AMF-UMOA

AUTORITÉ DES MARCHÉS FINANCIERS DE L'UNION MONÉTAIRE OUEST AFRICAINE

INSTRUCTION N° 7 6 /AMF-UMOA/2023

RELATIVE À LA GOUVERNANCE DU DÉPOSITAIRE CENTRAL / BANQUE DE RÈGLEMENT (DC/BR)

L'Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine,

Vu le Traité révisé de l'Union Monétaire Ouest Africaine (UMOA) du 12 juillet 2019, entré en vigueur le 1er octobre 2022, modifiant la dénomination du Conseil Régional de l'Epargne Publique et des Marchés Financiers (CREPMF) en Autorité des Marchés Financiers de l'UMOA (AMF-UMOA) ;

Vu la Convention du 3 juillet 1996 portant création du Conseil Régional de l'Épargne Publique et des Marchés Financiers (ci-après le « Conseil Régional ») et son Annexe portant composition, organisation, fonctionnement et attributions du Conseil Régional de l'Épargne Publique et des Marchés Financiers, notamment en son article 21 ;

Vu le Règlement Général n°001/97 du 28 novembre 1997 relatif à l'organisation, au fonctionnement et au contrôle du marché financier régional notamment en ses articles 10 et 16 ;

Vu l'Acte Uniforme de l'OHADA relatif au droit des sociétés commerciales et du groupement d'intérêt économique du 30 janvier 2014 ;

Vu l'Instruction n°3/97 du 29 novembre 1997 relative à l'habilitation du Dépositaire Central/Banque de Règlement ;

Vu la Décision n° 004 du 29/04/2021/CM/UMOA portant nomination du Président du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu les délibérations de l'AMF-UMOA en sa 98ème session ordinaire du 23 décembre 2023, tenue à Cotonou en République du Bénin ;

ARRÊTE

TITRE 1. DISPOSITIONS GÉNÉRALES

Article 01 : Définitions

Aux fins de la présente Instruction, an entend par :

a) Administrateur : une personne physique désignée par les statuts ou par l'Assemblée Générale, conformément aux dispasitians du droit des sociétés commerciales applicables au Dépositaire Central / Banque de Règlement. Il est membre de l'organe délibérant. La personne physique, représentant permanent d'une personne morale administrateur, est assimilée aux administrateurs.

b) Administrateur indépendant : un administroteur qui n'entretient aucune relation de quelque nature que ce sait avec le DC/BR ou son groupe, susceptible d'altérer son indépendance de jugement ou de le placer dans une situation de conflit d'intérêts apparent ou potentiel.

c) Administrateur non exécutif : un administrateur qui n'a aucune responsabilité de gestian au sein du DC/BR.

d) Assemblée Générale : l'instance regroupant les détenteurs d'actions formont le capital social du DC/BR. Elle a le pouvoir de prendre toute décision intéressant le DC/BR, sous réserve des compétences ou pouvoirs dévolus légalement à l'argane exécutif au à l'organe délibérant. A cet effet, elle délibère dans les conditions de quorum définies par le droit des sociétés applicable au DC/BR et les statuts.

e) Conflits d'intérêts : une situation aù les intérêts personnels d'un membre des organes de gouvernance ou d'un membre du personnel ou de ceux des personnes avec qui ils ont un lien de parenté ne sont pas compatibles avec les intérêts du DC/BR et pourraient, de ce fait, influencer l'impartialité attendue d'eux dans l'accamplissement de leurs fonctions.

f) Déclaration de gouvernance d'entreprise : Déclaration portant sur l'ensemble des informations clés relatives à l'application des règles de gauvernance du DC/BR au caurs d'une année.

g) Dépositaire Central / Banque de Règlement ou DC/BR : La société autorisée, par agrément de l'AMF-UMOA à exercer, sur l'ensemble du territoire des Étots de l'Union, las activités ci-après : la conservation et la circulation scripturale des titres admis à ses apérations, la gestion du cycle des règlements-livraisons, le paiement en numéraire, en qualité de Banque de Règlement, des soldes issus des compensations relatives aux transactians boursières.

h) Directeur Général : une personne physique, nommée par l'organe légalement habilité à cet effet, natamment le Conseil d'Administratian, pour assurer la direction du DC/BR et le représenter dans ses rapports avec les tiers. Le Directeur Général est investi des pouvoirs les plus étendus pour agir au nom du DC/BR, dans la limite de l'abjet social et sous réserve de ceux expressément attribués aux Assemblées Générales ou spécialement réservés à l'organe délibérant par des dispasitions légales ou statutaires.

i) Dirigeants : Les personnes membres de l'organe exécutif, notamment celles ayant la qualité de directeur, de responsable en charge des antennes ou bureaux de représentation ou succursales, d'administrateur provisoire et de liquidateur.

j) Gouvernance d'entreprise : l'ensemble des relations entre l'organe exécutif du DC/BR, son organe délibérant, ses actionnaires et d'autres parties prenantes qui établissent le cadre dans lequel sont fixés les objectifs du DC/BR ainsi que les moyens de les atteindre et d'en contrôler la réalisation. La gouvernance détermine l'attribution des pouvoirs et des responsabilités ainsi que les mécanismes de prise de décision dans le cadre des textes internes régissant le DC/BR ;

k) Lien de parenté : la relation entre deux personnes appartenant à la même famille, notamment les conjoints, les parents en ligne directe et collatérale jusqu'au quatrième degré que sont les parents, grands-parents, arrière-grands-parents, enfants, petits-enfants, arrière-petits-enfants, frères et sœurs, oncles et tantes, grands-oncles et grands-tantes, neveux et nièces, cousins germains ;

l) Obligation de diligence : l'obligation, pour tout administrateur et tout membre de l'organe exécutif, de prendre des décisions et d'agir de façon éclairée et prudente en ce qui concerne le DC/BR. L'obligation de diligence fait référence à la prudence avec laquelle l'administrateur ou le membre de l'organe exécutif gérerait ses propres affaires ;

m) Obligation de loyauté : l'obligation, pour tout administrateur et tout membre de l'organe exécutif, d'agir en toute bonne foi dans l'intérêt du DC/BR. En vertu de cette obligation, l'administrateur ou le membre de l'organe exécutif ne doit pas agir, dans son propre intérêt ou dans l'intérêt d'une personne ou d'un groupe, au détriment du DC/BR et de l'ensemble du marché financier régional de l'UMOA ;

n) Organes de gouvernance : l'organe délibérant, y compris ses comités spécialisés ainsi que l'organe exécutif ;

o) Organe délibérant : le Conseil d'Administration dans les sociétés anonymes ou l'organe collégial dans les sociétés constituées sous une autre forme. Il est investi de tous les pouvoirs pour agir en toutes circonstances au nom du DC/BR, dans la limite de l'objet social et des compétences réservées à l'Assemblée Générale ;

p) Organe exécutif : l'ensemble des structures qui concourent à la gestion courante du DC/BR et assurent l'application effective de l'orientation de l'activité définie par l'organe délibérant. Sont notamment considérés comme membres de l'organe exécutif, le Directeur Général, les Directeurs Généraux Adjoints, le Secrétaire Général, les Responsables des fonctions de contrôle, les Directeurs des Départements regroupant des Directions et des Directeurs des Directions directement rattachées au Directeur Général.

q) Parties liées : les personnes physiques et morales qui sont directement ou indirectement liées au DC/BR. Les parties liées regroupent notamment :

i. la maison-mère du DC/BR et toute entité sur laquelle ce dernière exerce un contrôle exclusif, un contrôle conjoint ou une influence notable ;

ii. toute entité sur laquelle le DC/BR exerce un contrôle exclusif, un contrôle conjoint ou une influence notable ;

iii. une personne physique qui exerce un contrôle exclusif, un contrôle conjoint ou une

influence notable sur le DC/BR ;

iv. une personne physique ou morale qui détient au moins 10% des droits de vote au sein du DC/BR ;

v. les administrateurs et les dirigeants du DC/BR ;

vi. les entreprises privées dans lesquelles les personnes physiques visées aux points iii), iv) et v) ci-dessus exercent des fonctions de direction, d'administration, de gérance, ou détiennent plus de 25% du capital social ;

vii. les personnes ayant un lien de parenté proche avec les personnes physiques visées aux points iii), iv) et v) ci-dessus.

Les termes qui ne sont définis ni dans la présente Instruction, ni dans ses Annexes, auront le sens qui leur est habituellement attribué.

Article 02 : Objet et champ d'application

La présente instruction fixe les règles minimales en matière de gouvernance devant être observées par le Dépositaire Central / Banque de Règlement (DC/BR).

TITRE 2. DISPOSITIF ET PRINCIPES DIRECTEURS DE LA GOUVERNANCE D'ENTREPRISE

Article 03 : Principes directeurs de la gouvernance d'entreprise

Le DC/BR doit :

1. avoir des objectifs axés sur sa sécurité et son efficience et qui soutiennent explicitement la stabilité du système financier et le développement du marché financier régional.
2. avoir des dispositions relatives à sa gouvernance qui soient documentées et qui définissent des niveaux de responsabilité clairs et directs. Ces dispositions devraient être communiquées aux actionnaires, aux autorités compétentes, aux parties prenantes et, plus généralement, au public.
3. énoncer clairement les rôles et les responsabilités du Conseil d'Administration et les procédures régissant le fonctionnement dudit conseil, notamment les procédures servant à identifier, gérer et régler les conflits d'intérêts des membres, devraient être documentées. Le conseil doit examiner chaque année à la fois ses performances globales et les performances de ses différents membres.
4. désigner au sein de son Conseil d'Administration des membres, disposant des compétences, de l'honorabilité et des incitations appropriées pour remplir leurs rôles.

Article 04 : Principes de proportionnalité et de transparence

Le DC/BR met en place un dispositif de gouvernance transparent et adapté à sa taille, sa structure, la nature et la complexité de ses activités ainsi qu'à son profil de risque et, le cas échéant, à celui du groupe auquel il appartient.

Le cadre de gouvernance doit être adapté à son envergure et aux conséquences de sa défaillance éventuelle sur la stabilité du marché financier régional de l'UMOA.

Le dispositif de gouvernance doit notamment :

- être élaboré et mis en œuvre en tenant compte notamment de la sécurité des systèmes d'information, de la couverture de l'ensemble des risques encourus par le DC/BR et des éventuels conflits d'intérêts ;
- établir et formaliser les stratégies, politiques et procédures à mettre en place, pour définir et organiser les divers moyens nécessaires à l'atteinte d'une saine gouvernance ;
- définir les rôles et obligations des intervenants ;
- répondre aux besoins du DC/BR dans son ensemble et de chacune de ses unités organisationnelles et opérationnelles ;
- intégrer des mécanismes visant à maintenir et/ou rétablir son fonctionnement en cas de discontinuité ;
- refléter, au fil du temps, les changements découlant des caractéristiques du DC/BR et de son environnement externe ainsi que des évolutions relatives aux meilleures pratiques en matière de gouvernance ;
- prévoir des mécanismes permettant de s'assurer de l'intégrité et de l'engagement des intervenants, qui doivent être en nombre suffisant, compétents et avoir une bonne connaissance des activités du DC/BR, de ses risques ainsi que de ses obligations juridiques.

Les statuts du DC/BR doivent intégrer le principe de transparence tenant à la diffusion des informations aux parties prenantes.

Article 05 : Structure d'organisation de la gouvernance d'entreprise

Le DC/BR est doté d'un Conseil d'Administration et des Comités spécialisés. Il est dirigé par un Président du Conseil d'Administration et un Directeur Général.

Article 06 : Charte de Gouvernance d'Entreprise

Le DC/BR doit disposer d'une Charte de Gouvernance d'Entreprise, qui reprend les principes et règles sur la base desquels fonctionnent le Conseil, ses administrateurs et ses comités. Cette charte doit être approuvée par le Conseil d'Administration de la société.

Cette charte doit comporter au minimum les dispositions du modèle en annexe de la présente Instruction.

TITRE 3. CONSEIL D'ADMINISTRATION ET COMITES SPECIALISES

Article 07 : Responsabilités générales du Conseil d'Administration

Le Conseil d'Administration du DC/BR doit :

1. définir et approuver la stratégie globale du DC/BR, son cadre général de gouvernance, sa culture d'entreprise ainsi que ses principes et ses valeurs ;
2. énoncer clairement les rôles et les responsabilités de l'organe exécutif ;
3. définir un cadre de gestion des risques clair et documenté, incluant la politique de tolérance aux risques du DC/BR, assignant la responsabilité des décisions relatives aux risques et traitant de la prise de décisions en situation de crise ou d'urgence. Les dispositions relatives à la gouvernance devraient permettre aux fonctions de gestion des risques et de contrôle interne d'avoir un pouvoir, une indépendance, des ressources et un accès au conseil suffisants ;
4. veiller à ce que la conception, les règles, la stratégie globale et les décisions majeures du DC/BR tiennent compte, de manière appropriée, des intérêts légitimes de ses participants directs et indirects, ainsi que de ceux des autres parties prenantes concernées. Les décisions majeures devraient être clairement communiquées aux parties prenantes concernées et rendues publiques en cas de répercussions sur le marché dans son ensemble.

Le Conseil d'Administration assume la responsabilité ultime de la solidité financière du DC/BR et de sa conformité aux dispositions légales et réglementaires régissant ses activités.

Il doit s'impliquer de manière effective dans les activités du DC/BR, conformément à ses attributions légales, réglementaires et statutaires. Il est tenu à cet effet, de s'informer des changements importants découlant de l'environnement économique ou opérationnel du DC/BR et d'agir en temps opportun pour protéger les intérêts à long terme du marché financier régional et du DC/BR.

Article 08 : Responsabilités spécifiques du Conseil d'Administration

Dans le cadre de la mise en œuvre de ses responsabilités spécifiques, le Conseil d'Administration doit notamment :

1. s'assurer, en permanence, de l'adéquation des niveaux de fonds propres au regard des engagements définis, notamment dans le cadre de la concession de service public accordée au DC/BR ;
2. surveiller la conception et la mise en œuvre du système de rémunération du DC/BR ainsi que des processus de contrôle y afférents ;
3. veiller à ce que les transactions avec les parties liées, y compris les transactions intra-groupes, soient identifiées, évaluées et soumises à des exigences appropriées ;
4. promouvoir une culture d'entreprise valorisant un comportement éthique, adhérer à ces valeurs et veiller à leur respect par l'organe exécutif et le personnel du DC/BR ;

5. s'assurer que le DC/BR entretient des relations régulières avec l'AMF-UMOA ;
6. veiller à la réalisation des investissements nécessaires pour assurer la continuité de l'activité et garantir les objectifs de performance ;
7. prendre connaissance des rapports et Décisians de l'AMF-UMOA et suivre la mise en œuvre, dans les délais requis, des Décisions et recommandations y contenues.

Le Conseil d'Administration doit notamment approuver :

8. toutes les politiques du DC/BR ;
9. le Règlement Général du DC/BR et ses textes d'application ;
10. le degré d'appétence pour le risque du DC/BR et les limites de risque ;
11. les décisions d'externalisatian des activités et d'utilisation de nouveaux produits au services, les modifications substantielles de produits ou services existants oinsi que les initiatives et les opérations stratégiques importantes telles que les grandes opérations d'acquisition, la modification des systèmes, des processus et du modèle économique ;
12. les dispositifs de gouvernance des risques et de contrôle interne. Il est tenu de veiller à ce que la mise en œuvre desdits dispositifs soit conforme à l'ensemble des exigences énoncées respectivement dons l'Instruction relotive à la gestion des risques et celle relative ou contrôle interne.

Article 09 : Obligations de l'organe délibérant vis-à-vis de l'organe exécutif

En plus des attributions et des obligations qui lui sont dévolues, le Conseil d'Administration doit superviser la gestion des activités de l'organe exécutif du DC/BR.

À ce titre, le Conseil d'Administration doit notamment :

1. surveiller et évaluer les performances du Directeur Général, des Directeurs Généraux Adjoints et des responsables des fonctions de contrôle ;
2. s'assurer du respect des exigences de la Concession de service public accordée par les États membres de l'Union au DC/BR ;
3. veiller à l'évaluation des tarifs oppliqués par le DC/BR ;
4. s'assurer de la mise en œuvre des actions innovantes et des octivités de développement ;
5. fixer à l'organe exécutif des objectifs de performance et des niveoux de rémunération adéquats et cahérents avec lo stratégie à long terme et la solidité finoncière du DC/BR.

Article 10 : Délégation de pouvoirs et compétences du Conseil d'Administration

Le Conseil d'Administration peut déléguer certains de ses pouvoirs et compétences aux comités spécialisés.

La délégation de pouvoirs au l'externalisation de certaines activités du DC/BR n'exonère pos l'organe délibérant de ses responsabilités.

Article 11 : Composition du Conseil d'Administration

Le Conseil d'Administration doit être compasé, de manière équilibrée, d'administrateurs dotés de compétences et d'expériences complémentaires dans les domaines d'intérêts du DC/BR. Sans préjudice des dispositions légales ou statutaires, l'effectif des membres du Conseil d'Administration tient compte du principe de prapartiannalité et fait l'objet d'examens périodiques.

Les administrateurs non-exécutifs doivent représenter, à tout mament, au moins trois quart (3/4) des membres du Conseil d'Administration.

Le Conseil d'Administration doit être compasé d'au moins deux (02) odministroteurs indépendants.

Article 12 : Critères de qualification d'un administrateur indépendant

Sans préjudice de lo définitian énoncée à l'article premier, les critères pour qualifier un administrateur d'indépendant sont les suivants :

1. ne pas être ou avoir été au cours des quatre années précédentes salarié ou membre de l'organe exécutif du DC/BR ;
2. ne pas être salarié, ou administrateur de la maison-mère du DC/BR ou d'une société que celle-ci contrôle au cours des quatre années précédentes ;
3. ne pas être membre de l'organe exécutif d'une entreprise où le DC/BR détient directement ou indirectement un mandat au sein de l'organe délibérant ou dans laquelle un membre de l'organe exécutif du DC/BR, en exercice ou l'ayant été au cours des quatre dernières années, détient un mandat au sein de son organe délibérant ;
4. ne pas être membre des organes délibérant et exécutif d'un client, adhérent, affilié ou d'un fournisseur significatif du DC/BR ou de son groupe, ou pour lequel le DC/BR ou son groupe représente une part significative de l'activité ;
5. ne pas avoir directement au indirectement, avec le DC/BR, une relation d'offaires en cours ou durant les quatre années précédentes ;
6. ne pas avair de lien familial proche avec un membre de l'argane exécutif ou un membre du Canseil d'Administration représentant un actionnaire privé du DC/BR ;
7. ne pas avair été commissaire aux comptes du DC/BR au cours des quatre années précédentes ;
8. ne pas être membre du Conseil d'Administration du DC/BR depuis plus de dix ans ;
9. ne pas exercer un mandat électif à caractère politique ou des fonctions ministérielles ;
10. être libre de taute influence, de nature palitique ou patrimoniale d'origine interne au externe au DC/BR, qui puisse compramettre l'exercice de sa liberté de jugement.

Le statut d'administrateur indépendant est réexaminé chaque année par le Canseil d'Administration ou le camité dédié à la namination, le cas échéant.

L'AMF-UMOA peut décider qu'un administrateur, bien que remplissant les critères visés ci-dessus, ne doit pas être qualifié d'indépendant lorsqu'il est en situation de conflit d'intérêts réel, opparent au potentiel. Dans le cas où cette décision ne permet pas d'avoir l'effectif minimum requis d'administrateurs indépendants, le DC/BR doit procéder, dans un délai de six (06) mois à la cooptation ou lo nomination d'un nouvel administrateur indépendant prenant en compte les observations justifiant la décision de l'AMF-UMOA.

Article 13 : Compétences des membres du Conseil d'Administration

Les membres de l'organe délibérant doivent disposer individuellement ou collectivement de compétences appropriées dans les domaines des opérations de bourse, de dépositaire, de banque, de l'analyse financière, des technologies de l'information, de la planification stratégique, de la gouvernance, de la gestion des risques, du contrôle interne, des marchés de capitaux ou des politiques de rémunération ou de tout autre domaine jugé pertinent pour le développement du DC/BR.

Article 14 : Processus de sélection des membres du Conseil d'Administration

Le Conseil d'Administration doit disposer d'un processus formalisé pour identifier, évaluer et sélectionner les administrateurs qui seront désignés par les stoiuts ou, le cas échéant, por l'Assemblée Générale.

Les membres du Conseil d'Administration ont des obligations vis-ò-vis des intérêts du DC/BR dons son ensemble et ce, indépendamment de l'instance qui les nomme. A cet égard, le Conseil d'Administration doit être doté de pouvoirs lui permettant de s'assurer que les administroteurs nommés par les actionnaires sont qualifiés pour le paste.

Article 15 : Renforcement des capacités des membres du Conseil d'Administration

Le Conseil d'Administration est tenu de mettre en place des programmes de formation continue à l'intention des administrateurs ou de prendre toutes mesures visant à leur assurer l'accès aux connaissances nécessaires pour exercer pleinement leurs responsabilités.

Les membres du Conseil d'Administration doivent également ovoir lo possibilité de recourir, en cas de besoin, à des consultants externes et des experts pour acquérir, maintenir et oméliorer leurs connaissances et leurs compétences en vue de remplir leurs responsabilités.

Article 16 : Organisation et fonctionnement du Conseil d'Administration

Le Conseil d'Administration formalise et met ò jour, ou moins une fois tous les trois (03) ans, les règles et procédures régissant son organisation et son fonctionnement, ses droits, ses obligations et ses activités essentielles.

Le Conseil d'Administrotion instoure, en s'inspirant des meilleures pratiques internationoles, des règles spécifiques de renouvellement des mandats de ses membres et de ceux issus des participations croisées oinsi que des règles de renouvellement au niveau des responsabilités au sein des comités.

L'AMF-UMOA peut exiger des modifications dans la composition du Conseil d'Administration s'il constate que certains de ses membres ne s'acquittent pas de leurs obligations, conformément aux dispositions de la présente Instruction.

Les procès-verbaux des réunians du Conseil d'Administration doivent être transmis à l'AMF-UMOA.

Article 17 : Présidence du Conseil d'Administration

Le Président du Conseil d'Administration doit notamment :

a) être un administrateur non exécutif ou un administrateur indépendant ;

b) assurer le bon fonctionnement de l'organe en veillant au respect des règles fixées à cet effet et pour les prises de décisions ;

c) disposer d'expérience et de compétences avérées dans les domaines jugés pertinents pour le développement du DC/BR ainsi que de qualités personnelles lui permettant d'assurer pleinement ses attributions ;

d) veiller à ce que les décisions prises par cette instance reposent sur des règles précises et soient suffisamment étayées ;

e) promouvoir une culture de débat au sein de l'organe, en établissant notamment une relation de confiance ovec les membres et en veillant à l'expression et à l'examen des avis divergents ;

f) être disponible pour l'exercice de ses responsabilités.

Article 18 : Évaluation du Conseil d'Administration

Au moins une fois par an, l'organe délibérant procède seul ou avec l'aide d'experts externes, à une évaluation de l'organe délibérant dans son ensemble, de ses comités spécialisés et de chacun de ses membres. Les résultats de cette évaluation doivent être consignés dans un rappart présenté à l'Assemblée Générale et communiqués à l'AMF-UMOA.

Tous les trois (3) ans une évaluation formelle est entreprise, sous la direction d'un administrateur indépendant, avec l'assistance d'un expert extérieur ayant des références dans ce domaine.

Article 19 : Comités spécialisés

Le Conseil d'Administration peut constituer, en son sein, autant de comités spécialisés que nécessaire, notamment dans les domaines ce l'audit, des risques, de la rémunération, de la nomination, de l'éthique et de la conformité.

L'organe délibérant doit disposer au moins :

- d'un comité d'audit ;
- d'un comité des risques ;
- d'un comité de nomination ;
- d'un comité de rémunération ; et

- d'un comité d'éthique et de déontologie.

Les comités d'audit et de risques peuvent être regroupés en un seul Comité. De même, les comités de rémunération, de nomination, d'éthique et de déontologie peuvent être regroupés en un seul comité.

Article 20 Pouvoirs des comités et relation avec le Conseil d'Administration

1. Pouvoir consultatif

Les comités sont dotés d'un pouvoir purement consultatif, à la saisine par le Conseil d'Administration ou de l'Assemblée Générale, pour effectuer des missions déterminées por le Conseil d'Administration ou l'Assemblée Générale et relatives à la société, sa gestion, sa stratégie et la mise en œuvre de l'objet social.

Les missions sont assignées aux comités dès que cela est estimé nécessaire par le Conseil d'Administration ou l'Assemblée Générale.

2. Relations entre le ou les comités (s) et le Conseil d'Administration

Les comités préparent des travaux et des rapports transmis au Conseil d'Administration.

Les comités ne sont pas un démembrement du Conseil d'Administration. Ils peuvent dans le cadre de leurs travaux prendre contact avec les départements de la société, après en avoir préalablement informé le Directeur Général et le Président du Conseil d'Administration ou le Conseil d'Administration.

Article 21 : Composition, organisation et fonctionnement des comités spécialisés

Le Conseil d'Administration fixe, par écrit, le mandat et la composition des comités spécialisés. Il veille à ce que lesdits comités interagissent et lui rendent compte au moins deux fois par an.

Ces Comités doivent être exclusivement composés d'administrateurs non-exécutifs et au moins d'un administrateur indépendant. Un administrateur ne peut appartenir à plus de deux comités spécialisés à la fois.

Le Président de chaque comité spécialisé est choisi parmi les membres dudit Comité. Il ne peut être le Président du Conseil d'Administration ou d'un autre comité. Il doit disposer de connaissances approfondies dans le domoine d'activité du comité qu'il préside.

Chaque Comité spécialisé doit disposer d'une Charte ou d'un document équivalent retroçant son mandat, l'étendue de ses travaux et les modalités de son fonctionnement. Les Comités spécialisés se réunissent, au moins deux fois par an, et en tant que de besoin. Les délibérations, décisions et recommandations des réunions ainsi que les opinions divergentes exprimées sont consignées dans un procès-verbal ou compte-rendu signé du Président du Comité. Le DC/BR dait adopter un système de rotation périadique des sièges et de la présidence de ces comités.

Article 22 : Comité d'Audit

Le Comité d'Audit assiste le Conseil d'Administration dans les domaines de l'information financière et du contrôle interne, y compris l'audit interne. Pour l'exercice de ses attributions, le Comité d'Audit doit être composé de membres disposant d'une expérience avérée en matière d'audit, d'information financière ou de comptabilité. Le secrétariat du Comité d'Audit est assuré par le responsable de la fonction audit. Le Comité d'Audit doit notamment :

- s'assurer du déploiement et de la bonne mise en œuvre du Dispositif de Contrôle Interne du DC/BR ;
- approuver les procédures de contrôle interne et assurer le suivi de leur efficacité ;
- veiller à la fiabilité des informations financières ;
- superviser, examiner et approuver les programmes d'audit interne et externe du DC/BR ;
- s'assurer que l'organe exécutif prend, dans les délais, des mesures pour remédier aux déficiences de contrôle interne relevées ;
- sanctionne le non-respect par le personnel des politiques et textes juridiques en vigueur et résout tout autre problème identifié ;
- proposer ou recommander au Conseil d'Administration, pour approbation, la naminatian, la rémunération et la révocation des Commissaires aux Comptes selon les voies appropriées.

Article 23 : Comité des Risques

Le Comité des Risques assiste le Conseil d'Administration dans sa mission de surveillance de la mise en œuvre du dispositif de gestion des risques du DC/BR. Pour l'exercice de ses attributions, le Comité des Risques doit être composé de membres disposant d'une expérience avérée en matière d'audit ou de gestion des risques. Le secrétariat du Comité des risques est assuré par le responsable de la fonction risque.

Le Comité des Risques doit notamment :

- veiller à la définition d'une politique de gestion des risques par l'organe délibérant ;
- s'assurer de la mise en place, au sein du DC/BR, d'un dispositif de gestion intégrée des risques conforme aux exigences règlementaires ;
- participer à l'élaboration des stratégies de gestion des risques et procéder annuellement à leur examen, à la fois sur une base agrégée, et par type de risques ;
- soumettre à l'organe délibérant, pour approbation, des propositions relatives au degré d'appétence pour le risque actuel et futur à l'échelle du DC/BR ainsi que les limites en matière d'acceptation ou de maintien de la relation avec un adhérent ou un participant ;
- veiller à ce que l'organe exécutif prenne les mesures nécessaires pour contrôler et maîtriser tous les risques significatifs conformément aux stratégies et degré d'appétence pour le risque qui ont été approuvés ;
- réviser, au moins une fois tous les trois (03) ans, les politiques et procédures de risques du DC/BR au regard des évolutions enregistrées dans ses activités et s'assurer qu'elles sont adoptées aux stratégies et au degré d'appétence pour le risque approuvés par l'organe délibérant.

Article 24 : Comité de Nomination

Le Comité de Nomination assiste le Conseil d'Administration dans le processus de sélection de nouveoux odministrateurs et de nominotion des membres de l'organe exécutif.

Le Comité de Nomination doit notamment :

- veiller à ce que le processus de nomination et de renouvellement soit organisé d'une manière rigoureuse, objective, professionnelle et transporente ;
- s'ossurer de la mise en place et du respect de la procédure de nomination des membres des organes de gouvernance ;
- veiller à ce que le DC/BR dispose d'un plan de succession adéquot pour les postes de direction ;
- identifier, traiter, voire éliminer les situations de conflit d'intérêts qui émanent du processus de nomination en vue de veiller à l'objectivité et ò l'indépendonce du Conseil d'Administration par une sélection adéquate de ses membres ;
- formuler des avis et recommandotions ou Conseil d'Administration sur la politique de ressources humaines du DC/BR.

Article 25 : Comité de Rémunérotion

Le Comité de Rémunération ossiste le Conseil d'Administration dans so mission relative ò la rémunération des administrateurs, du Directeur Général, des autres membres de l'organe exécutif et des codres supérieurs du DC/BR.

Le Comité de Rémunération doit ou minimum :

- élaborer lo politique de rémunération des administrateurs, des membres de l'organe exécutif et des cadres supérieurs du DC/BR ;
- surveiller l'élaboration et la mise en œuvre du système de rémunération du DC/BR ;
- examiner, onolyser et suivre, ou moins une fois par on, les plans, les procédures et les résultats du système de rémunération à l'échelle du DC/BR ;
- travailler en étroite collaboration ovec le Comité des Risques qui doit également déterminer si les incitotions générées par le système de rémunération tiennent dûment compte du profil de risque du DC/BR, de ses besoins de fonds propres et de liquidité ainsi que la prévision de ses revenus ;
- intégrer le résultat de ses travaux au rapport annuel adressé à l'Assemblée Générale ordinoire.

Article 26 Comité d'Éthique et de Déontologie

Le Comité d'Éthique et de Déontologie assiste le Conseil d'Administrotion dans sa mission de surveillonce de la mise en œuvre du dispositif d'éthique et de déontologie du DC/BR. Le Comité d'Éthique et de Déontologie est composé de membres disposant d'une expérience avérée en motière de déontologie et de gestion des risques. Le secrétariat du Comité d'Éthique et de Déontologie est assuré par une personne désignée « Personne responsoble en éthique et déontologie ». Cette personne coordonne avec les autres comités et les agents toutes les actions relatives à la mise en œuvre de l'éthique et de la déontologie ou sein du DC/BR.

Le Comité d'Éthique et de Déontologie peut, à son initiative ou à la demande du Directeur Général ou du Conseil d'Administration, enquêter sur des faits ou informations relatifs à un manquement à l'éthique ou la déontologie.

Le Comité d'Éthique et de Déontologie doit notamment :

- s'assurer de la mise en place, au sein du DC/BR d'un dispositif de suivi des dispositions du Code d'Éthique et de Déontologie conforme aux exigences de la réglementation ;
- mettre à jour le Code d'Éthique et de Déontologie selon les procédures d'évaluation de la mise en œuvre du code et de la Charte de Gouvernance et de l'évolution des activités du DC/BR ;
- soumettre à l'organe délibérant pour approbation et présentation à l'Assemblée Générale ordinaire annuelle, des propositions relatives aux mises à jour du Code de déontologie, aux procédures d'évaluation de l'application du Code et aux mesures à prendre pour une application efficace du Code ;
- s'assurer de la mise en place de mécanismes de sensibilisation aux questions d'éthique et de déontologie des agents, représentants et sous-traitants du DC/BR ;
- veiller à l'établissement d'un rapport d'éthique par la Direction Générale adressé à l'organe délibérant.

TITRE 4 : ORGANE EXECUTIF

Article 27 : Qualification des membres de l'organe exécutif

Les membres de l'organe exécutif doivent posséder les compétences professionnelles, l'honorabilité, l'expérience et les qualités personnelles nécessaires pour gérer les activités du DC/BR et le personnel qui relève de leur autorité.

Les membres de l'organe exécutif doivent bénéficier d'un programme de formation continue à l'effet de garantir une mise à niveau de leurs connaissances dans l'exercice de leurs responsabilités.

Article 28 : Responsabilités de l'organe exécutif

L'organe exécutif doit notamment :

- communiquer au Conseil d'Administration toutes informations et données pertinentes nécessaires à sa prise de décision ;
- mettre en place une organisation qui responsabilise le personnel du DC/BR et favorise la transparence ;
- disposer, à tout moment, d'informations suffisantes sur la nature et le degré du risque pris par le DC/BR, comprendre les interrelations qui existent entre ces différents risques et appréhender les niveaux de fonds propres et les mesures requises pour couvrir ces expositions ;

- être en mesure de suivre et de gérer, en permanence, les risques liés aux nouvelles activités, aux nouveaux produits et aux modifications des systèmes ;
- s'assurer, en permanence, du bon fonctionnement des dispositifs de contrôle interne et de gestion des risques et prendre des mesures nécessaires pour remédier, en temps opportun, à toute carence ou insuffisance relevée ;
- s'assurer que les rôles et les obligations des différentes fonctions ou sein de l'organe exécutif, y compris ceux du Directeur Général, sant clairement délimités ;
- œuvrer pour l'adhésion de l'ensemble du personnel aux principes d'éthique et de professionnalisme ainsi qu'aux saines pratiques en matière de gouvernance ;
- entretenir des relations régulières ovec le Secrétoriot Général de l'AMF-UMOA et les outres superviseurs.

Article 29 : Responsabilités du Directeur Général

Le Directeur Général est chargé de la gestion couronte des activités du DC/BR.

A cet effet, il doit notamment :

- veiller à ce que les activités du DC/BR soient conformes aux orientotions stratégiques fixées par le Conseil d'Administration, à l'appétence pour le risque, à la politique de rémunération et aux autres politiques opprouvées par cette instance ;
- s'assurer, en permanence, du respect des politiques internes ainsi que des exigences légales et réglementaires régissant les activités du DC/BR ;
- mettre en œuvre la stratégie des risques approuvée par le Conseil d'Administration, s'engager activement dans la maîtrise, la gestion et le cantrôle de l'ensemble des risques significatifs encourus par le DC/BR et s'assurer que des ressources adéquates y sant consacrées ;
- respecter et promouvoir l'indépendonce des fonctions de contrôle et ne pas interférer dons l'exercice des responsabilités qui leur sont dévolues ;
- s'assurer que toutes les responsobilités de l'organe exécutif, énoncées à l'article 28, ci-dessus, sont adéquatement respectées par les acteurs concernés ;
- sélectionner, superviser et, le cas échéant, remplacer les membres du personnel, sans préjudice des dispositians énancées aux articles 9 et 33 de la présente Instructian.
- communiquer au Canseil d'Administration au au Comité Spécialisé en charge de la stratégie le cas échéant, un rapport trimestriel sur la mise en œuvre de lo stratégie du DC/BR, en dehors des rapports requis par le droit des sociétés commerciales et la réglementatian en vigueur, au sujet de la gestion et des camptes.

Article 30 : Fonctions de contrôle

Le DC/BR doit disposer o minima des fonctions d'audit interne, de gestion des risques et de la conformité.

Les rôles et obligations de choque fonction de contrôle doivent être clairement définis oinsi que les domaines d'intervention communs, en vue d'une meilleure coordination de leurs octivités.

Les responsabilités de lo fonction conformité peuvent être exercées par une fonction indépendonte des unités opérationnelles, autre que l'audit interne.

Article 31 : Responsabilités des fonctions de contrôle

Chaque fonction de contrôle, placée sous l'autorité d'un responsable distinct, doit notomment :

- être dotée de ressources humaines compétentes et quantitativement suffisantes pour mener à bien so mission ;
- mointenir à jour les connaissances acquises et assurer une formation continue et actuolisée ò chacun des membres du personnel qui lui sont affectés ;
- être indépendante et permanente ;
- disposer de la notoriété et de l'autorité suffisantes pour que les responsables s'acquittent de leurs devoirs ;
- détecter et gérer les conflits d'intérêts réels, opparents et potentiels ;
- communiquer oux organes de gouvernance des informations exactes, à jour et intelligibles pour leur permettre de prendre des décisions éclairées.

Article 32 : Rattachement des responsables des fonctions de contrôle

Les responsables des fonctions de contrôle dépendent hiérarchiquement du Directeur Général et fonctionnellement du Conseil d'Administration qui est responsoble de leur sélection, de la supervision de leur performance ainsi que de leur révocation.

Chaque responsable d'une fonction de contrôle doit pouvoir accéder directement ou Conseil d'Administration ou, le cas échéant, aux Comités spécialisés qui en émonent, aux Commissaires aux Comptes du DC/BR, en vue de discuter de ses opinions, constatations et conclusions de ses travaux.

Article 33 : Désignation, mutation et révocation des responsables des fonctions de contrôle et des auditeurs internes

La désignation, la mutation ou la révocation des responsables des fonctions de contrôle autre que l'audit interne doit être soumise à l'approbation préalable du Conseil d'Administration, sur proposition dûment motivée du Directeur Générol.

La désignation, la mutation ou la révocation du responsable de la fonction d'audit interne doit être soumise à l'approbation préalable du Conseil d'Administration, sur proposition dûment motivée du Comité d'audit.

La désignation, la mutation ou la révocation du responsable des auditeurs internes doit être soumise à l'approbation préalable du Conseil d'Administration, sur proposition dûment motivée du Responsable de la fonction d'audit interne.

Ces décisions doivent être portées à la connaissance de l'AMF-UMOA.

Article 34 : Audit interne

La fonction d'audit interne est chargée de donner aux organes de gouvernance une assurance raisonnable sur l'efficacité du système de contrôle interne, des dispositifs de gouvernance et de gestion des risques en vue de leur permettre d'avoir une meilleure maîtrise des activités du DC/BR et des risques encourus.

Les responsabilités spécifiques de la fonction d'audit interne sont explicitées dans l'Instruction relative au dispositif de contrôle interne et de gestion des risques du DC/BR.

Article 35 : Gestion des risques

La fonction gestion des risques supervise les risques pris sur l'ensemble des activités du DC/BR.

Les responsabilités spécifiques de la fonction gestion des risques sont explicitées dans l'Instruction relative au dispositif de contrôle interne et de gestion des risques du DC/BR.

Article 36 : Conformité

La fonction conformité a pour rôle de veiller à ce que le DC/BR mène ses activités de manière intègre et en conformité avec les textes juridiques en vigueur et les politiques internes.

Les responsabilités spécifiques de la fonction conformité sont explicitées dans l'Instruction relative au dispositif de contrôle interne et de gestion des risques du DC/BR.

TITRE 5 : GESTION DES CONFLITS D'INTERETS ET PRINCIPES DE BONNE CONDUITE

Article 37 : Politiques en matière de conflits d'intérêts

Les membres des organes de gouvernance doivent éviter de se placer dans une situation susceptible d'engendrer des conflits d'intérêts. L'organe délibérant doit s'assurer que l'organe exécutif élabore et met en place une politique ainsi que des procédures visant à détecter les conflits d'intérêts apparents et potentiels et, lorsqu'ils ne peuvent être prévenus, à les gérer de manière appropriée. Il doit également se doter d'un processus de contrôle de la conformité avec cette politique. Cette politique, applicable à tout membre du personnel ainsi qu'aux membres des organes exécutif et délibérant, doit notamment prévoir :

- l'obligation de maintenir en toute circonstance une indépendance d'analyse, de jugement et de décision ;
- d'éviter de se trouver, de façon directe ou indirecte, dans une situation pouvant donner lieu à un conflit d'intérêts apparent ou potentiel ;
- des dispositions explicites relatives à la démarche à adopter pour informer rapidement la hiérarchie ou l'orgone délibéront lorsqu'un membre de l'orgone du DC/BR est confronté à un conflit d'intérêts apparent ou potentiel ;
- un processus rigoureux d'examen et d'approbation, par l'organe délibérant, qui s'applique à tout membre des organes de gouvernance souhaitant siéger dans un autre organe délibérant, ou entreprendre des activités qui pourraient créer des conflits d'intérêts ;
- l'interdiction à tout membre de l'orgone délibérant de participer aux débats et aux prises de décision sur des sujets qui les mettent en situotion de conflits d'intérêts ou qui sont susceptibles de compromettre leur objectivité et leur indépendance ;
- des exemples de situatians de conflits d'intérêts susceptibles de se présenter dans le cadre de l'exercice des différentes activités au sein du DC/BR ;
- des procédures qui encadrent de monière adéquate les transactions avec les parties liées afin qu'elles respectent les dispositions prévues à cet effet dans l'Instruction sur la gestion des risques ;
- les modalités et conditions de traitement des cas de non-respect de cette politique.

Article 38 : Déclarations de conflits d'intérêts et d'honneur

Préolablement à son entrée en fonction et chaque année durant son mandat, l'administrateur soumet au Conseil d'Administration une déclaration de conflits d'intérêts relative aux liens de toute nature qu'il entretient directement ou indirectement avec le DC/BR, ses dirigeants, ses partenaires et ses concurrents.

Article 39 : Obligations de diligence et de loyauté

Les membres des organes de gouvernance ainsi que le personnel sous leur autorité ont une obligation de diligence et une obligation de loyouté envers le DC/BR, les octionnaires, les investisseurs et les autres parties prenantes. Les administrateurs nommés par des actionnaires d'influence dominonte doivent conserver leur importialité et exercer intégralement leurs obligations de diligence et de loyauté vis-ô-vis de le DC/BR.

Article 40 : Solvabilité des membres des organes de gouvernance

Les membres des organes de gouvernance ne doivent pos être en défaut de poiement sur leurs engagements auprès du DC/BR ou en situation d'interdiction boncaire dans l'UMOA. En pareil cas, ils doivent être suspendus de leurs fonctions.

Le Régulateur doit être informé par le Président du Conseil d'Administration dès leur survenance. La levée de cette suspensian ne peut intervenir que larsque la créance redevient saine, conformément aux règles comptables en vigueur dans l'UMOA ou l'interdiction bancaire levée. L'AMF-UMOA doit également être informée de cette levée de suspension, par une correspondance accompagnée des justificatifs nécessoires.

Les attributions du membre de l'organe délibérant ou exécutif suspendu doivent être transférées à d'autres homologues selan des procédures prédéfinies. Un membre de l'orgone de gouvernance frappé d'interdiction bancaire dans l'UMOA ou dont le défaut de paiement dure plus d'un an sans être régularisé ou dont le défaut s'est produit plus d'une fois sur ses engagements vis-à-vis du DC/BR au cours des cinq dernières années, doit être révoqué et remplacé selon les procédures du DC/BR. Cette situation peut emporter interdiction d'exercer une fanction d'administrateur ou de dirigeant au sein d'une entité supervisée par l'AMF-UMOA, conformément aux dispositions de la réglementation en vigueur dans l'UMOA.

TITRE 6 : TRANSPARENCE ET DIFFUSION D'INFORMATIONS

Article 41 : Mécanisme de communication

Les organes de gouvernance doivent assurer la diffusion en temps opportun d'informations exactes sur tous les sujets significatifs cancernant le DC/BR, notamment son actionnariat et sa gouvernance. Les actionnaires, les adhérents, les investisseurs ainsi que les autres parties prenantes doivent disposer de toutes les informations pertinentes et utiles qui leur permettent d'évaluer l'efficacité avec laquelle les organes de gouvernance administrent et gèrent le DC/BR.

Article 42 : Mode de diffusion des informations

Les informations doivent être accessibles sur le site internet du DC/BR, dans ses rapports financiers annuels et périodiques et par taut autre moyen adéquat.

TITRE 7 : DISPOSITIONS TRANSITOIRES ET FINALES

Article 43 : Vacances des postes de Président du Conseil d'Administration et de Directeur Général

La vacance des pastes de Président du Conseil d'Administration et de Directeur Général ainsi que les motifs doivent être notifiés à l'AMF-UMOA dans les vingt-quatre (24) heures qui suivent la survenance de cet événement. L'intérim des postes de Président du Conseil d'Administration et de Directeur Général peut être assuré par un remplaçant désigné conformément à la réglementation en vigueur.

Article 44 : Abrogation

La présente Instruction abroge et remplace toutes dispositions antérieures et contraires traitant du même objet.

Article 45 : Dispositions transitoires

Le DC/BR dispose d'un délai maximum de deux (02) ans à compter de sa date de signature pour se mettre en conformité avec les dispositions de la présente Instruction.

Article 46 : Sanctions

Le non-respect des règles prévues par la présente Instruction est sanctionné par l'AMF-UMOA, conformément aux dispositions réglementaires en vigueur sur le Marché Financier Régional de l'UMOA.

Article 47 : Publication et date d'entrée en vigueur

La présente Instruction, qui sera publiée partout où besoin sera, entre en vigueur à compter de sa date de signature.

Fait à Abidjan, le 29 DEC. 2023

Pour l'Autorité des Marchés Financiers de l'UMOA

Le Président

Marchés Financiers de l'Union Monétaire Ouest Africaine * Autorité des Le Président 01 BPM 1878 ABIDJAN 01

Badanam PATOKI

ANNEXE

DISPOSITIONS MINIMALES DE LA CHARTE DE GOUVERNANCE D'ENTREPRISE

Raison sociale :

.....

1. INTRODUCTION

La présente Charte de Gouvernance d'Entreprise reprend les principes et règles sur la base desquels fonctionnent le Conseil, ses administrateurs et ses comités.

L'évolution des pratiques et règles de gouvernance des entités similaires au DC/BR ainsi que la situation actuelle de la Société requiert la mise en place d'un code de référence (la « Charte de Gouvernance d'Entreprise » ou la « Charte »).

Cette Charte est conforme aux recommandations sur la gouvernance d'entreprise des infrastructures de marché, à la réglementation sur les marchés financiers et à l'Acte Uniforme relatif au droit des sociétés commerciales et du GIE du Traité de l'OHADA.

2. CONSEIL D'ADMINISTRATION

2.1 Pouvoirs et responsabilités du Conseil d'Administration

Les missions du Conseil d'Administration (ci-après le « Conseil »), en sus de celles prévues par l'Acte Uniforme relatif au droit des sociétés commerciales et du GIE du Traité de l'OHADA et les statuts du DC/BR sont :

2.1.1 Responsabilités de contrôle

(i) Faire en sorte que soient mis en place un système et des procédures de contrôle interne, y compris un système adéquat d'identification et de gestion des risques et des procédures visant à assurer la conformité aux lois ;
(ii) Contrôler le fonctionnement et le caractère adéquat du système de contrôle interne et des procédures en tenant compte de l'examen auquel procède le comité d'audit ;
(iii) Prendre les mesures nécessaires pour garantir l'intégrité des états financiers.

2.1.2 Évaluation

(i) évaluer les performances des dirigeants ;
(ii) contrôler et évaluer l'efficacité des comités spécialisés du Conseil d'Administration ;
(iii) contrôler les activités des Commissoires oux Comptes et de la fonction d'audit interne, en tenant compte de l'examen auquel procède le Comité d'Audit ;
(iv) examiner la composition et la rémunération de l'Organe Exécutif et des membres des Comités ;
(v) décider des principes gouvernant la rémunération des membres de l'Organe Exécutif, et des Comités. L'Organe Exécutif se définit comme l'ensemble des structures qui concourent à la gestion courante du DC/BR et assurent l'application effective de l'orientation de l'activité définie par l'organe délibérant.
Sont notamment considérés comme membres de l'Organe Exécutif, le Directeur Général, les Directeurs Généraux Adjoints, le Secrétaire Général, les Responsables des fonctions de contrôle, les Directeurs des Départements regroupant des Directions et les Directeurs rattachés au Directeur Général.

2.1.3 Plan stratégique d'entreprise

(i) réexaminer régulièrement le plan d'entreprise (ou plan d'affaires) préparé par le Directeur Général, notamment (a) en acquérant une connaissance approfondie des affaires traitées, (b) en veillant à comprendre et à remettre en question les hypothèses sous-jacentes du plan et à se former une opinion indépendante sur la probabilité que le plan puisse être réalisé et (c) en contrôlant les performances de la société au regard des objectifs stratégiques et du plan d'entreprise ;
(ii) examiner, approuver, et contrôler les objectifs financiers du DC/BR.

2.1.4 Délégations de pouvoirs

(i) décider des principes gouvernant la délégation de pouvoirs au sein du DC/BR ;
(ii) examiner, approuver et contrôler les délégations de pouvoirs ;
(iii) décider de toute délégation de pouvoirs au comité spécialisé.

2.1.5 Informations du Conseil

Le Conseil prendra les mesures nécessaires pour s'assurer qu'il sera informé de façon régulière :

(i) des progrès de la mise en œuvre du plan d'entreprise par le biais, notamment, de rapports trimestriels préparés par l'Organe Exécutif sur les activités et sur les aspects financiers de cette mise en œuvre ;
(ii) des développements significatifs intervenus dans les activités et des décisions les plus importantes prises par les Comités et par le Directeur Général, par le biais de comptes de résultats et de trésorerie, comparatifs, trimestriels et non audités, établis selon les règles en vigueur et accompagnés d'un rapport préparé par la Direction, qui discute et analyse ces développements et décisions.

2.2 COMPOSITION DU CONSEIL

2.2.1 Généralités

La composition du Conseil doit gorantir le respect par la DC/BR des exigences en motière de conflits d'intérêts et d'indépendance, des dispositions relatives aux incompatibilités.

Le Conseil doit tenir compte de ces dispositions, lorsqu'il envisoge des propositions de nomination, ou lorsqu'il est amené à présenter un condidat à une nomination ou à une élection.

La composition du Conseil d'Administration doit garantir que les décisions sont prises dans l'intérêt du DC/BR, et que tont les administrateurs exécutifs, les administrateurs non exécutifs, ainsi que les administrateurs indépendants du Conseil disposent des compétences, de l'expérience et de l'expertise nécessaire pour s'acquitter de leurs responsabilités. Le profil de compétences des administrateurs, du Canseil d'Administrotion est joint en Annexe 1.

Les Mandataires sociaux du DC/BR, intuitu personae ou représentants de personne morale, ne peuvent être mandataires sociaux d'une autre DC/BR, sans préjudice des autres incompatibilités qui pourraient leur être appliquées.

2.2.2 Nomination

Les membres du Conseil d'Administration sont nommés confarmément aux dispositians des Statuts du DC/BR. Le Conseil proposera uniquement des candidats qui ant été proposés par le Comité de Rémunération et de Nomination en vue d'une nomination por l'Assemblée Générale.

Le/la Président(e) du Conseil d'Administration s'assure que le Conseil d'Administration dispose, avant d'examiner cette candidature, d'informations suffisantes sur le candidot, telles un curriculum vitae, une évaluation du candidat basée sur un entretien préliminaire, une liste des autres fonctions que le candidat a accupées, des fonctions qu'il occupe et, lorsque le candidat est présenté pour être élu en qualité d'administrateur indépendant, toute autre information nécessaire pour évaluer l'indépendance du candidat.

2.2.3 Droit de proposition des actionnaires

Chaque actionnaire ou groupe d'actionnaire (ou plusieurs SGI) en possession d'au moins 15% des actions du DC/BR a le droit de proposer un candidat en vue d'une nomination comme administrateur au pra rata de so participation.

Le nombre d'administrateurs pour lesquels un actionnaire peut propaser des candidats en application de ce drait de proposition (éventuel) est calculé le 1er janvier de l'année dans laquelle les postes vacants devront être pourvus. Les mandats en cours au sein du Conseil d'Administration, pour lesquels cet actiannaire a exercé son droit de proposition, sont saustraits de ce nombre. Le résultot du calcul au pro rato est toujours arrondi au nombre entier inférieur.

Afin d'éviter toute ambiguïté, les changements dans la structure de l'actionnariat intervenus entre le 1er janvier et la date de l'Assemblée Générale en question ne seront pas pris en compte pour

le calcul du nombre de mandats du Conseil d'Administration pour lesquels un actionnaire peut exercer son droit de proposition.

S'il n'y a pas assez de postes d'administrateur vacants en raison de la règle selon laquelle le Conseil d'Administration doit toujours compter au moins deux (02) administrateurs indépendants, le nombre d'administrateurs que chaque actionnaire a le droit de proposer sera diminué au prorata du nombre de postes vacants à pourvoir. Le résultat du calcul au prorata est toujours arrondi au nombre entier inférieur.

Le calcul du seuil relatif au droit de proposition, les actions possédées par un actionnaire et par les sociétés directement contrôlées par lui (au sens de l'article 174 de l'Acte Uniforme de l'OHADA relatif aux sociétés commercioles) seront additionnées.

Lorsqu'ils proposent des candidats pour un mandat au sein du Conseil d'Administration, les actionnaires devront tenir compte du profil de compétences du Conseil d'Administration.

2.2.4 Administrateurs indépendants

Au moins deux (02) administroteurs doivent satisfaire aux critères d'indépendance prévus par l'Instruction relative à la gouvernance des Structures de Marché qui est la référence dans les présentes.

Les postes vacants devant être pourvus par des candidats-administrateurs qui ne sant pas proposés par un actionnaire, doivent être pourvus par des administrateurs indépendants.

Un administrateur indépendant qui ne satisfait plus à un des critères d'indépendance doit en informer par écrit le Conseil immédiatement. Il est attendu de cet administrateur qu'il démissionne de son mandat dans le mois qui suit lo perte de ce statut.

2.2.5 Durée du mandat et limite d'âge

Les administrateurs sont nommés pour une période de trois (03) ans renouvelables sans préjudice des restrictions pour les administrateurs indépendants, tel qu'exposé dans la présente Charte. Lo durée du mandat d'administrateur prendra immédiatement fin après l'Assemblée Générale suivant son 75ème anniversaire. Il est attendu de cet administrateur qu'il démissionne de son mandat lors de cette Assemblée Générale.

2.2.6 Vacance d'un poste d'administrateur

En cas de vacance d'un poste d'administrateur, le Conseil conformément à l'Article 429 de l'Acte Uniforme de l'OHADA relotif aux sociétés commerciales et aux statuts de la société, y pourvoit provisoirement jusqu'à ce qu'une nominotion définitive intervienne conformément oux statuts. Le candidat au poste vacant est proposé par le Comité de Rémunération et de Nomination. En cas de vacance d'un poste d'administrateur proposé en vue d'une nominotion par un actionnaire conformément au droit de proposition décrit ci-dessus, le Conseil peut uniquement nommer un nouvel administrateur, afin de pourvoir provisoirement au poste vacont sur proposition de cet actionnaire.

2.2.7 Président(e)

Le/la Président(e) du Conseil d'Administration est nommé(e) et, le cos échéant, révoqué(e) de sa présidence conformément aux dispositions statutaires.

Le/la Président(e) est responsable de la direction du Conseil d'Administration. Le/la Président(e) prend les mesures nécessaires pour développer au sein du Conseil un climat de confiance qui permette des discussions ouvertes, lo critique constructive et le soutien des décisions que prend le Conseil d'Administration. Il/elle s'assure que le Conseil fonctionne de manière efficace et conforme aux statuts et à lo Charte de Gouvernonce d'Entreprise.

2.2.8 Autres mandots et fonctions

Il est permis aux membres du Conseil de siéger au Conseil d'autres sociétés, et d'assumer d'autres mondats ou fonctions, excepté chez une autre DC/BR, pour autont (i) que les dispositians des statuts soient respectées, (ii) que ces mandats ou fonctions n'interfèrent pas avec la capacité du membre du Conseil à remplir ses fonctians de membre du Conseil du DC/BR et (iii) qu'ils n'acceptent pas plus de cinq mandats d'administrateurs dans des sociétés non cotées (en ce compris leur mandat en tant que membre du Conseil).

Les chongements relotifs à ces autres mandats au fonctians des membres du Conseil d'Administration sont communiqués ou Président(e) lorsqu'ils surviennent. Tout odministrateur, y compris le Directeur Généro̲l, nommé pour un nouveau mandat externe doit en informer le Comité de Rémunération et de Nomination. Tout nouveau mandot externe que le Directeur Général voudroit exercer est saumis à l'approbatian préalable du Conseil d'Administration Conseil d'Administration statuant sur recommandation du Comité de Rémunération et de Nominotion.

2.3 FONCTIONNEMENT DU CONSEIL

Le Conseil se réunit conformément aux dispositions des Statuts du DC/BR et de la Chorte de Gouvernance d'entreprise et les délibérations, conclusions et décisions issues de ses travaux sont consignées dans un procès-verbal.

Le procès-verbal contient un résumé des délibérations, précise les décisions prises et mentianne toute obstentian ou réserve exprimée par tout administrateur. Le procès-verbal de lo réunion est préparé et communiqué aux membres du Conseil d'Administration Conseil d'Administration dans les quinze (15) jours colendaires suivant la dote de la réunion.

Si un membre du Conseil d'Administration désire que certaines modificotions soient apportées au procès-verbol, il peut le demander dans les dix (10) jours ouvrés à compter de la réception du projet de procès-verbal. Le procès-verbal sera approuvé définitivement lors de lo réunion suivante du Conseil d'Administration. Les procès-verbaux sont signés conformément aux dispositions de l'Acte Uniforme de l'OHADA relatif aux sociétés commerciales. Afin de faciliter la rédaction des procès-verbaux, les réunions du Conseil d'Administration peuvent être enregistrées, pour autant que ces enregistrements soient détruits sous la responsabilité du secrétaire de séonce, après approbation du procès-verbal de la réunion concernée.

3. ÉVALUATION

Sous lo direction du/de lo Président(e), le Conseil d'Administration évolue régulièrement l'étendue de ses activités, sa composition, so performance et celle de ses comités, de même que l'interaction avec l'Organe Exécutif. Le cas échéant, le/la Président(e) proposera les mesures nécessaires pour remédier aux éventuelles déficiences du Conseil d'Administration ou de ses comités.

4. COMPORTEMENT DES ADMINISTRATEURS

4.1 Indépendance

Chaque membre du Conseil d'Administration est tenu :

4.1.1 de prendre pour guide exclusif l'objectif général du Conseil d'Administrotion du DC/BR de poursuivre le succès du DC/BR sur le long terme et de veiller à ce que toutes les décisions soient prises dons l'intérêt social du DC/BR.

4.1.2 de maintenir en toutes circonstances son indépendance dans ses jugements, décisions et actions.

4.2 Conflits d'intérêts

4.2.1 Les membres du Conseil d'Administration sont tenus d'éviter toute action, situation ou prise de participotion qui les mettrait en situation de conflit, ou d'opparence de conflit, avec les intérêts du DC/BR ou de l'une de ses filiales. Avant d'accepter leur nominotion au Conseil d'odministration, les personnes pressenties pour être administrateur doivent s'être assurées que ni elles, ni aucun des membres de leur famille (en ce compris leur conjoint ou autre compagnon de vie, parents biologiques ou por alliance jusqu'au second degré et enfants adoptés) n'ont d'intérêt personnel, professionnel ou financier lié du DC/BR, qui les mette en situation permanente ou récurrente de conflit d'intérêts avec lo DC/BR.

4.2.2 Si une telle situation survient oprès lo nomination, le Conseil d'Administration apprécie la situation et peut recommander à l'actionnaire ou aux actionnoires qui ont nommé ou proposé l'odministrateur concerné de prendre toutes les mesures nécessaires de sorte qu'il soit remplacé. Chaque membre du Conseil organise ses affaires personnelles et professionnelles de manière à éviter tout conflit d'intérêts de nature personnelle, professionnelle ou financière avec la DC/BR, directement ou par le biais des membres de so famille (tels que définis ci-dessus).

4.2.3 Si un membre du Conseil d'Administration a, directement ou indirectement, un intérêt opposé de nature patrimoniale à une décision ou ò une opération relevant du Conseil, l'administrateur ne participe pas à la discussion ni ne prend port au vote sur le point en question. Le procès-verbal de la réunion du Conseil d'Administration reproduit les déclarations de l'administrateur ayant un intérêt opposé, de même qu'une description por le Conseil de l'intérêt

opposé et de la nature de la décision ou de l'opération dont il s'agit. En outre, le procès-verbal comporte une justification par le Conseil de la décision ou de l'opération et une description des conséquences financières pour la DC/BR. Le procès- verbal est reproduit dans le rapport annuel du Conseil. Le membre du Conseil d'Administration en situation de conflit d'intérêts en informe également le Comité d'Ethique et de Déontologie. Le Comité d'Ethique et de Déontologie décrit dans son rapport annuel les conséquences financières de la décision à propos de laquelle un conflit d'intérêts a surgi.

4.2.4 Les opérations et/ou les relations d'affaires entre administrateurs et la DC/BR ou une ou plusieurs des sociétés qui lui sont liées et qui ne tombent pas strictement dans le champ d'application de la présente charte doivent toujours être conclues à des conditions normales de marché. L'administrateur concerné doit informer le/la président(e) de telles opérations préalablement à celles-ci.

4.3 Opérations sur des actions du DC/BR

Les administrateurs se conformeront entièrement aux dispositions de la Charte et des statuts du DC/BR.

4.3.1 Contrats de services

Les administrateurs non-exécutifs ne peuvent conclure, directement ou indirectement, de contrats de fourniture de biens ou de services, à titre onéreux, avec la DC/BR ou une de ses filiales, sans l'autorisation expresse du Conseil. Tout service rendu par la DC/BR ou l'une de ses filiales à un membre du Conseil l'est exclusivement à des conditions commerciales conformes aux conditions de marché en vigueur.

4.3.2 Interactions avec l'Organe Exécutif

Les administrateurs peuvent prendre contact avec l'Organe Exécutif du DC/BR moyennant le respect des principes directeurs suivants. A l'initiative du/de la Président(e) ou de deux administrateurs ou plus, il peut être demandé aux membres du Conseil d'Administration de donner un avis sur des questions précises relatives à la gestion des affaires de la société et de contacter le ou les membres du management concernés. Le/la Président(e) veille à ce que les administrateurs reçoivent des informations pertinentes, claires et en temps utile. L'Organe Exécutif est tenu de fournir ces informations mais lorsque des clarifications ou des compléments d'information sont nécessaires, les administrateurs doivent les demander.

Les membres du Conseil d'Administration sont invités à consulter le Directeur Général avant tout contact avec un autre membre de l'Organe Exécutif et de faire preuve de discernement, pour que ces contacts ne nuisent pas à la conduite des affaires et aux responsabilités de gestion qu'exercent les membres de l'Organe Exécutif.

4.3.3 Interactions avec des tiers

Les administrateurs peuvent, à la demonde du/de la président(e) ou du Directeur Général ou en consultotion avec ceux-ci, porticiper à des activités de communication du DC/BR. En particulier, l'on attend des administroteurs qu'ils soutiennent, dans les sphères publique et privée, lo position du Conseil relative à lo stratégie, aux politiques et aux actions du DC/BR.

4.3.4 Confidentialité

Les discussions ouvertes au cours des réunions du Conseil entre les administrateurs et les outres participants (observoteurs, experts invités, membres du management) sont protégés par la confidentialité des informations et délibérations, conformément aux dispositions légales et sous réserve de celles-ci.

5. DIRECTION GENERALE

5.1 DIRECTEUR GENERAL

Le Conseil nomme et révoque le Directeur Général. Le Directeur Général est nommé pour un mandat dont la durée est définie par le Conseil. Ce mandot est renouveloble une fois.

Dons les limites des pouvoirs qui lui sont confiés par ou en vertu des statuts de la société, le Directeur Général peut déléguer des pouvoirs spéciaux et limités à toute personne. Il peut en autoriser la sous délégation. Le Directeur Général communique au Conseil d'Administration l'identité des délégataires et les pouvoirs délégués.

5.2 LES AUTRES MEMBRES DE LA DIRECTION GENERALE

Les codres occupant les postes les plus importants en termes de responsabilité sont membres de l'Organe Exécutif. Ils mettent en œuvre la stratégie indiquée par le Conseil d'Administration sous la supervision et la respansabilité du Directeur Général.

6. COMITÉS DU CONSEIL

6.1 GÉNÉRAL

Pour assumer efficacement son rôle et ses responsabilités, le Conseil d'Administration met en place, le Comité de Nominotion et de Rémunération, le Comité d'Audit, un Comité d'Éthique et de Déontologie et le Comité dos Risques (ci-après « Comités du Conseil d'Administrotion » ou « Comités »).

L'existence des Comités au côté du Conseil d'Administration n'affecte en rien la capocité du Conseil d'Administration de créer, le cos échéant, d'autres comités ad hoc pour troiter de problèmes spécifiques, sans préjudice des pouvoirs et compétences du Conseil.

Le Conseil est assisté de quatre (4) comités obligatoires : le Comité de Risques, le Comité d'Audit, le Comité d'Ethique de Déontologie, le Comité de Rémunération et le Comité de nomination. Le

Conseil pourra constituer un Comité Stratégique s'il le juge nécessaire. Ce comité ne peut disposer de compétences contraires ou déjà traitées dans les comités obligatoires, ni être doté de pouvoirs qui seraient supérieurs à ceux des autres comités.

Le cadre du mandat de ces Comités est établi ci-dessous. Chaque Comité doit examiner régulièrement (au moins tous les deux (2) ans) le cadre de son mandat et son efficacité propre et recommander au Conseil toute modification nécessaire.

La nomination des membres des Comités est fondée (i) sur leurs compétences et expériences spécifiques, qui s'ajoutent à la compétence générale requise des membres du Conseil et (ii) sur la nécessité que chaque comité possède les compétences et l'expérience suffisantes pour mener à bien ses tâches. La durée du mandat d'un membre d'un comité ne peut excéder la durée de son mandat d'administrateur.

6.2 ASPECTS COMMUNS À TOUS LES COMITÉS

Les Comités doivent être composés exclusivement d'administrateurs non-exécutifs. Un administrateur ne peut appartenir à plus de deux comités spécialisés à la fois. Le Président de chaque Comité spécialisé est choisi parmi les membres dudit comité. Il ne peut être le Président de l'organe délibérant ou d'un autre comité. Il doit disposer de connaissances approfondies dans le domaine d'activité du comité qu'il préside. Chaque comité spécialisé doit disposer d'une charte ou d'un document équivalent retraçant son mandat, l'étendue de ses travaux et les modalités de son fonctionnement. Les comités spécialisés se réunissent conformément à leur Charte approuvée par le Conseil.

7. POLITIQUE DE RÉMUNÉRATION

Le Conseil détermine la rémunération du Directeur Général et des autres membres de l'Organe Exécutif et des Comités. La rémunération des membres de l'Organe Exécutif garantit des conditions de rétribution compétitives permettant de recruter, conserver et motiver des professionnels experts et qualifiés.

Le rapport annuel du DC/BR inclut un rapport de rémunération séparé, qui fournit tous les détails relatifs à (i) la procédure de détermination de la politique de rémunération des membres de l'Organe Exécutif, (ii) les composantes de la rémunération des cadres dirigeants et (iii) le contenu et le montant de la rémunération et les autres avantages accordés aux membres de l'Organe Exécutif au cours de l'année visée. Les modalités contractuelles principales des conventions portant sur l'embauche et le départ des membres de l'Organe Exécutif seront également publiées dans le Rapport Annuel.

8. POLITIQUE DE DISTRIBUTION DE DIVIDENDE

Le montant de tout dividende annuel et la décision de paiement d'un dividende peuvent, chaque année, être influencés par différents facteurs, comme les perspectives commerciales du DC/BR, les besoins de trésorerie et la performance financière, les conditions du marché et le climat économique général et d'autres facteurs, comme des considérations fiscales ou réglementaires.

La politique de distribution doit tenir compte des engagements d'investissements et de développement du DC/BR.

9. COMITE STRATEGIQUE (OPTION)

Le Conseil peut constituer un comité stratégique (le « Comité Stratégique »). Le Comité Stratégique conseille le Conseil d'Administration sur des questions stratégiques et aura pour responsabilité, en particulier :

- d'analyser, périodiquement, les développements du secteur, les objectifs et stratégies du DC/BR et de ses filiales et de recommander les adoptations nécessaires ;
- de revoir le projet de plan d'entreprise soumis chaque onnée par l'Organe Exécutif ;
- d'onalyser les transactions strotégiques proposées par le Directeur Général en ce compris les ocquisitions et cessions stratégiques, lo formation et la résiliation d'alliances strotégiques ou d'accords de coopération de long terme, le loncement d'une nouvelle ligne de produits ou l'entrée sur un nouveau marché géographique ou de produits, ou le retrait de cette ligne de produits ou de ce marché géographique ;
- de contrôler la mise en œuvre de ces projets stratégiques et du plan d'entreprise.

10. COMITE D'AUDIT (obligatoire)

10.1 Rôle et responsabilités

Conformément à lo réglementation, le Conseil constitue un comité d'audit (le « Comité d'Audit »).

Le Comité d'Audit conseille le Conseil sur les questions de comptabilité, d'audit et de contrôle interne et oura notamment pour responsabilité :

- de contrôler les règles d'évaluation et les conventions comptables ;
- de contrôler les projets de comptes onnuels et d'examiner si l'affectation des résultats et bénéfices proposée est cohérente avec le plan d'entreprise et le respect des ratios de solvabilité et de couverture de la dette ;
- de contrôler le projet de budget annuel présenté par le Directeur Général et le respect du budget au cours de l'année ;
- de contrôler lo qualité de l'information financière fournie oux actionnaires et au marché ;
- de contrôler et de superviser le processus d'oudit interne, de contrôle interne et de gestion des risques, en ce compris pour le DC/BR, ses filioles et Affiliés de façon globole ;
- de proposer des condidats pour les mandats des deux Commissaires nommés par l'Assemblée Générale des actionnaires ;
- de suivre le contrôle légal des comptes annuels et consolidés, y compris le suivi sur toutes questions et recommandations faites par les Commissaires aux Comptes ;
- de revoir et contrôler l'indépendonce des commissoires, en particulier en ce qui concerne la prestation de services additionnels ou profit du DC/BR. Le Comité d'Audit se réunira suffisamment à l'avance des réunions du Conseil pour permettre aux membres du Comité

de faire des recommandations odéquates au Conseil. Il se réunira au moins quatre à cinq fois par an. Le Comité d'Audit rencontrera les auditeurs internes et les commissaires oux comptes ou moins deux (02) fois por an pour s'entretenir des matières liées à son mondat et de toute difficulté découlant du processus d'audit, et, en particulier, de tout manquement important aux contrôles internes.

10.1.1 Dans le domaine de l'audit, le Comité d'Audit contrôle :

- la performonce financière du DC/BR ;
- l'application cohérente des principes comptables (et des modifications y opportées) et lo quolité du contrôle interne en matière de reporting financier ;
- la qualité du processus d'audit externe : le Comité d'Audit supervise le trovail effectué par les ouditeurs externes, approuve leur plon d'oudit, procède à une évoluation formelle de leurs performonces ou moins tous les trois ans au regard de critères définis, et adresse au Conseil des recommandations portant sur leur désignatian, sur le renouvellement de leur mandat et sur leur rémunérotion. Le Comité d'Audit vérifie égolement le respect par le cabinet d'auditeurs externes de la politique d'indépendance adoptée por le Conseil, et notamment lo mise en œuvre correcte de lo procédure d'approbation préalable des services non-oudit ;
- la qualité du processus d'oudit interne : le Comité d'Audit supervise les travaux de lo fonction d'Audit du DC/BR et approuve le plan d'audit annuel, y compris les audits thématiques, le périmètre et le budget d'oudit. Tous les trois (3) ans ou moins, le Comité d'Audit organise une évaluotion externe de qualité et opprouve la nominotion ou la révocation du Responsable de l'Audit Interne ;
- la conception et l'efficacité opérationnelle du système de contrôle interne en général, et du système de gestion des risques en particulier ;
- les procédures de contrôle de conformité aux législations, aux réglementations et aux politiques du DC/BR. Régulièrement, le Comité d'Audit passe aussi en revue l'efficocité de ses politiques, et approuve la nomination ou la révocation de la Personne Responsable la Conformité ;
- lo politique de la société en motière de planification fiscale, et la mise en application de technologies de l'information et de communication ;
- le financement de lo société ;
- la conformité aux recommandations et aux observations des auditeurs internes et externes ;
- l'efficacité de la gouvernance du Comité d'Audit, et en particulier le contrôle de la mise en œuvre ainsi que l'examen périodique des règles présidant à la création, la composition et ou fonctionnement des comités d'audit au niveau des entreprises opérotionnelles du DC/BR, en prenant en compte les législations et règlementations spécifiques applicobles aux entités concernées, oinsi que leurs relations avec le Comité d'Audit.

En outre, le Comité d'Audit formule des recommandations à l'attention du Conseil sur :

- tout autre sujet lié à l'audit qu'il juge utile ;
- toute mission liée au contrôle interne, à l'audit interne ou externe, que le Conseil ou le Président du Conseil d'Administration pourrait lui assigner ;
- les informations relatives au contrôle interne, ainsi qu'aux activités du Comité d'Audit publiées dans le Rapport annuel.

10.1.2 Le Comité d'audit présente un rappart au Conseil concernant notamment :

- l'oudit interne ;
- les relations avec les commissaires aux Comptes du DC/BR ;
- l'analyse des risques ;
- les états financiers trimestriels ;
- le suivi de la mise en ploce de procédures internes de contrôle interne ;
- le contenu des communiqués de presse ;
- le respect des dispositions légales en matières financières ;
- le respect de l'harmonisation des règles comptables et de consolidatian du DC/BR ;
- le suivi du budget, la validité des hypothèses retenues et les mesures proposées ;
- les risques liés oux projets d'acquisition et de désinvestissement ;
- l'évolution des projets majeurs ;
- le niveau de contingences (contraintes/aléas) par branches d'activités, à mettre en rapport avec la valeur des contrats en caurs et leur avancement ;
- le niveau des réclamatians reconnues.

Le Comité examine les états financiers semestriels sociaux et consolidés, ainsi que les comptes annuels sociaux et consalidés de la société. Il étudie les modifications apportées, le cas échéant, aux principes comptables et aux règles d'évaluation, en particulier sous l'angle de leur impact sur les états financiers.

Le Comité révise de manière critique les comptes sociaux de la société et les comptes consolidés, ainsi que les comptes intermédiaires destinés à être publiés.

Après la clôture comptable de l'exercice écaulé et au plus tard au mois de mai, le Comité demandera au Commissaire aux comptes du DC/BR d'établir un document reprenant ses observations sur les documents de clôture. Le Comité communiquera, le cas échéant, ce document au Conseil d'administration.

10.2 Le Dispositif de Contrôle Interne

Le Comité évalue le dispositif de contrôle interne, en tenant compte de la gestion des risques, avec les auditeurs externes et tout expert dont il juge l'intervention nécessaire.

10.3 L'audit externe

Le Comité prend connaissance des rapports établis par les auditeurs externes. Il examine la nature, l'étendue et les conclusions de leurs travaux.

Il fait rapport au Conseil d'administration sur l'évaluation de la performance et des honoraires des auditeurs externes. Le Comité est également chargé de s'assurer de l'indépendonce de ces derniers.

Il vérifie si leur mission est compatible avec d'éventuels autres mandats ou missions exercés por ces auditeurs.

11. COMITE DE REMUNERATION ET DE NOMINATIONS

11.1 Fonctionnement

Conformément à lo réglementation, le Conseil constitue un Comité de Rémunération et de Nomination (le « Comité de Rémunération et de Nomination »).

Le Comité de Rémunération et de Nomination fonctionne conformément à sa chorte approuvée por le Conseil.

11.2 Rôle et responsabilités

Le Comité de Rémunération et de Nomination assiste principalement le Conseil sur les questions de nomination et de rémunération des administrateurs, du Directeur Général et des autres membres de l'Organe Exécutif et aura notamment pour responsabilité :

- d'identifier et de proposer à l'approbation du Conseil, des condidats, en tenont compte de leur statut. A cet effet, le Comité de Rémunération et de Nomination devra prendre en compte les propositions faites par les Parties concernées, en ce compris les actionnoires ;
- de proposer pour nominotion les candidats émanant des actionnoires ;
- de conseiller le Conseil sur la nomination du ou de lo Président(e) du Conseil ;
- de conseiller le Conseil sur la proposition de nomination du Directeur Général et sur les propositions faites por le Directeur Général pour la nomination des outres membres de l'Organe Exécutif ;
- de conseiller le Conseil sur la rémunération du Directeur Générol et des autres membres de l'Orgone Exécutif et sur les arrangements relatifs à la résiliation anticipée de leurs contrats ;
- de revoir tout méconisme d'intéressement, en numéraire, pour l'Orgone Exécutif et les travoilleurs ;
- d'étoblir des objectifs de performance et de conduire des évaluations de performance du Directeur Général et des autres membres des Comités et de l'Organe Exécutif ; et
- de soumettre un rapport annuel relatif aux conditions de rémunération de la société.
  Le Comité de Rémunération et de Nominotion se réunira suffisamment à l'avance des réunions du Conseil pour permettre aux membres du Comité de foire des recommandotions adéquates au Conseil.

Le Comité de Rémunération et de Nomination doit notamment :

- veiller à ce que le processus de nomination et de renouvellement soit organisé d'une manière rigoureuse, objective, professionnelle et transparente ;
- mettre en place une procédure clairement définie pour la nomination des membres des organes de gouvernance ;
- s'assurer en permanence que les procédures établies sont transparentes et respectées ;
- veiller à ce que l'établissement dispose d'un plan de succession adéquat pour les postes de direction et s'assurer que les successeurs envisagés soient qualifiés et répondent aux critères de compétence et d'honorabilité requis ;
- identifier, traiter, voire éliminer les situations de conflit d'intérêts qui émanent du processus de nomination, en vue de veiller à l'objectivité et à l'indépendance de l'organe délibérant par une sélection adéquate de ses membres ;
- participer au processus d'évaluation des organes de gouvernance ;
- identifier les administrateurs indépendants potentiels à retenir ;
- veiller à ce qu'une seule personne ou un groupe de personnes ne domine l'organe délibérant au détriment des intérêts de l'établissement dans son ensemble ;
- formuler des avis et recommandations à l'organe délibérant sur la politique de ressources humaines de l'établissement.

Le Comité de Rémunération et de Nomination formule des recommandations au Conseil d'Administration sur :

- la politique de rémunération des Exécutive Managers et des Fonctions de Contrôle transversales. La procédure d'actualisation régulière de la politique de rémunération des membres de l'Organe Exécutif intègre les recommandations émises par un cabinet international réputé de conseil en rémunérations, qui ne fournit aucun conseil à l'Organe Exécutif ni à aucun autre manager du DC/BR ;
- la rémunération des membres de l'Organe Exécutif et des Fonctions de Contrôle transversales, et sa cohérence avec la politique de rémunération ;
- les modalités contractuelles de fin de mandat convenues avec les Exécutive Managers et les paiements effectués à leur profit en vue de vérifier leur conformité à la politique de rémunération et leur caractère équitable à l'égard tant de la personne que de la Société ;
- Le Comité de Rémunération et de Nomination formule des recommandations au Conseil d'Administration sur :
  - les objectifs annuels et l'évaluation subséquente des performances du Directeur Général, toujours sur la base d'une proposition du Président du Conseil d'Administration ;
  - les objectifs annuels et l'évaluation subséquente des performances des autres Exécutive Managers, sur la base d'une proposition conjointement soumise par le Président du Conseil d'Administration.

Les autres responsabilités du Comité de Rémunération et de Nomination incluent la formulation de recommandations au Conseil d'Administration sur les informations publiées concernant la politique de rémunération (présentée en annexe de la présente Charte de gouvernance d'entreprise), le rapport relatif aux rémunérations (publié dans le Rapport annuel) et le rapport d'activité du Comité de Rémunération et de Nomination, qui fait partie de la Déclaration de

gouvernance d'entreprise figurant dans le Rapport annuel, et en veillant au respect de toutes les obligations légales et réglementaires de publication.

12. COMITE DE RISQUES

12.1 Objet et compétences

Le Comité des Risques est chargé d'assister l'organe délibérant dans so mission de surveillance de lo mise en œuvre du dispositif de gestion des risques du DC/BR. Pour l'exercice de ses ottributions, le Comité des Risques doit être composé de membres disposant d'une expérience ovérée en matière de gestion des risques. Le secrétariat du Comité des Risques est assuré por le responsable de la fonction risque.

Le Comité des Risques doit notamment :

- s'assurer de la mise en place, ou sein du DC/BR d'un dispositif de gestion intégrée des risques conforme aux exigences énoncées par les Principes sur les Infrastructures de Marchés relative à la gestion des risques ;
- avoir une bonne connaissance de la nature et de l'ampleur des risques encourus par la DC/BR les interrelations qui existent entre ces différents risques oinsi que les niveaux de fonds propres et de liquidité requis pour couvrir ces expositions ;
- examiner la cartographie des risques élaborée par les services du DC/BR ,
- participer à l'éloborotion des strotégies de gestion des risques prévues le Cohier des Charges du DC/BR et procéder annuellement à leur examen, à la fois sur une base agrégée, et par type de risques ;
- soumettre au Conseil pour approbation et présentation à l'Assemblée Générale ordinaire, des propositions relatives au risque actuel et futur à l'échelle du DC/BR, de ses Services Concédés, ainsi que de leurs limites. Le Comité des Risques est chargé d'assister le Conseil dans sa mission de surveillance de lo mise en œuvre du dispositif de gestian des risques de l'établissement y compris le Plan de Continuité.

Le Comité des Risques doit notamment :

- o réviser, au moins une fois tous les trois (03) ans, les politiques et procédures de risques du DC/BR au regard des évolutions enregistrées dans les Services Concédés et s'assurer qu'elles sont adaptées aux stratégies approuvées par l'Assemblée Générale ;
- o veiller à ce que le Conseil mette en place des procédures visant à promouvoir lo mise en œuvre effective des stratégies et politiques par le Concessionnaire dont le Plan de Continuité ;
- o veiller à ce que le Conseil et l'Assemblée Générale prennent les mesures nécessaires à leurs niveaux respectifs, pour contrôler et maîtriser tous les risques significatifs conformément aux stratégies approuvées ;
- o s'assurer de la mise en place d'une saine culture de la gestion des risques à l'échelle du DC/BR ; et
- o exiger de l'Organe Exécutif et faire approuver par le Conseil d'Administration du DC/BR un rapport, au mains semestriel, sur les risques significatifs ouxquels le DC/BR est exposée, l'état actuel de la culture du risque, le degré de risque, la gestion des limites de risque, les dépassements de ces limites et les mesures d'atténuotion mises en place.

13. COMITÉ D'ETHIQUE ET DE DEONTOLOGIE

13.1 Compétences

Le Comité d'Ethique et de Déontologie est chargé d'assister l'organe délibérant dans sa mission de surveillance de la mise en œuvre du Code d'Ethique et de Déontologie du DC/BR. Pour l'exercice de ses attributions, le Comité d'Ethique et de Déontologie doit être composé de membres disposant d'une expérience avérée en matière de déontologie et de gestion des risques. Le secrétariat du Comité d'Ethique et de Déontologie est ossuré par une personne désignée « Personne responsable en éthique et déontologie ».

Cette personne coordonne avec les autres comités et les agents toutes les actions relatives à la mise en œuvre de l'éthique et de la déontologie au sein du DC/BR.

Le Comité d'Ethique et de Déontologie peut ò son initiotive ou à la demande du Directeur Général ou du Conseil d'Administration effectuer une enquête sur des faits ou information relatifs un manquement à l'éthique ou la déontologie. Elle obtient des agents du DC/BR, les documents et informations, afin de l'éclairer sur les manquements allégués et rendre des conclusions sur la violation alléguée et les mesures préconisées. Le Comité peut entendre toute personne en relation avec les Services Concédés (dirigeant, employés, sous-traitants) dans le cadre d'une enquête ou de travoux.

Le Comité d'Ethique et de Déontologie doit notamment :

- s'assurer de la mise en place, au sein du DC/BR d'un dispositif de suivi des dispositions du Code d'éthique et de déontologie conforme aux exigences de la réglementation et celles énoncées par les recommandations de l'OICV relative à la gestion des risques ;
- avoir une bonne connaissance de la nature et de l'ampleur des risques encourus par le Concessionnaire en raison du non-respect des règles éthiques et déontologiques ;
- mettre ò jour le Code d'Ethique et de Déontologie selon les procédures d'évaluation de la mise en œuvre du code et de la Charte de Gouvernance et de l'évolution des Services Concédés ;
- soumettre ou Conseil pour approbation et présentotion à l'Assemblée Générale ordinaire annuel, des propositions relatives aux mises à jour du Code de déontologie, aux procédures d'évaluation de l'application du Code, aux mesures à prendre pour une application efficace du Code ; `
- réviser les politiques et procédures en matière d'éthique et de déontologie du DC/BR au regard des évalutions enregistrées dans les Services Concédés et s'assurer qu'elles sont adaptées aux stratégies approuvées par l'Assemblée Générale ;
- veiller à ce que le Conseil mette en place des procédures visont à promouvoir la mise en œuvre effective du Code d'éthique et de Déontologie ;
- veiller à ce que le Conseil et l'Assemblée Générale prennent les mesures nécessaires ò leurs niveaux respectifs, pour prendre les décisions de prévention et de sonctions portont sur la présente Charte et le Code d'Ethique et de Déontologie ;

- s'assurer de la mise en place d'une sensibilisation aux questions d'éthique et de déontologie des agents, représentants et sous-traitonts du DC/BR ;
- exiger de l'Organe Exécutif et faire approuver par le Conseil d'Administration du DC/BR un rapport annuel sur la conformité des comportements et procédures du DC/BR et de ses agents, saus–traitants et octionnaires en relation avec les règles d'éthique et de déontologie en vigueur, les mesures prises ou préconisées et leurs effets le cos échéant, les limites juridiques institutionnelles rencontrées lors de l'opplication du code, les recommandations formulées à l'attention de l'Organe Exécutif et du Conseil d'administration.

13.2 Relations avec les organes du DC/BR

Le Comité d'Ethique et de Déontologie odresse au Directeur, avec copie au Conseil d'Administration, tout rapport, note ou lettre d'information au sujet d'incident, de risques ou de manquements en matière d'éthique et de déontologie.

Il adresse au Conseil d'Administration aux fruits de la présentation à l'Assemblée Générale ordinaire onnuel un rapport, sur la conformité des comportements et procédures du DC/BR et de ses agents, sous-traitants et octionnaires en relation avec les règles d'éthique et de déontologie en vigueur, les mesures prises ou préconisées et leurs effets le cas échéant, les limites juridiques et institutionnelles rencontrées lors de l'opplication du Code, les recommandations formulées à l'attention de l'Organe Exécutif et du Conseil d'administration.

14. EVALUATION DES MEMBRES DES COMITES

14.1 Chaque Comité réexamine régulièrement (au moins tous les deux (02) ans) son règlement d'ordre intérieur, évalue sa propre efficacité et recommande au Conseil d'Administration les améliorations qui seraient le cas échéont nécessaires.

14.2 Dans le codre de son évoluation, le Conseil d'Administration procède régulièrement (au moins tous les trois ans), à une évaluation des Comités, de leurs fonctions et leurs compétences.

14.3 Les améliorations et recommandations éventuellement décidées par le Conseil d'Administration sont mises en œuvre par le Comité de Rémunération et Nominations.

15. GESTION DES CONFLITS D'INTERETS ET PRINCIPES DE BONNE CONDUITE

15.1 Politiques en matière de conflits d'intérêts

Les membres des organes de gouvernance doivent éviter de se placer dans une situation susceptible d'engendrer des conflits d'intérêts. L'Assemblée Générale doit s'assurer que l'organe exécutif élabore et met en place une politique ainsi que des procédures visont à détecter les

conflits d'intérêts apparents et potentiels et, lorsqu'ils ne peuvent être prévenus, à les gérer de manière appropriée. Il doit également se doter d'un processus de contrôle de la conformité avec cette politique.

Cette politique, applicable à tout membre du personnel ainsi qu'aux membres des organes exécutifs et délibérant, doit notomment prévoir :

- l'obligation de maintenir en toute circonstance une indépendance d'analyse, de jugement et de décision ;
- éviter de se trouver, de foçon directe ou indirecte, dans une situotion pouvant donner lieu à un conflit d'intérêts ovéré ou potentiel ;
- mettre en place des dispositions explicites relotives à la démorche à adopter pour informer rapidement lo hiérarchie ou de l'Assemblée Générale ou du Conseil d'Administration lorsqu'un acteur du DC/BR est confronté à un conflit d'intérêts avéré ou potentiel ;
- un processus rigoureux d'examen et d'opprobation, por l'Assemblée Générale ou le Conseil d'Administrotion, qui s'applique à tout membre des organes de gouvernance souhaitant siéger dans un autre organe délibérant, ou entreprendre des activités qui pourraient créer des conflits d'intérêts ;
- l'interdiction à tout membre de l'Assemblée Générale ou du Conseil d'Administration de participer aux débats et aux prises de décision sur des sujets qui les mettent en situation de conflits d'intérêts ou qui sont susceptibles de compromettre leur objectivité et leur indépendonce ;
- des exemples de situations de conflits d'intérêts susceptibles de se présenter dons le codre de l'exercice des différentes activités ou sein du DC/BR ;
- des procédures qui encadrent de manière adéquote les transactions avec les porties liées ofin qu'elles respectent les dispositions prévues à cet effet dans le Cahier des Chorges sur la gestion des risques ;
- les modalités et conditions de traitement des cos de non-respect de cette politique.

15.2 Déclarations de conflits d'intérêts et d'honneur

Préalablement à son entrée en fonction et chaque année durant son mandat, chaque administrateur soumet à l'organe délibérant une déclaration de conflits d'intérêts relative aux liens de toute nature qu'il entretient directement ou indirectement avec la DC/BR, ses dirigeants, ses partenaires, ses concurrents et ses cinquante plus gros clients.

En outre, chaque administrateur soumet avant son entrée en fonction et annuellement à l'Assemblée Générale ordinaire statuant sur les comptes de l'exercice sociol précédent une déclaration sur l'honneur, dans laquelle il atteste notamment ne pas disposer de créances ou de dettes en souffrance dans une société actionnaire du DC/BR ou du DC/BR.

15.3 Obligations de diligence et de loyauté

Les membres des organes de gouvernance, ainsi que le personnel sous leur autorité, ont une obligation de diligence et une obligation de loyauté envers lo Société. Ils respectent le Code d'Éthique et de Déontologie, en sus des dispositians de la présente charte et de toute autre règlementatian qui leur serait applicable en matière d'éthique et de déantalogie. Les

administrateurs nommés par des actionnaires d'influence dominante doivent conserver leur impartialité et exercer intégralement leurs obligations de diligence et de loyauté vis-à-vis du DC/BR.

La prévention des délits d'initiés et de la divulgation illicite d'informations privilégiées ou sein du DC/BR est confiée à un Comité de Transparence composé du Directeur Financier du DC/BR, du Responsable Conformité du DC/BR, et du Directeur Général des Ressources Humaines du DC/BR.

Les Administrateurs et membres des Comités ne peuvent réaliser aucune transaction au cours des périodes fermées (i.e. 30 jours calendaires préalable ò la mise en cotation, ou précédant l'annonce des résultats onnuels, semestriels et trimestriels) ou au cours de toute période spécifiquement interdite par la réglementotion ou là DC/BR.

Les membres du Conseil d'Administration et des Comités ont l'obligotion de notifier au Président du Conseil d'Administration et / ou au Directeur Général et au Directeur Juridique du DC/BR toute opération liée aux actions ou instruments de dette, aux instruments dérivés ou aux autres instruments financiers qui leur sont liés à une société catée en bourse ou en cours de cotation avant la réalisation d'une telle opération.

En outre, les membres du Conseil d'Administrotion et des Comités, ainsi que les personnes qui leur sant étroitement liées au sens de la présente Charte, sont légalement tenus de notifier à l'Autorité Concédante toutes les apérations portont plus porticulièrement sur des actions ou instruments de dette émis par la DC/BR.

Le Conseil d'Administrotion et chacun des Administroteurs individuellement respectent strictement les règles relatives aux conflits d'intérêts entre la Société et un Administrateur, telles que définies par la présente Charte et toute réglementation applicable aux conflits d'intérêts actuelle ou future.

Tout Administrateur se trouvant dans une situation de conflit d'intérêts de nature patrimoniale à toute question relevant des activités du DC/BR est tenu de le communiquer à ses collègues Administrateurs avant les délibérations. Il indiquera la nature du conflit d'intérêts et les raisons paur lesquelles il se trouve dans cette situation et ne pourro participer à aucune délibérotion portant sur ces questions.

So déclaration, ainsi que les raisons justifiant l'intérêt opposé qui existe dans le chef de l'Administrateur concerné, doivent figurer dons le procès-verbal du Conseil d'Administration qui devra prendre la décision.

L'Administrateur concerné doit également en informer par écrit contre récépissé le Comité d'Ethique et de Déontologie. Les extraits du procès-verbal comportont la déclaration de l'Administrateur au sujet du conflit d'intérêts dans lequel il se trouve, à la délibération et à lo décision sur le point donnont lieu au conflit d'intérêts sont intégrolement repris dans le rapport de gestion de l'exercice concerné.

Les Commissaires aux Comptes reçoivent une copie du procès-verbal de lo réunion sur ce point.

Les Administrateurs respectent également lo réglementation en vigueur au sein de la Société en ce qui concerne la Prévention des Abus de Marché.

ANNEXES A LA CHARTE DE GOUVERNANCE

1. PROFIL DE COMPÉTENCE DU CONSEIL

Les nominations ou Conseil se feront ou mérite et sur lo bose de critères objectifs. Les administrateurs doivent rencontrer des standards élevés de compétence et d'expertises professionnelles et doivent s'engager, avec les autres administrateurs, à servir les intérêts à long terme du DC/BR.

Chaque administroteur doit individuellement ovoir des compétences et une expérience complémentaire au regard des besoins du DC/BR, et doit apporter au Conseil un regard critique et objectif susceptible de remettre le monogement en question si nécessoire. En outre, les administrateurs doivent mettre à jour leurs compétences et oméliorer leur connaissonce du DC/BR, pour accomplir leur fonction tant au Conseil que dons les comités du Conseil.

Les odministrateurs doivent être désireux de consacrer suffisomment de temps à l'exécution efficace de leurs fonctions et responsobilités et doivent être en mesure de siéger au Conseil d'Administrotion de façon prolongée. Chaque administrateur adhère aux politiques du DC/BR en vigueur en matière d'intégrité, d'éthique et de conduite des affaires comme défini dans le Code d'éthique et de déontologie, validé por le Conseil d'odministrotion, et l'Autorité Concédonte de même que dans les documents similoires du DC/BR.

Le Conseil d'Administration doit être globalement composé de personnes qui, dons une certaine mesure, se complètent mutuellement, et représentent différents domaines de compétence et d'expertise. En autre, la composition du Conseil doit refléter une diversité de genre raisonnable et être en totale conformité avec les règles statutaires relatives à la parité linguistique et aux incompatibilités.

Les différents domaines de compétence et d'expertise devant être représentés au sein du Conseil sont au moins les suivants :

- vision et stratégie : ovoir une vision stratégique à long terme qui ojoute de la voleur et être capable de la développer ;
- Compétences en matière de direction et de gestion – expérience en matière de gestion à un niveau exécutif au sein d'un groupe multinational ;
- Capacité à développer une orgonisotion complexe et à gérer des équipes et maîtrise de la communication et de la gestion des ressources humaines ;
- Compétences en motière de finance et de comptabilité – expérience approfondie dans le domaine de la finance et de la comptabilité, permettant une compréhension critique de dossiers complexes relatifs aux activités du DC/BR et contribuant de façon constructive à son analyse ;
- Connaissances et expérience en matière de services boursiers et financiers, produits dérivés ;
- Connaissance et expérience en matière de compétences pour l'avenir dans le domoine digital, de l'internet et de l'innovation ;
- Connaissonces et expérience en motière d'activités bancaires et d'activités déterminées liées à celles-ci.

Chaque administrateur doit disposer de fortes compétences linguistiques, en ce compris une excellente maîtrise orale et écrite du français et/ou de l'anglais des affaires.

Le Comité de Rémunération et de Nomination est responsable avec le Conseil de l'examen périodique des compétences et caractéristiques requises de chaque administrateur, ainsi que de la composition globale du Conseil et de faire les recommandations adéquates au Conseil à ce sujet. Le Comité de Rémunération et de Nomination tiendra compte, pour ce qui est de la composition générale du Conseil, du besoin de représentation proportionnelle de personnes ayant des affinités avec les domaines d'activités principales du DC/BR.

Au vu de la limite d'âge fixée en principe à 70 ans, le Comité de Rémunération et de Nomination s'efforce à ce que les candidats nommés puissent assurer un mandat complet.

Par souci de clarté, les membres du Conseil, qui ont la qualité d'administrateur indépendant au sens de la Charte ci-dessus sont, en plus des exigences d'indépendance soumis à des critères de compétence managériale : Les administrateurs indépendants doivent être des chefs d'entreprise reconnus à l'échelle internationale ou communautaire UEMOA.

L'objectif premier du Conseil d'Administration en matière d'indépendance des administrateurs est d'identifier des administrateurs compétents pour servir au Conseil, dont l'indépendance n'est ni compromise ni entravée, en fait ou en apparence, et qui peuvent exercer leur jugement commercial au profit de tous les actionnaires sans distinction. Lorsqu'un administrateur indépendant ne rencontre plus les exigences définies par la présente Charte et son Annexe 1, il en avertit le Conseil d'Administration promptement.

2. SYSTEME ET POLITIQUE DE REMUNERATION DES CADRES

2.1 Système de rémunération

Le système de rémunération doit notamment être :

- assorti d'incitations appropriées et correspondant à une prise de risque prudente ;
- compatible avec les objectifs et la solidité financière à long terme du DC/BR et réajusté en cas de besoin ;
- encadré par une politique approuvée por l'organe délibérant.

2.2 Politique de rémunération

La politique de rémunération doit couvrir tous les aspects de la rémunération, notamment les rémunérations fixes, les rémunérations variables, les avantages en nature, les pensions discrétionnaires et toutes prestations similaires.

AMF-UMOA
AUTORITÉ DES MARCHÉS FINANCIERS DE L'UNION MONÉTAIRE OUEST AFRICAINE

Le Secrétaire Général

INSTRUCTION N° 77 /AMF-UMOA/2023
RELATIVE AU DISPOSITIF DE CONTRÔLE INTERNE ET DE GESTION DES RISQUES DE LA BOURSE RÉGIONALE DES VALEURS MOBILIÈRES (BRVM)

L'Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine,

Vu le Traité révisé de l'Union Monétaire Ouest Africaine (UMOA) du 12 juillet 2019, entré en vigueur le 1er octobre 2022, modifiant la dénomination du Conseil Régional de l'Epargne Publique et des Marchés Financiers (CREPMF) en Autorité des Marchés Financiers de l'UMOA (AMF-UMOA) ;

Vu la Convention du 3 juillet 1996 portant création du Conseil Régional de l'Épargne Publique et des Marchés Financiers, notamment son Annexe portant composition, organisation, fonctionnement et attributions du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu le Règlement Général n°001/97 du 28 novembre 1997 relatif à l'organisation, au fonctionnement et au contrôle du marché financier régional notamment en ses articles 10 et 16 ;

Vu l'Instruction n°2/97 du 29 novembre 1997 relative à l'habilitation de la Bourse Régionale des Valeurs Mobilières ;

Vu la Décision n° 004 du 29/04/2021/CM/UMOA portant nomination du Président du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu les délibérations de l'AMF-UMOA en sa 50ème session extraordinaire du 24 septembre 2021 tenue par visioconférence ;

Vu les délibérations de l'AMF-UMOA en sa 98ème session ordinaire du 23 décembre 2023, tenue à Cotonou en République du Bénin ;

ARRÊTE :

TITRE 1. DISPOSITIONS GENERALES

Article 1 Définitions

Aux fins de la présente Instruction, on entend par :

a) Audit interne : Activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. L'audit interne doit évaluer les processus de gouvernance de l'organisation, de management des risques et de contrôle, et contribuer à leur amélioration sur la base d'une approche systématique, méthodique et fondée sur une approche par les risques.

b) Appétence pour le risque : Le niveau et le type de risque que la BRVM est disposée à assumer dans ses expositions et ses activités pour réaliser ses objectifs stratégiques et ses obligations.

c) Bourse Régionale des Valeurs Mobilières ou BRVM : La société autorisée, par Agrément de l'AMF-UMOA, à exercer sur l'ensemble du territoire des États de l'UMOA, les activités de cotation des valeurs mobilières, ainsi que de la diffusion des informations boursières.

d) Chartes d'audit interne et de conformité : Documents qui définissent le positionnement des fonctions d'audit interne et de conformité au sein de la structure agréée et précisent l'organisation, les pouvoirs, les responsabilités et les modalités de fonctionnement desdites fonctions.

e) Cartographie des risques : Représentation synthétique et visuelle des risques de la BRVM. Elle constitue ainsi un outil de mise en évidence des risques à couvrir en priorité.

La cartographie des risques est établie sur la base d'un système d'identification et d'évaluation rigoureuse des risques inhérents à la BRVM à partir des facteurs internes (métiers et activités, modifications organisationnelles, etc.) et externes (conditions économiques, progrès technologiques, changements législatifs et réglementaires, etc.).

f) Comité d'audit : Comité institué par l'organe délibérant pour l'assister dans l'exercice de ses missions, et en particulier vérifier la fiabilité et la transparence des informations financières, apprécier la pertinence des méthodes comptables ainsi que la qualité du dispositif de contrôle interne et du dispositif de gestion des risques, évaluer la stratégie d'audit et proposer le cas échéant, des pistes d'amélioration.

g) Contrôle Interne : Mesures mises en place par les organes exécutifs et qui ont pour but d'assurer que :

- les objectifs posés par la BRVM sont réalistes et atteints ;
- les ressources sont utilisées de façon économique et efficiente, les risques sont contrôlés adéquatement ;
- le patrimoine est protégé ;
- l'information financière et l'information de gestion sont complètes et fiables ;

- les lois et réglementations ainsi que les politiques, les plans, les règles et les procédures internes sont respectés.

h) Cycle des contrôles : Intervalle au cours duquel toutes les activités et les entités de la BRVM auront été vérifiées au moins une fois par la fonction d'audit interne.

i) Dispositif de Contrôle Interne (DCI) : Ensemble des règles, méthodes et mesures de contrôle régissant la structure organisationnelle et opérationnelle de la BRVM. Il comprend les processus de reporting et les fonctions de contrôle.

j) Fonctions de contrôle : Les fonctions indépendantes de la gestion opérationnelle, dont le rôle est de fournir des évaluations objectives quant à la qualité et à l'efficacité du DCI, des dispositifs de gouvernance, de gestion des risques de non-conformité, en vue de faciliter la maîtrise des activités et des risques encourus. Elles comprennent notamment la fonction d'audit interne, la fonction de gestion des risques et la fonction de conformité.

k) Gestion des risques : L'ensemble des stratégies, politiques et procédures mises en place afin que tout risque significatif et toute concentration de risques associée soient détectés, mesurés, limités, maîtrisés et atténués, et qu'il en soit rendu compte, de façon précoce et exhaustive.

l) Normes en vigueur : Ensemble des règles régissant l'exercice des activités de la BRVM, notamment :

- les dispositions légales et réglementaires ;
- les codes de conduite et de déontologie internes ;
- les principes pour les Infrastructures de Marché édictés par le Comité de Bâle et l'Organisation Internationale des Commissions de Valeurs (OICV).

m) Organe délibérant : Le Conseil d'Administration dans les sociétés anonymes ou l'organe collégial dans les sociétés constituées sous une autre forme. Il est investi de tous les pouvoirs pour agir en toutes circonstances au nom de la BRVM, dans la limite de l'objet social et des compétences réservées à l'Assemblée Générale.

n) Organe exécutif : Tout comité ou structure qui concourt à la gestion courante de la BRVM et assure l'application effective de l'orientation de l'activité définie par l'organe délibérant.

o) Piste d'audit : Ensemble de procédures internes permanentes permettant d'assurer la traçabilité des opérations, de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter, par un cheminement ininterrompu, au document de synthèse et réciproquement et d'expliquer l'évolution des soldes d'un arrêté comptable à l'autre, grâce à la conservation des mouvements ayant affecté les postes comptables.

p) Risque de non-conformité : le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, que la BRVM peut subir en raison de l'inobservation des normes en vigueur régissant l'exercice de ses activités.

q) Risque opérationnel : le risque de pertes résultant de carences ou de défaillances attribuables à des processus, des personnes, des systèmes internes ou à des événements

externes. Cette notion inclut le risque juridique mais exclut les risques stratégiques et de réputation.

r) Risque stratégique : le risque que les stratégies d'affaires de la BRVM soient inefficaces, ne soient pas bien mises en œuvre ou adaptées aux changements touchant le contexte commercial.

Article 2 Objet

La présente Instruction fixe les règles en matière de dispositif de contrôle interne applicables à la BRVM dont l'objectif est de :

- vérifier que les opérations réalisées, l'organisation et les procédures internes sont conformes aux dispositions législatives et règlementaires en vigueur, aux normes et usages professionnels et déontologiques ainsi qu'aux orientations des organes délibérant et exécutif ;
- s'assurer que les orientations, les instructions et les limites fixées par l'organe délibérant en matière de risques sont strictement respectées ;
- veiller à la fiabilité de l'information comptable et financière, en particulier aux conditions de collecte, d'évaluation, d'enregistrement, de conservation et de disponibilité de cette information.

Elle fixe également les règles en matière de gestion des risques applicables à la BRVM, telle que définie à l'article 1 de ladite Instruction.

Article 3 Périmètre de contrôle

La gouvernance d'entreprise de la BRVM intègre un DCI sur lequel doit reposer la gestion saine et prudente de l'entité. Ce dispositif comporte :

- la surveillance de la fiabilité et l'intégrité des informations financières et opérationnelles et les moyens utilisés pour identifier, évaluer, classer et rapporter ces informations ;
- la vérification de la conformité des opérations réalisées et de l'organisation avec les dispositions législatives, réglementaires et prudentielles en vigueur, les normes et usages professionnels et déontologiques, les orientations et décisions des organes délibérants et exécutifs, notamment en matière de risques, de pouvoirs et de signature ainsi que les procédures internes ;
- le suivi et l'évaluation de l'efficacité du dispositif de gestion des risques de l'entité.

L'organisation du contrôle interne doit s'appuyer sur l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication et le pilotage.

Article 4 Environnement de contrôle

L'organe délibérant doit veiller à la mise en place d'un environnement de contrôle adéquat, lequel constitue le cadre et la structure nécessaires à la réalisation des objectifs du dispositif de contrôle interne.

Un environnement de contrôle adéquat implique :

- l'engagement des organes de gouvernance en faveur de la promotion de l'intégrité et des valeurs éthiques au sein de la BRVM ;
- l'instauration d'une culture qui met en évidence, à tous les niveaux de l'organisation, l'importance du contrôle interne ;
- une implication effective de l'organe délibérant dans le suivi des composantes du dispositif de contrôle interne ;
- une définition claire et cohérente des missions, fonctions et responsabilités, y compris des délégations de pouvoirs explicites en matière de limites ;
- l'existence d'un personnel compétent et d'un dispositif de gestion des ressources humaines permettant à la BRVM d'attirer, de développer et de maintenir des compétences en lien avec ses objectifs ;
- une forte adhésion du personnel aux exigences de contrôle qui lui sont assignées ainsi qu'au devoir de rendre compte de ses responsabilités en la matière ;
- les supervisions par chaque responsable hiérarchique de l'application effective des procédures de contrôle interne par ses collaborateurs ;
- la définition de critères qualitatifs par les organes délibérants et exécutifs de la BRVM afin de mesurer et d'évaluer l'efficacité du Dispositif du Contrôle Interne.

Article 5 Les lignes de défense du DCI

Le DCI est organisé de façon à fournir des appréciations objectives de la situation de la BRVM, la maitrise des risques et la conformité de son fonctionnement aux règles et procédures en vigueur. Il comprend :

- un contrôle permanent de premier niveau qui correspond, à l'ensemble des contrôles réalisés par les unités opérationnelles et leur hiérarchie dans le cadre du traitement des opérations quotidiennes, ce qui constitue la première ligne de défense ;
- un contrôle permanent de deuxième niveau qui correspond, aux contrôles exécutés par les fonctions supports indépendantes des unités opérationnelles, qui forment la deuxième ligne de défense représentée par les fonction de conformité et de gestion des risques ;
- un contrôle périodique qui correspond aux contrôles a posteriori réalisés dans le cadre d'un plan d'audit élaboré à partir d'une cartographie des risques, ce qui constitue la dernière ligne de défense représentée par la fonction d'audit interne. Le plan d'audit élaboré par l'approche par les risques doit être réaliste et flexible afin de permettre le

respect du cycle de contrôle et la prise en charge des activités imprévues. Il doit régulièrement faire l'objet de mise à jour en vue de répondre aux changements de l'environnement interne et externe de la BRVM.

Article 6 Responsabilité de l'organe délibérant

L'organe délibérant est responsable en dernier ressort de l'existence d'un dispositif de contrôle interne au sein de la BRVM ainsi que de la bonne application du DCI à l'ensemble de l'organisation de la structure agréée. Il est tenu de :

- définir et valider, selon une périodicité adaptée, le niveau de risque acceptable auquel la BRVM est exposée, notamment par la fixation de limites acceptables de risques de contrepartie, de liquidité et de marché ainsi que par la mise en place de dispositifs appropriés pour encadrer les risques opérationnels et de non-conformité ;
- veiller à la mise en place et à la mise à jour d'une organisation, des politiques et procédures écrites de contrôle interne, pour une saine et prudente gestion des activités de la BRVM ;
- veiller à la séparation des tâches incompatibles, notamment les fonctions de décision, de détention des valeurs, d'enregistrement et de contrôle ;
- s'assurer que les fonctions de contrôle disposent de moyens appropriés pour exécuter ses missions en toute indépendance.

Article 7 Comité d'audit

Les prérogatives minimales du Comité d'audit consistent à :

- examiner l'efficacité du DCI mis en place pour identifier, évaluer, gérer et contrôler les risques financiers et non financiers ;
- évaluer la politique d'audit interne et le cycle des contrôles, y compris la politique d'escalade lors de la matérialisation de risques importants ;
- participer à la sélection des Commissaires aux Comptes et à l'examen des conclusions de leurs travaux, conformément aux dispositions légales et réglementaires ;
- analyser la conformité du respect des principes déontologiques et comptables appliqués avec les normes et usages professionnels en vigueur ;
- examiner de manière approfondie les états de synthèse annuels avant leur présentation aux organes délibérants ;
- donner aux organes de gouvernance une assurance raisonnable quant à la qualité et à l'efficacité du dispositif de contrôle interne, des dispositifs de gouvernance et de gestion des risques en vue de faciliter leur maîtrise des activités de la BRVM et des risques encourus.

Il fait également des propositions auxdits organes pour renforcer l'efficacité de ces systèmes et dispositifs.

Article 8 Responsabilités de l'organe exécutif

L'organe exécutif est tenu de mettre en place un DCI conforme aux bonnes pratiques et de surveiller son adéquation et son efficacité. Le DCI doit être adapté au profil de risque de la BRVM.

L'organe exécutif veille à ce que les politiques et procédures soient développées et appliquées efficacement par les personnes qui disposent de la compétence en la matière et que toutes les personnes concernées comprennent et assument leurs responsabilités à cet égard. Il définit les critères d'escalade en réponse à la matérialisation des risques et s'assure de la mise en œuvre des mesures appropriées.

Il doit notamment :

- s'assurer, du bon fonctionnement des dispositifs de contrôle interne et de gestion des risques et prendre des mesures nécessaires pour remédier, en temps opportun, à toute carence ou insuffisance relevée ;
- informer les fonctions de contrôle, à temps, de tous nouveaux développements, initiatives, projets, produits et changements opérationnels ainsi que des risques y relatifs ;
- s'assurer que des mesures appropriées sont prises dans les délais fixés pour mettre en œuvre toutes les actions correctrices découlant des recommandations de l'audit interne, des Commissaires aux Comptes ou de l'AMF-UMOA ;
- promouvoir l'indépendance des fonctions de contrôle et mettre à leur disposition les ressources nécessaires pour mener à bien leurs missions ;
- rendre compte régulièrement à l'organe délibérant de l'efficacité du dispositif de contrôle interne.

Article 9 Obligations du personnel

Chaque membre du personnel de la BRVM doit :

- effectuer avec diligence l'ensemble des activités de contrôle qui lui sont attribuées ;
- disposer de toutes les informations nécessaires pour notamment établir, faire fonctionner et surveiller le dispositif de contrôle interne.

TITRE 2. GESTION DE LA CONFORMITE

Article 10 Caractéristiques de la politique de conformité

La BRVM doit se doter d'une politique de conformité qui, notamment :

- assure le respect des principes fondamentaux fixés par l'organe délibérant ;
- instaure la fonction conformité au sein de la BRVM ;
- prescrit l'élaboration d'une charte de conformité ;
- précise les aspects fondamentaux du risque de non-conformité ;
- établit les responsabilités des organes de gouvernance dans la mise en œuvre du cadre de gestion du risque de non-conformité ;
- institue un programme de formation continue à l'intention des employés et de tous ceux qui sont chargés de la mise en œuvre et de la surveillance de la politique de conformité.

Article 11 Charte de conformité

La charte de conformité doit notamment :

- exposer les objectifs de la fonction conformité, établir son indépendance et définir ses responsabilités ainsi que ses compétences ;
- décrire clairement les relations de la fonction conformité avec les autres fonctions de contrôle et les services de la BRVM qui exécutent des tâches liées à ses responsabilités ;
- accorder à la fonction conformité le droit de communiquer avec tout membre du personnel et d'accéder à tout dossier physique ou électronique nécessaire à l'exercice de ses responsabilités ;
- conférer à la fonction conformité le pouvoir de diligenter des investigations ;
- formaliser les tâches et les obligations de la fonction conformité qui peuvent être déléguées à d'autres services et fonctions de la BRVM ou externalisées auprès de prestaires externes ;
- définir les conditions dans lesquelles la fonction conformité peut recourir, en cas de besoin, à des experts externes.

La charte de conformité doit refléter les évolutions enregistrées dans les normes en vigueur. La BRVM est tenue de la mettre à jour dans les meilleurs délais pour tenir compte de ces changements.

Tout projet d'externalisation de la fonction conformité doit être approuvé par l'organe délibérant et soumis à l'autorisation de l'AMF-UMOA avant sa mise en œuvre.

Article 12 Indépendance

La fonction conformité doit être indépendante des unités qu'elle contrôle. Pour assurer l'indépendonce de cette fonction, l'organe exécutif doit veiller à meitre en place un dispasitif organisotionnel exempt de conflits de tâches et de fonctions. En outre, les ressources y dédiées ne doivent pas être en situation de conflits d'intérêts.

Article 13 Ressources

La fonction conformité doit avoir accès aux organes délibérant et exécutif, ofin de signaler = doit être adoptée à la taille de la BRVM, la nature et lo complexité de ses octivités oinsi qu'à son profil de risque.

La BRVM doit désigner un responsable de la fonction en chorge de lo coordinatian à l'échelle de l'organisotion de la gestion du risque de non-conformitć ainsi que de la supervision des activités de lo fonction. Le responsable de la fonction conformité doit être doté d'une expérience avérée en matière d'audit et de conformité.

Article 14 Compétence

Les ressources humaines affectées à la fonction conformité doivent posséder un niveau élevé de connoissance des activités de la BRVM et des normes qui lui sont applicables.

La BRVM doit prendre les dispositions pour que ces ressources humaines maintiennent à jour leurs connaissances desdites normes.

Article 15 Responsabilités générales

La fonction conformité est chargée d'aider l'organe exécutif à identifier et à gérer avec diligence tout risque d'inobservation, par la BRVM, des obligations que lui imposent les normes en vigueur régissant l'exercice de ses activités.

Article 16 Responsabilités spécifiques

Les responsabilités spécifiques de la fonction conformité consistent notamment à :

- recenser et à communiquer à l'ensemble du personnel concerné, les normes en vigueur régissant l'exercice des activités de la BRVM ;
- identifier, évaluer et gérer, de manière proactive, les risques de non-conformité, y compris lors du développement de nouveaux produits ou marchés, activités ou relations émetteurs et adhérents aux services de la BRVM.

En outre, si la BRVM dispose d'un Comité de nouveaux produits ou marchés, la fonction conformité doit y être représentée.

La fonction conformité doit également :

- centraliser et analyser tous les manquements aux normes en vigueur et à la politique de conformité ;
- recommander des mesures correctrices pour remédier aux manquements et insuffisances relevées ;
- effectuer le suivi de la mise en œuvre de toutes ses recommandations ;
- évaluer l'adéquation de la politique de conformité, au regard des évolutions enregistrées dans les activités de la BRVM, les normes en vigueur et sur la base des insuffisances relevées. Elle doit, le cas échéant, formuler des propositions d'amendements ;
- veiller à une mise en œuvre diligente de la politique de conformité. La fonction conformité doit s'assurer que les règles édictées dans la politique de conformité sont déclinées dans des procédures, des manuels de conformité et des contrôles internes pour les domaines relevant directement de la fonction conformité. Les domaines d'intervention relevant directement de la fonction conformité concernent notamment la lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi que la protection des intérêts des émetteurs et des investisseurs.

En outre, d'autres prérogatives compatibles avec ses missions peuvent lui être confiées, notamment assurer la liaison avec les organismes externes de réglementation et de normalisation.

La fonction conformité doit être impliquée et consultée préalablement à la mise en place de procédures de contrôle interne.

Elle doit s'assurer en permanence que la politique de conformité de la BRVM est respectée à tous les niveaux de l'organisation, notamment :

- Sensibiliser et former le personnel : La fonction conformité doit initier des actions visant à sensibiliser et former le personnel sur l'importance de l'appropriation des normes en vigueur et du respect de la politique conformité. Elle établit et met en œuvre, à cet effet, un programme de formation destiné au personnel.
- Documenter ses travaux : La fonction conformité est tenue de documenter l'ensemble de ses travaux en vue de garantir une traçabilité de ses interventions et de ses conclusions.

Article 17 Détection d'anomalies de conformité

Toutes anomalies et déficiences significatives de conformité qui constitueraient un manquement aux dispositions réglementaires de l'AMF-UMOA doivent faire l'objet d'une documentation et d'un rapport circonstancié spécifique adressé à l'organe délibérant de la BRVM et à l'AMF-UMOA.

Les rapports de la fonction conformité contenant des constats mettant en cause les dirigeants ne peuvent être modifiés par ces derniers.

Toutefois, les personnes mises en cause peuvent formuler des observations sur les constats dressés. Les observations formulées doivent être jointes au rapport de contrôle.

Le non-respect de ces dispositions expose les contrevenants aux sanctions prévues par la réglementation, sans préjudice des sanctions pénales.

Article 18 Contrôle de la fonction conformité par la fonction d'audit interne

Les activités de la fonction conformité doivent être soumises à un examen périodique par la fonction d'audit interne. Pour éviter tout conflit de responsabilité et de fonction, la fonction conformité ne peut faire partie de la fonction d'audit interne.

Article 19 Reporting du Responsable de la Conformité aux organes de gouvernance

Le responsable de la fonction conformité doit communiquer aux organes de gouvernance, dans les meilleurs délais, les incidents significatifs de non-conformité et les manquements à la politique de conformité. Il rend compte à l'organe délibérant ou à un comité spécialisé auquel il est rattaché, au moins une fois par an, de l'exécution de sa mission. Il produit un rapport semestriel sur l'évaluation du risque de non-conformité. Ce rapport doit être adapté au profil de risque et aux activités de la BRVM et couvrir notamment :

- les réalisations de la fonction conformité, au regard des objectifs qui lui ont été fixés ;
- les moyens humains et matériels mis en œuvre pour atteindre ses objectifs ;
- la cartographie des incidents de non-conformité à l'échelle de la BRVM, en mettant en exergue les principales insuffisances relevées, les mesures correctrices engagées et le suivi effectué.

TITRE 3. GESTION DES RISQUES

Article 20 Principe de proportionnalité

La BRVM doit se doter d'un dispositif de gestion des risques lui permettant de gérer intégralement les risques juridiques, de contrepartie, de liquidité et opérationnel, ainsi que tout autre risque.

Article 21 Stratégies, politiques et procédures

Le dispositif de gestion des risques doit être basé sur des stratégies, politiques et procédures bien documentées qui permettent d'identifier, de mesurer, d'évaluer, de suivre, de déclarer et de contrôler ou d'atténuer l'ensemble des risques significatifs de la BRVM.

Les stratégies, politiques et procédures doivent être dynamiques, de manière à refléter l'évolution du degré d'appétence au risque de la BRVM, son profil de risque ainsi que les conditions de marché et l'environnement macroéconomique.

La BRVM doit veiller à la mise en œuvre de stratégies, politiques et procédures permettant d'avoir une vision globale, à l'échelle de l'organisation, de ses expositions sur chaque type de risque.

Article 22 Cartographie des risques

Le dispositif de gestion des risques doit comporter une cartographie des risques validée par l'organe délibérant, qui recense, évalue et hiérarchise l'ensemble des risques de la BRVM. La BRVM est tenue de se doter de cet outil de pilotage aux fins d'assurer une bonne gestion et un suivi adéquat des risques. La mise à jour de la cartographie doit être dynamique avec une revue globale au moins une fois par an.

Article 23 Culture du risque

La BRVM doit encourager le développement de la culture du risque à tous les niveaux de son organisation à travers notamment la formation et les actions de sensibilisation au profit de son personnel.

Article 24 Appétence au risque et gestion des limites

La BRVM doit mettre en place un dispositif d'appétence au risque approuvé, supervisé et révisé annuellement par le Conseil d'Administration et mis en œuvre par l'organe exécutif. La BRVM est également tenue de :

- fixer des limites globales et des limites opérationnelles au niveau de ses différentes entités. Ces limites doivent être établies de manière cohérente, conformément au degré d'appétence ou risque de la BRVM, à son profil de risque et à son assise financière ;
- s'assurer d'une bonne appropriation de ces limites par le personnel concerné et d'une communication interne régulière ;
- se doter d'un dispositif d'identification et de gestion des dépassements de limites, comprenant une procédure de communication des dépassements au niveau hiérarchique approprié, de régularisation, de suivi de la régularisation et de sanction en cas de dépassement persistant ;
- définir clairement la procédure à suivre en vue de soumettre, de manière diligente, à l'examen et à l'autorisation des organes habilités, les cas d'exceptions aux politiques, procédures et limites établies.

Article 25 Systèmes d'information

La BRVM doit mettre en place des systèmes d'information et de contrôle des risques qui lui permettent d'obtenir en temps requis les informations nécessaires pour la mise en œuvre des politiques et procédures de gestion des risques.

À cet effet, la BRVM doit se doter d'un dispositif de gouvernance des données sur les risques, d'une orchitecture de données relotives aux risques et d'une infrastructure informatique.

Les systèmes d'informotion mis en ploce por la BRVM devraient, en particulier :

- permettre, oussi bien en situation normole qu'en période de crise, de mesurer et d'agréger précisément et en temps requis les expositions aux risques dans toute la BRVM, de gérer les expositions individuelles oux risques, ainsi que leurs interdépendances, et d'évaluer l'impact de divers chocs économiques et financiers qui pourroient l'affecter ;
- suivre ses expositions aux risques identifiés ;
- s'odapter pour mesurer et évaluer la taille, la composition et la qualité de l'exposition au risque à l'échelle de la BRVM et pour l'ensemble des types de risques, des produits et des contreparties ;
- assurer la disponibilité, la qualité, lo fiabilité et l'intégrité des données ;
- garantir la transmission en temps opportun, aux organes de gouvernance, de toutes informations pertinentes et utiles à leur prise de décision.

Article 26 Simulation de crise

La BRVM doit établir des programmes de simulations de crise, aux fins de la gestion des risques, en vue d'évaluer l'impact potentiel de scénarios adverses sévères mais plausibles sur sa solidité financière.

Ces programmes doivent inclure tous les risques importants auxquels la BRVM est exposée. Ils doivent, en outre, prévoir des mesures correctives lorsque les résultats des simulations de crise décèlent des fragilités potentielles qui pourraient avoir une incidence négative sur la solidité financière de la BRVM.

Article 27 Rôles et obligations des organes de gouvernance

Les organes de gouvernance doivent notamment :

- veiller à ce que lo BRVM soit dotée d'un dispositif de gestion des risques conforme oux dispositions de la présente Instruction ;
- mettre en place une fonction gestion des risques couvrant tous les risques significatifs, à l'échelle de la BRVM et disposant d'attributions distinctes de celles des unités opérotionnelles ;
- préserver l'existence d'une fonction gestion des risques indépendonte et dotée des ressources nécessoires ainsi que d'une autorité suffisante pour mener à bien ses missions ;
- exercer pleinement les responsabilités qui leur sont dévolues en matière de risque, conformément aux dispositions énancées dans l'Instruction relative à la gouvernance de la Bourse Régionale des Voleurs Mobilières.

Article 28 Rôles et obligations de la fonction gestion des risques

La fonction gestion des risques doit notamment :

- appliquer la stratégie de risque approuvée par l'organe délibérant et veiller à l'élaboration de toutes les politiques et procédures afférentes à la gestion des risques ;
- contribuer à la mise en place effective, au sein de la BRVM, d'un dispositif de gestion intégrée des risques qui soit soutenu par une gouvernance fiable impliquant les organes de gouvernance ;
- identifier, évaluer, suivre et maîtriser, en temps opportun, tous les risques significatifs ;
- améliorer les systèmes, les politiques, les processus et les rapports relatifs à la gestion des risques ;
- élaborer et mettre en œuvre, sous réserve de l'examen et de l'approbation par l'organe délibérant, le dispositif de gestion des risques, qui comprend la culture du risque à l'échelle de la BRVM, l'appétence pour le risque ainsi que les limites ;
- mettre en place un système d'alerte précoce visant à détecter les cas d'infraction à l'appétence au risque et aux limites fixées par l'organe délibérant ;
- orienter, voire récuser, toute décision qui engendre une prise de risque importante pour la BRVM, rendre compte aux organes de gouvernance de toutes ces questions et proposer des mesures appropriées pour atténuer ces risques.

La fonction gestion des risques ne doit pas s'impliquer dans les activités opérationnelles, en particulier, celles qui sont génératrices de revenus. Elle doit garder son indépendance vis-à-vis des entités opérationnelles, tout en travaillant en étroite collaboration avec celles-ci.

Les ressources humaines affectées à la fonction gestion des risques doivent posséder un niveau élevé de connaissance des activités de la BRVM, de tout risque auquel elle est exposée ainsi que de la manière dont ces risques sont gérés. La BRVM prend les dispositions pour que ces ressources humaines maintiennent à jour leurs connaissances en matière de gestion des risques.

Article 29 Responsable de la fonction gestion des risques

Le responsable de la fonction gestion des risques doit être doté d'une expérience avérée en la matière. Il a notamment la charge :

- de surveiller l'élaboration et la mise en œuvre du dispositif de gestion des risques ;
- de renforcer constamment les compétences de ses équipes ;
- d'apporter son assistance à l'organe délibérant ou au comité des risques, le cas échéant, lorsqu'il détermine et surveille l'appétence pour le risque et les limites ;
- de participer, conjointement avec l'organe exécutif, au suivi des performances en matière de risques et de respect des limites.

Le responsable de la fonction gestion des risques doit être impliqué dans les processus clés de prise de décision relatifs notamment à la planification stratégique, la planification des fonds

propres et de la liquidité, l'élaboration et la mise en œuvre du système de rémunération, les nouveaux produits, services et marchés ainsi que les initiatives et les opérations stratégiques importantes.

Article 30 Contrôle des risques

Le dispositif de gestion des risques de la BRVM doit intégrer des contrôles internes rigoureux, adaptés à l'ampleur, à la nature et à la complexité de ses expositions. Ce dispositif doit également faire l'objet d'examen annuel par l'audit interne et les commissaires aux comptes qui apprécient de manière indépendante l'efficacité des systèmes et processus d'évaluation et de mesure des risques de la BRVM.

Article 31 Reporting à l'organe délibérant

Un rapport sur la nature et le niveau d'exposition à chaque type de risques encourus par la BRVM ainsi que ses besoins de fonds propres et de liquidité doit être soumis à l'organe délibérant, au moins une fois par semestre. Ce rapport, basé sur des informations fiables et à jour, doit également rendre compte notamment :

- de la nature et du niveau de l'exposition au risque de concentration de la BRVM, y compris notamment les expositions par contrepartie, par secteur et par zone géographique ;
- des principaux événements de pertes opérationnelles ;
- des transactions avec les parties liées, y compris les créances en souffrance et les créances irrécouvrables ;
- des faits saillants relatifs à chaque type de risques identifiés dans la cartographie des risques de la BRVM.

Article 32 Événements de pertes opérationnelles

Les événements de pertes opérationnelles ou incidents opérationnels doivent être classés dans l'une des sept catégories ci-après définies, afin d'assurer la cohérence au niveau de l'identification, de l'évaluation et de la fixation des objectifs de gestion des risques opérationnels à l'échelle de la BRVM :

1. fraude interne : risque de pertes dues à des actes intentionnels, impliquant au moins une partie interne à la BRVM, visant à frauder, détourner des biens appartenant à la BRVM ou à sa clientèle, manipuler des informations, contourner les règlements, la législation ou la politique de la BRVM ;
2. fraude externe : risque de pertes résultant des actes, de la part d'un tiers, visant à frauder, détourner des biens appartenant à la BRVM ou à sa clientèle, manipuler des informations ou contourner la législation ;

3. pratiques en matière d'emploi et de sécurité sur le lieu de travail : risque de pertes découlant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, y compris les litiges ou différends entre la BRVM et ses employés ;
4. pratiques concernant les clients, les produits et l'activité commerciale : risque de pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients ou d'un manquement imputable à la nature ou à la conception d'un produit donné ;
5. dommages occasionnés aux actifs physiques : risque de pertes lié à des destructions ou dommages résultant d'une catastrophe naturelle ou des causes externes ;
6. interruptions d'activités et défaillances des systèmes : risque de pertes résultant d'interruptions de l'activité ou de dysfonctionnements des systèmes technologiques ;
7. exécution des opérations, livraison et gestion des processus : risque de pertes lié à une défaillance dans le traitement d'une transaction ou dans la gestion des processus et les pertes subies dans le cadre des relations avec les contreparties commerciales et les fournisseurs.

Article 33 Collecte des données de pertes opérationnelles

La BRVM doit collecter les données relatives aux événements de pertes opérationnelles. Le processus y relatif doit être documenté et mis à jour périodiquement. Les données de pertes collectées doivent répondre à certains critères minimaux, afin d'uniformiser le processus de collecte à l'échelle de la BRVM ainsi qu'à travers le marché financier et faciliter les analyses comparatives. Les pertes doivent être directes, intègres, intégrales et retraçables :

- la perte est directe lorsque l'événement a eu une incidence négative directe reconnue sur les résultats de la BRVM et, par conséquent comptabilisée. Il s'agit de l'ensemble des frais/dépenses internes et externes encourus par la BRVM mais qui ne l'auraient pas été sans l'événement. Les coûts d'opportunité et les revenus manqués liés à l'événement, les coûts relatifs aux modifications apportées à un processus ou à l'ajout de contrôles post-événementiels, les coûts des programmes d'investissement réactifs ou proactifs à l'événement ne sont pas considérés comme directs ;
- l'intégrité des données signifie que celles-ci représentent bien des pertes opérationnelles ;
- l'intégralité des données veut dire que celles-ci incluent l'ensemble des pertes opérationnelles subies par la BRVM, y compris celles qui sont liées aux risques de crédit et de marché, dans la limite du seuil minimal de collecte approuvé par l'organe délibérant ;
- la traçabilité découle du fait que l'intégralité et l'intégrité des données sont assurées par leur réconciliation avec les écritures comptables appropriées et par leur validation par le responsable de la BRVM.

Chaque événement à l'origine des pertes doit être documenté et conservé dans une base de données, dans le respect des politiques définies por la BRVM en matière de conservation de données. La documentation doit comprendre, entre outres, la référence interne du dossier, la catégorie d'événements de pertes opérationnelles, le type de risque, la description de l'incident ainsi que les entités ou les lignes de métiers concernées, le cas échéant.

Article 34 Outils de gestion du risque opérationnel

La gestion du risque opérationnel doit couvrir l'ensemble des sept catégories d'événements de pertes opérationnelles citées à l'article 32. Pour identifier et évaluer le risque opérationnel, la BRVM peut recourir notamment aux outils de gestion ci-oprès :

- les autoévoluotions du risque opérationnel ;
- la cortographie des processus opérationnels ;
- les indicateurs de risque et de performonce en motière de surveillance du risque opérationnel et les indicateurs d'efficacité du dispositif de contrôle interne ;
- les analyses des événements de pertes opérationnelles tant à l'intérieur qu'à l'extérieur de la BRVM ;
- les onolyses de risques spécifiques ò choque produit, processus et système en place ;
- les analyses de scénorios.

Les outils mis en place doivent être utilisés de foçon uniforme dans toutes les unités afin de parvenir ò une évaluation complète de l'exposition au risque opérationnel.

Article 35 Contrôle et atténuation du risque opérationnel

La BRVM doit prendre des mesures préventives pour réduire les pertes opérotionnelles découlant d'une insuffisance liée notamment à :

- lo documentation, la tenue à jour et le respect des procédures ;
- lo sécurisation des actifs de lo BRVM et de leur utilisation ;
- lo mise ò niveau des compétences et la formotion des employés ;
- la vérification et le ropprochement réguliers des opérations et des comptes ;
- l'éloborotion, lo mise en place et l'octuolisotion d'un dispositif de sécurité physique et logique du système d'information et des infrastructures de télécommunicotion ;
- lo couverture adéquate des valeurs par des polices d'assurance.

Article 36 Gestion des risques liés aux nouveaux produits, processus, systèmes et activités

Le dispositif de gestion du risque opérationnel doit, entre autres :

- prendre en compte l'identification et l'évaluation des risques inhérents aux nouveaux produits, aux nouvelles activités, aux grandes opérations d'acquisition ainsi que ceux découlant de chongements de systèmes, de processus ou de modèle économique ;

- permettre d'identifier les plus significatifs d'entre eux et d'apprécier la vulnérabilité de la BRVM à ces risques ;
- prendre en compte à la fois les facteurs internes et externes qui pourraient empêcher la BRVM d'atteindre ses objectifs.

Les procédures et politiques mises en place, doivent permettre de comprendre et de gérer ces nouveaux risques. Ce processus doit prendre en compte notamment :

- les risques inhérents y relatifs ;
- les modifications du profil de risque, de l'appétence au risque qui en découlerait ;
- les contrôles nécessaires, les stratégies et processus d'atténuation des risques ainsi que le risque résiduel.

Article 37 Principes généraux en matière d'externalisation

Le recours à l'externalisation ne soustrait pas les organes de gouvernance de la BRVM de leurs obligations relatives à la conformité des contrats aux exigences légales et réglementaires applicables aux activités externalisées. En outre, il ne les exonère pas de leurs obligations vis-à-vis de toutes les parties prenantes, notamment les adhérents, les Commissaires aux Comptes et les Autorités de contrôle. Il ne modifie pas les conditions d'exercice de l'agrément.

Avant de s'engager dans un contrat d'externalisation, la BRVM doit en évaluer l'opportunité et procéder à une évaluation approfondie des risques y relatifs. Ce contrat doit être soumis à l'approbation préalable de l'organe délibérant qui doit notamment :

- examiner, au moins deux fois par an, la liste complète des contrats d'externalisation ;
- s'imprégner des rapports d'exécution desdits contrats qui lui sont transmis par l'organe exécutif.

La BRVM doit veiller à ce que les dispositions contractuelles permettent :

- la mise à la disposition des Commissaires aux Comptes et de l'AMF-UMOA, de toutes les informations nécessaires à l'exercice de leurs contrôles ;
- la tenue de la comptabilité ainsi que la production des états de reporting conformément aux dispositions en vigueur ;
- la préservation de la sécurité du système d'information et de la confidentialité des informations ;
- la protection du consommateur et de la vie privée de l'investisseur.

L'ensemble des données physiques et électroniques de la BRVM doivent être disponibles dans l'UMOA, nonobstant l'externalisation et toute disposition prise dans le cadre de leurs plans de secours et de continuité d'activités. A cet effet, doivent être conservés et accessibles en permanence dans l'UMOA :

- les serveurs informatiques stockant les données et hébergeant les applications ;
- l'ensemble des dossiers physiques relatifs au personnel, au patrimoine, aux opérations du marché et annexes ainsi qu'à toutes les autres transactions réalisées par la BRVM ;

- les archives et documents divers durant la période fixée par les dispositions légales et réglementaires.

En l'absence des serveurs primaires dans l'UMOA, des serveurs secondaires de secours doivent être disponibles dans l'Union avec une réplication de l'ensemble des données.

Tout projet de contrat d'externalisation doit être soumis à l'appréciation préalable de l'AMF-UMOA avant sa mise en œuvre. En outre, l'AMF-UMOA se réserve le droit d'ordonner la réalisation d'un audit externe auprès du prestataire.

Article 38 Contrat de prestations

L'externalisation d'une activité doit reposer sur des contrats et/ou des conventions de service solides, lesquels doivent notamment préciser sans équivoque :

- une description circonstanciée des activités externalisées, la nature et la portée des prestations attendues ainsi que les coûts supportés par la BRVM ;
- les devoirs et obligations respectifs du prestataire et de la BRVM ;
- le type et la fréquence des informations que la BRVM reçoit du prestataire ;
- les actifs de la BRVM que le prestataire peut utiliser, à savoir les données, le matériel, les logiciels ou la propriété intellectuelle ;
- les conditions de résiliation, y compris le préavis du prestataire et l'exigence de restitution des actifs de la BRVM dans les délais fixés ;
- les mesures à prendre par le prestataire pour garantir la continuité de l'activité importée en cas d'événements pouvant empêcher d'assurer les services attendus ;
- les indicateurs de performance qualitatifs et quantitatifs permettant à la BRVM d'évaluer, au moins une fois par an, la performance du prestataire.

Le contrat doit contenir les clauses nécessaires en matière de confidentialité, de secret professionnel, de propriété intellectuelle. Il doit être soumis à un avis juridique avant toute approbation par l'organe délibérant.

Article 39 Évaluation du prestataire

Préalablement à la conclusion de tout contrat d'externalisation, la BRVM est tenue de procéder à une évaluation approfondie ou due diligence de la capacité technique, financière et opérationnelle du prestataire.

Cette évaluation est mise à jour au moins une fois par an ainsi que lors du renouvellement et de la renégociation du contrat d'externalisation. Elle doit être documentée.

Article 40 Gestion des risques liés à l'externalisation

La BRVM est tenue :

- de se doter de politiques et procédures qui définissent les modalités d'externalisation et lui permettent d'identifier, de mesurer, d'atténuer et de contrôler adéquatement les risques liés à l'externalisation ;
- d'intégrer les activités externalisées dans son dispositif de contrôle interne ;
- de se doter de compétences internes lui permettant de suivre le pilotage opérotionnel du contrat d'externalisotion et l'appréciotion des prestations reçues ;
- de disposer d'un plan de secours et de continuité des activités externalisées visant à ossurer la continuité d'exploitation de la BRVM à la suite de la résiliation de contrat d'externalisation, ou de l'incapacité du prestataire à honorer ses engagements, ou d'une décision volontaire de lo BRVM de ropatrier les activités externolisées ;
- d'assurer un suivi adéquat des activités externalisées et veiller à ce que le prestataire procède au contrôle régulier de son plan de continuité des activités en cas de défaillance et qu'il dispose des compétences et moyens requis pour les corriger ;
- de produire, dans le ropport d'audit interne, un résumé du résultat des contrôles effectués liés oux activités externalisées.

TITRE 4. EXERCICE DE L'AUDIT INTERNE

Article 41 Mise en place de la fonction d'audit interne

La BRVM doit se doter d'une fonction d'audit interne qui dispose du statut, des compétences, des ressources et de l'autarité suffisante pour exécuter ses missions avec efficacité et objectivité. La mission, les pouvoirs et les responsobilités de l'audit interne sont décrits dans une charte d'audit interne qui fait partie intégrante des procédures internes de la BRVM.

Elle adopte une approche systématique et disciplinée des actions de contrôle sur la base d'un plan de contrôle établi à partir d'une cartographie recensant les risques qu'il encourt.

Article 42 Responsabilités de la fonction d'audit interne

La fonction d'audit interne assiste les membres des organes délibérant et exécutif respectivement dans leur mission de surveillance et de gestion. Pour ce faire, elle doit notamment :

- disposer d'une charte d'audit interne, de procédures de contrôle et d'un code de déontologie ;
- avoir un mandat clair et indépendant des activités auditées, y compris les activités des autres fonctions de contrôle ;

- se doter d'outils performants lui permettant d'effectuer une surveillance bosée sur les risques de l'ensemble des activités de la BRVM ainsi qu'un suivi de la mise en œuvre des recommandations, classées par degré de criticité ;
- bénéficier d'un accès complet à toutes données physiques et électroniques nécessaires à l'accomplissement de sa mission ;
- effectuer une évaluation périodique de l'efficacité de toutes les autres fonctions de contrôle, notamment les fonctions de gestion des risques et de conformité ;
- réaliser des examens périodiques des responsabilités et fonctions des personnes détenant les postes clés, afin de s'assurer que ces responsables ne sont pas en mesure de dissimuler des agissements inappropriés.

Article 43 Compétences et conscience professionnelle

Les auditeurs internes doivent posséder les connaissonces, les savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités.

Le responsable de l'audit interne est tenu de solliciter l'avis et l'assistance de ressources qualifiées et indépendantes si les auditeurs internes ne possèdent pas les connaissances et le savoir-faire nécessaires pour s'acquitter d'une portie de leur mission.

Les auditeurs internes doivent apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent. La conscience professionnelle n'implique pas l'infaillibilité.

La fonction d'audit interne doit être dotée de compétences en matière d'infrastructure et de sécurité des systèmes d'information pour mieux appréhender les contrôles requis en la matière.

Article 44 Désignation du Responsable de la fonction d'audit interne

Sur proposition de l'organe exécutif, l'organe délibérant désigne un Responsable de lo fonction d'audit qui doit disposer d'une indépendance fonctionnelle et jouir de prérogatives étendues quant au champ de ses interventions et ò la communication de ses travaux auxdits orgones.

En vue de consacrer cette indépendance, le Responsable de la fonction d'audit doit, au moins, être fonctionnellement rottaché à l'organe délibérant, auquel il rend compte.

Article 45 Révocation du Responsable de la fonction d'audit interne

La BRVM est tenue, dans un délai de quinze (15) jours après lo révocation, d'en informer l'AMF-UMOA en indiquant les motifs.

Article 46 Responsabilité du Responsable de la fonction d'audit interne

Le Responsable de la fonction d'audit interne est chargé de gérer la fonction d'Audit Interne. Il doit être rattaché à un niveau de l'organisation qui permette à la fonction d'audit interne d'exercer ses responsabilités.

Il a la responsabilité de dresser le plan de contrôles sur la base de la cartographie des risques, s'impliquer dans sa réalisation, veiller au respect du cycle des contrôles et s'assurer de la qualité des travaux de la fonction. Il vérifie que les anomalies et déficiences de contrôle interne identifiées sont documentées dans un rapport écrit.

Il élabore la charte d'audit interne, veille à sa révision régulière et la diffuse à toutes les parties prenantes après son approbation par l'organe délibérant par l'intermédiaire du comité d'audit.

Le responsable de l'audit interne doit, au moins chaque année, confirmer au Conseil, l'indépendance de l'audit interne dans l'organisation.

Le responsable de l'audit interne doit communiquer et dialoguer directement avec le Conseil d'Administration.

Le Responsable de la fonction d'audit interne peut, si ceci n'emporte pas conflit d'intérêts :

- être impliqué en amont des projets afin d'identifier et d'évaluer de façon proactive les enjeux et risques potentiels de non-conformité ;
- aider à sensibiliser et à former le personnel et fournir des orientations aux membres du personnel quant à l'application appropriée des lois et règlements.

Article 47 Charte d'audit interne

Le responsable de l'audit interne doit élaborer et réviser, au moins tous les trois ans, la charte d'audit interne et la soumettre à l'approbation de l'organe délibérant par l'intermédiaire du Comité d'audit avant sa mise en application.

La charte d'audit interne précise la position de la fonction d'audit interne ou sein de l'organisation de la BRVM, sa mission, ses pouvoirs, ses obligations et son périmètre d'intervention. Elle définit les caractéristiques de la fonction et son mode de fonctiannement et de communication avec les personnes n'appartenant pas à la fonction.

Article 48 Plan d'audit

Le responsable de la fonction d'audit doit établir un plan d'audit annuel ou pluriannuel basé sur les risques. Il doit également communiquer à l'organe délibérant, pour examen et approbation, son plan d'audit, ses besoins ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Ce plan, établi à partir d'une cartographie des risques de la BRVM, doit notamment :

- s'appuyer sur une évaluation rigoureuse des risques liés à l'ensemble de ses activités et entités ;

- intégrer l'évaluation des moyens humains, matériels et financiers nécessaires à la réalisation des actions prévues ;
- être réaliste et flexible afin de permettre le respect du cycle d'audit et la prise en chorge des activités imprévues ;
- foire l'objet d'une mise à jour en vue de répondre aux changements de son environnement interne et externe.

La fonction d'audit interne peul initier des missions non prévues dans son planning de contrôle, lorsque des circonstances porticulières le nécessitent, ou sur demande de l'organe délibéront, des Comités spécialisés, du Directeur Général.

Article 49 Piste d'audit

La fonction d'audit interne doit garantir l'existence de la piste d'oudit telle que définie au o) de l'orticle 1 et veiller au respect des dispositions du référentiel comptable. Les éléments constitutifs de la piste d'audit doivent être conservés pendant au moins dix (10) ans.

Article 50 Maintien et sécurité des données informatisées

La fonction d'audit interne doit comprendre des procédures internes de sauvegarde et de reprise des systèmes qui utilisent des données informatisées, des politiques de développement et de mointenance appropriées de ces systèmes ainsi que des contrôles de sécurité d'accès physiques et logiques.

Article 51 Examen du rapport d'audit par le Comité d'Audit

Les rapports d'audit interne sont portés à la connaissance du Comité d'Audit afin de foire l'objet d'un examen et d'un suivi odéquat.

TITRE 5. REPORTING A L'AMF-UMOA

Article 52 Reporting semestriel et occasionnel à l'AMF-UMOA

La BRVM doit tronsmettre à l'AMF-UMOA, le 15 ooût au plus tard un rapport semestriel consolidé présentant par rubrique les travaux réalisés por les fonctions de conformité, de gestion des risques et de l'oudit interne.

En outre, lo BRVM informe, sans délai, l'AMF-UMOA de toutes insuffisances relevées par les fonctions de contrôle et ayant un impact significatif sur la réputation de la BRVM et/ou sa solidité financière.

Article 53 Reporting annuel

La BRVM doit transmettre à l'AMF-UMOA, le 15 mai au plus tard, pour le compte de l'exercice précédent, un rapport annuel consolidé présentant par rubrique les travaux réalisés par les fonctions de contrôle interne.

Ce rapport devra préalablement être validé par l'organe délibérant de la BRVM.

Article 54 Contenu des rapports d'Audit interne

Le format de présentation des rapports d'audit interne destinés à l'AMF-UMOA est précisé par une Circulaire de l'AMF-UMOA.

TITRE 6. DISPOSITIONS TRANSITOIRES ET FINALES

Article 55 Dispositions transitoires

La Bourse Régionale des Valeurs Mobilières dispose d'un délai maximum de deux (02) ans à compter de sa date de signature pour se mettre en conformité avec les dispositions de la présente Instruction.

Article 56 Sanctions

Le non-respect des règles prévues par la présente Instruction est sanctionné par l'AMF-UMOA, conformément aux dispositions réglementaires en vigueur sur le Marché Financier Régional de l'UMOA.

Article 57 Publication et date d'entrée en vigueur

La présente Instruction, qui sera publiée partout où besoin sera, abroge toutes dispositions antérieures contraires et entre en vigueur à compter de sa date de signature.

La BRVM est tenue d'en transmettre copie à tous les membres de l'organe délibérant et aux Commissaires aux comptes.

Fait à Abidjan, le 29 DEC. 2023

Pour l'Autorité des Marchés Financiers de l'UMOA

Le Président

Le Président
01 BPM 1878
ABIDJAN 01

Badanam PATOKI

AMF-UMOA

AUTORITÉ DES MARCHÉS FINANCIERS DE L'UNION MONÉTAIRE OUEST AFRICAINE

Le Secrétaire Général

INSTRUCTION N° 78 /AMF-UMOA/2023
RELATIVE AU DISPOSITIF DE CONTRÔLE INTERNE ET DE GESTION DES RISQUES DU DÉPOSITAIRE CENTRAL / BANQUE DE RÈGLEMENT (DC/BR)

L'Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine,

Vu le Traité révisé de l'Union Monétaire Ouest Africaine (UMOA) du 12 juillet 2019, entré en vigueur le 1er octobre 2022, modifiant la dénomination du Conseil Régional de l'Epargne Publique et des Marchés Financiers (CREPMF) en Autorité des Marchés Financiers de l'UMOA (AMF-UMOA) ;

Vu la Convention du 3 juillet 1996 portant création du Conseil Régional de l'Épargne Publique et des Marchés Financiers, notamment son Annexe portant composition, organisation, fonctionnement et attributions du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu le Règlement Général n°001/97 du 28 novembre 1997 relatif à l'organisation, au fonctionnement et au contrôle du marché financier régional notamment en ses articles 10 et 16 ;

Vu l'Instruction n°3/97 du 29 novembre 1997 relative à l'habilitation du Dépositaire Central/Banque de Règlement ;

Vu la Décision n° 004 du 29/04/2021/CM/UMOA portant nomination du Président du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu les délibérations de l'AMF-UMOA en sa 50ème session extraordinaire du 24 septembre 2021 tenue par visioconférence ;

Vu les délibérations de l'AMF-UMOA en sa 98ème session ordinaire du 23 décembre 2023, tenue à Cotonou en République du Bénin ;

ARRÊTE :

TITRE 1. DISPOSITIONS GENERALES

Article 1 Définitions

Aux fins de la présente Instruction, on entend par :

a) Audit interne : Activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. L'audit interne doit évaluer les processus de gouvernance de l'organisation, de management des risques et de contrôle, et contribuer à leur amélioration sur la base d'une approche systématique, méthodique et fondée sur une approche par les risques.

b) Appétence pour le risque : Le niveau et le type de risque que le DC/BR est disposé à assumer dans ses expositions et ses activités pour réaliser ses objectifs stratégiques et ses obligations.

c) Chartes d'audit interne et de conformité : Documents qui définissent le positionnement des fonctions d'audit interne et de conformité au sein de la structure agréée et précisent l'organisation, les pouvoirs, les responsabilités et les modalités de fonctionnement desdites fonctions.

d) Cartographie des risques : Représentation synthétique et visuelle des risques du DC/BR. Elle constitue ainsi un outil de mise en évidence des risques à couvrir en priorité.

La cartographie des risques est établie sur la base d'un système d'identification et d'évaluation rigoureuse des risques inhérents au DC/BR à partir des facteurs internes (métiers et activités, modifications organisationnelles, etc.) et externes (conditions économiques, progrès technologiques, changements législatifs et réglementaires, etc.).

e) Comité d'audit : Comité institué par l'organe délibérant pour l'assister dans l'exercice de ses missions, et en particulier vérifier la fiabilité et la transparence des informations financières, apprécier la pertinence des méthodes comptables ainsi que la qualité du dispositif de contrôle interne et du dispositif de gestion des risques, évaluer la stratégie d'audit et proposer le cas échéant, des pistes d'amélioration.

f) Contrôle Interne : Mesures mises en place par les organes exécutifs et qui ont pour but d'assurer que :

- les objectifs posés par le DC/BR sont réalistes et atteints ;
- les ressources sont utilisées de façon économique et efficiente, les risques sont contrôlés adéquatement ;
- le patrimoine est protégé ;
- l'information financière et l'information de gestion sont complètes et fiables ;
- les lois et réglementations ainsi que les politiques, les plans, les règles et les procédures internes sont respectés.

g) Cycle des contrôles : Intervalle au cours duquel toutes les activités et les entités du DC/BR auront été vérifiées au moins une fois par la fonction d'audit interne.

h) Dépositaire Central / Banque de Règlement ou DC/BR : La société autorisée, par agrément de l'AMF-UMOA à exercer, sur l'ensemble du territoire des États de l'Union, les activités ci-après : la conservation et la circulation scripturale des titres, la gestion du cycle des règlements-livraisons, le règlement des soldes des compensations relatives aux transactions boursières.

i) Dispositif de Contrôle Interne (DCI) : Ensemble des règles, méthodes et mesures de contrôle régissant la structure organisationnelle et opérationnelle du DC/BR. Il comprend les processus de reporting et les fonctions de contrôle.

j) Fonctions de contrôle : Les fonctions indépendantes de la gestion opérationnelle, dont le rôle est de fournir des évaluations objectives quant à la qualité et à l'efficacité du DCI, des dispositifs de gouvernance, de gestion des risques de non-conformité, en vue de faciliter la maîtrise des activités et des risques encourus. Elles comprennent notamment la fonction d'audit interne, la fonction de gestion des risques et la fonction de conformité.

k) Gestion des risques : L'ensemble des stratégies, politiques et procédures mises en place afin que tout risque significatif et toute concentration de risques associée soient détectés, mesurés, limités, maîtrisés et atténués, et qu'il en soit rendu compte, de façon précoce et exhaustive.

l) Normes en vigueur : L'ensemble des règles régissant l'exercice des activités du DC/BR, notamment :

- les dispositions légales et réglementaires ;
- les codes de conduite et de déontologie internes ;
- les principes pour les Infrastructures de Marché édictés par le Comité de Bâle et l'Organisation Internationale des Commissions de Valeurs (OICV).

m) Organe délibérant : Le Conseil d'Administration dans les sociétés anonymes ou l'organe collégial dans les sociétés constituées sous une autre forme. Il est investi de tous les pouvoirs pour agir en toutes circonstances au nom du DC/BR, dans la limite de l'objet social et des compétences réservées à l'Assemblée Générale.

n) Organe exécutif : Tout comité ou structure qui concourt à la gestion courante du DC/BR et assure l'application effective de l'orientation de l'activité définie par l'organe délibérant.

o) Piste d'audit : Ensemble de procédures internes permanentes permettant d'assurer la traçabilité des opérations, de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter, par un cheminement ininterrompu, au document de synthèse et réciproquement et d'expliquer l'évolution des soldes d'un arrêté comptable à l'autre, grâce à la conservation des mouvements ayant affecté les postes comptables.

p) Risque de non-conformité : le risque de sanction judicioire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, que le DC/BR peut subir en raison de l'inobservation des normes en vigueur régissant l'exercice de ses activités.

q) Risque opérationnel : le risque de pertes résultant de carences ou de défaillances attribuables à des processus, des personnes, des systèmes internes ou à des événements externes. Cette notion inclut le risque juridique mais exclut les risques stratégiques et de réputation.

r) Risque stratégique : le risque que les stratégies d'affaires du DC/BR soient inefficaces, ne soient pas bien mises en œuvre ou adaptées aux changements touchant le contexte commercial.

Article 2 Objet

La présente Instruction fixe les règles en matière de dispositif de contrôle interne applicables au DC/BR dant l'objectif est de :

- vérifier que les opérations réalisées, l'organisation et les procédures internes sont conformes aux dispositions législatives et règlementaires en vigueur, aux normes et usages professionnels et déontologiques ainsi qu'aux orientations des organes délibérant et exécutif ;
- s'assurer que les orientations, les instructions et les limites fixées par l'organe délibérant en matière de risques sont strictement respectées ;
- veiller à la fiabilité de l'information comptable et financière, en particulier aux conditions de collecte, d'évoluation, d'enregistrement, de conservation et de disponibilité de cette information.

Elle fixe également les règles en matière de gestion des risques applicables au DC/BR, telle que définie à l'article 1 de ladite Instruction.

Article 3 Périmètre de contrôle

La gouvernance d'entreprise du DC/BR intègre un DCI sur lequel doit reposer la gestion saine et prudente de l'entité. Ce dispositif comporte :

- la surveillance de la fiabilité et l'intégrité des informations financières et opérationnelles et les moyens utilisés pour identifier, évaluer, classer et rapporter ces informations ;
- la vérification de la conformité des opérations réalisées et de l'organisation avec les dispositions législatives, réglementaires et prudentielles en vigueur, les normes et usages professionnels et déontologiques, les orientations et décisions des organes délibérants et exécutifs, notamment en matière de risques, de pouvoirs et de signature ainsi que les procédures internes ;
- le suivi et l'évaluation de l'efficacité du dispositif de gestion des risques de l'entité.

L'organisation du contrôle interne doit s'appuyer sur l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication et le pilotage.

Article 4 Environnement de contrôle

L'organe délibérant doit veiller à la mise en place d'un environnement de contrôle adéquat, lequel constitue le cadre et la structure nécessaires à la réalisation des objectifs du dispositif de contrôle interne.

Un environnement de contrôle adéquat implique :

- l'engagement des organes de gouvernance en faveur de la promotion de l'intégrité et des valeurs éthiques au sein du DC/BR ;
- l'instauration d'une culture qui met en évidence, à tous les niveaux de l'organisation, l'importance du contrôle interne ;
- une implication effective de l'organe délibéront dans le suivi des composantes du dispositif de contrôle interne ;
- une définition claire et cohérente des missions, fonctions et responsabilités, y compris des délégations de pouvoirs explicites en matière de limites ;
- l'existence d'un personnel compétent et d'un dispositif de gestion des ressources humaines permettant au DC/BR d'attirer, de développer et de maintenir des compétences en lien avec ses objectifs ;
- une forte adhésion du personnel aux exigences de contrôle qui lui sont assignées ainsi qu'au devoir de rendre compte de ses responsabilités en la matière ;
- les supervisions par chaque responsable hiérarchique de l'application effective des procédures de contrôle interne par ses collaborateurs ;
- la définition de critères qualitatifs par les organes délibérants et exécutifs du DC/BR afin de mesurer et d'évaluer l'efficacité du Dispositif de Contrôle Interne.

Article 5 Les lignes de défense du DCI

Le DCI est organisé de façon à fournir des appréciations objectives de la situation du DC/BR, la maitrise des risques et la conformité de son fonctionnement aux règles et procédures en vigueur. Il comprend :

- un contrôle permanent de premier niveau qui correspond, à l'ensemble des contrôles réalisés par les unités opérationnelles et leur hiérarchie dans le cadre du traitement des opérations quotidiennes, ce qui constitue la première ligne de défense ;
- un contrôle permanent de deuxième niveau qui correspond, aux contrôles exécutés par les fonctions supports indépendantes des unités opérationnelles, qui forment la deuxième ligne de défense représentée par les fonctions de conformité et de gestion des risques ;
- un contrôle périodique qui correspond aux contrôles a posteriori réalisés dans le cadre d'un plan d'audit élaboré à partir d'une cartographie des risques, ce qui constitue la dernière ligne de défense représentée par la fonction d'audit interne. Le plan d'audit élaboré par l'approche par les risques doit être réaliste et flexible afin de permettre le

respect du cycle de contrôle et la prise en charge des activités imprévues. Il doit régulièrement faire l'objet de mise à jour en vue de répondre aux changements de l'environnement interne et externe du DC/BR.

Article 6 Responsabilité de l'organe délibérant

L'organe délibérant est responsable en dernier ressort de l'existence d'un dispositif de contrôle interne au sein du DC/BR ainsi que de la bonne application du DCI à l'ensemble de l'organisation de la structure agréée. Il est tenu de :

- définir et valider, selon une périodicité adaptée, le niveau de risque acceptable auquel le DC/BR est exposé, notamment par la fixation de limites acceptables de risques de contrepartie, de liquidité et de marché ainsi que par la mise en place de dispositifs appropriés pour encadrer les risques opérationnels et de non-conformité ;
- veiller à la mise en place et à la mise à jour d'une organisation, des politiques et procédures écrites de contrôle interne, pour une saine et prudente gestion des activités du DC/BR ;
- veiller à la séparation des tâches incompatibles, notamment les fonctions de décision, de détention des valeurs, d'enregistrement et de contrôle ;
- s'assurer que les fonctions de contrôle disposent de moyens appropriés pour exécuter ses missions en toute indépendance.

Article 7 Comité d'audit

Les prérogatives minimales du Comité d'audit consistent à :

- examiner l'efficacité du DCI mis en place pour identifier, évaluer, gérer et contrôler les risques financiers et non financiers ;
- évaluer la politique d'audit interne et le cycle des contrôles, y compris la politique d'escalade lors de la matérialisation de risques importants ;
- participer à la sélection des Commissaires aux Comptes et à l'examen des conclusions de leurs travaux, conformément aux dispositions légales et réglementaires ;
- analyser la conformité du respect des principes déontologiques et comptables appliqués avec les normes et usages professionnels en vigueur ;
- examiner de manière approfondie les états de synthèse annuels avant leur présentation aux organes délibérants ;
- donner aux organes de gouvernance une assurance raisonnable quant à la qualité et à l'efficacité du dispositif de contrôle interne, des dispositifs de gouvernance et de gestion des risques en vue de faciliter leur maîtrise des activités du DC/BR et des risques encourus.

Il fait également des propositions auxdits organes pour renforcer l'efficacité de ces systèmes et dispositifs.

Article 8 Responsabilités de l'organe exécutif

L'organe exécutif est tenu de mettre en place un DCI conforme aux bonnes pratiques et de surveiller son adéquation et son efficacité. Le DCI doit être adapté au profil de risque du DC/BR.

L'organe exécutif veille à ce que les politiques et procédures soient développées et appliquées efficacement par les personnes qui disposent de la compétence en la matière et que toutes les personnes concernées comprennent et assument leurs responsabilités à cet égard. Il définit les critères d'escalade en réponse à la matérialisation des risques et s'assure de la mise en œuvre des mesures appropriées.

Il doit notamment :

- s'assurer, du bon fonctionnement des dispositifs de contrôle interne et de gestion des risques et prendre des mesures nécessaires pour remédier, en temps opportun, à toute corence ou insuffisance relevée ;
- informer les fonctions de contrôle, à temps, de tous nouveaux développements, initiotives, projets, produits et changements opérationnels ainsi que des risques y relatifs ;
- s'assurer que des mesures appropriées sont prises dans les délais fixés pour mettre en œuvre toutes les octions correctrices découlont des recommandations de l'oudit interne, des Commissaires aux Comptes ou de l'AMF-UMOA ;
- promouvoir l'indépendance des fonctions de contrôle et mettre à leur disposition les ressources nécessaires pour mener à bien leurs missions ;
- rendre compte régulièrement à l'organe délibéront de l'efficacité du dispositif de contrôle interne.

Article 9 Obligations du personnel

Chaque membre du personnel du DC/BR doit :

- effectuer avec diligence l'ensemble des activités de contrôle qui lui sont attribuées ;
- disposer de toutes les informations nécessaires pour notamment établir, faire fonctionner et surveiller le dispositif de contrôle interne.

TITRE 2. GESTION DE LA CONFORMITE

Article 10 Caractéristiques de la politique de conformité

Le DC/BR doit se doter d'une politique de conformité qui, notamment :

- assure le respect des principes fondamentaux fixés par l'organe délibérant ;
- instaure la fonction conformité au sein du DC/BR ;
- prescrit l'élaboration d'une charte de conformité ;
- précise les aspects fondamentaux du risque de non-conformité ;
- établit les responsabilités des organes de gouvernance dans la mise en œuvre du cadre de gestion du risque de non-conformité ;
- institue un programme de formation continue à l'intention des employés et de tous ceux qui sont chargés de la mise en œuvre et de la surveillance de la politique de conformité.

Article 11 Charte de conformité

La charte de conformité doit notamment :

- exposer les objectifs de la fonction conformité, établir son indépendance et définir ses responsabilités ainsi que ses compétences ;
- décrire clairement les relations de la fonction conformité avec les autres fonctions de contrôle et les services du DC/BR qui exécutent des tâches liées à ses responsabilités ;
- accorder à la fonction conformité le droit de communiquer avec tout membre du personnel et d'accéder à tout dossier physique ou électronique nécessaire à l'exercice de ses responsabilités ;
- conférer à la fonction conformité le pouvoir de diligenter des investigations ;
- formaliser les tâches et les obligations de la fonction conformité qui peuvent être déléguées à d'autres services et fonctions du DC/BR ou externalisées auprès de prestataires externes ;
- définir les conditions dans lesquelles la fonction conformité peut recourir, en cas de besoin, à des experts externes.

La charte de conformité doit refléter les évolutions enregistrées dans les normes en vigueur. Le DC/BR est tenu de la mettre à jour dans les meilleurs délais pour tenir compte de ces changements.

Tout projet d'externalisation de la fonction conformité doit être approuvé par l'organe délibérant et soumis à l'autorisation de l'AMF-UMOA avant sa mise en œuvre.

Article 12 Indépendance

La fonction conformité doit être indépendante des unités qu'elle contrôle. Pour assurer l'indépendance de cette fonction, l'organe exécutif doit veiller à mettre en place un dispositif organisationnel exempt de conflits de tâches et de fonctions. En outre, les ressources y dédiées ne doivent pas être en situation de conflits d'intérêts.

La fonction conformité doit avoir accès aux organes délibérant et exécutif, afin de signaler toute irrégularité constatée ou manquement éventuel.

Article 13 Ressources

La fonction conformité doit disposer des ressources humaines nécessaires à la réalisation de ses missions. Elle doit être adaptée à la taille du DC/BR, la nature et la complexité de ses activités ainsi qu'à son profil de risque.

Le DC/BR doit désigner un responsable de la fonction en charge de la coordination à l'échelle de l'organisation de la gestion du risque de non-conformité ainsi que de la supervision des activités de la fonction. Le responsable de la fonction conformité doit être doté d'une expérience avérée en matière d'audit et de conformité.

Article 14 Compétence

Les ressources humaines affectées à la fonction conformité doivent posséder un niveau élevé de connaissance des activités du DC/BR et des normes qui lui sont applicables.

Le DC/BR doit prendre les dispositions pour que ces ressources humaines maintiennent à jour leurs connaissances desdites normes.

Article 15 Responsabilités générales

La fonction conformité est chargée d'aider l'organe exécutif à identifier et à gérer avec diligence tout risque d'inobservation, par le DC/BR, des obligations que lui imposent les normes en vigueur régissant l'exercice de ses activités.

Article 16 Responsabilités spécifiques

Les responsabilités spécifiques de la fonction conformité consistent notamment à :

- recenser et à communiquer à l'ensemble du personnel concerné, les normes en vigueur régissant l'exercice des activités du DC/BR ;
- identifier, évaluer et gérer, de manière proactive, les risques de non-conformité, y compris lors du développement de nouveaux produits ou marchés, activités ou relations émetteurs et adhérents aux services du DC/BR.

En outre, si le DC/BR dispose d'un Comité de nouveaux produits ou marchés, la fonction conformité doit y être représentée.

La fonction conformité doit également :

- centraliser et analyser tous les manquements aux normes en vigueur et à la politique de conformité ;
- recommander des mesures correctrices pour remédier aux manquements et insuffisances relevées ;
- effectuer le suivi de la mise en œuvre de toutes ses recommandations ;
- évaluer l'adéquation de la politique de conformité, au regard des évolutions enregistrées dans les activités du DC/BR, les normes en vigueur et sur la base des insuffisances relevées. Elle doit, le cas échéant, formuler des propositions d'amendements ;
- veiller à une mise en œuvre diligente de la politique de conformité. La fonction conformité doit s'assurer que les règles édictées dans la politique de conformité sont déclinées dans des procédures, des manuels de conformité et des contrôles internes pour les domoines relevont directement de la fonction conformité. Les domaines d'intervention relevant directement de lo fonction conformité concernent notamment lo lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi que la protection des intérêts des émetteurs et des investisseurs.

En outre, d'autres prérogatives campatibles avec ses missions peuvent lui être confiées, notomment assurer la liaison ovec les organismes externes de réglementation et de normalisation.

La fonction conformité doit être impliquée et consultée préalablement à la mise en place de procédures de contrôle interne.

Elle doit s'assurer en permanence que la politique de conformité du DC/BR est respectée à tous les niveaux de l'orgonisation, notamment :

- Sensibiliser et former le personnel : La fonction conformité doit initier des actions visont à sensibiliser et former le personnel sur l'importance de l'appropriation des normes en vigueur et du respect de la politique conformité. Elle établit et met en œuvre, à cet effet, un programme de formotion destiné au personnel.
- Documenter ses travaux : La fonction conformité est tenue de documenter l'ensemble de ses travoux en vue de garantir une traçabilité de ses interventions et de ses conclusions.

Article 17 Détection d'anomalies de conformité

Toutes anomalies et déficiences significatives de conformité qui constitueroient un manquement aux dispositions réglementoires de l'AMF-UMOA doivent faire l'objet d'une documentation et d'un rapport circonstancié spécifique adressé ò l'organe délibérant du DC/BR et à l'AMF-UMOA.

Les rapports de la fonction conformité contenant des constats mettant en cause les dirigeants ne peuvent être modifiés por ces derniers.

Toutefois, les personnes mises en couse peuvent formuler des observations sur les constats dressés. Les observations formulées doivent être jointes au rapport de contrôle.

Le non-respect de ces dispositions expose les contrevenonts aux sanctions prévues par lo réglementation, sans préjudice des sanctions pénoles.

Article 18 Contrôle de la fonction conformité par la fonction d'audit interne

Les activités de la fonction conformité doivent être soumises à un examen périodique par lo fonction d'audit interne. Pour éviter tout conflit de responsabilité et de fonction, la fonction conformité ne peut faire partie de la fonction d'oudit interne.

Article 19 Reporting du Responsable de la Conformité aux organes de gouvernance

Le responsable de la fonction conformité doit communiquer oux organes de gouvernance, dans les meilleurs délais, les incidents significatifs de non-conformité et les manquements à la politique de conformité. Il rend compte à l'organe délibérant ou à un comité spécialisé auquel il est rattaché, au moins une fois par an, de l'exécution de sa mission. Il produit un rapport semestriel sur l'évaluation du risque de non-conformité. Ce rapport doit être adapté au profil de risque et aux activités du DC/BR et couvrir notamment :

- les réalisations de la fonction conformité, au regard des objectifs qui lui ont été fixés ;
- les moyens humains et matériels mis en œuvre pour atteindre ses objectifs ;
- la cartographie des incidents de non-conformité à l'échelle du DC/BR, en mettant en exergue les principales insuffisances relevées, les mesures correctrices engagées et le suivi effectué.

TITRE 3. GESTION DES RISQUES

Article 20 Principe de proportionnalité

Le DC/BR doit se doter d'un dispositif de gestion des risques lui permettant de gérer intégralement les risques juridiques, de contrepartie, de liquidité et opérationnel, ainsi que tout autre risque.

Article 21 Stratégies, politiques et procédures

Le dispositif de gestion des risques doit être basé sur des stratégies, politiques et procédures bien documentées qui permettent d'identifier, de mesurer, d'évaluer, de suivre, de déclarer et de contrôler ou d'atténuer l'ensemble des risques significatifs du DC/BR.

Les stratégies, politiques et procédures doivent être dynamiques, de manière à refléter l'évolution du degré d'appétence au risque du DC/BR, son profil de risque ainsi que les conditions de marché et l'environnement macroéconomique.

Le DC/BR doit veiller à la mise en œuvre de stratégies, politiques et procédures permettant d'avoir une vision globale, à l'échelle de l'organisation, de ses expositions sur chaque type de risque.

Article 22 Cartographie des risques

Le dispositif de gestion des risques doit comporter une cartographie des risques validée par l'organe délibérant, qui recense, évalue et hiérarchise l'ensemble des risques du DC/BR. Le DC/BR est tenu de se doter de cet outil de pilotage aux fins d'assurer une bonne gestion et un suivi adéquat des risques. La mise à jour de la cartographie doit être dynamique avec une revue globale au moins une fois par an.

Article 23 Culture du risque

Le DC/BR doit encourager le développement de la culture du risque à tous les niveaux de son organisation à travers notamment la formation et les actions de sensibilisation au profit de son personnel.

Article 24 Appétence au risque et gestion des limites

Le DC/BR doit mettre en place un dispositif d'appétence au risque approuvé, supervisé et révisé annuellement par le Conseil d'Administration et mis en œuvre par l'organe exécutif. Le DC/BR est également tenue de :

- fixer des limites globales et des limites opérationnelles au niveau de ses différentes entités. Ces limites doivent être établies de manière cohérente, conformément au degré d'appétence au risque du DC/BR, à son profil de risque et à son assise financière ;
- s'assurer d'une bonne appropriation de ces limites par le personnel concerné et d'une communication interne régulière ;
- se doter d'un dispositif d'identification et de gestion des dépassements de limites, comprenant une procédure de communication des dépassements au niveau hiérarchique approprié, de régularisation, de suivi de la régularisation et de sanction en cas de dépassement persistant ;
- définir clairement la procédure à suivre en vue de soumettre, de manière diligente, à l'examen et à l'autorisation des organes habilités, les cas d'exceptions aux politiques, procédures et limites établies.

Article 25 Systèmes d'information

Le DC/BR doit mettre en place des systèmes d'information et de contrôle des risques qui lui permettent d'obtenir en temps requis les informations nécessaires pour la mise en œuvre des politiques et procédures de gestion des risques.

À cet effet, le DC/BR doit se doter d'un dispositif de gouvernance des données sur les risques, d'une architecture de données relatives aux risques et d'une infrastructure informatique.

Les systèmes d'information mis en place par le DC/BR devraient, en particulier :

- permettre, aussi bien en situation normale qu'en période de crise, de mesurer et d'agréger précisément et en temps requis les expositions aux risques du DC/BR, de gérer les expositions individuelles aux risques, ainsi que leurs interdépendances, et d'évaluer l'impact de divers chocs économiques et financiers qui pourraient l'affecter ;
- suivre ses expositions aux risques identifiés ;
- s'adapter pour mesurer et évaluer la taille, la composition et la qualité de l'exposition au risque à l'échelle du DC/BR et pour l'ensemble des types de risques, des produits et des contreparties ;
- assurer la disponibilité, la qualité, la fiabilité et l'intégrité des données ;
- garantir la transmission en temps opportun, aux organes de gouvernance, de toutes informations pertinentes et utiles à leur prise de décision.

Article 26 Simulation de crise

Le DC/BR doit établir des programmes de simulations de crise, aux fins de la gestion des risques, en vue d'évaluer l'impact potentiel de scénarios adverses sévères mais plausibles sur sa solidité financière.

Ces programmes doivent inclure tous les risques importants auxquels le DC/BR est exposé. Ils doivent, en outre, prévoir des mesures correctives lorsque les résultats des simulations de crise décèlent des fragilités potentielles qui pourraient avoir une incidence négative sur la solidité financière du DC/BR.

Article 27 Rôles et obligations des organes de gouvernance

Les organes de gouvernance doivent notamment :

- veiller à ce que le DC/BR soit doté d'un dispositif de gestion des risques conforme aux dispositions de la présente Instruction ;
- mettre en place une fonction gestion des risques couvrant tous les risques significatifs, à l'échelle du DC/BR et disposant d'attributions distinctes de celles des unités opérationnelles ;
- préserver l'existence d'une fonction gestion des risques indépendante et dotée des ressources nécessaires ainsi que d'une autorité suffisante pour mener à bien ses missions ;
- exercer pleinement les responsabilités qui leur sont dévolues en matière de risque, conformément aux dispositions énoncées dans l'Instruction relative à la gouvernance du Dépositaire Central / Banque de Règlement.

Article 28 Rôles et obligations de la fonction gestion des risques

La fonction gestion des risques doit notamment :

- appliquer la stratégie de risque approuvée par l'organe délibérant et veiller à l'élaboration de toutes les politiques et procédures afférentes à la gestion des risques ;
- contribuer à la mise en place effective, au sein du DC/BR, d'un dispositif de gestion intégrée des risques qui soit soutenu par une gouvernance fiable impliquant les organes de gouvernance ;
- identifier, évaluer, suivre et maîtriser, en temps opportun, tous les risques significatifs ;
- améliorer les systèmes, les politiques, les processus et les rapports relatifs à la gestion des risques ;
- élaborer et mettre en œuvre, sous réserve de l'exomen et de l'approbotion par l'organe délibérant, le dispositif de gestion des risques, qui comprend la culture du risque à l'échelle du DC/BR, l'appétence pour le risque ainsi que les limites ;
- mettre en ploce un système d'alerte précoce visant à détecter les cas d'infraction à l'appétence au risque et aux limites fixées par l'orgone délibérant ;
- orienter, voire récuser, toute décision qui engendre une prise de risque importante pour le DC/BR, rendre compte aux orgones de gouvernance de toutes ces questions et propaser des mesures oppropriées pour otténuer ces risques.

La fonction gestion des risques ne doit pas s'impliquer dans les activités opérationnelles, en particulier, celles qui sont génératrices de revenus. Elle doit garder son indépendance vis-à-vis des entités opérationnelles, tout en travaillant en étroite collaboration ovec celles-ci.

Les ressources humaines affectées à la fonction gestion des risques doivent posséder un niveau élevé de connaissance des activités du DC/BR, de tout risque auquel il est exposé ainsi que de la manière dont ces risques sont gérés. Le DC/BR prend les dispositions pour que ces ressources humoines maintiennent à jour leurs connaissances en matière de gestion des risques.

Article 29 Responsable de la fonction gestion des risques

Le responsable de la fonction gestion des risques doit être doté d'une expérience avérée en la matière. Il a notamment la charge :

- de surveiller l'élaboration et la mise en œuvre du dispositif de gestion des risques ;
- de renforcer constamment les compétences de ses équipes ;
- d'opporter son assistance à l'organe délibérant ou au comité des risques, le cas échéant, lorsqu'il détermine et surveille l'oppétence pour le risque et les limites ;
- de participer, conjointement ovec l'organe exécutif, au suivi des performonces en matière de risques et de respect des limites.

Le responsable de lo fonction gestion des risques doit être impliqué dans les processus clés de prise de décision relatifs notamment à la planification stratégique, la planification des fonds

propres et de la liquidité, l'élaboration et la mise en œuvre du système de rémunération, les nouveaux produits, services et marchés ainsi que les initiatives et les opérations stratégiques importantes.

Article 30 Contrôle des risques

Le dispositif de gestion des risques du DC/BR doit intégrer des contrôles internes rigoureux, adaptés à l'ampleur, à la nature et à la complexité de ses expositions. Ce dispositif doit également faire l'objet d'examen annuel par l'audit interne et les commissaires aux comptes qui apprécient de manière indépendante l'efficacité des systèmes et processus d'évaluation et de mesure des risques du DC/BR.

Article 31 Reporting à l'organe délibérant

Un rapport sur la nature et le niveau d'exposition à chaque type de risques encourus par le DC/BR ainsi que ses besoins de fonds propres et de liquidité doit être soumis à l'organe délibérant, au moins une fois par semestre. Ce rapport, basé sur des informations fiables et à jour, doit également rendre compte notamment :

- de la nature et du niveau de l'exposition au risque de concentration du DC/BR, y compris notamment les expositions par contrepartie, par secteur et par zone géographique ;
- des principaux événements de pertes opérationnelles ;
- des transactions avec les parties liées, y compris les créances en souffrance et les créances irrécouvrables ;
- des faits saillants relatifs à chaque type de risques identifiés dans la cartographie des risques du DC/BR.

Article 32 Événements de pertes opérationnelles

Les événements de pertes opérationnelles ou incidents opérationnels doivent être classés dans l'une des sept catégories ci-après définies, afin d'assurer la cohérence au niveau de l'identification, de l'évaluation et de la fixation des objectifs de gestion des risques opérationnels à l'échelle du DC/BR :

1. fraude interne : risque de pertes dues à des actes intentionnels, impliquant au moins une partie interne au DC/BR, visant à frauder, détourner des biens appartenant au DC/BR ou à sa clientèle, manipuler des informations, contourner les règlements, la législation ou la politique du DC/BR ;
2. fraude externe : risque de pertes résultant des actes, de la part d'un tiers, visant à frauder, détourner des biens appartenant au DC/BR ou à sa clientèle, manipuler des informations ou contourner la législation ;

3. pratiques en matière d'emploi et de sécurité sur le lieu de travail : risque de pertes découlant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, y compris les litiges ou différends entre le DC/BR et ses employés ;
4. pratiques concernant les clients, les produits et l'activité commerciale : risque de pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients ou d'un manquement imputable à la nature ou à la conception d'un produit donné ;
5. dommages occasionnés aux actifs physiques : risque de pertes lié à des destructions ou dommages résultant d'une catastrophe naturelle ou des causes externes ;
6. interruptions d'activités et défaillances des systèmes : risque de pertes résultant d'interruptions de l'activité ou de dysfonctionnements des systèmes technologiques ;
7. exécution des opérations, livraison et gestion des processus : risque de pertes lié à une défaillance dans le traitement d'une transaction ou dans la gestion des processus et les pertes subies dans le cadre des relations avec les contreparties commerciales et les fournisseurs.

Article 33 Collecte des données de pertes opérationnelles

Le DC/BR doit collecter les données relatives aux événements de pertes opérationnelles. Le processus y relatif doit être documenté et mis à jour périodiquement. Les données de pertes collectées doivent répondre à certains critères minimaux, afin d'uniformiser le processus de collecte à l'échelle du DC/BR ainsi qu'à travers le marché financier et faciliter les analyses comparatives. Les pertes doivent être directes, intègres, intégrales et retraçables :

- la perte est directe lorsque l'événement a eu une incidence négative directe reconnue sur les résultats du DC/BR et, par conséquent comptabilisée. Il s'agit de l'ensemble des frais/dépenses internes et externes encourus par le DC/BR mais qui ne l'auraient pas été sans l'événement. Les coûts d'opportunité et les revenus manqués liés à l'événement, les coûts relatifs aux modifications apportées à un processus ou à l'ajout de contrôles post-événementiels, les coûts des programmes d'investissement réactifs ou proactifs à l'événement ne sont pas considérés comme directs ;
- l'intégrité des données signifie que celles-ci représentent bien des pertes opérationnelles ;
- l'intégralité des données veut dire que celles-ci incluent l'ensemble des pertes opérationnelles subies par le DC/BR, y compris celles qui sont liées aux risques de crédit et de marché, dans la limite du seuil minimal de collecte approuvé par l'organe délibérant ;
- la traçabilité découle du fait que l'intégrolité et l'intégrité des données sont assurées par leur réconciliation avec les écritures comptables appropriées et par leur validation par le responsable du DC/BR.

Chaque événement à l'origine des pertes doit être documenté et conservé dans une base de données, dans le respect des politiques définies par le DC/BR en matière de conservation de données. La documentation doit comprendre, entre autres, la référence interne du dossier, la catégorie d'événements de pertes opérationnelles, le type de risque, la description de l'incident ainsi que les entités ou les lignes de métiers concernées, le cas échéant.

Article 34 Outils de gestion du risque opérationnel

La gestion du risque opérationnel doit couvrir l'ensemble des sept catégories d'événements de pertes opérationnelles citées à l'article 32. Pour identifier et évaluer le risque opérationnel, le DC/BR peut recourir notamment aux outils de gestion ci-après :

- les autoévaluations du risque opérationnel ;
- la cartographie des processus opératiannels ;
- les indicateurs de risque et de performance en matière de surveillance du risque apérationnel et les indicateurs d'efficacité du dispositif de contrôle interne ;
- les analyses des événements de pertes opérationnelles tant à l'intérieur qu'à l'extérieur du DC/BR ;
- les analyses de risques spécifiques à chaque produit, processus et système en place ;
- les analyses de scénarios.

Les outils mis en place daivent être utilisés de façon uniforme dans toutes les unités afin de parvenir à une évoluation complète de l'expasition ou risque opérotionnel.

Article 35 Contrôle et otténuation du risque opérationnel

Le DC/BR doit prendre des mesures préventives pour réduire les pertes opérationnelles découlant d'une insuffisance liée notamment à :

- la documentation, la tenue à jour et le respect des procédures ;
- lo sécurisation des actifs du DC/BR et de leur utilisation ;
- la mise à niveau des compétences et la formation des employés ;
- la vérification et le rapprochement réguliers des opérations et des comptes ;
- l'élaboration, la mise en place et l'actuolisation d'un dispositif de sécurité physique et logique du système d'information et des infrastructures de télécommunicotion ;
- lo couverture odéquate des valeurs par des polices d'assurance.

Article 36 Gestion des risques liés aux nouveoux produits, processus, systèmes et activités

Le dispositif de gestion du risque opérationnel doit, entre autres :

- prendre en compte l'identification et l'évaluotion des risques inhérents aux nouveaux produits, aux nouvelles activités, aux grandes opérations d'acquisition ainsi que ceux découlant de changements de systèmes, de processus ou de modèle économique ;

- permettre d'identifier les plus significatifs d'entre eux et d'apprécier la vulnérabilité du DC/BR à ces risques ;
- prendre en compte à lo fois les facteurs internes et externes qui pourraient empêcher le DC/BR d'atteindre ses objectifs.

Les procédures et politiques mises en place, doivent permettre de comprendre et de gérer ces nouveaux risques. Ce processus doit prendre en compte notamment :

- les risques inhérents y relatifs ;
- les modifications du profil de risque, de l'appétence au risque qui en découlerait ;
- les contrôles nécessaires, les stratégies et processus d'otténuation des risques ainsi que le risque résiduel.

Article 37 Principes généraux en matière d'externalisation

Le recours à l'externolisation ne soustrait pas les organes de gouvernance du DC/BR de leurs obligations relatives à la conformité des controts aux exigences légales et réglementaires applicobles aux activités externalisées. En outre, il ne les exonère pas de leurs obligations vis-à-vis de toutes les parties prenantes, notamment les adhérents, les Commissaires aux Comptes et les Autorités de contrôle. Il ne modifie pas les conditions d'exercice de l'agrément.

Avant de s'engager dans un contrat d'externalisation, le DC/BR doit en évaluer l'opportunité et procéder ò une évaluation opprofondie des risques y relatifs. Ce controt doit être soumis à l'opprobation préaloble de l'organe délibérant qui doit notamment :

- exominer, ou moins deux fois por an, la liste complète des contrats d'externalisation ;
- s'imprégner des rapports d'exécution desdits contrats qui lui sont transmis par l'organe exécutif.

Le DC/BR doit veiller à ce que les dispositions contractuelles permettent :

- la mise à la disposition des Commissaires aux Comptes et de l'AMF-UMOA, de toutes les informotions nécessaires à l'exercice de leurs cantrôles ;
- lo tenue de la comptabilité ainsi que la production des états de reporting conformément aux dispositions en vigueur ;
- la préservation de la sécurité du système d'informatian et de la confidentialité des informations ;
- lo protection du consommateur et de la vie privée de l'investisseur.

L'ensemble des données physiques et électroniques du DC/BR doivent être disponibles dans l'UMOA, nonobstant l'externalisation et toute disposition prise dans le cadre de leurs plans de secours et de continuité d'activités. A cet effet, doivent être conservés et accessibles en permanence dans l'UMOA :

- les serveurs informatiques stockant les données et hébergeant les opplications ;
- l'ensemble des dossiers physiques relatifs ou personnel, au patrimoine, aux opérations du marché et connexes ainsi qu'à toutes les autres transactions réalisées par le DC/BR ;

- les archives et documents divers durant la période fixée par les dispositions légales et réglementaires.

En l'absence des serveurs primaires dans l'UMOA, des serveurs secondoires de secours doivent être disponibles dans l'Union avec une réplication de l'ensemble des données.

Tout projet de contrat d'externalisation doit être soumis à l'appréciation préalable de l'AMF-UMOA avant sa mise en œuvre. En outre, l'AMF-UMOA se réserve le droit d'ordonner la réalisatian d'un audit externe auprès du prestotaire.

Article 38 Contrat de prestations

L'externalisatian d'une activité doit reposer sur des contrats et/ou des conventions de service solides, lesquels doivent notamment préciser sans équivoque :

- une description circonstanciée des activités externalisées, la nature et la portée des prestations attendues ainsi que les coûts supportés par le DC/BR ;
- les devoirs et obligations respectifs du prestataire et du DC/BR ;
- le type et la fréquence des informations que le DC/BR reçait du prestataire ;
- les actifs du DC/BR que le prestataire peut utiliser, à sovoir les données, le matériel, les logiciels ou la prapriété intellectuelle ;
- les conditions de résiliatian, y campris le préavis du prestataire et l'exigence de restitution des actifs du DC/BR dans les délais fixés ;
- les mesures à prendre par le prestataire pour garantir la cantinuité de l'activité impartie en cas d'événements pouvant empêcher d'assurer les services attendus ;
- les indicateurs de performance qualitatifs et quantitatifs permettant au DC/BR d'évaluer, au moins une fois par an, la performance du prestataire.

Le cantrat doit contenir les clauses nécessaires en matière de confidentialité, de secret prafessiannel, de propriété intellectuelle. Il doit être soumis à un avis juridique avant toute apprabation par l'organe délibérant.

Article 39 Évaluation du prestataire

Préalablement à la conclusion de tout contrat d'externalisation, le DC/BR est tenu de procéder à une évaluatian approfondie ou due diligence de la capacité technique, financière et opérationnelle du prestataire.

Cette évaluatian est mise à jaur au mains une fais par an ainsi que lors du renauvellement et de la renégociation du contrat d'externalisation. Elle doit être documentée.

Article 40 Gestion des risques liés à l'externalisation

Le DC/BR est tenu :

- de se doter de politiques et procédures qui définissent les modalités d'externalisation et lui permettent d'identifier, de mesurer, d'atténuer et de contrôler adéquatement les risques liés à l'externalisation ;
- d'intégrer les activités externalisées dans son dispositif de contrôle interne ;
- de se doter de compétences internes lui permettant de suivre le pilotage opérationnel du contrat d'externalisation et l'appréciation des prestations reçues ;
- de disposer d'un plan de secours et de continuité des activités externalisées visant à assurer la continuité d'exploitation du DC/BR à la suite de la résiliation de contrat d'externalisation, ou de l'incapacité du prestataire à honorer ses engagements, ou d'une décision volontaire du DC/BR de rapatrier les activités externalisées ;
- d'assurer un suivi adéquat des activités externalisées et veiller à ce que le prestataire procède au contrôle régulier de son plan de continuité des activités en cas de défaillance et qu'il dispose des compétences et moyens requis pour les corriger ;
- de produire, dans le rapport d'audit interne, un résumé du résultat des contrôles effectués liés aux activités externalisées.

TITRE 4. EXERCICE DE L'AUDIT INTERNE

Article 41 Mise en place de la fonction d'audit interne

Le DC/BR doit se doter d'une fonction d'audit interne qui dispose du statut, des compétences, des ressources et de l'autorité suffisante pour exécuter ses missions avec efficacité et objectivité. La mission, les pouvoirs et les responsabilités de l'audit interne sont décrits dans une charte d'audit interne qui fait partie intégrante des procédures internes du DC/BR.

Il adopte une approche systématique et disciplinée des actions de contrôle sur la base d'un plan de contrôle établi à partir d'une cartographie recensant les risques qu'il encourt.

Article 42 Responsabilités de la fonction d'audit interne

La fonction d'audit interne assiste les membres des organes délibérant et exécutif respectivement dans leur mission de surveillance et de gestion. Pour ce faire, elle doit notamment :

- disposer d'une charte d'audit interne, de procédures de contrôle et d'un code de déontologie ;
- avoir un mandat clair et indépendant des activités auditées, y compris les activités des autres fonctions de contrôle ;

- se doter d'outils performonts lui permettont d'effectuer une surveillonce bosée sur les risques de l'ensemble des octivités du DC/BR ainsi qu'un suivi de la mise en œuvre des recommandations, classées par degré de criticité ;
- bénéficier d'un accès complet à toutes données physiques et électroniques nécessoires à l'accomplissement de so mission ;
- effectuer une évaluation périodique de l'efficacité de toutes les autres fonctions de contrôle, notamment les fonctions de gestion des risques et de conformité ;
- réaliser des examens périodiques des responsabilités et fonctions des personnes détenant les postes clés, ofin de s'assurer que ces responsables ne sont pas en mesure de dissimuler des agissements inappropriés.

Article 43 Compétences et conscience professionnelle

Les auditeurs internes doivent posséder les connoissances, les savoir-faire et les outres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités.

Le responsable de l'audit interne est tenu de solliciter l'avis et l'assistance de ressources quolifiées et indépendantes si les auditeurs internes ne possèdent pas les connaissances et le savoir-faire nécessaires pour s'acquitter d'une partie de leur mission.

Les ouditeurs internes doivent apporter à leur travail lo diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnoblement overti et compétent. La conscience profassionnelle n'implique pas l'infaillibilité.

La fonction d'audit interne doit être dotée de compétences en matière d'infrastructure et de sécurité des systèmes d'information pour mieux oppréhender les contrôles requis en la matière.

Article 44 Désignation du Responsable de la fonction d'audit interne

Sur proposition de l'organe exécutif, l'organe délibérant désigne un Responsable de lo fonction d'oudit qui doit disposer d'une indépendance fonctionnelle et jouir de prérogatives étendues quant au champ de ses interventions et à la communication de ses travaux auxdits organes.

En vue de consacrer cette indépendonce, le Responsable de la fonction d'audit doit, au moins, être fonctionnellement rattaché à l'organe délibérant, auquel il rend compte.

Article 45 Révocation du Responsable de la fonction d'audit interne

Le DC/BR est tenu, dans un délai de quinze (15) jours après la révocotion, d'en informer l'AMF-UMOA en indiquant les motifs.

Article 46 Responsabilité du Responsable de la fonction d'audit interne

Le Responsable de la fonction d'audit interne est chargé de gérer la fonction d'Audit Interne. Il doit être rattaché à un niveau de l'organisation qui permette à la fonction d'audit interne d'exercer ses responsabilités.

Il a la responsabilité de dresser le plan de contrôles sur la base de la cartographie des risques, s'impliquer dans sa réalisation, veiller au respect du cycle des contrôles et s'assurer de la qualité des travaux de la fonction. Il vérifie que les anomalies et déficiences de contrôle interne identifiées sont documentées dans un rapport écrit.

Il élabore la charte d'audit interne, veille à sa révision régulière et la diffuse à toutes les parties prenantes après son approbation par l'organe délibérant par l'intermédiaire du comité d'audit.

Le responsable de l'audit interne doit, au mains chaque année, confirmer au Conseil, l'indépendance de l'audit interne dans l'organisation.

Le responsable de l'audit interne doit communiquer et dialoguer directement avec le Conseil d'Administration.

Le Responsable de la fonction d'audit interne peut, si ceci n'emporte pas conflit d'intérêts :

- être impliqué en amont des projets afin d'identifier et d'évaluer de façon proactive les enjeux et risques potentiels de non-conformité ;
- aider à sensibiliser et à former le personnel et fournir des orientations aux membres du personnel quant à l'application appropriée des lois et règlements.

Article 47 Charte d'audit interne

Le responsable de l'audit interne doit élaborer et réviser, au moins tous les trois ans, la charte d'audit interne et la soumettre à l'approbation de l'organe délibérant par l'intermédiaire du Comité d'audit avant sa mise en application.

La charte d'audit interne précise la position de la fonction d'audit interne au sein de l'organisation du DC/BR, sa mission, ses pouvoirs, ses obligations et son périmètre d'intervention. Elle définit les caractéristiques de la fonction et son mode de fonctionnement et de communication avec les personnes n'appartenant pas à la fonction.

Article 48 Plan d'audit

Le responsable de la fonction d'audit doit établir un plan d'audit annuel ou pluriannuel basé sur les risques. Il doit également communiquer à l'organe délibérant, pour examen et approbation, son plan d'audit, ses besoins ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Ce plan, établi à partir d'une cartographie des risques du DC/BR, doit notamment :

- s'appuyer sur une évaluation rigoureuse des risques liés à l'ensemble de ses activités et entités ;

- intégrer l'évaluation des moyens humains, matériels et financiers nécessaires à la réalisation des actions prévues ;
- être réaliste et flexible afin de permettre le respect du cycle d'audit et la prise en charge des activités imprévues ;
- faire l'objet d'une mise à jour en vue de répondre aux changements de son environnement interne et externe.

La fonction d'audit interne peut initier des missions non prévues dans son planning de contrôle, lorsque des circonstances particulières le nécessitent, ou sur demande de l'organe délibérant, des Comités spéciolisés, du Directeur Général.

Article 49 Piste d'audit

La fonction d'audit interne doit garantir l'existence de la piste d'audit telle que définie au o) de l'article 1 et veiller au respect des dispositions du référentiel comptable. Les éléments constitutifs de la piste d'audit doivent être conservés pendant au moins dix (10) ans.

Article 50 Maintien et sécurité des données informatisées

La fonction d'audit interne doit comprendre des procédures internes de sauvegarde et de reprise des systèmes qui utilisent des données informatisées, des politiques de développement et de maintenance appropriées de ces systèmes ainsi que des contrôles de sécurité d'accès physiques et logiques.

Article 51 Examen du rapport d'audit par le Comité d'Audit

Les rapports d'audit interne sont portés à la connaissonce du Comité d'Audit afin de foire l'objet d'un examen et d'un suivi adéquat.

TITRE 5. REPORTING A L'AMF-UMOA

Article 52 Reporting semestriel et occasionnel à l'AMF-UMOA

Le DC/BR doit transmettre à l'AMF-UMOA, le 15 août au plus tard un rapport semestriel consolidé présentant par rubrique les travaux réalisés par les fonctions de conformité, de gestion des risques et de l'audit interne.

En outre, le DC/BR informe, sans déloi, l'AMF-UMOA de toutes insuffisonces relevées par les fonctions de contrôle et ayant un impact significatif sur la réputation du DC/BR et/ou sa solidité financière.

Article 53 Reporting annuel

Le DC/BR doit transmettre à l'AMF-UMOA, le 15 mai au plus tard, pour le compte de l'exercice précédent, un rapport annuel consolidé présentant par rubrique les travaux réalisés par les fonctions de contrôle interne.

Ce rapport devra préalablement être validé par l'organe délibéront du DC/BR.

Article 54 Contenu des rapports d'Audit interne

Le format de présentation des rapports d'audit interne destinés à l'AMF-UMOA est précisé par une Circulaire de l'AMF-UMOA.

TITRE 6. DISPOSITIONS TRANSITOIRES ET FINALES

Article 55 Dispositions transitoires

Le Dépositaire Central / Banque de Règlement dispose d'un délai maximum de deux (02) ans à compter de sa date de signature pour se mettre en conformité ovec les dispositions de la présente Instruction.

Article 56 Sanctions

Le non-respect des règles prévues par la présente Instruction est sanctionné par l'AMF-UMOA, conformément aux dispositions réglementaires en vigueur sur le Marché Financier Régional de l'UMOA.

Article 57 Publication et date d'entrée en vigueur

La présente Instruction, qui sera publiée partout où besoin sera, abroge toutes dispositions antérieures contraires et entre en vigueur à compter de sa date de signature.

Le DC/BR est tenu d'en transmettre copie à tous les membres de l'organe délibérant et aux Commissaires aux comptes.

Fait à Abidjan, le 29 DEC. 2023

Pour l'Autorité des Marchés Financiers de l'UMOA

Le Président

Le Président
01 BPM 1878
ABIDJAN 01

Badanam PATOKI

AMF-UMOA

AUTORITÉ DES MARCHÉS FINANCIERS DE L'UNION MONÉTAIRE OUEST AFRICAINE

INSTRUCTION N° 79 /AMF-UMOA/2023
RELATIVE AUX EXIGENCES DES SYSTEMES D'INFORMATION DE LA BOURSE RÉGIONALE DES VALEURS MOBILIÈRES (BRVM)

L'Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine,

Vu le Traité révisé de l'Union Monétaire Ouest Africaine (UMOA) du 12 juillet 2019, entré en vigueur le 1er octobre 2022, modifiant la dénomination du Conseil Régional de l'Epargne Publique et des Marchés Financiers (CREPMF) en Autorité des Marchés Financiers de l'UMOA (AMF-UMOA) ;

Vu la Convention du 03 juillet 1996 portant création du Conseil Régional de l'Épargne Publique et des Marchés Financiers, notamment son Annexe portant composition, organisation, fonctionnement et attributions du Conseil Régianal de l'Épargne Publique et des Marchés Financiers ;

Vu le Règlement Général relotif à l'organisation, au fonctionnement et au contrôle du marché financier régional de l'UMOA ;

Vu l'Instruction n°2/97 du 29 novembre 1997 relative à l'habilitation de la Bourse Régionale des Valeurs Mobilières ;

Vu la Décision n° 004 du 29/04/2021/CM/UMOA portant nomination du Président du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu les délibérations de l'AMF-UMOA en sa 98ème session ordinaire du 23 décembre 2023, tenue à Cotonou en République du Bénin ;

ARRETE :

TITRE 1. DISPOSITIONS ET OBLIGATIONS GENERALES

Article 01 : Définitions

Aux fins de la présente Instruction, on entend par :

a) Incident informatique : Tout événement qui ne fait pos partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la quolité de ce service.

b) Plateforme logicielle : Logiciel métier utilisé par la Bourse Régionale des Valeurs Mobilières (logiciel de cotation, logiciel de surveillance, etc.).

c) Piste d'audit : Enregistrement chronalogique des activités d'un système montrant tous les ajouts, suppressions et changements apportés au système, qui permet de reconstituer et de contrôler une opération depuis son origine jusqu'à son aboutissement.

d) Plan de Continuité d'Activités : Document stratégique formalisé et régulièrement mis à jour, de planification de la réaction à une catastrophe ou à un sinistre grave. Son objectif est de minimiser les impacts d'une crise ou d'une catastrophe naturelle, technologique ou sociale sur l'activité (et donc la pérennité) d'une entreprise.

e) Profil utilisateur : Description d'un utilisateur montrant les droits dont il bénéficie dans le logiciel métier.

f) RPO (Recovery Point Objective) : Le RPO quantifie les données qu'un Système d'Information peut perdre par suite d'un incident. Usuellement, le RPO exprime une durée entre l'incident provoquant la perte de données et la dote la plus récente des données qui seront utilisées en remplacement des données perdues.

g) RTO (Recovery Time Objective) : Le RTO représente la durée maximale d'interruption admissible pendant laquelle une ressource (ordinateur, système, réseau, logiciel) peut ne pas être fonctionnelle à la suite d'une panne ou d'un désastre.

Article 02 : Objet

La présente instruction fixe les règles en matière de sécurité et de gestion des risques du système d'information de la Bourse Régionale des Valeurs mobilières (BRVM).

Article 03 : Champ d'application

La présente instruction s'applique à la Bourse Régionale des Valeurs Mobilières.

TITRE 2 : DISPOSITIF DE SECURITE DU SYSTEME D'INFORMATION DE LA BRVM

Article 04 : Piste d'audit

Une piste d'audit doit être configurée sur toute plateforme logicielle métier afin de garantir l'enregistrement des actions effectuées par les utilisateurs de cette plateforme et de garantir ainsi leur traçabilité. De plus, l'accès à cette piste d'audit doit être restreint, de sorte à être non accessible aux administrateurs des données.

Article 05 : Journalisation et droit d'accès à la piste d'audit

Les logiciels métier, les Bases de Données et les Systèmes d'Exploitation de la BRVM, doivent posséder des caractéristiques de sécurité, qui permettent de journaliser les actions effectuées et ainsi de détecter et analyser toute irrégularité.

Cette journalisation (activation de la piste d'audit) doit être effective sur les logiciels métier.

La piste d'audit des logiciels métier doit être sécurisée (protégée contre toute modification) et archivée de manière adéquate afin de garantir son intégrité et sa qualité de pièce probante. Elle doit être uniquement accessible à la Direction de l'audit ou du contrôle interne.

La piste d'audit des logiciels métier ainsi que les logs des bases de données et systèmes d'exploitation doivent être conservés pendant au moins cinq (5) ans afin de pouvoir servir ultérieurement lors d'éventuels litiges ou à des fins d'analyses.

Article 06 : Identifiant et mot de passe pour l'authentification des utilisateurs

L'accès aux logiciels métier doit se faire via une authentification des utilisateurs (combinaison de l'identification et du mot de passe) de manière à n'autoriser que les utilisateurs habilités. De plus, l'identité de chaque utilisateur devra être unique de sorte à lier chaque activité sur le logiciel à un utilisateur spécifique.

Article 07 : Prohiber l'accès simultané avec le même compte utilisateur

Les logiciels métier ne devraient pas permettre à un même utilisateur d'ouvrir plusieurs sessions à partir d'une seule ou de plusieurs machines.

Article 08 : Profils utilisateurs

Chaque logiciel métier doit avoir la fonctionnalité de gestion des profils utilisateurs. Les profils utilisateurs doivent permettre d'éviter le cumul de fonctions incompatibles et garantir que les rôles ou les droits d'accès des utilisateurs à chaque logiciel métier sont conformes aux attributions des utilisateurs au sein de la BRVM.

Article 09 : Changement de mot de passe à la première connexion

Généralement, chaque nouvel utilisateur d'un logiciel métier est créé avec un mot de posse générique. De ce fait, un changement de ce mot de passe à lo première connexion doit être obligotoire afin de réduire le risque d'usurpatian d'identité.

Article 10 : Déconnection automatique des utilisateurs après un temps d'inactivité

Les logiciels métier doivent offrir la possibilité de paramétrer la déconnection des utilisateurs de leur session en cas d'inactivité dans le logiciel pendont une durée maximale de dix (10) minutes.

Article 11 : Paramétrage des mats de passe (langueur, complexité, durée, historique, verrouillage)

Les mots de passe des logiciels métier daivent être paramétrables de sarte à définir les voleurs des paramètres suivants :

- la longueur minimale du mot de passe doit être de huit (08) caractères ;
- la complexité du mat de passe (au moins une majuscule, au moins une minuscule, au mains un caractère spécial, au moins un caractère olphanumérique) ;
- la durée maximale du mat de passe ne peut excéder quatre-vingt-dix (90) jours) ;
- le verrauillage des comptes après un nombre de tentatives de connexions n'excédant pas trois (03).

Article 12 : Cryptage ou hachage des fichiers/tables des mots de passe

Les fichiers ou tables des mots de passe des logiciels métier doivent être cryptés ou hachés afin que les mots de passe ne saient pas lisibles par les administrateurs des lagiciels métier au des Bases de données.

Article 13 : Surveillance et réalisation d'examen en matière de sécurité

La BRVM doit étroitement surveiller le personnel disposant des privilèges d'accès élevés à ses systèmes, car celui-ci passède les connaissances et les ressources nécessaires pour contourner les contrôles implémentés dans ces systèmes et les procédures de sécurité. La BRVM doit obligatairement procéder, une fais taus les trois (03) ans, à un audit de sécurité dont les résultats sont transmis à l'AMF-UMOA au plus tard le 15 mai de l'année suivant la période triennale.

Elle doit adopter les contrâles et pratiques suivants :

- mettre en œuvre des mécanismes d'authentificatian farts pour les utilisateurs privilégiés, natamment pour les accès à distance ;
- limiter le nambre d'utilisateurs privilégiés ;
- accorder un accès privilégié sur une base stricte des besains fonctiannels ;

- cansigner les activités effectuées sur les systèmes par des utilisateurs privilégiés en activant les journaux d'audit ;
- interdire aux utilisoteurs privilégiés d'accéder aux journaux des systèmes dans lesquels leurs activités et celles des autres utilisateurs sont consignés ;
- examiner les activités des utilisateurs privilégiés en temps opportun ;
- interdire le partage de comptes privilégiés ;
- interdire aux fournisseurs de bénéficier d'un accès privilégié aux systèmes sans une surveillance étroite.

Le contrôle interne de la BRVM devra effectuer des vérifications (revues des profils, des accès aux systèmes informatiques, revue des logs d'audit) en vue d'identifier toute irrégularité liée à l'utilisation des systèmes informatiques. Périodiquement et au moins chaque semestre (les mois de janvier et juillet), les rapports de ces contrôles doivent être transmis à l'AMF-UMOA et conservés par la BRVM.

TITRE 3 : GOUVERNANCE ET GESTION DES RISQUES

Article 14 : Dispositif de sécurité

Dans le cadre de la gestion des risques inhérents aux systèmes d'information, la BRVM doit mettre en place un dispositif permettant, de manière continue, d'identifier et d'évaluer les risques, en vue de les réduire ou de les gérer. Elle élabore, à cet effet, so stratégie de gestion des risques approuvée par ses instances dirigeantes.

Elle doit utiliser les bonnes pratiques non exhaustives suivantes :

- veiller à ce qu'un cadre solide de gestion des risques technologiques soit établi et maintenu ;
- veiller à ce que des contrôles internes efficaces et des pratiques de gestion des risques soient mis en œuvre pour assurer la sécurité, la fiabilité, la résilience des systèmes et la reprise des activités ;
- établir des politiques, des normes et des procédures informatiques, qui sont des composantes essentielles du cadre de gestion des risques technologiques. En raison des changements rapides dans l'environnement et dans la sécurité informatique, les politiques, les normes et les procédures devraient être régulièrement revues et mises à jour ;
- mettre en œuvre des processus de conformité pour vérifier que les normes et procédures de sécurité informatique sont appliquées. Des processus de suivi devraient être mis en œuvre pour que les écarts de conformité soient connus et corrigés en temps opportun ;
- mettre en place un programme de sensibilisation des employés à la sécurité informatique. Ce programme devrait être mis régulièrement à jour pour s'ossurer que son contenu reste pertinent, compte tenu de l'évolution de la technologie ainsi que des risques qui y sont associés ;
- procéder à un audit tri-annuel de son système d'information.

Article 15 : Politique de sécurité informatique

La BRVM élabore une politique de sécurité informatique adaptée à son activité et à son infrastructure informatique propre, conforme aux exigences de sécurité les plus répandus sur le marché et notamment la norme ISO 27001.

Cette politique doit être approuvée par le Conseil d'Administration de la BRVM et communiquée à tous les utilisateurs du Système d'Information (employé, prestataire). Elle est actualisée régulièrement, au moins tous les trois ans, pour tenir compte de l'évolution de l'environnement interne et externe.

Article 16 : Plan de Continuité d'Activités

La BRVM doit veiller à ce que son organisation, son système et ses procédures soient conçus pour maintenir leurs fonctions critiques ou les rétablir le plus rapidement possible afin de remplir leurs obligations vis-à-vis de l'autorité de régulation et des usagers agréés du marché.

A cet effet, l'élaboration d'un plan de continuité d'activités comprenant un plan de secours informatique s'avère obligatoire. Le plan de continuité d'activités doit être approuvé par le Conseil d'Administration. Ce plan doit prévoir, entre autres, au minimum les aspects ci-après :

- une identification des processus de l'entreprise ayant une importance stratégique, qui sont critiques et nécessaires à sa survie et une configuration minimale du système d'information capable de soutenir lesdits processus ;
- une évaluation des risques, des vulnérabilités et des impacts qui débouchera sur l'identification des ressources humaines indispensables, des données importantes pour la BRVM et l'efficience des contrôles d'atténuation pour des risques existants ;
- une définition de la stratégie de continuité d'activités, incluant les critères de déclenchement du plan, un site de reprise avec sa description, une présentation de l'équipe de crise avec les personnes autorisées à déclencher le plan, le délai acceptable de reprise des activités (RTO : Recovery Time Objective) et la quantité acceptable de perte de données (RPO : Recovery Point Objective) ;
- les programmes de formation et de sensibilisation du plan ;
- le programme de mise à jour et de test du plan de continuité.

La BRVM doit disposer d'un site de repli.

Le site de repli de la BRVM doit être établi dans au moins un autre État membre de l'UMOA afin d'atténuer le risque qu'un même sinistre touche les deux sites.

Le délai acceptable de reprise complète des activités (RTO : Recovery Time Objective) après un désastre est de 24 heures.

La quantité acceptable de perte de données (RPO) est fixée à deux (02) heures de données.

L'exercice d'évaluation de l'efficacité du plan doit concerner, de façon non exhaustive, des aspects vérifiables : (i) la procédure d'alerte, (ii) le fonctionnement de la cellule de crise, (iii) les procédures techniques de basculement en mode secours, (iv) la coordination des différentes parties prenantes, lors d'un exercice de réponse à un incident grave simulé, (v) la formation ciblée

des personnels oux procédures techniques, (vi) le degré d'appropriation du plan par le personnel de la BRVM, (vii) les tests des éléments critiques du plan au moins une fois por on et (viii) les tests réguliers de la procédure de récupération des souvegordes pour vérifier son adéquation oux besoins de l'organisation.

Périodiquement et ou moins une fois por on, le plon doit être testé afin de vérifier son efficocité. Le rapport du test doit indiquer les résultats du test, les points de faiblesses identifiés et un plan d'exécution pour corriger ces faiblesses.

Article 17 : Sauvegarde et restauration des données

La BRVM s'assure que sa politique de sécurité de l'informotion gorantit l'intégrité des sauvegardes des données sur des supports appropriés, la réalisation de tests réguliers de restaurotion et la délocolisation des supports de sauvegarde sur un site distant.

Article 18 : Accès à l'infrastructure informatique

L'accès à l'infrastructure infarmatique de la BRVM doit s'oppuyer sur des solutions d'authentification solides qui permettent, avec un degré d'assurance très élevé, de vérifier l'identité des utilisoteurs. Elle doit utiliser à cet égard des posserelles contrôlées entre internet et son infrastructure informatique propre, telles que des firewalls, des proxys servers, des scanners antivirus et des scanners de contenu, ou d'outres solutions de sécurité similaires à jour. Elle doit veiller à ce que ces passerelles soient correctement conçues, configurées et sécurisées, et ò ce qu'elles fassent l'objet d'une gestion quotidienne professionnelle et d'un suivi rigaureux.

Article 19 : Gestion des incidents

La BRVM met en place un cadre de gestion des incidents de sécurité de l'informatian, afin de les traiter et de contenir leur impact. Elle doit disposer d'une procédure de gestion des incidents validée par la Direction Générale, qui doit :

- préciser ò quels types d'incidents elle s'applique ;
- établir les rôles et les responsabilités du personnel impliqué dans le processus de gestion des incidents ;
- définir une méthode de déclaratian des incidents après leur détection ;
- préciser la priarité des incidents en fonctian de l'urgence et de l'impact ;
- définir la stratégie d'attribution des incidents au personnel en charge de leurs résalutians en tenont compte des escalades ;
- permettre de suivre et de superviser lo gestion des incidents (traçabilité de tout incident) afin de savoir à tout moment le niveau de résolution d'un incident et de clôturer les incidents résolus ;
- expliquer les tâches et responsabilités en matière de communicatian interne et externe quant aux incidents majeurs.

Un rapport d'incidents prenant en compte, l'état et l'impact de l'incident, les mesures de correction adoptées, les recommandations et le plan de mise en œuvre doit être transmis annuellement, au mois de janvier, à l'AMF-UMOA.

Enfin, tout incident majeur doit être systématiquement communiqué à l'AMF-UMOA, dans un délai de 24 heures.

TITRE 4 : GESTION DES CHANGEMENTS

Article 20 : Maintenance des applications

La BRVM doit mettre en place un environnement formalisé de maintenance des applications. Celui-ci doit comporter un environnement de test (homologation) et d'un environnement de production. Ces deux environnements doivent être nettement séparés et permettre le processus de maintenance d'une application par les phases de correction, recette et validation avant mise en production.

Périodiquement, l'environnement d'homologation doit être mis à jour au niveau de sa configuration afin de répondre de manière efficiente et objective aux tests qui y seront effectués.

Article 21 : Processus de gestion des changements aux systèmes de production

La BRVM doit établir un processus de gestion des changements pour s'assurer que les modifications apportées aux systèmes de production sont évaluées, approuvées, mises en œuvre et examinées de manière appropriée. Le processus de gestion des changements doit s'appliquer aux modifications relatives aux changements et mises à jour de logiciels, aux configurations systèmes et de sécurité.

Ce processus doit être régi par une procédure de gestion des changements. Cette procédure validée par le Conseil d'Administration, doit inclure les principales étapes suivantes :

- l'initiation du changement ;
- l'analyse des risques et de l'impact du changement ;
- l'autorisation du changement ;
- la priorisation du changement ;
- les tests d'assurance qualité, tests d'acceptation utilisateurs (UAT) ;
- le plan de retour (roll-back plan) ;
- la décision de mise en production du changement ;
- la mise en production du changement en respectant les principes de séparation des tâches ;
- la documentation du changement, la formation des utilisateurs et la diffusion des supports de formation aux utilisateurs ;
- le suivi post-implémentation du changement.

TITRE 5 : GESTION DES RISQUES LIES AU SYSTÈME D'INFORMATION

Article 22 : Processus de gestion des risques liés aux systèmes d'informotion

Dans le cadre de la gestion des risques inhérents aux systèmes d'information, la BRVM met en ploce un dispositif permettont, de manière continue, d'identifier et d'évaluer les risques, en vue de les réduire ou de les gérer. Elle élobore, à cet effet, so strotégie de gestion des risques approuvée por son Conseil d'Administration. La BRVM procède ou fait procéder, le cas échéont, à ses frais, aux contrôles nécessaires à la sécurité des installations et autres matériels. Elle adresse les procès-verbaux de ces contrôles à l'AMF-UMOA, à sa demonde expresse. La BRVM met en œuvre les moyens humains et motériels nécessoires à lo sécurité et à la sûreté, pour l'exploitotion des instollations à sa disposition.

Article 23 : Protection contre les logiciels malveillants et le piratage informatique

La BRVM met en place des mesures de prévention, de détection et de correction, afin de protéger son système d'information contre des logiciels molveillants et le piratage informotique.

La Direction Générale de la BRVM devra intégrer dans son rapport annuel de gestion à l'attention du Conseil d'Administration une situation des incidents majeurs survenus durant la précédente année.

Article 24 : Sécurisation des réseaux, des terminaux et des informations

La BRVM prend des mesures de sécurité appropriées pour protéger les informations qui transitent par son réseau, ainsi qu'à travers ses connexians avec les utilisateurs, les fournisseurs de données et l'AMF-UMOA. Elle s'assure que les terminaux qui accèdent à son système dispose des autorisations nécessaires. En outre, elle met en place le paramétrage adéquat, en vue de gérer les risques inhérents à la connexian d'utilisateurs externes à son système d'information.

Article 25 : Gestion des identités et des accès logiques aux systèmes d'information

La BRVM s'assure que chaque utilisateur, faurnisseur de données ou membre de son personnel est identifié et authentifié avant tout accès aux systèmes d'information, et qu'il dispose des droits d'accès adéquats. Chaque action dait pauvoir être rattachée à son auteur.

Article 26 : Dispositif de sécurité physique et environnementale

La BRVM se dote d'un dispositif de gestion des accès physiques de son personnel et des tierces personnes à ses locaux sécurisés. Les locaux hébergeant son centre de données doivent être pourvus de dispositifs oppropriés de protection environnementale, notamment de détecteurs de fumée et d'eau, de systèmes d'extinction automatique d'incendie ainsi que de sondes de température.

Article 27 : Gestion des prestataires informatiques

Les prestataires informatiques jouent un rôle important dans la gestion des systèmes et des processus de la BRVM. Une sélection minutieuse et un contrôle des prestataires informatiques sont essentiels pour minimiser les risques de sécurité auxquels elle pourrait être confrontée. Celle-ci doit mettre en œuvre des mesures pour répondre aux menoces de sécurité qui peuvent survenir au cours de ses relations avec les prestataires en utilisant une approche basée sur les risques. Pour faire face à ces menaces, et en vue de s'assurer du respect de la confidentialité, de la disponibilité et de l'intégrité des données, elle devra utiliser les pratiques suivantes :

- effectuer une diligence raisonnoble (due diligence) préalable à la passation de contrat avec les prestataires pour des services éventuels. Cette diligence devra permettre de déterminer la viabilité, la fiabilité, les antécédents des prestataires ;
- veiller à ce que les conditions contractuelles régissant les rôles, les relations, les obligations et les responsabilités des prestataires soient énoncées dans des accords écrits (contrat de niveau de service) qui précisent également les obligations après la fin de la relation. Les exigences et les conditions couvertes par ces accords comprennent habituellement les objectifs de rendement, les niveoux de service, la disponibilité, la fiabilité, l'évolutivité, la conformité, l'audit, la sécurité ;
- mettre en œuvre des accords de non-divulgation des informations confidentielles appelés "Non-disclosure agreement (NDA)" avec les prestataires ;
- veiller à ce que l'utilisation de prestataires, l'externalisation des systèmes informatiques, n'entraînent pas un affaiblissement ou une dégradation des contrôles internes de la BRVM. Elle doit exiger des prestotaires de services qu'ils appliquent rigoureusement des procédures et contrôles de sécurité afin de protéger la confidentialité et la sécurité des infarmations sensibles ou confidentielles telles que ses données financières et celles de ses clients ;
- effectuer un contrôle (évaluation des clauses définies dans les contrats de niveau de service) continu des prestataires de services afin d'évaluer l'adéquation et la conformité des opérations et services qu'ils fournissent ;
- établir, maintenir et surveiller les droits et les actions des prestataires dans leurs systèmes ;
- établir et mettre en œuvre des procédures pour mettre fin à l'accès des prestataires de services aux systèmes dès la résiliation du contrat ;
- vérifier, la capacité du prestataire de services à récupérer les systèmes et les services informatiques externolisés en étant conformes aux délais acceptables de reprise des activités (RTO : Recovery Time Objective) avant de conclure tout accord avec les fournisseurs de services. Aussi, à la résiliation du contrat, la BRVM doit avoir le pouvoir contractuel et les moyens de retirer ou de détruire rapidement les données stockées dons les systèmes et les sauvegardes des prestotaires de services.

TITRE 6 : PLATEFORME LOGICIELLE

Article 28 : Logiciel métier

La BRVM doit disposer de logiciels métiers approuvés par l'AMF-UMOA et qui doivent être mis à jour conformément aux évolutions de l'environnement technologique et du marché.

Ces logiciels métier doivent être adaptés à ses activités réglementaires.

Article 29 : Fonctionnalités minimales du logiciel métier dédié à la cotation

Le logiciel métier dédié à la cotation doit disposer des fonctionnalités minimales ci-après :

a) cotation en continu et au fixing et la négociation des principaux types d'instruments financiers autorisés sur le marché financier régional ;

b) prise en charge de toutes les activités de négociation, de contrôle, de surveillonce des transactions ;

c) module d'observation pour le réguloteur ;

d) génération des flux de données à destination de l'AMF-UMOA, selon le format requis ;

e) interface permettant la mise en œuvre par les SGI de la bourse en ligne pour leurs clients ;

f) colcul fiable des indices et des capitalisations boursières ;

g) gestion des périodes de saisie des ordres ;

h) prise en charge de toutes les stipulations d'ordre autorisées ;

i) gestion des carnets d'ordres actifs, inactifs, etc.

Article 30 : Dispositif de secours et de continuité

Pour la sécurisation de ses activités, la BRVM doit :

- doter son logiciel métier d'un système de secours en vue de garantir la continuité du marché boursier ;
- organiser un système alternatif d'échanges d'informations entre le site central, le site de secours et les adhérents ;
- prévoir une clause contractuelle permettant le renouvellement ou la prorogation de la licence d'exploitation du logiciel métier par le Régulateur ou tout autre entité désignée par celui-ci en cas de cessation d'activité de la BRVM.

TITRE VII : DISPOSITIONS TRANSITOIRES ET FINALES

Article 31 : Dispositions transitoires

Le Dépositaire Central / Banque de Règlement dispose d'un délai maximum de deux (02) ans à compter de cette date pour se mettre en conformité avec les dispositions de la présente Instruction.

Article 32 : Publication et date d'entrée en vigueur

La présente Instruction, publiée partout où besoin sera, abroge toutes dispositions règlementaires antérieures contraires et entre en vigueur à compter de sa date de signature.

Fait à Abidjan, le 29 DEC. 2023

Paur l'Autarité des Marchés Financiers de l'UMOA

Le Président

Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine
Le Président
01 BPM 1878
ABIDJAN 01

Badanam PATOKI

AMF-UMOA

AUTORITÉ DES MARCHÉS FINANCIERS DE L'UNION MONÉTAIRE OUEST AFRICAINE

INSTRUCTION N° 8 0 /AMF-UMOA/2023

RELATIVE AUX EXIGENCES DES SYSTEMES D'INFORMATION DU DEPOSITAIRE CENTRAL / BANQUE DE REGLEMENT (DC/BR)

L'Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine,

Vu le Traité révisé de l'Union Monétaire Ouest Africaine (UMOA) du 12 juillet 2019, entré en vigueur le 1er octobre 2022, modifiant la dénomination du Conseil Régional de l'Epargne Publique et des Marchés Financiers (CREPMF) en Autorité des Marchés Financiers de l'UMOA (AMF-UMOA) ;

Vu la Convention du 03 juillet 1996 portant création du Conseil Régional de l'Épargne Publique et des Marchés Financiers, notamment son Annexe portant composition, organisation, fonctionnement et attributions du Canseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu le Règlement Général relatif à l'organisation, au fonctionnement et au contrôle du marché financier régional de l'UMOA ;

Vu l'Instruction n°3/97 du 29 novembre 1997 relative à l'habilitation du Dépasitoire Central/Bonque de Règlement ;

Vu la Décisian n° 004 du 29/04/2021/CM/UMOA portant naminatian du Président du Conseil Régional de l'Épargne Publique et des Marchés Financiers ;

Vu les délibérations de l'AMF-UMOA en sa 98ème session ordinaire du 23 décembre 2023, tenue à Cotonou en République du Bénin ;

ARRETE :

TITRE 1. DISPOSITIONS ET OBLIGATIONS GENERALES

Article 01 : Définitions

Aux fins de la présente Instruction, on entend par :

a) Incident informatique : Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.

b) Plateforme logicielle : Logiciel métier utilisé par le DC/BR, notamment le logiciel dépositaire.

c) Piste d'audit : Enregistrement chronologique des activités d'un système montrant tous les ajouts, suppressions et chongements apportés au système, qui permet de reconstituer et de contrôler une opération depuis son origine jusqu'à son aboutissement.

d) Plan de Continuité d'Activités : Document strotégique formalisé et régulièrement mis à jour, de planification de la réaction à une catastrophe ou à un sinistre grave. Son objectif est de minimiser les impacts d'une crise ou d'une catastrophe naturelle, technologique ou sociale sur l'octivité (et donc la pérennité) d'une entreprise.

e) Profil utilisateur : Description d'un utilisateur montrant les droits dont il bénéficie dans le logiciel métier.

f) RPO (Recavery Point Objective) : Le RPO quontifie les données qu'un Système d'Information peut perdre par suite d'un incident. Usuellement, le RPO exprime une durée entre l'incident provoquant la perte de données et la date la plus récente des données qui seront utilisées en remplacement des données perdues.

g) RTO (Recavery Time Objective) : Le RTO représente la durée maximale d'interruption odmissible pendant laquelle une ressource (ardinateur, système, réseau, logiciel) peut ne pas être fonctionnelle à la suite d'une panne au d'un désostre.

Article 02 : Objet

La présente instruction fixe les règles en matière de sécurité et de gestian des risques du système d'infarmation du Dépositaire Central / Banque de Règlement (DC /BR).

Article 03 : Champ d'application

La présente instruction s'applique au Dépasitaire Central / Banque de Règlement.

TITRE 2 : DISPOSITIF DE SECURITE DU SYSTEME D'INFORMATION DU DC/BR

Article 04 : Piste d'audit

Une piste d'audit doit être configurée sur taute plateforme logicielle métier ofin de gorontir l'enregistrement des octions effectuées par les utilisateurs de cette plateforme et de gorantir ainsi leur troçobilité. De plus, l'accès à cette piste d'audit doit être restreint, de sorte à être non accessible oux administrateurs des données.

Article 05 : Journalisatian et droit d'accès à la piste d'audit

Les logiciels métier, les Bases de Données et les Systèmes d'Exploitation du DC/BR doivent posséder des caractéristiques de sécurité, qui permettent de journaliser les actions effectuées et oinsi de détecter et analyser toute irrégulorité.

Cette journalisation (activation de la piste d'audit) doit être effective sur les logiciels métier.

La piste d'audit des logiciels métier doit être sécurisée (protégée cantre toute modification) et archivée de manière adéquate afin de garantir son intégrité et so qualité de pièce prabante. Elle dait être uniquement accessible ò la Direction de l'audit au du contrâle interne.

La piste d'audit des logiciels métier ainsi que les logs des bases de données et systèmes d'exploitation doivent être conservés pendant au moins cinq (5) ons afin de pouvair servir ultérieurement lors d'éventuels litiges au à des fins d'analyses.

Article 06 : Identifiant et mat de passe pour l'authentification des utilisateurs

L'accès aux logiciels métier doit se foire via une authentification des utilisateurs (combinaison de l'identification et du mot de passe) de manière à n'autoriser que les utilisateurs habilités. De plus, l'identité de chaque utilisateur devra être unique de sorte à lier chaque activité sur le logiciel à un utilisateur spécifique.

Article 07 : Prohiber l'accès simultané avec le même compte utilisateur

Les logiciels métier ne devraient pas permettre à un même utilisateur d'ouvrir plusieurs sessions à partir d'une seule ou de plusieurs machines.

Article 08 : Profils utilisateurs

Chaque logiciel métier doit avoir la fonctionnalité de gestion des profils utilisateurs. Les profils utilisateurs doivent permettre d'éviter le cumul de fonctions incompatibles et garantir que les rôles ou les droits d'accès des utilisateurs à chaque lagiciel métier sont conformes oux attributions des utilisateurs au sein du DC/BR.

Article 09 : Changement de mot de passe à la première connexion

Généralement, chaque nouvel utilisateur d'un logiciel métier est créé avec un mot de passe générique. De ce fait, un changement de ce mot de passe à la première connexion doit être obligatoire afin de réduire le risque d'usurpation d'identité.

Article 10 : Déconnection automatique des utilisateurs après un temps d'inactivité

Les logiciels métier doivent offrir la possibilité de paramétrer la déconnection des utilisateurs de leur session en cas d'inactivité dans le logiciel pendant une durée maximale de dix (10) minutes.

Article 11 : Paramétrage des mots de passe (longueur, complexité, durée, historique, verrouillage)

Les mots de passe des logiciels métier doivent être paramétrables de sorte à définir les valeurs des paramètres suivants :

- la longueur minimale du mot de passe doit être de huit (08) caractères ;
- la complexité du mot de passe (au moins une majuscule, au moins une minuscule, au moins un caractère spécial, au moins un caractère alphanumérique) ;
- la durée maximale du mot de passe ne peut excéder quatre-vingt-dix (90) jours) ;
- le verrouilloge des comptes après un nombre de tentatives de connexions n'excédant pas trois (03).

Article 12 : Cryptage ou hachage des fichiers/tables des mots de passe

Les fichiers ou tables des mots de passe des logiciels métier doivent être cryptés ou hachés afin que les mots de passe ne soient pas lisibles par les administrateurs des logiciels métier ou des Bases de données.

Article 13 : Surveillance et réalisation d'examen en matière de sécurité

Le DC/BR doit étroitement surveiller le personnel dispasant des privilèges d'accès élevés à ses systèmes, car celui-ci possède les cannaissances et les ressources nécessaires pour cantourner les contrôles implémentés dans ces systèmes et les procédures de sécurité. Le DC/BR doit abligatoirement procéder, une fois tous les trois (03) ons, à un audit de sécurité dont les résultats sont transmis à l'AMF-UMOA au plus tard le 15 mai de l'année suivant lo période triennale.

Il dait adopter les contrôles et pratiques suivonts :

- mettre en œuvre des mécanismes d'authentification farts pour les utilisateurs privilégiés, notamment pour les accès à distance ;
- limiter le nombre d'utilisateurs privilégiés ;
- accorder un accès privilégié sur une base stricte des besoins fonctionnels ;
- consigner les activités effectuées sur les systèmes par des utilisateurs privilégiés en activant les journaux d'audit ;

- interdire aux utilisateurs privilégiés d'accéder aux journaux des systèmes dans lesquels leurs activités et celles des autres utilisateurs sont consignés ;
- examiner les activités des utilisateurs privilégiés en temps opportun ;
- interdire le partage de comptes privilégiés ;
- interdire aux fournisseurs de bénéficier d'un accès privilégié aux systèmes sans une surveillance étroite.

Le contrôle interne du DC/BR devra effectuer des vérifications (revues des profils, des accès aux systèmes informatiques, revue des logs d'oudit) en vue d'identifier toute irrégularité liée à l'utilisotion des systèmes informatiques. Périodiquement et au moins chaque semestre (les mois de janvier et juillet), les rapports de ces contrôles doivent être transmis à l'AMF-UMOA et conservés par le DC/BR.

TITRE 3 : GOUVERNANCE ET GESTION DES RISQUES

Article 14 : Dispositif de sécurité

Dans le cadre de la gestion des risques inhérents aux systèmes d'information, le DC/BR doit mettre en place un dispositif permettant, de manière continue, d'identifier et d'évaluer les risques, en vue de les réduire ou de les gérer. Il élabore, à cet effet, sa stratégie de gestion des risques approuvée par ses instances dirigeantes.

Il doit utiliser les bonnes pratiques non exhaustives suivontes :

- veiller à ce qu'un cadre solide de gestion des risques technolagiques sait établi et maintenu ;
- veiller à ce que des contrôles internes efficaces et des pratiques de gestion des risques soient mis en œuvre pour assurer la sécurité, la fiabilité, la résilience des systèmes et la reprise des activités ;
- établir des politiques, des normes et des procédures informatiques, qui sont des composantes essentielles du cadre de gestion des risques technologiques. En raison des chongements rapides dans l'environnement et dans la sécurité informatique, les politiques, les normes et les procédures devraient être régulièrement revues et mises à jour ;
- mettre en œuvre des processus de conformité pour vérifier que les normes et procédures de sécurité informatique sont appliquées. Des processus de suivi devraient être mis en œuvre pour que les écarts de conformité soient connus et corrigés en temps opportun ;
- mettre en place un programme de sensibilisotion des employés à la sécurité informatique. Ce programme devrait être mis régulièrement ò jour pour s'assurer que son contenu reste pertinent, compte tenu de l'évolution de la technologie ainsi que des risques qui y sont associés ;
- procéder à un audit tri-annuel de son système d'information.

Article 15 : Politique de sécurité informatique

Le DC/BR élabore une politique de sécurité informatique adaptée à son activité et à son infrostructure informatique propre, conforme oux exigences de sécurité les plus répandus sur le marché et notamment la norme ISO 27001.

Cette politique doit être approuvée par le Canseil d'Administration du DC/BR et communiquée ò tous les utilisoteurs du Système d'Information (employé, prestatoire). Elle est octuolisée régulièrement, au moins tous les trois ans, pour tenir compte de l'évolution de l'environnement interne et externe.

Article 16 : Plan de Continuité d'Activités

Le DC/BR doit veiller à ce que son organisation, son système et ses procédures soient conçus pour maintenir leurs fonctions critiques ou les rétablir le plus rapidement possible ofin de remplir leurs obligations vis-à-vis de l'autorité de régulation et des usogers du morché.

A cet effet, l'éloboration d'un plan de continuité d'activités comprenant un plon de secours informatique est obligatoire. Le plon de continuité d'activités doit être approuvé par le Conseil d'Administration. Ce plan doit prévoir, entre autres, ou minimum les aspects ci-aprés :

- une identification des processus de l'entreprise ayant une importance stratégique, qui sont critiques et nécessaires à sa survie et une configuration minimale du système d'information capable de soutenir lesdits processus ;
- une évoluation des risques, des vulnérobilités et des impacts qui débouchera sur l'identification des ressources humaines indispensables, des données impartantes pour le DC/BR et l'efficience des contrôles d'atténuotion paur des risques existonts ;
- une définition de lo stratégie de continuité d'activités, incluant les critères de déclenchement du plan, un site de reprise avec sa description, une présentotion de l'équipe de crise avec les personnes outorisées à déclencher le plan, le délai acceptable de reprise des activités (RTO : Recovery Time Objective) et la quantité acceptable de perte de données (RPO : Recovery Point Objective) ;
- les programmes de formation et de sensibilisation du plon ;
- le pragramme de mise à jour et de test du plan de continuité.

Le DC/BR doit disposer d'un site de repli.

Le site de repli du DC/BR doit être établi dans au moins un outre État membre de l'UMOA afin d'atténuer le risque qu'un même sinistre touche les deux sites.

Le délai acceptoble de reprise complète des activités (RTO : Recovery Time Objective) après un désastre est de 24 heures.

La quantité acceptable de perte de données (RPO) est fixée à deux (02) heures de données.

Périodiquement et au moins une fois par an, le plan doit être testé afin de vérifier son efficacité.

L'exercice d'évaluation de l'efficacité du plan doit concerner, de façon non exhaustive, des aspects vérifiables : (i) la procédure d'alerte, (ii) le fonctionnement de la cellule de crise, (iii) les

procédures techniques de basculement en mode secours, (iv) la coordination des différentes parties prenantes, lors d'un exercice de réponse à un incident grave simulé, (v) la formation ciblée des personnels aux procédures techniques, (vi) le degré d'appropriation du plan par le personnel du DC/BR, (vii) les tests des éléments critiques du plan au moins une fois par an et (viii) les tests réguliers de la procédure de récupération des sauvegardes pour vérifier son adéquation aux besoins de l'organisation.

Le rapport du test doit indiquer les résultats du test, les points de faiblesses identifiés et un plan d'exécution pour corriger ces faiblesses.

Article 17 : Sauvegarde et restauration des données

Le DC/BR s'assure que sa politique de sécurité de l'information garantit l'intégrité des sauvegardes des données sur des supports appropriés, la réalisation de tests réguliers de restauration et la délocalisation des supports de sauvegarde sur un site distant.

Article 18 : Accès à l'infrastructure informatique

L'accès à l'infrastructure informatique du DC/BR doit s'appuyer sur des solutions d'authentification solides qui permettent, avec un degré d'assurance très élevé, de vérifier l'identité des utilisateurs. Le DC/BR doit utiliser à cet égard des passerelles contrôlées entre internet et son infrastructure informatique propre, telles que des firewalls, des proxys servers, des scanners antivirus et des scanners de contenu, ou d'autres solutions de sécurité similaires à jour. Il doit veiller à ce que ces passerelles soient correctement conçues, configurées et sécurisées, et à ce qu'elles fassent l'objet d'une gestion quotidienne professionnelle et d'un suivi rigoureux.

Article 19 : Gestion des incidents

Le DC/BR met en place un cadre de gestion des incidents de sécurité de l'information, afin de les traiter et de contenir leur impact. Il doit disposer d'une procédure de gestion des incidents validée par la Direction Générale, qui doit :

- préciser à quels types d'incidents elle s'applique ;
- établir les rôles et les responsabilités du personnel impliqué dans le processus de gestion des incidents ;
- définir une méthode de déclaration des incidents après leur détection ;
- préciser la priorité des incidents en fonction de l'urgence et de l'impact ;
- définir la stratégie d'attribution des incidents au personnel en charge de leurs résolutions en tenant compte des escalades ;
- permettre de suivre et de superviser la gestion des incidents (traçabilité de tout incident) afin de savoir à tout moment le niveau de résolution d'un incident et de clôturer les incidents résolus ;
- expliquer les tâches et responsabilités en matière de communication interne et externe quant aux incidents majeurs.

Un rapport d'incidents prenont en compte, l'état et l'impact de l'incident, les mesures de correction adoptées, les recommandotions et le plan de mise en œuvre doit être transmis annuellement, au mois de jonvier, à l'AMF-UMOA.

Enfin, tout incident mojeur doit être systématiquement communiqué à l'AMF-UMOA, dans un délai de 24 heures.

TITRE 4 : GESTION DES CHANGEMENTS

Article 20 : Maintenance des applications

Le DC/BR doit mettre en place un environnement formalisé de maintenance des applicatians. Celui-ci doit comporter un environnement de test (homologation) et d'un environnement de production. Ces deux environnements doivent être nettement séparés et permettre le processus de maintenance d'une application par les phases de correction, recette et validation avont mise en production.

Périadiquement, l'environnement d'homologation doit être mis à jour au niveau de sa configuration afin de répandre de manière efficiente et objective aux tests qui y seront effectués.

Article 21 : Processus de gestion des changements aux systèmes de production

Le DC/BR doit établir un processus de gestion des changements pour s'assurer que les modificotions apportées aux systèmes de production sont évaluées, approuvées, mises en œuvre et examinées de manière appropriée. Le processus de gestian des changements doit s'appliquer aux modifications relatives aux changements et mises à jour de logiciels, aux configurations systèmes et de sécurité.

Ce processus doit être régi par une procédure de gestion des chongements. Cette procédure validée par le Conseil d'Administration, doit inclure les principales étapes suivantes :

- l'initiation du changement ;
- l'analyse des risques et de l'impact du changement ;
- l'outorisation du changement ;
- la priorisation du changement ;
- les tests d'assurance qualité, tests d'acceptation utilisateurs (UAT) ;
- le plan de retour (rall-back plan) ;
- la décision de mise en production du changement ;
- la mise en production du changement en respectant les principes de séporation des tâches ;
- la documentation du changement, la formatian des utilisateurs et la diffusian des supports de formation aux utilisateurs ;
- suivi post-implémentotion du changement.

TITRE 5 : GESTION DES RISQUES LIES AU SYSTÈME D'INFORMATION

Article 22 : Processus de gestion des risques liés aux systèmes d'information

Dans le cadre de la gestion des risques inhérents aux systèmes d'information, le DC/BR met en place un dispositif permettant, de monière continue, d'identifier et d'évoluer les risques, en vue de les réduire ou de les gérer. Il élobore, à cet effet, sa stratégie de gestion des risques opprouvée par son Conseil d'Administration. Le DC/BR procède au fait procéder, le cas échéont, à ses frais, oux contrôles nécessoires à la sécurité des installations et autres motériels. Il odresse les procès-verbaux de ces contrôles à l'AMF-UMOA, à sa demande expresse. Le DC/BR met en œuvre les moyens humains et matériels nécessaires ò la sécurité et à la sûreté, pour l'exploitation des instollatians à sa disposition.

Article 23 : Protection contre les logiciels malveillants et le piratage informatique

Le DC/BR met en place des mesures de prévention, de détectian et de correction, afin de pratéger son système d'information contre des logiciels malveillants et le piratage informatique.

Lo Direction Générale du DC/BR devra intégrer dans son rapport annuel de gestion à l'attention du Conseil d'Administration une situation des incidents majeurs survenus durant la précédente année.

Article 24 : Sécurisation des réseaux, des terminaux et des informations

Le DC/BR prend des mesures de sécurité appropriées pour pratéger les infarmations qui transitent par son réseau, ainsi qu'à travers ses connexions avec les utilisateurs, les fournisseurs de données et l'AMF-UMOA. Il s'assure que les terminaux qui accèdent à son système dispose des autarisations nécessaires. En autre, il met en place le paramétrage adéquat, en vue de gérer les risques inhérents à la connexion d'utilisoteurs externes à son système d'information.

Article 25 : Gestion des identités et des accès logiques aux systèmes d'information

Le DC/BR s'assure que chaque utilisateur, faurnisseur de données ou membre de son personnel est identifié et authentifié avant taut accès aux systèmes d'informatian, et qu'il dispose des droits d'occès adéquots. Chaque action doit pouvoir être rattachée à son auteur.

Article 26 : Dispositif de sécurité physique et environnementale

Le DC/BR se dote d'un dispositif de gestion des accès physiques de son personnel et des tierces personnes à ses locaux sécurisés. Les locoux hébergeont son centre de données doivent être pourvus de dispositifs appropriés de protectian environnementale, notamment de détecteurs de fumée et d'eau, de systèmes d'extinction automatique d'incendie ainsi que de sondes de température.

Article 27 : Gestion des prestataires informatiques

Les prestataires informatiques jouent un rôle important dans la gestion des systèmes et des processus du DC/BR. Une sélection minutieuse et un contrôle des prestataires informatiques sont essentiels pour minimiser les risques de sécurité auxquels il pourrait être confrantée. Celle-ci doit mettre en œuvre des mesures pour répondre aux menaces de sécurité qui peuvent survenir au cours de ses relations avec les prestataires en utilisont une approche basée sur les risques. Pour faire face à ces menaces, et en vue de s'assurer du respect de la confidentialité, de la disponibilité et de l'intégrité des données, il devro utiliser les pratiques suivantes :

- effectuer une diligence raisonnable (due diligence) préolable ò la passation de controt avec les prestotaires pour des services éventuels. Cette diligence devra permettre de déterminer la viabilité, la fiabilité, les antécédents des prestataires ;
- veiller à ce que les conditions contractuelles régissant les râles, les relations, les obligations et les responsabilités des prestataires saient énoncées dans des accords écrits (contrat de niveau de service) qui précisent également les obligations oprès lo fin de la relation. Les exigences et les conditions couvertes par ces accords comprennent habituellement les objectifs de rendement, les niveaux de service, lo disponibilité, la fiabilité, l'évolutivité, la conformité, l'oudit, la sécurité ;
- mettre en œuvre des accords de non-divulgotion des informotions confidentielles appelés "Non-disclosure agreement (NDA)" avec les prestataires ;
- veiller ò ce que l'utilisotion de prestataires, l'externalisatian des systèmes informatiques, n'entraînent pas un affaiblissement au une dégradation des contrôles internes du DC/BR. Il doit exiger des prestataires de services qu'ils appliquent rigoureusement des procédures et contrôles de sécurité afin de protéger la confidentialité et la sécurité des informotions sensibles ou confidentielles telles que ses données finoncières et celles de ses clients ;
- effectuer un contrôle (évaluation des clauses définies dans les contrats de niveau de service) continu des prestataires de services afin d'évaluer l'odéquation et lo conformité des opérations et services qu'ils fournissent ;
- établir, maintenir et surveiller les droits et les octions des prestataires dans leurs systèmes ;
- établir et mettre en œuvre des procédures pour mettre fin à l'accès des prestataires de services aux systèmes dès la résiliation du contrat ;
- vérifier, la capacité du prestataire de services à récupérer les systèmes et les services informatiques externalisés en étant conformes aux délais acceptables de reprise des activités (RTO : Recavery Time Objective) avant de conclure tout accord avec les fournisseurs de services. Aussi, à la résiliotion du contrat, le DC/BR doit avoir le pauvoir contractuel et les moyens de retirer ou de détruire rapidement les données stockées dans les systèmes et les sauvegardes des prestataires de services.

TITRE 6 : PLATEFORME LOGICIELLE

Article 28 : Logiciel métier

Le DC/BR doit disposer de logiciels métier approuvés por l'AMF-UMOA et qui doivent être mis à jour conformément aux évolutions de l'environnement technologique et du morché.

Ces logiciels métier doivent être odoptés à ses activités réglementoires.

Article 29 : Fonctionnalités minimales du logiciel métier dédié

Le logiciel métier dédié au Dépositaire doit disposer des fonctionnalités minimales ci-après :

Tout logiciel dédié aux activités de dépositaire doit posséder les fonctionnalités minimales ci-après :

a) gestion des émetteurs de titres ;

b) codification des instruments financiers ;

c) gestion des adhérents ;

d) inscription en compte des clients finaux ;

e) gestion des portefeuilles-titres des adhérents ;

f) valorisation des titres ;

g) interface permettant un accès direct aux adhérents ;

h) gestion du règlement – livroison (identification du titre, quantité, montant, date de négociation, date de règlement, acheteur, vendeur) ;

i) le contrôle de provisions en titres et en espèces ;

j) génération des flux de données à destinatian de l'AMF-UMOA, selon le format requis ;

k) Édition des statistiques.

Article 30 : Dispositif de secours et de continuité

Pour la sécurisation de ses activités, le DC/BR doit :

- doter son logiciel métier d'un système de secours en vue de garantir la continuité du marché baursier ;
- organiser un système alternatif d'échanges d'informations entre son site central, son site de secours et les adhérents ;
- prévoir une clause contractuelle permettant le renouvellement ou la prorogation de la licence d'exploitation du logiciel métier par le Régulateur ou tout autre entité désignée par celui-ci en cas de cessation d'activité du DC/BR.

TITRE VII : DISPOSITIONS TRANSITOIRES ET FINALES

Article 31 : Dispositions transitoires

Le Dépositaire Central / Banque de Règlement dispose d'un délai maximum de deux (02) ans à compter de cette date pour se mettre en conformité avec les dispositions de la présente Instruction.

Article 32 : Publication et date d'entrée en vigueur

La présente Instruction, publiée partout où besoin sera, abroge toutes dispositions règlementaires antérieures contraires et entre en vigueur à compter de sa date de signature.

Fait à Abidjan, le 29 DEC. 2023

Pour l'Autorité des Marchés Financiers de l'UMOA

Le Président

Autorité des Marchés Financiers de l'Union Monétaire Ouest Africaine * Le Président 01 BPM 1878 ABIDJAN 01

Badanam PATOKI

BULLETIN OFFICIEL

OPCVM: FONDS COMMUNS DE PLACEMENT ET SOCIETES D'INVESTISSEMENT A CAPITAL VARIABLE

mercredi 20 mars 2024

Sociétés de gestion	Dépositaire	OPCVM	Catégorie	Valeur Liquidative							
				Origine	Précédente		Actuelle		Variation Origine		Variation Précédent
					Valeur	Date	Valeur	Date	Date	%	%
QUOTIDIENNES											
AFRICABOURSE ASSET MANAGEMENT	AFRICABOURSE SA	FCP AAM CAPITAL SUR	M	5 000	8 236,45	27/11/2023	ND	ND	10/10/2012	-	-
		FCP AAM EPARGNE CROISSANCE	D	5 000	8 240,19	07/03/2024	ND	ND	19/11/2012	-	-
		FCP AAM OBLIGATIS	OATC	5 000	8 469,60	07/03/2024	ND	ND	12/09/2012	-	-
		FCP AAM EPARGNE ACTION	A	5 000	5 579,03	07/03/2024	ND	ND	16/01/2017	-	-
AFRICAM SA	SBIF	FCP EXPANSIO	D	5 000	9 758,73	14/07/2023	ND	ND	01/01/2013	-	-
		FCP SECURITAS	OMLT	5 000	7 357,96	14/07/2023	ND	ND	01/01/2013	-	-
		FCP VALORIS	A	5 000	9 000,43	14/07/2023	ND	ND	01/01/2013	-	-
AFRICAINE DE GESTION D'ACTIFS	SGI AGI	FCP CAPITAL PLUS	D	1 000	1 329,96	18/03/2024	1 327,87	19/03/2024	11/03/2019	32,79%	-0,16%
		FCP CONFORT PLUS	OMLT	1000	1 336,25	18/03/2024	1 334,77	19/03/2024	11/03/19	33,48%	-0,111%
ATLANTIC ASSET MANAGEMENT	ATLANTIQUE FINANCE	FCP ATLANTIQUE CROISSANCE	D	5 000	5 254,09	14/03/2024	ND	ND	30/05/2015	-	-
		FCP ATLANTIQUE LIQUIDITE	OCT	5 000	6 233,19	14/03/2024	ND	ND	12/07/2019	-	-
		FCP ATLANTIQUE ACTIONS	A	5 000	8 160,48	14/03/2024	ND	ND	25/10/2019	-	-
		FCP ATLANTIQUE SERENITE	OMLT	5 000	6 508,95	14/03/2024	ND	ND	12/07/2019	-	-
		FCP ATLANTIQUE HORIZON	D	5 000	7 794,41	14/03/2024	ND	ND	25/10/2019	-	-
		FCP ATLANTIQUE SECURITE	OMLT	5 000	6 918,07	14/03/2024	ND	ND	30/05/2015	-	-
BNI GESTION	BNI FINANCES	FCP CAPITAL CROISSANCE	D	10 000	ND	17/08/2023	ND	18/08/2023			
		OBLIG SECURITE	OMLT	10 000	9 930,44	18/08/2023	ND	ND	06/06/2014	-	-
		FCP DYNAMIC SAVINGS	A	10 000	ND	17/08/2023	ND	18/08/2023			
BOA ASSET MANAGEMENT	BOA CAPITAL SECURITIES	FCP Emergence	D	5 000	7 486,17	18/03/2024	ND	ND	Fev.2010	-	-
		FCP Treso Monea	OCT	25 000 000	38 678 589,76	23/10/2023	ND	ND	Dec. 2013	-	-
BRM ASSET MANAGEMENT	BRM	FCP "BRM DYNAMIQUE"	D	10 000	12 923,13	08/09/2014	ND	ND	12/03/2009	-	-
		FCP "BRM OBLIGATAIRE"	D	10 000	12 057,50	17/10/2014	ND	ND	12/03/2009	-	-
CGF GESTION	CGF BOURSE	FCP ACTIONS PHARMACIE	D	1000	1 041,17	18/03/2024	1 041,36	19/03/2024	25/07/14	4,14%	0,02%
		FCP AL BARAKA	D	1000	1 014,65	18/03/2024	1 014,33	19/03/2024	01/03/17	1,43%	-0,03%
		FCP AL BARAKA 2	D	1000	1 171,53	18/03/2024	1 171,80	19/03/2024	25/01/18	17,18%	0,02%
		FCP ASSUR SENEGAL	D	1000000	1 215 333,46	18/03/2024	1 215 914,36	19/03/2024	06/07/14	21,59%	0,05%
		FCP PLACEMENT AVANTAGE	D	1000	1 562,84	18/03/2024	1 563,13	19/03/2024	29/03/13	56,31%	0,02%
		FCP PLACEMENT CROISSANCE	A	1000	1 256,53	18/03/2024	1 258,41	19/03/2024	29/03/13	25,84%	0,15%
		FCP POSTEFINANCES HORIZON	D	1000	1 880,87	18/03/2024	1 888,43	19/03/2024	27/06/09	88,84%	0,40%
		FCP PLACEMENT QUIETUDE	O	1000	1 588,44	18/03/2024	1 588,79	19/03/2024	29/03/13	58,88%	0,02%
		FCP LIQUIDITE-OPTIMUM	D	10000	12 189,14	18/03/2024	12 191,44	19/03/2024	01/10/17	21,91%	0,019%
		FCP BNDE VALEURS	D	1000	1 165,24	18/03/2024	1 165,18	19/03/2024	02/09/16	16,52%	-0,005%
CORIS ASSET MANAGEMENT	CORIS BOURSE	FCP CORIS ACTIONS	A	5 000	6 973,65	18/03/2024	ND	ND	11/11/2014	-	-
		FCP ASSURANCES	OCT	5 000	5 702,89	18/03/2024	ND	ND	22/11/2019	-	-
		FCP CORIS PERFORMANCE	D	5 000	7 372,82	18/03/2024	ND	ND	11/11/2014	-	-
NSIA AM	UBA CI	NSIA FONDS DIVERSIFIE	D	5 000	5 820,89	18/03/2024	5 818,25	19/03/2024	03/12/2018	16,37%	-0,05%
		AURORE OPPORTUNITES	A	5 000	6 078,10	18/03/2024	6 076,22	19/03/2024	08/03/2019	21,52%	-0,03%
	NSIA BANQUE CI	AURORE SECURITE	OMLT	5 000	5 772,52	18/03/2024	5 770,69	19/03/2024	03/09/2021	15,41%	-0,03%
		NSIA ASSURANCES OPTIMUM	D	1 000 000	1 028 328,21	18/03/2024	1 028 430,46	19/03/2024	30/09/2021	2,84%	0,01%
OAM S.A	SGI TOGO	FCP-1 OPTI PLACEMENT	A	5 000	15 630,38	18/03/2024	15 740,00	19/03/2024	01/02/2002	214,80%	0,70%
		FCP-2 OPTI REVENU	OMLT	5 000	8 645,58	18/03/2024	8 656,25	19/03/2024	01/02/2002	73,13%	0,12%
		FCP-3 OPTI CAPITAL	D	5 000	19 645,58	18/03/2024	19 743,53	19/03/2024	24/01/2003	294,87%	0,50%
SOGESPAR	SOGEBOURSE	FCP SOGEAVENIR	D	500	1 670,00	11/03/2024	ND	ND	01/10/2002	-	-
		FCP SOGEDEFI	D	4 888	3 885,00	11/03/2024	ND	ND	23/12/2014	-	-
		FCP SOGEDYNAMIQUE	A	4 888	3 883,00	11/03/2024	ND	ND	23/12/2014	-	-
		FCP SOGELIQUID	M	10 000 000	10 862 617,00	11/03/2024	ND	ND	16/06/2020	-	-
		FCP SOGEPRIVILEGE	D	4 888	4 094,00	11/03/2024	ND	ND	23/12/2014	-	-
		FCP SOGESECURITE	OMLT	4 888	5 124,00	11/03/2024	ND	ND	23/12/2014	-	-
		FCP SOGEVALOR	A	1 000	3 531,00	11/03/2024	ND	ND	04/06/2002	-	-
SOAGA-SA	SGI-BOA CAPITAL SECURITIES	FCP SOAGA EPARGNE ACTIVE	D	10 000	10 878,25	18/03/2024	10 949,50	19/03/2024	28/10/2016	9,49%	0,65%
		SICAV Abdou DIOUF	D	10 000 000	14 626 005,31	18/03/2024	14 620 838,63	19/03/2024	01/12/2003	46,21%	-0,04%
		FCP BOAD CAPITAL RETRAITE	OMLT	10 000	13 030,91	18/03/2024	13 032,54	19/03/2024	08/07/2020	30,33%	0,01%
		FCP SOAGA EPARGNE OBLIGATIONS	OMLT	5 000	5 854,60	18/03/2024	5 844,98	19/03/2024	28/04/2021	16,90%	-0,16%
		FCP SOAGA EPARGNE ACTIONS	A	5 000	8 782,18	18/03/2024	8 814,17	19/03/2024	11/03/2020	76,28%	0,36%
		FCP SOAGA EPARGNE SERENITE	OMLT	10 000	15 121,00	18/03/2024	15 047,25	19/03/2024	28/10/2016	50,47%	-0,49%
BRIDGE ASSET MANAGEMENT	BRIDGE SECURITIES	FCP BRIDGE EQUILIBRE	D	25 000 000	31 010 704,77	11/03/2024	ND	ND	27/09/2017	-	-
	BRIDGE SECURITIES	FCP BRIDGE DIVERSIFIE CROISSANCE	D	5 000	6 052,86	11/03/2024	ND	ND	13/03/2018	-	-
	BRIDGE SECURITIES	FCP BRIDGE OBLIGATIONS	OMLT	5 000	6 235,65	11/03/2024	ND	ND	01/10/2019	-	-
ENKO CAPITAL WEST AFRICA	SOCIETE GENERALE COTE	FCP ENKO CAPITAL GARANTI	D	10 000	16 139,05	18/03/2024	16 144,71	19/03/2024	21/09/2020	61,45%	0,04%
		FCP PATRIMOINE	OMLT	10 000	12 263,20	18/03/2024	12 264,66	19/03/2024	18/10/2020	22,65%	0,01%
		FCP ENKO CAPITAL OBLIGATIONS	OMLT	10 000	11 474,89	18/03/2024	11 476,36	19/03/2024	16/03/2021	14,76%	0,01%
SAPHIR ASSET MANAGEMENT	SGI BENIN	FCP SAPHIR DYNAMIQUE	D	5 000	5 907,97	18/03/2024	ND	ND	28/08/2017	-	-
		FCP SAPHIR QUIETUDE	OMLT	5 000	6 211,09	18/03/2024	ND	ND	28/08/2017	-	-
WAFI CAPITAL S.A.	SGI AGI BENIN	SICAV WAFI CAPITAL	D	10 000	8 466,83	19/09/2022	ND	ND	05/06/2020	-	-
SGO MALI FINANCES	SGI MALI SA	FCP NYESIGUI	D	10 000	12 499,89	12/03/2024	ND	ND	01/07/2018	-	-
HEBDOMADAIRES											
BNI GESTION	BNI FINANCES	FCP INITIATIVES SOLIDARITE	D	5 000	5 062,52	30/06/2023	5 194,30	31/07/2023	22/05/2013	3,89%	2,60%
		FCPE SODEFOR	D	2 500	7 065,16	30/06/2023	6 959,13	31/07/2023	18/12/2009	178,37%	-1,50%
PhoenixAfrica Asset Management	Phoenix Capital Management	FCP PAM ACTIONS	A	10 000	13 403,33	05/02/2024	13 582,60	22/02/2024	13/12/2017	35,83%	1,34%
		FCP PAM DIVERSIFIE EQUILIBRE	D	10 000	14 183,99	05/02/2024	14 273,58	22/02/2024	13/12/2017	42,74%	0,63%
		FCP PAM DIVERSIFIE OBLIGATIONS	D	10 000	13 017,56	05/02/2024	13 073,30	22/02/2024	13/12/2017	30,73%	0,43%
BOA ASSET MANAGEMENT	BOA CAPITAL SECURITIES	FCP Global Investors	D	25 000	31 315,37	08/03/2024	31 238,63	15/03/2024	Dec. 2012	24,95%	-0,25%
		FCP Boa Obligations	OMLT	10 000	12 695,95	08/03/2024	12 708,16	15/03/2024	Mars. 2017	27,08%	0,10%
		FCP Boa Sécurité	OMLT	100 000	112 963,83	05/03/2024	113 113,12	12/03/2024	Mai. 2021	13,11%	0,13%
		FCP Boa Actions	A	10 000	13 048,29	08/03/2024	13 001,95	15/03/2024	Juil. 2017	30,02%	-0,36%
		FCP Boa Rendement	OMLT	25 000 000	35 811 638,35	08/03/2024	35 844 460,65	15/03/2024	Dec. 2017	43,38%	0,09%
NSIA AM	UBA CI	EVOLUTIS	D	5 000	4 394,76	08/03/2024	4 322,21	15/03/2024	16/12/2019	-13,56%	-1,65%
BAOBAB ASSET MANAGEMENT	FGI	FCP BAM TRESOR	OCT	10 000	10 182,23	07/03/2024	10 192,71	14/03/2024	21/12/2023	1,93%	0,10%
BRM ASSET MANAGEMENT	IMPAXIS	FCP "SDE"	D	1 000	2 083,36	05/09/2014	ND	ND	14/03/2011	-	-
CGF GESTION	CGF BOURSE	FCPCR SONATEL	D	1 000	7 842,97	08/03/2024	7 843,21	15/03/2024	19/02/2004	684,32%	0,00%
	IMPAXIS SECURITIES	FCPE FORCE PAD	D	1 000	1 912,90	07/03/2024	1 916,22	14/03/2024	16/02/2014	91,62%	0,17%
	CGF BOURSE	FCPE SINI GNESIGUI	D	1 000	1 585,46	13/03/2024	1 592,06	20/03/2024	25/02/2014	59,21%	0,42%
	CGF BOURSE	FCP EXPAT	D	1 000	1 117,64	07/03/2024	1 118,48	14/03/2024	20/03/2019	11,85%	0,08%
	CGF BOURSE	FCP CAPITAL RETRAITE	D	1 000	1 136,12	13/03/2024	1 136,12	20/03/2024	20/03/2019	13,61%	0,00%
	CGF BOURSE	FCP RENTE PERPETUELLE	D	1 000	1 098,52	13/03/2024	1 098,35	20/03/2024	20/03/2019	9,84%	-0,02%
	CGF BOURSE	FCP WALO	A	1 000	1 087,42	22/03/2021	1 091,92	29/03/2021	26/03/2019	9,19%	0,41%
	CGF BOURSE	FCP DJOLOF	O	1 000	1 217,98	12/03/2024	1 218,49	19/03/2024	26/03/2019	21,85%	0,04%
	CGF BOURSE	FCP DIASPORA	D	1 000	1 185,97	12/03/2024	1 185,75	19/03/2024	19/03/2019	18,58%	-0,02%
	CGF BOURSE	FCP IFC-BOAD	O	100 000	134 637,40	11/03/2024	134 741,24	18/03/2024	01/01/2018	34,74%	0,08%
	CGF BOURSE	FCPE DP WORLD DAKAR	D	1 000	1 282,31	12/03/2024	1 282,53	19/03/2024	04/10/2016	28,25%	0,02%
EDC Asset Management	EDC Investment Corporation	FCP ECOBANK UEMOA DIVERSIFIE	D	5 000	7 959,00	28/02/2024	7 931,00	06/03/2024	19/09/2007	59,82%	59,82%
		FCP ECOBANK UEMOA OBLIGATAIRE	OMLT	20 000	20 730,00	28/02/2024	20 729,00	06/03/2024	01/01/2018	66,90%	66,90%
		FCP ECOBANK UEMOA RENDEMENT	OMLT	1 000 000	1 657 109,00	28/02/2024	1 651 295,00	06/03/2024	10/10/2007	65,13%	65,13%
		FCP ECOBANK ACTIONS UEMOA	A	5 000	3 996,00	28/02/2024	3 964,00	06/03/2024	20/04/2016	-16,31%	-16,31%
SGO MALI FINANCES	SGI MALI SA	FCPE ORANGE MALI	D	10 000	30 857,57	28/02/2024	30 912,43	06/03/2024	03/09/2012	209,12%	0,18%
SGO MALI FINANCES	SGI MALI SA	FCP TOUNKARANKE	OMLT	100 000	117 228,48	28/02/2024	117 198,19	06/03/2024	01/07/2018	17,198%	-0,026%
ATTIJARI ASSET MANAGEMENT	SGI AFRICAINE DE BOURSE	ATTIJARI OBLIG	OMLT	10000	13650,98	05/01/2024	13661,01	12/01/2024	13/07/2012	36,61%	0,07%
		ATTIJARI LIQUIDITE	OCT	10000	13973,65	05/01/2024	13985,68	12/01/2024	30/08/2013	39,86%	0,09%
		ATTIJARI HORIZON	OMLT	10000	15372,43	05/01/2024	15383,22	12/01/2024	30/08/2013	53,83%	0,07%
		ATTIJARI ACTIONS	A	10000	14732,06	05/01/2024	14679,3	12/01/2024	21/05/2015	46,79%	-0,36%
		ATTIJARI DIVERSIFIE	D	10000	16248,15	05/01/2024	16198,2	12/01/2024	21/05/2015	61,98%	-0,31%
		ATTIJARI INVEST	OMLT	10000	14490,28	05/01/2024	14501,96	12/01/2024	21/01/2016	45,02%	0,08%
		ATTIJARI PATRIMOINE	OMLT	10000	14685,13	05/01/2024	14 696,65	12/01/2024	21/01/2016	46,97%	0,08%
MENSUELLES											
BNI GESTION	BNI FINANCES	FCPE CNRA	D	2 500	3 263,98	30/06/2023	3 275,58	31/07/2023	06/06/2014	31,02%	0,36%
		FCPE BNI RETRAITE	D	2 500	4 198,14	30/06/2023	4 256,60	31/07/2023	06/06/2014	70,26%	1,39%
		FCP KARIMA ETHIQUE	D	1 000	1 890,07	30/06/2023	1 939,95	31/07/2023	22/05/2013	94,00%	2,64%

OPCVM : Organisme de Placement Collectif en Valeurs Mobilières
ND: Non Disponible
Catégories:
A: actions
OCT: obligations à court terme
OMLT: obligations à moyen et long terme
C: contractuels