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