande délivrée par un organisme financier de premier ordre reconnu par la BCEAO. La mainlevée de cette garantie est effectuée par la Banque Centrale, à la date de signature du dernier bordereau de livraison ;
- soixante-cinq pour cent (65 %) à la livraison et l'installation conformes des équipements, attestées par la signature du dernier procès-verbal de réception provisoire ;
- cinq pour cent (5 %) au titre de la restitution de la retenue de garantie libérable à la fin de la période de garantie, dès la réception définitive.

I.14. Présentation des soumissions

Les soumissions devront comprendre les quatre (4) parties distinctes suivantes :

- une lettre de soumission ;
- une présentation du soumissionnaire ;
- une proposition technique ;
- une proposition financière.

I.14.1. Lettre de soumission

Le soumissionnaire devra produire une lettre de soumission selon le modèle joint à **l'annexe I** précisant tous les éléments de sa proposition qui l'engage contractuellement.

Cette lettre devra être signée par un responsable dûment habilité de l'entreprise soumissionnaire.

I.14.2. Présentation du soumissionnaire

La présentation du soumissionnaire comprendra les informations ci-après :

- une présentation générale de la société (dénomination, siège social, domaines de spécialisation, partenaires, etc.) ;
- la liste et les adresses complètes des transitaires du soumissionnaire dans les deux (2) pays de l'UMOA concernés, à savoir la Côte d'Ivoire et le Sénégal ;
- le nom du représentant local pour la prise en charge de la maintenance des équipements pendant la période de garantie ;
- la copie des états financiers pour les trois (3) derniers exercices (2020, 2021 et 2022).
- toute information indispensable à une bonne connaissance du soumissionnaire.

En cas de sous-traitance, les mêmes informations concernant le sous-traitant, devront être communiquées à la Banque Centrale.

Par ailleurs, le soumissionnaire devra fournir dans son offre une copie des documents attestant de son statut juridique, son numéro d'immatriculation le cas échéant, ainsi que ses références bancaires conformes aux normes de codification bancaire internationales.

I.14.3. Offre technique

L'offre technique comprendra :

- les spécifications techniques, fonctionnelles et critères de performance des équipements, conformément aux exigences définies dans la deuxième partie du présent dossier d'appel d'offres ;
- les fiches techniques et prospectus en couleur des équipements proposés ;
- la liste d'au moins trois (3) références de projets similaires appuyées par des attestations de bonne exécution ou tout autre document équivalent ;
- le planning d'exécution ;
- la formulation d'avis et remarques ;
- le tableau d'évaluation des offres techniques dûment renseigné, conformément au canevas joint en annexe II ;
- la communication de toute autre information technique jugée utile.

I.14.4. Offre financière

Les prix indiqués par le soumissionnaire devront être établis en hors taxes et hors douane. Ils seront fermes, non révisables, et devront comprendre :

- un devis détaillé de l'offre de base pour les fournitures ;
- le coût annuel des services d'assistance et de support (mise à jour, réparation) ;
- un devis détaillé des options et services connexes ;
- les quantités ;
- les prix unitaires ;
- le coût total ;
- le taux de remise ;
- le total net ;
- les frais de livraison ;
- tous frais nécessaires non explicitement cités.

Ces prix devront comprendre tous les frais exposés, depuis l'expédition jusqu'à la livraison et l'installation des équipements (transport, assurance, transit départ et arrivée, dépotage, déchargement et installation).

Par ailleurs, ces prix devront être exprimés en tenant compte du TCO «Total Cost of Ownership» ou coût total de possession. A ce titre, ils devront indiquer la durée de vie des équipements et prendre en compte tous les coûts récurrents liés au cycle de vie de ces équipements à savoir :

- le coût de maintenance ;
- le coût d'exploitation ;
- le coût énergétique.

Le soumissionnaire indiquera toute remise inconditionnelle ou conditionnelle.

L'utilisation éventuelle de moyens de livraison exceptionnels, même avec l'accord de la BCEAO, ne saurait ouvrir au fournisseur un droit quelconque à supplément ou indemnité.

I.15. Actualisation des offres techniques

Au regard des évolutions technologiques du marché des matériels informatiques, il sera demandé au soumissionnaire retenu de réviser son offre pour tenir compte des évolutions technologiques éventuelles si un délai de six (6) mois s'écoule entre le lancement de l'appel d'offres et la signature du contrat de marché.

I.16. Agrément

Les soumissionnaires revendeurs devront communiquer, dans leur soumission, la preuve de leur agrément par les fabricants.

I.17. Assurance

Le ou les fournisseurs et/ou leurs sous-contractants devront, à leur charge, souscrire des polices d'assurance valables pendant toute la durée du contrat et couvrant au moins les risques de transport et de livraison.

I.18. Confidentialité

Dans le cadre de la mission, chaque partie devra s'engager à préserver le caractère confidentiel de toute information communiquée comme telle. Ainsi, le prestataire sera tenu notamment de :

- garder confidentiels tous documents et informations de quelque nature qu'ils soient, qui lui ont été communiqués par la BCEAO ou dont il a eu connaissance, quels qu'en soient la forme, le support et le contenu, dans le cadre de l'exécution du marché ;
- n'utiliser ces documents et informations qu'aux seules fins d'exécuter le marché. En conséquence, même après la cessation du contrat, le prestataire ne pourra les communiquer à des tiers ou les exploiter dans ses relations avec ceux-ci, sans avoir obtenu, au préalable, l'autorisation écrite de la BCEAO ;
- prendre toutes les dispositions nécessaires, notamment auprès des membres de son personnel appelés à prendre connaissance de ces documents ou à connaître ces informations, et dont le prestataire répond entièrement en la matière, pour prévenir et éviter leur divulgation à des tiers, de quelque manière que ce soit ;
- restituer sans délai à la BCEAO, à sa demande, au terme de l'exécution du marché ou à la date de sa prise d'effet, les documents, rapports et données ainsi que toutes autres informations qu'elle juge confidentielles.

I.19. Date et heure limite de transmission des offres

Les offres devront exclusivement être transmises en version PDF, par voie électronique à l'adresse courrier.ZDBA-SAMA@bceao.int au plus tard le **mercredi 06 septembre 2023 à 12 heures TU,** délai de rigueur.

Aucun pli expédié par voie postale (DHL, Chronopost, EMS, etc) ou par porteur ne sera recevable.

I.20. Evaluation des offres

Une Commission des Marchés procédera à la réception, la vérification de la conformité, l'évaluation ainsi qu'au classement des offres reçues.

Préalablement à l'évaluation des offres, la BCEAO se réserve le droit de procéder à la vérification de l'éligibilité des soumissionnaires, eu égard notamment aux législations relatives à la lutte contre les activités illégales visées dans la clause I.4 du présent dossier, en vigueur dans l'espace UMOA.

Les critères d'évaluation des offres se présentent, par ordre de priorité, comme ci-après :

- la conformité aux termes de références ;
- les références de missions similaires attestées par des lettres de bonne exécution ;
- la qualité technique des intervenants appréciée sur la base de leurs qualifications et expériences dans la conduite de prestations similaires ;
- la méthodologie et l'approche de mise en oeuvre ;
- le coût de la solution proposée.

Ainsi, l'évaluation des offres sera faite sur la base des critères d'évaluation précités d'une part, et de l'analyse ainsi que de la comparaison des prix proposés, qui s'effectueront au regard des critères économiques et financiers, d'autre part.

Il sera procédé à des ajustements de prix en cas d'erreurs arithmétiques. De même, s'il y a contradiction entre le prix indiqué en lettres et en chiffres, le montant en lettres fera foi.

A l'issue du dépouillement, le marché pourra faire l'objet de négociations commerciales avec le soumissionnaire pressenti.

I.21. Vérification de la qualification des candidats

La Banque Centrale se réserve le droit de vérifier les capacités techniques et financières du prestataire retenu à exécuter le marché de façon satisfaisante.

Cette vérification tiendra compte, notamment, de la capacité et de la solvabilité financières du soumissionnaire. Elle pourrait se fonder sur l'examen des preuves de qualification que la Banque Centrale jugera nécessaires.

Le cas échéant, son offre sera rejetée et la Banque Centrale examinera l'offre classée deuxième, puis appréciera également la capacité de ce soumissionnaire à exécuter le marché de façon satisfaisante.

I.22. Attribution du marché

Le marché sera attribué au soumissionnaire dont l'offre sera jugée la plus économiquement avantageuse pour la Banque Centrale et non celle dont le montant est le plus bas.

La BCEAO se réserve le droit d'accepter ou de refuser toute offre et d'annuler, le cas échéant, l'appel d'offres en rejetant toutes les soumissions, à tout moment, avant l'attribution du marché.

Avant l'attribution du contrat, la BCEAO se réserve le droit de procéder à une vérification du caractère raisonnable des prix proposés dans le cadre de la présente procédure.

Une conclusion négative (des prix déraisonnablement élevés ou bas) constituera un motif de rejet de l'offre, à la discrétion de la BCEAO. Dans le cas où cette conclusion concernerait la soumission classée première à l'issue de l'évaluation technique et financière, elle pourra inviter le soumissionnaire classé deuxième pour des négociations.

I.23. Publication des résultats et notification provisoire

Les résultats de l'appel d'offres seront publiés sur le site internet de la BCEAO. A cet égard, tout candidat pourra former un recours gracieux par écrit, adressé au Directeur Général de l'Administration et des Ressources Humaines, dans un délai maximum de cinq (5) jours ouvrés, à compter de la date de publication des résultats.

Ledit recours ne pourra porter que sur l'attribution du marché. Le délai de réponse de la BCEAO sera de dix (10) jours ouvrés maximum. Passé ce délai et sans une réponse de la BCEAO, le recours devra être considéré comme rejeté.

Lorsque les motifs exposés ne sont pas substantiels ou de nature à remettre en cause la décision d'attribution, la Banque Centrale n'est pas tenue de donner suite au recours. Dans ce cas, le recours devra être également considéré comme rejeté.

Dans l'attente de l'issue d'un éventuel recours, une notification provisoire sera adressée au soumissionnaire pressenti.

I.24. Délais de livraison, d'installation et de configuration

Les délais de livraison d'installation et de configuration, le cas échéant, devront être indiqués dans la soumission et commenceront à courir à compter de la date de signature du marché.

Lorsque les délais contractuels de livraison sont dépassés, le prestataire retenu encourt, sans mise en demeure préalable, une pénalité par jour calendaire de retard égale à un pour mille (1‰) qui sera retenue d'office sur les sommes qui lui sont dues.

Ce taux est applicable au montant de la prestation livrée hors délai. Toutefois, le montant total des pénalités qui seront appliquées n'excédera pas cinq pour cent (5%) du montant global du marché.

I.25. Lieux de livraison

La livraison des équipements se fera, dans les locaux de la BCEAO, aux adresses indiquées dans le tableau suivant :

PAYS	SITES	ADRESSES
COTE D'IVOIRE	Agence Principale d'Abidjan (*Secours*)	Avenue Abdoulaye FADIGA BP 01 1769 Abidjan 01 Tél. : (225) 20 20 84 00 / 20 20 85 00 Fax : (225) 20 22 28 52
SENEGAL	Siège (*Principal*)	Avenue Abdoulaye FADIGA 3108 Dakar Tél. : (221) 33 839 05 00 Fax : (221) 33 823 83 35
	Agence Principale de Dakar (*Back-up*)	Bd du Général de Gaulle, angle Triangle Sud BP 3159 Dakar Tél. : (221) 33 889 45 45 Fax : (221) 33 823 57 57

I.26. Réception

La réception sera effectuée en deux temps avec les étapes suivantes :

- réception provisoire après la livraison, l'installation et la configuration des équipements et le constat de leur bon fonctionnement ;
- réception définitive à la fin d'une période de garantie de cinq (5) ans, après la levée de toutes les réserves émises et la constatation du bon fonctionnement de l'ensemble des équipements livrés, installés et configurés.

Les réceptions provisoire et définitive feront l'objet de procès-verbaux signés par les deux parties.

I.27. Garantie

Tous les équipements devront être livrés neufs avec les dernières versions logicielles en date. Ils seront garantis pendant cinq (5) ans, pièces et main-d'œuvre dans les locaux de la BCEAO.

A cet égard, les soumissionnaires devront préciser dans leurs offres, la durée de la garantie de base et faire une offre pour porter à cinq (5) ans la durée totale de la garantie. En cas de non-conformité, le retour des équipements est fait entièrement à la charge du fournisseur.

La date de prise d'effet des garanties, des services d'appui technique et des licences d'utilisation associés aux équipements livrés devra être postérieure à la date de livraison desdits équipements dans les locaux de la BCEAO établie par le bordereau de livraison.

Le non-respect de cette clause constituera un motif de rejet ou de résiliation du marché pour cause de non-conformité.

La garantie couvrira les vices cachés pouvant affecter le fonctionnement des équipements, la fourniture de pièces détachées ainsi que tous les frais liés aux réparations qui seraient effectuées (transport, déplacement, hébergement, main d'œuvre, etc.) durant la période de référence.

La Banque Centrale appliquera une retenue de garantie égale à 5% du montant total du marché jusqu'au terme de la période de cinq (5) ans, à compter de la date de signature du procès-verbal de réception provisoire.

I.28. Litiges et contestations

Tout litige sera réglé à l'amiable. A défaut de règlement à l'amiable, tout différend sera, de convention expresse, soumis à l'arbitrage selon le Règlement d'arbitrage de la cour Commune de Justice et d'Arbitrage (CCJA) de l'Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA), et tranché par un arbitre ad hoc désigné par la CCJA.

L'arbitrage se déroulera en langue française à Dakar (Sénégal), selon le droit sénégalais.

Les frais de l'arbitrage sont à la charge de la partie succombante.

I.29. Informations complémentaires

Pour toute demande d'informations complémentaires, les soumissionnaires pourront prendre l'attache de la Direction du Budget et des Approvisionnements, par courriel au moins dix (10) jours calendaires avant la date limite de dépôt des offres à l'adresse : courrier.ZDBA-SAMA@bceao.int.

Toute demande de renseignements parvenue au-delà du délai précité ne sera pas prise en compte.

Les questions formulées ainsi que les réponses apportées seront mises en ligne sur le site Internet de la BCEAO à l'adresse www.bceao.int.

A ce titre, les soumissionnaires sont invités à consulter régulièrement le site.

DEUXIÈME PARTIE : CARACTÉRISTIQUES TECHNIQUES

II.1. Présentation de l'existant

II.1.1. Localisation géographique

Le Système d'Information de la BCEAO repose essentiellement sur des infrastructures de traitement, de stockage et de sauvegarde réparties dans trois (3) sites, à savoir : deux (2) sites de production dont un principal et un secondaire, et un troisième site, dit de secours.

Les sites de production sont localisés à Dakar et celui de secours, dont la fonction principale est de garantir la continuité d'activités en cas de sinistre majeur sur les sites de production, est hébergé à Abidjan.

II.1.2. Interconnexion WAN

Les sites de production sont interconnectés par une boucle en fibre optique de 36 brins, à travers laquelle les données sont répliquées de manière synchrone et bidirectionnelle.

Le site de secours est interconnecté au site principal par un lien en fibre optique de 150 Mbps et une liaison VSAT asymétrique de 4/40 Mbps, tous deux agrégés en SD-WAN.

II.1.3. Réseaux locaux

Les réseaux locaux sont segmentés en VLAN portés par des commutateurs de type Cisco et protégés par des équipements de sécurité fournis par différents constructeurs, principalement CISCO, BARRACUDA et FORTINET.

II.1.4. Solution de réplication

Le système de réplication repose sur une solution matérielle et logicielle permettant une réplication baie à baie des données.

La réplication des données entre les trois (3) sites est assurée par une solution permettant la reprise alternée entre les deux (2) sites de production en cas de sinistre. La reprise sur le site de secours est effectuée en cas de la survenue d'un sinistre majeur sur les sites de production.

La solution permet une réplication bidirectionnelle entre les sites de production (principal et secondaire) et unidirectionnelle depuis les sites de production vers celui de secours.

II.1.5. Infrastructures virtuelles

Chacun des sites de la Banque dispose d'une infrastructure virtuelle reposant sur des hôtes VMware ESXi. Ces hôtes hébergent principalement des machines virtuelles Windows et Linux dédiées aux services d'infrastructures, ainsi qu'aux serveurs d'applications et de bases de données.

Les caractéristiques techniques agrégées des différents serveurs physiques se présentent, peu ou prou, comme suit :

Site	Nbre de VM	Coeur(s)	Mémoire brute	Mémoire utilisée	Mémoire disponible
Principal	300	272	3 To	1.6 To	1.4 To
Secondaire	300	272	3 To	1.6 To	1.4 To
Secours	150	136	1.5 To	500 Go	1 To
Total	**750**	**680**	**7.5 To**	**3.7 To**	**3.8 To**

II.1.6. Réseau de stockage

La Banque dispose d'un réseau de stockage de type SAN comprenant trois baies de disques, dont deux installées sur les sites de production (Principal et Secondaire) et une sur celui de secours.

Les deux baies de production sont partiellement configurées en haute disponibilité à l'aide d'une infrastructure de virtualisation de stockage.

La Banque dispose également de deux serveurs de type NAS, pour le stockage des fichiers, installées sur les sites de production (principal et secondaire).

Les caractéristiques techniques des baies se présentent comme suit :

Site	Baie	Capacité stockage brute	Capacité stockage utilisée	Disques Flash SSD	Disques SAS
Principal	**SAN**	245 To	56 To	245 To	
	NAS	30 To	5 To		30 To
Secondaire	**SAN**	245 To	51 To	245 To	
	NAS	30 To	5 To		30 To
Secours	**SAN**	245 To	28 To	245 To	
Total		795 To	145 To	735 To	60 To

II.1.7. Composants Oracle

La Banque dispose de produits de la firme Oracle, qui sont hébergés par des infrastructures spécifiques aux fins d'optimiser l'utilisation de leurs licences.

Ainsi, le module General Ledger (GL) de la suite eBusiness (EBS), est hébergé sur un hôte physique dédié, installé sur le site de production principal.

Site	Type	Coeurs utilisés	Mémoire brute	Mémoire utilisée	Capacité Disque brute	Capacité Disque utilisée
Principal	**Serveur**	16	90 Go	87 Go	2.72 To	1.57 To

De même, les bases de données Oracle sont hébergées sur des machines dédiées, de type Oracle Database Appliances (ODA), déployées sur les deux (2) sites de production.

Site	Type	Coeurs utilisés	Mémoire brute	Mémoire utilisée	Capacité Disque brute	Capacité Disque utilisée
Principal	**ODA**	4	768 Go	268 Go	16 To	15.1 To
Secondaire	**ODA**	4	768 Go	291 Go	16 To	15.9 To

II.1.8. Infrastructures de sauvegarde et d'archivage

Le système de sauvegarde de la Banque, réparti dans les trois sites, repose sur des appliances Dell EMC Data Domain et le logiciel EMC Networker, offrant une capacité maximale de stockage de données sauvegardées de 62 To.

Les données de sauvegardes sont agrégées sur le site principal, puis répliquées sur les deux (2) autres sites, à savoir le site secondaire et celui de secours.

La sauvegarde et la restauration des données sont opérées sur disques, avec une déduplication à haute vitesse, permettant d'atteindre un débit maximal de 22 To/heure.

Les ressources dédiées à la sauvegarde sont réparties comme suit :

Site	Capacité de stockage brute (To)	Capacité de stockage utilisée (To)	Capacité de stockage disponible (To)
Principal	62	43	19
Secondaire	94	64	30
Secours	94	61	33

La Banque dispose aussi d'une solution de type Dell ECS pour l'archivage des données nécessitant une longue durée de rétention, notamment celles soumises à des exigences réglementaires et légales.

L'ECS déployé sur le site de production principal répond aux capacités, ci-après :

Site	Capacité de stockage brute (To)	Capacité de stockage utilisée (To)	Capacité de stockage disponible (To)
Principal	524	67	457

II.1.9. Applications critiques

Le portefeuille applicatif de la Banque se compose principalement d'un système d'information bancaire, de systèmes de paiement et d'opérations de marchés, d'applications de gestions administratives et comptables, de dispositifs de collecte de données auprès d'établissements assujettis et de centrales d'information.

II.1.10. Ressources humaines

Les systèmes et équipements de réseaux du SI de la Banque sont administrés par des équipes pluridisciplinaires essentiellement localisées au Siège.

II.2. Système d'information cible

Les soumissionnaires sont invités à proposer leurs meilleures offres, pour la fourniture et le déploiement d'une plateforme résiliente de traitement de données, reposant sur des infrastructures hyper-convergées (HCI), comprenant le matériel et les logiciels ainsi que les licences et services associés, et offrant une haute disponibilité des services informatiques, une capacité à opérer un volume important de transactions, une célérité de reprise après sinistre, une flexibilité d'exploitation des systèmes et une scalabilité des plateformes matérielles.

Par ailleurs, l'infrastructure proposée devra :

- faire partie des leaders du Magic Quadrant de Gartner, au titre des années 2021 et 2022, en termes d'infrastructures matérielles et logicielles hyper-convergées ;
- prendre en compte la taille de l'environnement, la charge de travail, la redondance et la disponibilité ainsi que les exigences de performance requises ;
- être dimensionnée conformément à l'architecture cible, afin de garantir la redondance et la haute disponibilité maximale des machines virtuelles (VM) ;
- être livrée avec toutes les licences requises pour un bon fonctionnement d'ensemble des composants et une conformité aux exigences des éditeurs ;
- supporter les principales solutions de virtualisation du marché ;
- être capable de présenter le stockage en mode bloc aux serveurs et de configurer des clusters de volumes ;
- pouvoir séparer les flux réseaux afin de les sécuriser et isoler les flux iSCSI ;
- permettre la mise à jour à chaud, sans impact sur les applications, couches logicielles, services, hyperviseur, stockage, disques, Bios, etc.;
- supporter le cryptage des données stockées, ainsi que celui des VM basé sur KMS ;
- permettre aux administrateurs de contrôler la qualité des services de stockage (QoS) et d'évaluer les IOPS des machines virtuelles ;
- intégrer un switch virtuel permettant d'administrer et de monitorer les configurations réseaux de la plate-forme ;
- permettre de visualiser la consommation des ressources matérielles et des VM et de créer différents tableaux de bord entièrement personnalisables ;
- intégrer des mécanismes d'automatisation des opérations et d'amélioration de la productivité, sans codage ;
- être couverte par une garantie et un support constructeur 24/7 sur une période de cinq (5) ans.

Il s'agira, *in fine*, de disposer d'une infrastructure répondant aux spécifications détaillées, ci-après.

Toutefois, il vaut de noter que les spécifications techniques énumérées ne sont pas limitatives. Les soumissionnaires peuvent intégrer dans leurs offres des propositions d'amélioration qui devront, le cas échéant, se traduire par des options par rapport aux spécifications de base.

II.2.1. Architecture cible

L'infrastructure cible devra être résiliente et articulée autour de trois clusters répartis dans trois (3) sites, à savoir un de production au Siège, un de backup à l'Agence Principale de Dakar et un de secours à l'Agence Principale d'Abidjan.

Le cluster de production devra être composé de plusieurs nœuds répartis dans deux (2) salles distinctes (A et B) interconnectées par une liaison LAN en fibre optique. Il devra permettre l'hébergement des VM en haute disponibilité. Les infrastructures localisées dans chacune des salles devront être dimensionnées de sorte à opérer toute la production de la Banque en cas de perte de l'une des salles, sans incidence sur les traitements et les transactions, et de manière transparente pour les utilisateurs.

Le site de backup devra héberger un cluster étendu pour une reprise à chaud de toutes les VM en cas d'indisponibilité du site de production, sans dégradation des performances ni perte de données. Le site de backup est connecté à celui de production par une boucle en fibre optique de type MAN.

Le site de secours, dont la fonction principale est de garantir la continuité d'activités en cas de sinistre majeur à Dakar, permet de disposer d'un cluster étendu sur un troisième site. Il est relié au site de production par une liaison en fibre optique de type WAN.

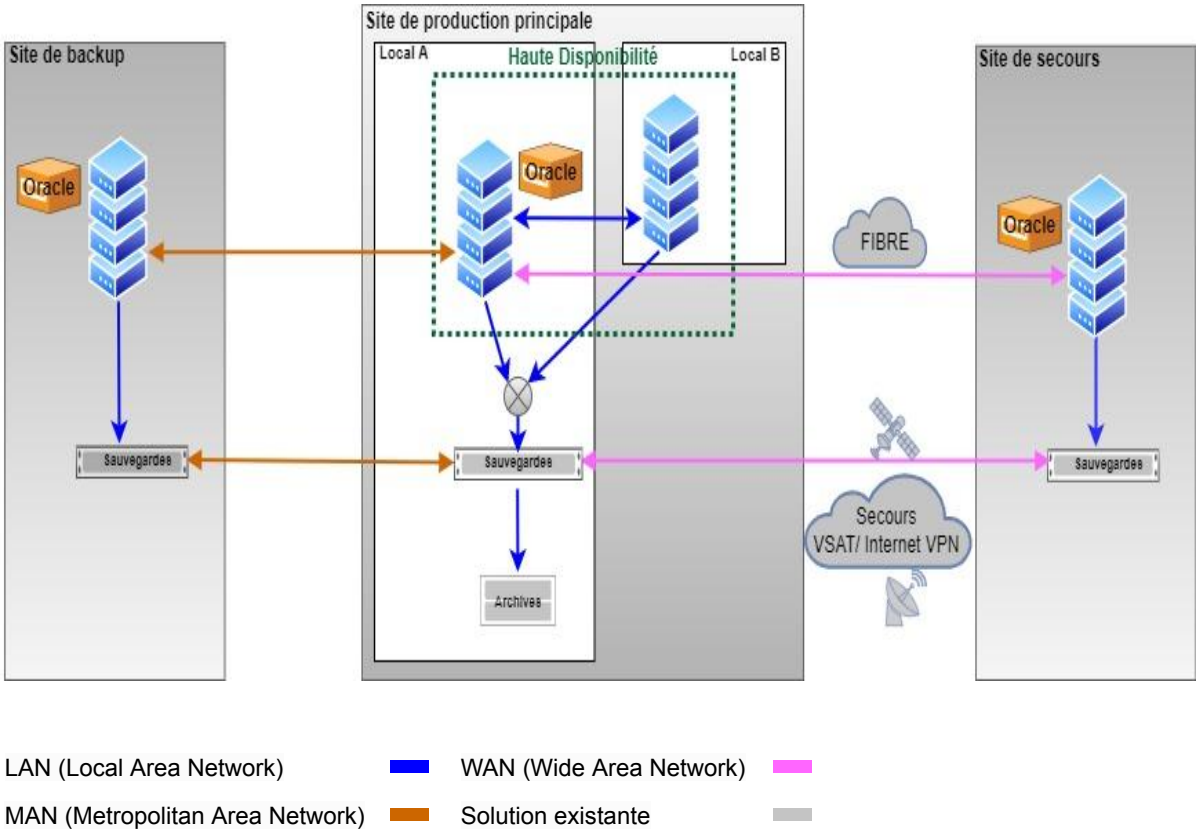

Figure 1: Architecture cible

II.2.2. Dimensionnement de la solution cible

La livraison des infrastructures devrait pouvoir se faire en deux (2) phases sur une période maximum de deux (2) ans, en lien avec les capacités en ressources existantes et celles estimées et projetées pour couvrir les besoins futurs.

A cet effet, les soumissionnaires sont invités à proposer dans leurs offres, les infrastructures matérielles et logicielles requises pour répondre au plan de capacité précisé dans le tableau ci-après.

Site	Local	Ressources	Capacités	
			Phase 1	Phase 2
Principal	Local A	Nombre de VM	300	500
		Disques Flash SSD (To)	245	445
		Disques SAS (To)	245	445
		Mémoire (To)	3	5
		Nombre de Coeurs	272	472
	Local B	Nombre de VM	300	500
		Disques Flash SSD (To)	245	445
		Disques SAS (To)	245	445
		Mémoire (To)	3	5
		Nombre de Coeurs	272	472
Backup		Nombre de VM	300	500
		Disques Flash SSD (To)	245	445
		Disques SAS (To)	245	445
		Mémoire (To)	3	5
		Nombre de Coeurs	272	472
Secours		Nombre de VM	300	500
		Disques Flash SSD (To)	245	445
		Disques SAS (To)	245	445
		Mémoire (To)	3	5
		Nombre de Coeurs	272	472

II.2.3. Architecture matérielle

Les nœuds des clusters devront être équipés de puissants processeurs Intel de type x86 Xeon de dernière génération ou équivalent ou supérieur, d'une grande capacité mémoire de type ECC ou supérieur, d'une capacité de stockage suffisante tenant compte du facteur de réplication RF2, de la configuration RAID1 et ne prenant pas en compte les optimisations liées au stockage (Parité, Erasure Coding, Compression, Déduplication, etc.), et des interfaces réseaux rapides (10 GbE ou plus) pour les transmissions de données.

Le matériel proposé devra utiliser une combinaison de disques durs de haute capacité (10 To ou plus) pour le stockage des données et de disques SSD de haute performance pour le stockage du cache et des métadonnées.

II.2.4. Licences

Il est attendu des soumissionnaires la fourniture de toutes les licences requises pour un bon fonctionnement de l'infrastructure, souscrites au nom de la BCEAO.

Par ailleurs, Ils devront fournir toutes les informations relatives à la politique de gestion des licences de leurs solutions (acquisition, renouvellement, fonctionnalités et pénalités).

II.2.5. Hyperviseur

L'infrastructure devra être fournie avec les licences hyperviseurs requises pour l'ensemble des nœuds. Par ailleurs, les hyperviseurs devront :

- permettre l'exécution des opérations usuelles telles que la création et/ou la modification de VM ;
- fournir des informations sur la performance des IO de stockage par disque virtuel, tels que le nombre d'IOPS, les débits en Mbps, la latence en milliseconde, sous format graphique ainsi que la source principale de distribution des IO (RAM, SSD et HDD) ;
- être capable de répartir automatiquement la charge des VM grâce à un algorithme d'équilibrage de charge, reposant sur l'utilisation de la mémoire, des CPU et des IOPS.

II.2.6. Évolutivité

L'infrastructure devra permettre une extension de ses capacités sans interruption de service. A cet égard, il devra être possible de rajouter des nœuds de différentes configurations dans un cluster, en mixant différentes technologies de disques (nœuds Full flash SSD ou NVMe, nœuds hybrides SSD/HDD ou NVMe/SSD, etc.) et de processeurs (nœuds de différentes générations de processeurs).

II.2.7. Résilience et haute disponibilité

L'infrastructure devra être entièrement redondante et être capable de procéder immédiatement à la reconstruction de données manquantes en cas de panne d'éléments matériels et/ou dysfonctionnements de composants logiciels. Elle devra être aussi capable de se prémunir contre la panne d'un élément matériel (contrôleur, disque, serveur) sans perte de données. A ce titre, la panne d'un disque ne devra pas occasionner une perte d'accès aux autres disques ou celle de données. De même, la panne d'un contrôleur de stockage ne devra pas entraîner le redémarrage ou l'arrêt des VM.

L'infrastructure devra également supporter les modes de réplication Factor 2 et Factor 3 avec la possibilité de définir le mode de réplication par conteneur de stockage sans arrêt des services.

Enfin, à la suite d'une panne, le système de reconstruction des données devra être capable de créer une seconde copie depuis les réplicas qui devront être répartis sur l'ensemble des nœuds afin d'éviter tout goulot d'étranglement.

II.2.8. Réplication

L'infrastructure devra être en mesure d'assurer la réplication site à site et/ou site à multisite, bidirectionnelle avec une fréquence synchrone (RPO=0) et asynchrone d'au moins 20s. Elle devra aussi permettre la réplication asynchrone entre deux ou plusieurs sites avec un RPO démarrant à partir de 20s.

De même, l'infrastructure devra offrir une granularité de réplication des VM avec un RPO modulable selon la criticité de la VM. Elle devra aussi permettre une segmentation des flux réseaux dédiés à la réplication synchrone et à la réplication asynchrone, et disposer d'un système de réplication hautement disponible et distribué sur plusieurs serveurs afin d'éviter toute rupture en cas d'incident d'un serveur physique ou virtuel. Elle devra aussi supporter le Volume Shadow Copy Service pour la consistance des données.

En outre, L'infrastructure devra permettre l'orchestration des opérations de basculement des applications vers un autre site à l'aide de fonctionnalités natives, à savoir l'ordonnancement du redémarrage des différentes VM, la dépendance entre certains groupes de VM, la gestion des adresses IP des VM (dynamiques ou statiques), l'exécution de tests de bascule sur un réseau spécifique hors production.

Il devra être aussi possible d'exécuter un script pendant la séquence de démarrage des VM, de tester à n'importe quel moment les plans de reprise ou de continuité d'activités et de générer des rapports de reprise et de conformité du système.

Les fonctions de réplication devront être natives et ne devront pas nécessiter l'ajout d'équipements ou de serveurs tiers.

II.2.9. Optimisation et performance

L'infrastructure devra permettre le rattachement des VM critiques de haute performance aux disques les plus rapides (Flash). Par ailleurs, il devra être possible de placer les données fréquemment utilisées dans le stockage rapide, la RAM ou les SDD. De même, les données moins sollicitées devront pouvoir être déplacées automatiquement sur des disques mécaniques.

L'infrastructure devra également implémenter, pour l'ensemble de la capacité offerte, des fonctions de compression en ligne ou à la volée (pour les écritures séquentielles), de compression en post-process (pour les données aléatoires), de déduplication, de snapshots et de clones. Elle devra aussi implémenter le support de codage à effacement (Erasure Coding) pour l'optimisation de l'espace de stockage.

Enfin, L'infrastructure devra permettre l'activation de la compression, la déduplication et le codage à effacement, en combinaison ou indépendamment les uns des autres.

II.2.10. Stockage unifié pour partage et archivage de données

L'infrastructure devra fournir des fonctions de partage de données, ainsi qu'une scalabilité pour répondre aux besoins de croissance future. Elle devra être évolutive afin de prendre en charge les technologies innovantes telles que le Machine Learning et l'analyse de données. Elle devra également être capable de supporter une grande volumétrie de données.

L'infrastructure devra permettre de mettre en place des stratégies de protection des données contre toute modification après stockage et les conserver dans un format non réinscriptible et non effaçable, conformément à la règle 17a-4 de la SEC, dans des archives conformes évolutives, par la suite WORM (Write Once Read Many). Elle devra être également conforme aux standards CIFS, SMB, NFS et S3.

L'infrastructure devra supporter un espace de noms global pour stocker («PUT») et retrouver («GET») les objets avec les commandes HTTPS du réseau, et intégrer les appels API REST dans des programmes ou scripts sans avoir à suivre les structures de répertoires complexes.

L'infrastructure devra permettre la gestion des versions d'un objet et les objets stockés devront pouvoir être soumis à des règles d'expiration.

L'infrastructure devra être évolutive à la hausse ou à la baisse (scale-out) et (Scale-up). Elle devra être hautement disponible avec une console de management web HTML5 distribuée sans aucun Single point of Failure (SPOF) avec un système d'auto-diagnostic et d'auto-réparation.

L'infrastructure devra supporter la réplication bidirectionnelle vers d'autres stockages objets et le tearing vers d'autres stockages objets. Elle devra disposer d'outils pertinents d'analyse des données hébergées.

II.2.11. Continuité des opérations et automatisation des tâches

Les soumissionnaires devront proposer, d'une part, des fonctions de sauvegarde locales convergées avec des snapshots. Ils devront mettre à disposition des fonctions de création illimitée de snapshots locaux avec une cohérence au niveau des VM des systèmes et des applications, d'une part, et de récupération instantanée de données, d'autre part.

Les soumissionnaires devront proposer également des fonctionnalités de sauvegarde à distance et de reprise après sinistre grâce à une fonction de réplication asynchrone ou équivalent, ou reposant sur la technologie des snapshots ou équivalent. Les snapshots de VM pourront être sauvegardés ou répliqués de manière asynchrone vers un autre centre de données selon un calendrier défini par l'utilisateur.

Les topologies de réplication proposées devront être souples et bidirectionnelles, et permettre des déploiements one-to-one, one-to-many et many-to-many. La réplication des données devra implémenter *a minima* des technologies de compression afin d'accroître son efficacité et réduire la consommation de la bande passante.

L'infrastructure proposée devra offrir une vue simplifiée de tous les snapshots locaux et distants, permettant ainsi aux administrateurs de restaurer une VM à partir d'un snapshot. En cas de sinistre, les administrateurs peuvent également basculer aisément une VM vers le site de backup ou de secours.

II.2.12. Sécurisation du trafic inter-VM

Les fonctions de sécurisation de trafic inter-VM devront permettre de sécuriser les applications à travers l'imposition de règles de pare-feu à une VM, à l'aide de tags, d'une part, et de séparer intégralement deux (2) environnements à travers l'application de catégories, étiquettes et tags, d'autre part.

Les fonctions de sécurisation devront permettre de gérer dynamiquement des politiques de sécurité basées sur un groupement logique de VM et une protection contre le changement d'adresses MAC au niveau des VM. Elles devront permettre, à partir d'une interface unique, d'appliquer des politiques de sécurité à des VM appartenant à différents clusters, avec la possibilité de suivre le déplacement des VM, indépendamment de l'infrastructure. Le monitoring et le recensement des flux de communication inter-VM devront être effectués de manière simple et graphique.

L'infrastructure devra permettre la mise en quarantaine d'une VM après détection d'un virus. Elle devra permettre aussi l'intégration d'une solution de *Service Chaining*, l'implémentation d'un cloud privé virtuel (VPC), la connection d'un VPC à des réseaux externes avec ou sans NAT, l'implémentation d'interconnexions VPN, et la gestion de politique d'accès au réseau avec des ACL sur VPC.

L'infrastructure devra permettre de corréler des vulnérabilités de sécurité potentielles à travers l'intégration d'un outil d'analyse, puis d'automatiser la réponse aux incidents ou de créer des workflows de micro-segmentation. Elle devra aussi permettre d'analyser les ressources de l'ensemble des charges de travail, puis d'auditer les résultats à l'aide de normes telles que CIS, NIST CSF v1.1, PCI-DSS v3.2.1, HIPAA et DISA STIG.

L'infrastructure devra permettre de développer une stratégie de flux d'applications et de données sous une architecture *Zero Trust* afin de créer des politiques d'autorisation et de blocage de trafics réseaux basées sur des ports et de hiérarchiser logiquement les charges de travail.

II.2.13. Authentification et chiffrement de données

L'outil de gestion centralisée devra utiliser le principe du moindre privilège et offrir un véritable modèle de défense en profondeur. La solution logiciel devra fournir des fonctionnalités d'authentification double facteurs et de chiffrement de données au repos. Le logiciel de gestion centralisée devra intégrer dans son cycle de vie de développement, un cycle de développement de la sécurité, afin de prendre en compte tout au long du développement du produit, les exigences de sécurité les plus fortes.

Le chiffrement des données au repos devra être fourni par des disques SED (Self Encrypting Drive) ou équivalent. Le chiffrement des données des utilisateurs et des applications devra être conforme à la norme FIPS 140-2 Level 2 ou équivalent, et permettre d'obtenir un niveau de protection élevé.

L'infrastructure devrait fournir une fonctionnalité de stockage sécurisé des clés de sécurité par l'intermédiaire du protocole standard KMIP (Key Management Interface Protocol) ou équivalent.

II.2.14. Microservices

L'infrastructure proposée devra permettre de déployer des applications cloud-natives, notamment celles livrées au format microservices, à travers des clusters Kubernetes. Elle devra permettre aussi de déployer des clusters Kubernetes Managés, incluant la gestion de la haute disponibilité des services Masters et Workers.

Par ailleurs, elle devra intégrer des outils de gestion et d'orchestration de containers. Elle devra être certifiée par le cloud native computing foundation (CNCF).

L'infrastructure devra prendre en compte la gestion des identités et des accès (IAM) avec Keycloak. Elle devra également prendre en charge de manière native le stockage persistant des clusters Kubernetes avec les trois types de stockage, à savoir le mode bloc, fichier et objet S3.

Les mises à jour des OS worker et la version de Kubernetes devront être assurées en pleine production ainsi que l'extension d'un cluster Kubernetes par l'ajout et suppression de worker sans arrêt de service.

Les outils de monitoring, de logs et d'alertes tels que Prometheus, ElasticSearch, Fluent Bit et Kibana (EFK Stack) devront être Intégrés. Par ailleurs, l'interface de déploiement et de management de cluster Kubernetes devra être hautement disponible et distribuée.

L'infrastructure devra permettre de déployer et de gérer des clusters Kubernetes hors ligne, en mode sombre (Dark Mode) afin de déconnecter les cluster Kubernetes de l'internet.

L'infrastructure devra permettre d'utiliser un registre Docker local et de verrouiller des nœuds par téléchargement de certificat éphémère pour accéder aux nœuds d'un cluster Kubernetes.

II.2.15. Infrastructure en tant que code

Il devra être proposé une approche de type "infrastructure en tant que code (IaC)", qui consiste à gérer et à provisionner l'infrastructure à l'aide de fichiers de code, et facilitant ainsi l'automatisation, la reproductibilité et la gestion cohérente de l'infrastructure applicative, système et réseau.

Une fonctionnalité de contrôle de version et de gestion des modifications devra être fournie pour permettre de suivre les modifications apportées à l'infrastructure au fil du temps, de collaborer avec d'autres membres de l'équipe et de revenir à des versions antérieures si nécessaire.

L'infrastructure devra intégrer également des fonctionnalités de Réseau en tant que code (NaC: Network as Code) pour la gestion automatisée de l'infrastructure réseau. Elle devra permettre de déployer et de configurer des infrastructures de réseau virtuel et physique via la configuration de commutateurs, d'interfaces, d'adresses IP, de VLAN, de routages, de règles de pare-feu, etc.

L'infrastructure en tant que code devra s'intégrer avec d'autres outils et processus, tels que la gestion des configurations, le monitoring, les sauvegardes, pour une gestion complète et harmonieuse de l'infrastructure.

II.2.16. Hybridation

L'infrastructure devra permettre d'étendre, de manière maîtrisée, ses capacités avec des ressources souscrites dans des environnements de type cloud public, tels que Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP). A ce titre, elle devra permettre de déplacer des applications, des charges de travail et des données entre clouds privés et publics, tout en maîtrisant les coûts.

Par ailleurs, l'infrastructure devra intégrer des mécanismes de sécurité de type *Zero Trust* afin de prévenir et de détecter les menaces et les pertes de données.

II.2.17. Service de fichiers

L'infrastructure devra supporter nativement le service de partage de fichiers en mode protocoles SMB et NFS (Besoin des partages de fichier utilisateurs) en tant que solution de stockage NAS avec des fonctions de gestion de quota, de sécurité, d'antivirus Offload scanning via ICAP, d'intégration à un contrôleur de domaine de type LDAP/SAMBA 4 et de protection de fichiers des utilisateurs avec la possibilité de les répliquer sur un autre cluster ou dans le cloud.

L'accès aux fichiers par les utilisateurs devra être possible, de manière sécurisée, à travers un navigateur web.

II.2.18. Self-service

L'infrastructure devra permettre la gestion du cycle de vie des applications à travers l'automatisation de la fourniture et la suppression des applications n-tier traditionnelles et des services distribués modernes, en utilisant des modèles pré-intégrés qui simplifient la gestion des applications dans les environnements privés et publics.

Elle devra permettre la création de Blueprint personnalisable pour simplifier la configuration et la gestion des applications à travers l'intégration des composants de chaque application, y compris les machines virtuelles, les Pods (containers), les configurations, les réseaux et les binaires associés, dans un modèle facile à utiliser pouvant être géré par les équipes en charge de l'infrastructure.

Il devra être également possible de déployer automatiquement des applications qui combinent des VM traditionnelles et de cloud natif (container) sur un cluster Kubernetes, de même que la publication des Blueprint d'application directement aux utilisateurs via un catalogue de services.

L'infrastructure devra être capable de maintenir le contrôle de la gouvernance à travers des rôles, limitant ainsi les opérations de l'utilisateur basées sur ses autorisations (approche RBAC).

II.2.19. Outil de management centralisé

L'outil de gestion centralisée devra être hautement disponible et distribué. Il devra disposer d'une unique interface centralisée "full" web, permettant d'assurer le monitoring des serveurs, des VM, du stockage, de la réplication et le catalogue de service, ainsi que de configurer, surveiller et administrer les composantes réseaux de toute la plateforme.

L'outil de gestion centralisée devra intégrer un moteur d'analyse prédictive basé sur des technologies de Machine Learning, permettant d'anticiper et de monitorer intelligemment les problèmes de performances et les manques de ressources. Il devra avoir des fonctions avancées de planification prédictive de la capacité, permettant d'optimiser l'expansion de celle-ci, en lien avec la consommation des ressources allouées (Capacity planning). Il devra aussi permettre de réaliser une analyse en temps réel des performances des VM afin de détecter des anomalies et permettre aux administrateurs d'automatiser des mesures correctives appropriées.

L'outil de gestion centralisée devra fournir en temps réel des rapports personnalisables et des tableaux de bord intelligents sur les performances et l'utilisation des VM, afin d'identifier simplement celles qui sont sous-dimensionnées, surdimensionnées ou dormantes. En outre, les administrateurs devront être capables d'utiliser des alertes intelligentes et des actions intégrées pour automatiser les tâches opérationnelles quotidiennes. Ils devront également user de fonctions d'orchestration pour définir des scénarios préétablis, afin d'effectuer une série d'actions en réaction au déclenchement d'un événement donné, notamment en cas d'incident.

Enfin, il devrait être possible de fournir aux équipes de développement ainsi qu'à la Direction un accès à des informations exploitables (métriques) sur l'infrastructure, d'exécuter des charges de travail (workloads) et de générer automatiquement des notifications via des alertes par courrier électronique, chat, etc..

II.2.20. Conformité à l'utilisation des produits Oracle

Les soumissionnaires sont invités à proposer dans leurs offres une infrastructure spécifique pour l'hébergement des produits Oracle, en l'occurrence le module General Ledger (GL) de la suite eBusiness (EBS) et les bases de données Oracle, en tenant compte des contraintes liées aux licences détenues par la Banque.

Il convient de noter que les licences Oracle Database devront être limitées strictement à celles existantes, à savoir 4 licences processeur au total.

Les soumissionnaires devront cependant, le cas échéant, proposer en option les licences complémentaires nécessaires pour conformer leurs propositions d'architecture aux exigences de l'éditeur Oracle.

L'infrastructure spécifique aux produits Oracle devra répondre à minima aux caractéristiques ci-après :

Site	Type	Coeurs utilisés	Mémoire brute	Capacité Disque brute
Principal	**HCI**	4	600 Go	32 To
Secondaire	**HCI**	4	600 Go	32 To

II.2.21. Intégration du système de sauvegarde et d'archivage existant

Le dispositif de sauvegarde existant, qui repose sur des appliances Dell EMC Data Domain et le logiciel EMC Networker, sera également conservé. Par conséquent, il devra être intégré à la solution cible.

A cet égard, les soumissionnaires devront définir une stratégie de sauvegarde, de restauration et d'archivage adéquate pour la solution cible. Cette stratégie devra offrir, au minimum, les mêmes performances et garanties que les techniques de sauvegarde en vigueur à la Banque. Elle devra, en outre, être testée et validée durant la phase de déploiement.

II.2.22. Infrastructure de postes de travail virtuels (VDI)

La Banque dispose d'un parc de postes de travail spécifiques, dédiés pour l'accès à des environnements sécurisés, étanches par rapport à l'internet et à l'intranet. Ces postes permettent par exemple d'accéder au périmètre des données de cartes bancaires (PCI-DSS), au réseau SWIFT, aux systèmes de paiement, aux réseaux d'administration des systèmes et des réseaux, etc.

Les soumissionnaires sont invités à proposer dans leurs offres une infrastructure pour la virtualisation de cent (100) postes de travail, répondant aux caractéristiques ci-après :

- processeur Intel Core i7 ou i5 ou équivalent ;
- 8 Go de RAM DDR4 minimum ;
- 500 Go de disque dur minimum ;
- système d'exploitation Windows 10 ou 11 64 bits ou Linux.

Les postes virtuels devront être accessibles en toute sécurité à distance, notamment en situation de crise.

En conséquence, les risques de perte et de fuite de données devront être entièrement pris en charge.

L'accès au bureau virtuel devra être possible à partir de divers périphériques, notamment des micro-ordinateurs fixes ou portables, ou des tablettes, préalablement autorisés.

L'infrastructure devra permettre une gestion centralisée des machines virtuelles, y compris le déploiement, la configuration, les mises à jour logicielles, la surveillance, les autorisations d'accès et la maintenance.

L'infrastructure devra fournir des fonctionnalités de sécurité robustes afin de protéger les données et les postes virtuels contre les menaces telles que les logiciels malveillants, les attaques par déni de service, les tentatives d'intrusion, etc.

L'infrastructure devra être capable de s'adapter à une augmentation ou à une diminution du nombre d'utilisateurs sans compromettre les performances et la disponibilité du système. Elle devra permettre une allocation dynamique des ressources système, telles que le processeur, la mémoire et le stockage, en fonction des besoins des utilisateurs.

Les administrateurs devront pouvoir gérer les profils des utilisateurs, personnaliser les bureaux virtuels par profil en installant des applications, en configurant des paramètres et en personnalisant l'interface utilisateur.

L'infrastructure devra prendre en charge l'exécution des applications hébergées localement et celles hébergées dans les centres de données de la BCEAO, en garantissant une expérience utilisateur fluide. Elle devra permettre la sauvegarde et la restauration des paramètres et des données spécifiques à chaque utilisateur.

La micro-segmentation réseau devra pouvoir être intégrée à un contrôleur de domaine LDAP/SAMBA 4 afin de garantir l'application automatique des règles de sécurité dès la connexion d'un utilisateur VDI.

Par ailleurs, le système de virtualisation devra être compatible avec les latences élevées inhérentes au réseau VSAT.

II.2.23. Prérequis réseaux

Les soumissionnaires devront préciser dans leurs offres, tous les prérequis réseaux à réunir pour un bon fonctionnement de leurs solutions, notamment en débits, latences, etc. entre nœuds d'un cluster, entre clusters synchrones et asynchrones, et entre la solution et le dispositif de sauvegarde existant.

II.2.24. Alimentations électriques

Tous les équipements devront être livrés avec des alimentations électriques 220-230V-50 Hz et cordons prise mâle type E/F (Norme CEE 7/7).

II.3. Prestations attendues

II.3.1. Intégration des socles techniques

Les soumissionnaires devront inclure dans leurs offres les prestations, ci-après :

- la fourniture des composants matériels et logiciels requis pour la mise en place des clusters dans les sites de production, de backup et de secours ;
- l'assemblage et l'installation des serveurs dans les racks ainsi que leur mise en service ;
- l'installation et la configuration des composants matériels et logiciels de la manière la plus optimisée possible ;

- la migration pilote, sur un échantillon représentatif des VM du SI ; les VM résiduelles seront migrées par les équipes internes, conformément aux procédures et modes opératoires à fournir par l'adjudicataire ;
- la migration des VM des bases de données Oracle hébergées sur les ODA et celles du module General Ledger (GL) de la suite eBusiness (EBS) vers l'infrastructure HCI spécifique, conformément aux exigences des licences ;
- la mise à niveau d'un échantillon représentatif des VM, en cohérence avec la version de l'hyperviseur (VMTools, drivers réseaux, disques), les VM résiduelles seront migrées par les équipes internes, conformément aux procédures et modes opératoires à fournir par l'adjudicataire ;
- l'équilibrage de la charge de travail sur l'ensemble des serveurs de virtualisation ;
- l'implémentation des nouvelles fonctionnalités attendues et celles éventuelles pour l'amélioration des performances, de sécurité et d'administration du SI ;
- la proposition d'un plan de gestion des risques sur les opérations de migration et de mise à niveau des systèmes (interruption de service, délais, cadencement, etc.).

II.3.2. Transfert de compétences

Il est attendu des soumissionnaires la proposition d'un programme de formations et de transfert de compétences pour l'installation, l'administration, l'exploitation et la maintenance de premier niveau de la solution, de manière autonome.

Le programme de formation devra être calibré pour huit (8) personnes, toutes compétences requises, et aboutir à des certifications délivrées par les constructeurs et éditeurs des composantes des solutions proposées.

Les formations devront se dérouler de préférence en présentiel, dans les locaux de la Banque.

II.3.3. Organisation du projet

Les soumissionnaires devront préciser tous les points d'organisation du projet, notamment les prérequis, le détail des prestations et un plan de migration. Ils devront préciser dans leurs offres la méthodologie de transfert des serveurs virtuels, en lien avec les contraintes de production interne.

L'infrastructure cible devra remplacer progressivement et de manière cohérente le système existant sur une durée maximum de deux (2) ans, selon les dispositions ci-après :

- la phase initiale portera sur la reprise des systèmes critiques sur l'ensemble des sites, y compris les bases de données et applications Oracle, en tenant compte des contraintes liées aux licences des produits détenues par la Banque ;
- la seconde phase consistera à étendre les infrastructures aux autres applications de production ainsi qu'à mettre en œuvre le dispositif de virtualisation des postes de travail qui accèdent à des environnements sécurisés.

Les soumissionnaires devront préciser dans leurs offres l'estimation de la durée de réalisation des prestations attendues. A cet égard, Ils devront proposer un planning détaillé des tâches à réaliser ainsi que les livrables à produire.

Le prestataire retenu travaillera avec les équipes pluridisciplinaires de la Direction des Systèmes d'Information qui apportera, au besoin, les appuis nécessaires au bon déroulement de la mission.

II.3.4. Documentation

Le prestataire retenu devra fournir la documentation complète des diverses solutions, notamment :

- les schémas d'intégration et les documents de configuration et d'installation des systèmes ;
- un dossier d'architecture technique, décrivant les composants déployés ;
- un dossier d'exploitation contenant les procédures d'accès aux composants, les fichiers de licences et le détail des configurations.

Enfin, le prestataire retenu devra livrer toute la documentation des constructeurs et éditeurs des composants de la solution proposée.

II.3.5. Recette du projet

Le prestataire retenu devra fournir une procédure de recette permettant de :

- valider le bon fonctionnement des services attendus ;
- valider les procédures livrées ;
- mesurer à un instant T : la charge des serveurs hôtes (CPU, RAM, Interfaces réseau), la charge IOPS sur le stockage et le taux de déduplication.
- A cet égard, Il devra proposer un dossier de réception dans lequel figureront, pour chaque fonctionnalité, la nature des tests à réaliser, les conditions de déroulement des tests et les résultats attendus.

ANNEXE I - FORMULAIRE DE SOUMISSION

(indiquer le lieu et la date)

A l' attention de :

MONSIEUR LE DIRECTEUR DU BUDGET ET DES APPROVISIONNEMENTS
BP 3108 DAKAR - BCEAO/SIEGE

Objet : Appel d'offres pour la fourniture et le déploiement d'une infrastructure résiliente de traitement de données à la BCEAO

Nous, soussignés....., soumettons par la présente, une offre de prix pour la fourniture et le déploiement d'une solution résiliente de traitement des données à la BCEAO pour un montant de….....FCFA HT/HD ou..... euros.

Nous déclarons, par la présente, que toutes les informations et affirmations faites dans cette offre sont authentiques et acceptons que toute déclaration erronée puisse conduire à notre disqualification.

Notre proposition engage notre responsabilité et, sous réserve des modifications résultant d'éventuelles négociations du marché, nous nous engageons, si notre proposition est retenue, à commencer la prestation au plus tard à la date convenue lors desdites négociations.

Signataire mandaté

Nom et titre du signataire

ANNEXE II - TABLEAU D'ÉVALUATION DES OFFRES TECHNIQUES

N°	Exigence	Conformité	Justificatifs et commentaires
Exigences d'ordre général			
1	Fournir une plateforme résiliente de traitement de données, reposant sur des infrastructures hyper-convergées (HCI)		
2	Faire partie des leaders du Magic Quadrant de Gartner, au titre des années 2021 et 2022, en termes d'infrastructures matérielles et logicielles hyperconvergées		
3	Supporter les principales solutions de virtualisation du marché		
4	Fournir une plateforme capable de présenter le stockage en mode bloc aux serveurs et de configurer des clusters de volumes		
5	Fournir la possibilité de séparer les flux réseaux afin de les sécuriser et d'isoler les flux iSCSI		
6	Fournir la possibilité de mettre à jour à chaud, sans déplacement de machines virtuelles et sans impact sur la production		
7	Supporter le cryptage des données stockées, ainsi que celui des VM basé sur KMS		
8	Permettre aux administrateurs de contrôler la qualité des services de stockage (QoS) et d'évaluer les IOPS des machines virtuelles		
9	Intégrer un switch virtuel permettant d'administrer et de monitorer les configurations réseaux de la plate-forme		
10	Permettre de visualiser la consommation des ressources matérielles et des VM et de créer différents tableaux de bord entièrement personnalisables		
11	Intégrer des mécanismes d'automatisation des opérations et d'amélioration de la productivité, sans codage		

12	Proposer une garantie et un support constructeur 24/7 sur une période de cinq (5) ans		
Architecture cible			
13	Proposer une infrastructure résiliente et articulée autour de trois clusters répartis dans trois (3) sites, à savoir un de production, un de backup et un de secours		
14	Proposer un cluster de production composé de plusieurs nœuds répartis dans deux (2) salles distinctes (A et B), permettant l'hébergement des VM en haute disponibilité		
15	Proposer un cluster étendu pour une reprise à chaud de toutes la charge de travail sur le site de backup		
16	Proposer un cluster étendu pour une reprise à chaud de toutes la charge de travail sur le site de secours		
Dimensionnement de la solution cible			
17	Fournir les infrastructures matérielles et logicielles requises pour répondre au plan de capacité précisé en II.2,2		
18	Livrer en deux (2) phases sur une période maximum de deux (2) ans conformément au plan de capacité précisé en II.2.2 couvrant les besoins futurs.		
Dimensionnement de la solution cible			
19	Fournir des nœuds équipés de puissants processeurs Intel de type x86 Xeon de dernière génération ou équivalent ou supérieur		
20	Fournir des nœuds équipés de mémoires de grande capacité de type ECC ou supérieur		
21	Fournir une capacité de stockage suffisante tenant compte du facteur de réplication RF2		
22	Fournir une capacité de stockage suffisante tenant compte de la configuration RAID1		
23	Fournir des interfaces réseaux rapides de 10 GbE ou plus		

24	Disposer de disques durs de haute capacité 10 To ou plus pour le stockage des données		
25	Disposer de disques SSD de haute performance pour le stockage du cache et des métadonnées		
Licences			
26	Fournir toutes les licences requises pour un bon fonctionnement de l’infrastructure		
27	Fournir toutes les informations relatives à la politique de gestion des licences de l'infrastructure (acquisition, renouvellement, fonctionnalités et pénalités)		
	Fournir des licences hyperviseurs requises pour l’ensemble des nœuds		
Hyperviseur			
28	Fournir des fonctions de répartition automatique de la charge des VM grâce à un algorithme d’équilibrage, reposant sur l’utilisation de la mémoire, des CPU et des IOPS		
29	Permettre l'exécution des opérations usuelles telles que la création et/ou la modification de VM		
30	Fournir des informations sur la performance des IO de stockage, des IO (RAM, SSD et HDD)		
Évolutivité			
31	Permettre l'extension des capacités disques (nœuds Full flash SSD ou NVMe, nœuds hybrides SSD/HDD ou NVMe/SSD, etc.) et processeurs (nœuds de différentes générations de processeurs) sans interruption de service		
Résilience et haute disponibilité			
32	Fournir une infrastructure entièrement redondante en cas de panne d’éléments matériels et/ou dysfonctionnements de composants logiciels		

33	Fournir une infrastructure supportant les modes de réplication Factor 2 et Factor 3 avec la possibilité de définir le mode de réplication sans arrêt des services		
Réplication			
34	Assurer une réplication site à site et/ou site à multisite		
35	Disposer d'une fonctionnalité bidirectionnelle avec une fréquence synchrone (RPO=0)		
36	Disposer d'une fonctionnalité asynchrone d’au moins 20s.		
37	Offrir une granularité de réplication des VM avec un RPO modulable selon la criticité de la VM		
38	Segmenter les flux réseaux dédiés à la réplication synchrone et à la réplication asynchrone		
39	Supporter la fonctionnalité Volume Shadow Copy Service		
40	Orchestrer les opérations de basculement des applications vers un autre site à l’aide de fonctionnalités natives		
41	Permettre l'ordonnancement du redémarrage des différentes VM		
42	Donner la possibilité de définir la dépendance entre les groupes de VM		
43	Donner la possibilité de gérer des adresses IP des VM (dynamiques ou statiques)		
44	Donner la possibilité d'exécuter des tests de bascule sur un réseau spécifique hors production		
45	Permettre l'exécution de script pendant la séquence de démarrage des VM		
46	Permettre de tester à n’importe quel moment les plans de reprise ou de continuité d’activités		
47	Permettre la génération de rapports de reprise et de conformité du système		

48	Disposer de fonctions de réplication natives ne nécessitant pas l'ajout d'équipements ou de serveurs tiers.		
Optimisation et performance			
49	Permettre le rattachement des VM critiques de haute performance aux disques les plus rapides (Flash)		
50	Placer les données fréquemment utilisées dans le stockage rapide, la RAM ou les SDD		
51	Déplacer automatiquement les données moins sollicitées sur des disques mécaniques		
52	Implémenter, pour l'ensemble de la capacité offerte, des fonctions de compression en ligne ou à la volée		
53	Implémenter, pour l'ensemble de la capacité offerte, des fonctions de compression en post-process de déduplication		
54	Implémenter des fonctions de snapshots et de clones		
55	Implémenter le support de codage à effacement (Erasure Coding) pour l'optimisation de l'espace de stockage		
56	Permettre l'activation de la compression, la déduplication et le codage à effacement, en combinaison ou indépendamment les uns des autres		
Stockage unifié pour partage et archivage de données			
57	Fournir des fonctions de partage de données scalable pour répondre aux besoins de croissance future		
58	Etre évolutive afin de prendre en charge les technologies innovantes telles que le Machine learning et l'analyse de données		
59	Etre capable de supporter une grande volumétrie de données		
60	Permettre de mettre en place des stratégies de protection des données contre toute modification après stockage		

61	Conserver les données dans un format non réinscriptible et non effaçable, conformément à la règle 17a-4 de la SEC		
62	Stockage des données d'archives implémentant la technologie WORM (Write Once Read Many)		
63	Etre conforme aux standards CIFS, SMB, NFS et S3		
64	Implémenter un espace de noms global pour stocker («PUT») et retrouver («GET») les objets avec les commandes HTTPS du réseau		
65	Permettre d'intégrer les appels API REST dans des programmes ou scripts sans avoir à suivre les structures de répertoires complexes		
66	Permettre la gestion des versions d'un objet		
67	Permettre de gérer des règles d'expiration de stockage des objets		
68	Permettre de faire évoluer le stockage à la hausse ou à la baisse (scale-out) et (Scale-up)		
69	Avoir une console de management web HTML5 distribuée sans aucun Single point of Failure (SPOF) avec un système d'auto-diagnostic et d'auto-réparation		
70	Supporter la réplication bidirectionnelle vers d'autres stockages objets		
71	Supporter le tearing vers d'autres stockages objets		
72	Disposer d'outils pertinents d'analyse des données hébergées		
Continuité des opérations et automatisation des tâches			
73	Fournir une fonction de création illimitée de snapshots locaux		
74	Fournir une fonction de récupération instantanée de données		
75	Fournir des fonctionnalités de sauvegarde à distance et de reprise après sinistre		
76	Fournir un mécanisme de réplication asynchrone ou équivalente		

77	Fournir des fonctionnalités de sauvegarde à distance et de reprise après sinistre reposant sur la technologie des snapshots ou équivalent		
78	Fournir une topologie de réplication bidirectionnelles		
79	Fournir une topologie de réplication permettant des déploiements one-to-one, one-to-many et many To many		
80	Implémenter a minima des technologies de compression		
81	Permettre un basculement aisé vers le site de backup ou de secours		
Sécurisation du trafic inter-VM			
82	Permettre la sécurisation de trafic inter-VM à travers l'imposition de règles de pare-feu à une VM, à l'aide de tags		
83	Permettre de séparer intégralement deux (2) environnements à travers l'application de catégories, étiquettes et tags		
84	Fournir des fonctions de sécurisation permettant de gérer dynamiquement des politiques de sécurité basées sur un groupement logique de VM		
85	Fournir des fonctions de sécurisation permettant une protection contre le changement d'adresses MAC au niveau des VM		
86	Permettre la mise en quarantaine d'une VM après détection d'un virus		
87	Permettre l'intégration d'une solution de Service Chaining		
88	Permettre l'implémentation d'un cloud privé virtuel (VPC)		
89	Permettre la connection d'un VPC à des réseaux externes avec ou sans NAT		
90	Permettre l'implémentation d'interconnexions VPN		
91	Permettre la gestion de politique d'accès au réseau avec des ACL sur VPC.		

92	Permettre de corréler des vulnérabilités de sécurité potentielles à travers l'intégration d'un outil d'analyse		
93	Permettre d'automatiser la réponse aux incidents ou de créer des workflows de micro-segmentation		
94	Permettre d'auditer les résultats selon les normes telles que CIS, NIST CSF v1.1, PCI-DSS v3.2.1, HIPAA et DISA STIG		
95	Permettre de développer une stratégie de flux d'applications et de données sous un modèle Zero Trust		
Authentification et chiffrement de données			
96	Fournir des fonctionnalités d'authentification double facteurs		
97	Fournir des fonctionnalités de chiffrement de données au repos		
98	Prendre en compte dans son cycle de vie de développement du logiciel de gestion centralisée un cycle de développement sécurisé		
99	Fournir des fonctionnalités de chiffrement des données au repos par des disques SED (Self Encrypting Drive) ou équivalent		
100	Chiffrer les données des utilisateurs et des applications conformément à la norme FIPS 140-2 Level 2 ou équivalent		
101	Fournir une fonctionnalité de stockage sécurisé des clés de sécurité par l'intermédiaire du protocole standard KMIP (Key Management Interface Protocol) ou équivalent.		
Microservices			
102	Permettre de déployer des applications cloud-natives		
103	Permettre de créer et gérer des clusters Kubernetes		
104	Intégrer des outils de gestion et d'orchestration de containers		

105	Etre certifiée par le cloud native computing foundation (CNCF)		
106	Prendre en charge de manière native le stockage persistant des clusters Kubernetes en mode bloc, fichier et objet S3		
107	Prendre en compte la gestion des identités et des accès (IAM) avec Keycloak		
108	Permettre les mises à jour des worker Kubernetes sans arrêt de service		
109	Monitorer les logs et alertes à l'aide de d'outils tels que Prometheus, ElasticSearch, Fluent Bit et Kibana (EFK Stack)		
110	Fournir une interface de déploiement et de management de cluster Kubernetes hautement disponible et distribuée		
111	Permettre de déployer et de gérer des clusters Kubernetes hors ligne, en mode sombre (Dark Mode)		
112	Permettre d’utiliser un registre Docker local		
113	Permettre de verrouiller des nœuds par téléchargement de certificat éphémère pour accéder aux nœuds d’un cluster Kubernetes		
Infrastructure en tant que code			
114	Proposer une approche de type “infrastructure en tant que code (IaC)”		
115	Proposer une fonctionnalité de contrôle de version pour la gestion des fichiers de code		
116	Proposer des fonctionnalités de Réseau en tant que code (NaC: Network as Code)		
Hybridation			
117	Permettre d’étendre les capacités avec des ressources souscrites dans des environnements de type cloud public		
118	Permettre de maîtriser les coûts dans le cas d'une extension des capacités avec des ressources souscrites dans des environnements de type cloud public		

119	Intégrer des mécanismes de sécurité de type Zero Trust afin de prévenir et de détecter les menaces et les pertes de données		
Service de fichiers			
120	Supporter nativement le service de partage de fichiers par les protocoles SMB et NFS pour les besoins de partages des fichiers utilisateurs		
121	Supporter nativement le service de partage de fichiers en tant que solution de stockage NAS		
122	Proposer des fonctions de gestion de quota		
123	Proposer des fonctions de sécurité et d'antivirus Offload scanning via ICAP		
124	Permettre l'intégration à un contrôleur de domaine de type LDAP/SAMBA 4		
125	Permettre l'accès aux fichiers par les utilisateurs de manière sécurisée, à travers un navigateur web		
Selfservice			
126	Permettre la gestion du cycle de vie des applications à travers l'automatisation de la fourniture des applications n-tier traditionnelles		
127	Permettre la gestion du cycle de vie des applications à travers l'automatisation de la fourniture des services distribués modernes		
128	Permettre la création de Blueprint personnalisable pour simplifier la configuration et la gestion des applications, des composants de chaque application, des machines virtuelles, des Pods, des configurations, des réseaux et des binaires associés		
129	Permettre de déployer automatiquement des applications qui combinent des VM traditionnelles et du cloud natif (container) sur un cluster Kubernetes		
130	Permettre la publication des Blueprint d'application directement aux utilisateurs via un catalogue de services		

131	Permettre le contrôle de la gouvernance à travers des rôles, limitant ainsi les opérations de l'utilisateur basées sur ses autorisations (approche RBAC)		
Outil de management centralisé			
132	Disposer d'un outil de gestion centralisée ayant une unique interface centralisée “full” web		
133	Disposer d'un outil de gestion centralisée hautement disponible et distribué		
134	Disposer d'un outil permettant d’assurer le monitoring des serveurs, des VM, du stockage, de la réplication, du catalogue de service, de la configuration, des composantes réseaux de toute la plateforme		
135	Intégrer un moteur d’analyse prédictive basé sur des technologies de Machine Learning, permettant d’anticiper et de monitorer intelligemment les problèmes de performances et les manques de ressources		
136	Disposer de fonctions avancées de planification prédictive de la capacité (Capacity planning)		
137	Permettre de réaliser une analyse en temps réel des performances des VM afin de détecter des anomalies		
138	Fournir en temps réel des rapports personnalisables et des tableaux de bord intelligents sur les performances et l'utilisation des VM		
139	Fournir des fonctions d'alertes intelligentes et des actions intégrées pour automatiser les tâches opérationnelles quotidiennes		
140	Fournir des fonctions d’orchestration permettant de définir des scénarios préétablis, en réaction au déclenchement d’un événement donné, notamment en cas d’incident		
141	Fournir un accès aux informations exploitables (métriques) de l'infrastructure, des charges de travail (workloads)		
142	Générer automatiquement des notifications via des alertes par courrier électronique, chat, etc.		

Conformité à l'utilisation des produits Oracle			
143	Proposer une infrastructure spécifique pour l'hébergement des produits Oracle		
144	Proposer une infrastructure spécifique conforme aux contraintes liées aux licences détenues par la Banque (licences Oracle Database limitées strictement à 4 licences processeur au total)		
Intégration du système de sauvegarde et d'archivage existant			
145	Intégrer à la solution cible le dispositif de sauvegarde existant, qui repose sur des appliances Dell EMC Data Domain		
146	Définir une stratégie de sauvegarde, de restauration et d'archivage adéquate pour la solution cible		
Infrastructure de postes de travail virtuels (VDI)			
147	Respecter les caractéristiques minimales des VDI ci-après : processeur Intel Core i7 ou i5 ou équivalent ; 8 Go de RAM DDR4 minimum ; 500 Go de disque dur minimum ; système d'exploitation Windows 10 ou 11 64 bits ou Linux.		
148	Fournir des solutions de maitrise des risques de perte et de fuite de données		
149	Permettre l'accès à partir de divers périphériques, notamment des micro-ordinateurs fixes ou portables, ou des tablettes, préalablement autorisés		
150	Fournir une interface de gestion centralisée des VDI		
151	Fournir des fonctionnalités de sécurité robustes afin de protéger les données et les postes virtuels contre les menaces telles que les logiciels malveillants, les attaques par déni de service, les tentatives d'intrusion, etc.		
152	Fournir une infrastructure scalable, capable de s'adapter à une augmentation ou à une diminution du nombre d'utilisateurs sans compromettre les performances et la disponibilité du système		

153	Permettre une allocation dynamique des ressources système, telles que le processeur, la mémoire et le stockage, en fonction des besoins des utilisateurs		
154	Permettre une gestion de profils par utilisateurs		
155	Permettre de personnaliser les bureaux virtuels par profil en installant des applications, en configurant des paramètres et en personnalisant l'interface utilisateur.		
156	Prendre en charge l'exécution des applications hébergées localement en garantissant une expérience utilisateur fluide		
157	Prendre en charge l'exécution des applications hébergées dans les centres de données de la BCEAO en garantissant une expérience utilisateur fluide		
158	Permettre la sauvegarde et la restauration des paramètres et des données spécifiques à chaque utilisateur		
159	Permettre d'implémenter une micro-segmentation réseau en intégrant un contrôleur de domaine LDAP/SAMBA 4 afin de garantir l'application automatique des règles de sécurité dès la connexion d'un utilisateur VDI		
160	Être compatible avec les latences élevées inhérentes au réseau VSAT		
Prérequis réseaux			
161	Préciser tous les prérequis réseaux à réunir pour un bon fonctionnement de la solution		
Alimentations électriques			
162	Fournir des alimentations électriques 220-230V-50 Hz et cordons prise mâle type E/F (Norme CEE 7/7).		
Intégration des socles techniques			
163	Fournir des composants matériels et logiciels requis pour la mise en place des clusters dans les sites de production, de backup et de secours		

164	Assembler et Installer des serveurs dans les racks ainsi que leur mise en service		
165	Installer et la configurer les composants matériels et logiciels de la manière la plus optimisée possible		
166	Procéder à la migration pilote, sur un échantillon représentatif des VM du SI et produire les procédures et modes opératoires de maîtrise		
167	Migrer les VM des bases de données Oracle hébergées sur les ODA et celles du module General Ledger (GL) de la suite eBusiness (EBS) vers l'infrastructure HCI spécifique		
168	Mettre à niveau un échantillon représentatif des VM, en cohérence avec la version de l'hyperviseur (VMTools, drivers réseaux, disques) et produire les procédures et modes opératoires de maîtrise		
169	Equilibrer de la charge de travail sur l'ensemble des serveurs de virtualisation		
170	Implémenter les nouvelles fonctionnalités attendues et celles éventuelles pour l'amélioration des performances, de sécurité et d'administration du SI		
171	Proposer un plan de gestion des risques sur les opérations de migration		
172	Proposer un plan de mise à niveau des systèmes (interruption de service, délais, cadencement, etc.)		
Transfert de compétences			
173	Proposer un programme de formations et de transfert de compétences pour l'installation, l'administration, l'exploitation et la maintenance de premier niveau de la solution, de manière autonome		
174	Préciser si les formations sont certifiantes pour huit (8) personnes, toutes compétences requises		
175	Dispenser les formations de préférence en présentiel, dans les locaux de la Banque		