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