Union Monétaire Ouest Africaine

CREPMF

Conseil Régional de l'Epargne Publique
et des Marchés Financiers

CIRCULAIRE N° 01./2019

RELATIVE AUX EXIGENCES FONCTIONNELLES MINIMALES DES LOGICIELS DE GESTION AINSI QU'A LA SECURITE DU SYSTEME D'INFORMATION DES SOCIETES DE GESTION ET D'INTERMEDIATION (SGI), DES BANQUES TENEURS DE COMPTES CONSERVATEURS (BTCC), DES SOCIETES DE GESTION D'ORGANISMES DE PLACEMENT COLLECTIF (SGO) ET DES SOCIETES DE GESTION DE FONDS COMMUNS DE TITRISATION DE CREANCES (SG-FCTC)

Le Secrétariat Général du Conseil Régional de l'Épargne Publique et des Marchés Financiers (CREPMF), porte à la connaissance des Sociétés de Gestion et d'Intermédiation (SGI), des Banques Teneurs de Comptes / Conservateurs (BTCC), des Sociétés de Gestion d'OPCVM (SGO) et des Sociétés de Gestion de Fonds Communs de Titrisation de Créances (SG-FCTC), qu'en application des dispositions de l'article 27 du Règlement Général relatif à l'organisation, au fonctionnement et au contrôle du Marché Financier Régional de l'UMOA, elles doivent se conformer aux dispositions du cahier de charges du Système d'Information joint en annexe de la présente circulaire.

Par ailleurs, il est rappelé aux SGI, aux BTCC, aux SGO et SG-FCTC que tout changement de logiciel de gestion métier doit faire l'objet d'une approbation préalable du Conseil Régional.

La présente Circulaire prend effet à compter de sa date de publication.

Fait à Abidjan, le 21 MAI 2019

Le Président

Mamadou NDIAYE

Conseil Régional de l'Epargne Publique et des Marchés Financiers
Le Président
01 B.P. 1878
ABIDJAN 01

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org

TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

CAHIER DE CHARGES DU SYSTEME D'INFORMATION DES SOCIETES DE GESTION ET D'INTERMEDIATION (SGI), DES BANQUES TENEURS DE COMPTES / CONSERVATEURS (BTCC), DES SOCIETES DE GESTION D'ORGANISMES DE PLACEMENT COLLECTIF (SGO) ET DES SOCIETES DE GESTION DE FONDS COMMUNS DE TITRISATION DE CREANCES (SG-FCTC)

Le présent cahier de charges a pour objet de définir les exigences fonctionnelles minimales des logiciels de gestion métier ainsi que la sécurité du Système d'Information des Sociétés de Gestion et d'Intermédiation (SGI), des Banques Teneurs de Comptes / Conservateurs (BTCC), des Sociétés de Gestion d'OPCVM et de FCTC.

SECTION I : DEFINITIONS

Article 1er : Définitions

On entend par :

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.
Logiciel de gestion métier	:	Logiciel utilisé par la SGI, la BTCC, la SGO ou la SG-FCTC pour la gestion des processus métiers (production, logistique, comptabilité, RH,...) de façon automatique.
Piste d'audit	:	Enregistrement chronologique 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.
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.
Profil utilisateur	:	Description d'un utilisateur montrant les droits dont il bénéficie dans le logiciel.
Protocole FIX	:	FIX (Financial Information Exchange) est un standard de messages développé dans le but de faciliter les échanges d'informations relatives aux transactions boursières.
RPO (Recovery Point Objective)	:	Le RPO quantifie les données qu'un Système d'Information peut être amené à 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.
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.

SECTION II : SPECIFICATIONS DES LOGICIELS DE GESTION METIER DES SGI, DES BTCC, DES SGO ET DES SG-FCTC

Article 2 : Spécifications des logiciels de gestion métier des SGI

Les spécifications minimales pour les logiciels de gestion métier des SGI sont énumérées ci-après :

2.1 Gestion de la clientèle

- ✓ Création, modification, consultation, activation/désactivation des clients ;
- ✓ Fiche client (nom, prénom, date de naissance, lieu de naissance, pays, ville, nationalité, profession, adresse, téléphone, email, type de la pièce d'identité, numéro de la pièce, date de délivrance, date d'expiration, lieu de délivrance, photo,...) ;
- ✓ Profil du client ;
- ✓ Historique de la modification des informations sur les clients ;
- ✓ Statut du client (activé, non activé, désactivé) ;
- ✓ Edition de la fiche LAB (Lutte Anti Blanchiment des Capitaux) ou KYC (Know Your Customer).

2.2 Gestion des comptes clients

- ✓ Création, modification, désactivation (clôture) des comptes-titres clients ;
- ✓ Création, modification, désactivation (clôture) des comptes-espèces clients ;
- ✓ Historique de la modification des informations sur les comptes clients ;
- ✓ Enregistrement des mouvements sur les comptes-titres et espèces avec les références des justificatifs ;
- ✓ Consultation et édition du portefeuille-titres (en volume et en valeur) à toute date (antérieure ou non) ;
- ✓ Consultation du relevé des mouvements des comptes-espèces de la clientèle ;
- ✓ Consultation du relevé des mouvements des comptes-titres de la clientèle ;
- ✓ Statut des comptes (comptes actifs, non actifs, dormants, désactivés) ;
- ✓ Edition des informations relatives à la gestion des comptes.

2.3 Gestion des titres

- ✓ Ajout, modification, désactivation des titres ;
- ✓ Gestion du changement de symbole des titres (notamment suite à la cotation d'une valeur) ;
- ✓ Enregistrement des tableaux d'amortissement des titres de créances ;
- ✓ Gestion des échéances de remboursement ou de paiement des coupons.

2.4 Mise à jour des cours

Mise à jour manuelle ou automatique par importation de fichiers.

2.5 Gestion du portefeuille

- ✓ Paramétrage du profil d'investissement ;
- ✓ Suivi des investissements suivant les profils risques des clients ;
- ✓ Valorisation du portefeuille ;
- ✓ Ajout, modification, annulation des blocages ;
- ✓ Gestion de la tarification ;
- ✓ Suivi des soldes après blocage des opérations en attente ;
- ✓ Edition de rapport de gestion.

2.6 Gestion des transactions sur titres

- ✓ Traitement des souscriptions ;
- ✓ Centralisation et allocation des souscriptions de titres ;
- ✓ Saisie (ajout, modification, annulation) des ordres d'achat et de vente ;
- ✓ Réception des ordres transmis par support électronique (internet, etc.) ;
- ✓ Horodatage ;
- ✓ Consultation de l'historique des modifications des informations concernant les ordres ;
- ✓ Importation des exécutions ;
- ✓ Edition du carnet d'ordres à exécuter ;
- ✓ Affectation des transactions ;
- ✓ Traitement du règlement/livraison des titres ;
- ✓ Gestion des suspens.

2.7 Gestion des opérations sur espèces

- ✓ Opérations de caisse (versement, retrait, transfert, ...) ;
- ✓ Blocage des espèces ;
- ✓ Retrait ou dépôt d'espèces, avec impression de reçus et affectation des fonds au client ;
- ✓ Transferts d'espèces de comptes à comptes ;
- ✓ Reporting (journal des opérations, requêtes par montant, nature (chèques, espèces) ;
- ✓ Edition des reçus de caisse.

2.8 Gestion des rapprochements

- ✓ Edition de l'état de solde des comptes titres (par numéros de compte dépositaire) ;
- ✓ Gestion de divers rapprochements ;
- ✓ États de rapprochement.

2.9 Gestion des opérations sur titres (OST)

- ✓ Traitement des Évènements sur Valeurs (ESV) ;
- ✓ Suivi des échéanciers des titres de créances ;
- ✓ Augmentation de capital ;
- ✓ Division de nominal ;
- ✓ Regroupement d'actions ;
- ✓ Fusion absorption de titres.

2.10 Gestion des reportings

- ✓ Génération et édition de la liasse (carnet d'ordres avant et après exécution, avis d'opéré, rapport des exécutions, journal des transactions) ;
- ✓ Journal des opérations (requêtes par montant, nature, ...).

2.11 Gestion de la comptabilité

- ✓ Paramétrage du plan comptable ;
- ✓ Paramétrage des opérations et des journaux ;
- ✓ Ouverture et clôture d'exercice ;
- ✓ Edition des journaux comptables ;
- ✓ Edition de la balance générale (à six colonnes au moins) et du grand livre ;
- ✓ Edition des états financiers.

Si le logiciel de la SGI n'intègre pas un module de comptabilité, il devra avoir une interface entre ce logiciel et le logiciel de gestion de la comptabilité, afin de réduire les opérations manuelles de déversement des écritures.

Article 3 : Spécifications des logiciels de gestion métier des BTCC

Les spécifications minimales pour les logiciels de gestion métier des BTCC sont énumérées ci-après :

3.1 Gestion de la clientèle

- ✓ Création, modification, consultation, activation/désactivation des clients ;
- ✓ Fiche client (nom, prénom, date de naissance, lieu de naissance, pays, ville, nationalité, profession, adresse, téléphone, email, type de la pièce d'identité, numéro de la pièce, date de délivrance, date d'expiration, lieu de délivrance, photo, ...) ;
- ✓ Profil du client ;
- ✓ Historique de la modification des informations sur les clients ;
- ✓ Statut du client (activé, non activé, désactivé) ;

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

- ✓ Edition de la fiche LAB (Lutte Anti Blanchiment des Capitaux) ou KYC (Know Your Customer).

3.2 Gestion des comptes clients

- ✓ Création, modification, désactivation (clôture) des comptes-titres clients ;
- ✓ Création, modification, désactivation (clôture) des comptes-espèces clients ;
- ✓ Historique de la modification des informations sur les comptes clients ;
- ✓ Enregistrement des mouvements sur les comptes titres et espèces avec les références des justificatifs ;
- ✓ Consultation et édition du portefeuille-titres (en volume et en valeur) à toute date (antérieure ou non) ;
- ✓ Consultation du relevé des mouvements des comptes espèces de la clientèle ;
- ✓ Consultation du relevé des mouvements des comptes de titres de la clientèle ;
- ✓ Statut des comptes (comptes actifs, non actifs, dormants, désactivés) ;
- ✓ Edition des informations relatives à la gestion des comptes.

3.3 Gestion des titres

- ✓ Ajout, modification, désactivation des titres ;
- ✓ Gestion du changement de symbole des titres (notamment suite à la cotation d'une valeur) ;
- ✓ Enregistrement des tableaux d'amortissement des titres de créances ;
- ✓ Gestion des échéances de remboursement ou de paiement des coupons.

3.4 Mise à jour des cours

- ✓ Mise à jour manuelle ou automatique par importation de fichiers.

3.5 Suivi du portefeuille

- ✓ Paramétrage du profil d'investissement ;
- ✓ Suivi des investissements suivant les profils risques des clients ;
- ✓ Valorisation du portefeuille ;
- ✓ Ajout, modification, annulation des blocages ;
- ✓ Gestion de la tarification ;
- ✓ Suivi des soldes après blocage des opérations en attente ;
- ✓ Edition de rapport de gestion.

3.6 Gestion des transactions sur titres

- ✓ Affectation des transactions ;
- ✓ Traitement du règlement/livraison des titres ;
- ✓ Gestion des suspens.

3.7 Gestion des opérations sur espèces relatives aux comptes dédiés aux opérations sur titres

- ✓ Opérations de caisse (versement, retrait, transfert, ...) ;

- ✓ Blocage des espèces ;
- ✓ Retrait ou dépôt d'espèces, avec impression de reçus et affectation des fonds au client ;
- ✓ Transferts d'espèces de comptes à comptes ;
- ✓ Reporting (journal des opérations, requêtes par montant, nature (chèques, espèces)) ;
- ✓ Edition des reçus de caisse.

3.8 Gestion des rapprochements

- ✓ Edition de l'état de solde des comptes titres (par numéros de compte dépositaire) ;
- ✓ Gestion de divers rapprochements ;
- ✓ États de rapprochement.

3.9 Gestion des opérations sur titres (OST)

- ✓ Traitement des Évènements sur Valeurs Évènements (ESV) ;
- ✓ Suivi des échéanciers des titres de créances ;
- ✓ Augmentation de capital ;
- ✓ Division de nominal ;
- ✓ Regroupement d'actions ;
- ✓ Fusion absorption de titres.

3.10 Gestion des reportings

- ✓ Génération et édition de la liasse (carnet d'ordres avant et après exécution, avis d'opéré, rapport des exécutions, journal des transactions) ;
- ✓ Journal des opérations (requêtes par montant, nature, ...).

3.11 Gestion de la comptabilité

- ✓ Paramétrage du plan comptable ;
- ✓ Paramétrage des opérations et des journaux ;
- ✓ Ouverture et clôture d'exercice ;
- ✓ Edition des journaux comptables ;
- ✓ Edition de la balance générale (à six colonnes au moins) et du grand livre ;
- ✓ Edition des états financiers.

Si le logiciel de la BTCC n'intègre pas un module de comptabilité, il devra avoir une interface entre ce logiciel et le logiciel de gestion de la comptabilité, afin de réduire les opérations manuelles de déversement des écritures.

Article 4 : Spécifications des logiciels de gestion métier des SGO

Les spécifications minimales pour les logiciels de gestion métier des SGO sont énumérées ci-après :

4.1 Gestion de la clientèle

- ✓ Création, modification, consultation, activation/désactivation des clients ;

- ✓ Fiche de renseignement client personne physique ou morale ;
- ✓ Historique de la modification des informations sur les clients ;
- ✓ Statut du client (activé, non activé, désactivé) ;
- ✓ Edition de la fiche LAB (Lutte Anti Blanchiment des Capitaux) ou KYC (Know Your Customer).

4.2 Gestion des comptes des porteurs de parts et des actionnaires

- ✓ Création, modification, désactivation (clôture) des comptes-parts ou actions et espèces des clients ;
- ✓ Historique de la modification des informations sur les comptes clients ;
- ✓ Consultation et édition du portefeuille parts ou actions à toute date (antérieure ou non) ;
- ✓ Consultation du relevé des mouvements des comptes-espèces de la clientèle ;
- ✓ Consultation du relevé des mouvements comptes des parts ou actions de la clientèle ;
- ✓ Statut des comptes (activés, non activés, désactivé) ;
- ✓ Edition des informations relatives à la gestion des comptes ;
- ✓ Dépôt et retrait d'espèces des porteurs parts ou actionnaires ;
- ✓ Traitement des souscriptions / rachats en Valeur Liquidative (VL) connue et inconnue ;
- ✓ Edition du registre des actionnaires ou des porteurs de parts ;
- ✓ Enregistrement des souscriptions et des rachats ;
- ✓ Traitement des distributions de dividendes aux porteurs de parts ou actionnaires.

4.3 Gestion de l'actif

- ✓ Création de titres : actions, obligations avec tableau d'amortissement (amortissement sur titre, sur capital, annuité constante, in fine) et bons du trésor ;
- ✓ Achat et vente de titres ;
- ✓ Consultation des mouvements sur les titres ;
- ✓ Valorisation du portefeuille-titres et calcul des différences d'estimation et des intérêts courus et précomptés ;
- ✓ Traitement des Évènements Sur Valeurs (ESV) ;
- ✓ Edition de portefeuilles ;
- ✓ Edition des états relatifs aux normes de gestion (règles de classification et d'allocation d'actifs, orientation de gestion, etc.) ;
- ✓ Calcul sur une base quotidienne des commissions et frais (valorisation, garde, de gestion, etc.) assis sur l'actif ou l'actif net ou la valorisation du portefeuille-titres.

4.4 Gestion de la trésorerie de l'OPCVM

- ✓ Approvisionnement et retrait sur les comptes-espèces domiciliés chez le dépositaire ;
- ✓ Enregistrement et suivi des dépôts à terme (DAT) ;
- ✓ Calcul des intérêts courus sur les comptes financiers (DAT, dépôt à vue rémunéré, etc.) à chaque calcul de la VL.

4.5 Gestion des Opérations sur titres en portefeuille

- ✓ Augmentation de capital ;
- ✓ Division de nominal ;
- ✓ Regroupement d'actions ;
- ✓ Assimilation de titres et de fusion absorption de titres.

4.6 Gestion de la tarification

- ✓ Paramétrage des taux à facturer pour les différentes commissions (courtage, gestion, dépositaire, droit d'entrée et de sortie, ...).

4.7 Gestion de la comptabilité

- ✓ Paramétrage du plan comptable ;
- ✓ Paramétrage des opérations et des journaux ;
- ✓ Ouverture et clôture d'exercice ;
- ✓ Paramétrage de la Valeur Liquidative (VL) ;
- ✓ Annulation, validation de la VL ;
- ✓ Edition du journal ;
- ✓ Edition de la balance générale (à six colonnes au moins) et du grand livre ;
- ✓ Edition des états financiers.

Si le logiciel de la SGO n'intègre pas un module de comptabilité, il devra avoir une interface entre ce logiciel et le logiciel de gestion de la comptabilité, afin de réduire les opérations manuelle de déversement des écritures.

Article 5 : Spécifications des logiciels de gestion métier des SG-FCTC

Les spécifications minimales pour les logiciels de gestion métier des SG-FCTC sont énumérées ci-après :

5.1 Gestion des porteurs de titres

- ✓ Création, modification, consultation activation/désactivation des porteurs de titres ;
- ✓ Fiche de renseignement des porteurs de titres (personne physique ou morale) ;
- ✓ Historique de la modification des informations sur les porteurs de titres ;
- ✓ Statut du porteur de titres (activé, non activé, désactivé) ;

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

- ✓ Edition de la fiche LAB (Lutte Anti Blanchiment des Capitaux) ou KYC (Know Your Customer).

5.2 Gestion des comptes des porteurs de parts et des actionnaires

- ✓ Création, modification, désactivation (clôture) des comptes-parts et espèces des porteurs de titres ;
- ✓ Historique de la modification des informations sur les comptes des porteurs de titres ;
- ✓ Consultation et édition du portefeuille parts ou titres de créance à toute date (antérieure ou non) ;
- ✓ Consultation du relevé des mouvements des comptes des porteurs de titres ;
- ✓ Statut des comptes (activés, non activés, désactivé) ;
- ✓ Edition des informations relatives à la gestion des comptes ;
- ✓ Enregistrement des souscriptions ;
- ✓ Traitement des distributions aux porteurs de titres.

5.3 Gestion des compartiments

- ✓ Création et paramétrage des compartiments.

5.4 Sélection de Pool de créances

- ✓ Chargement des créances à titriser ;
- ✓ Paramétrage des critères d'éligibilité ;
- ✓ Simulation des flux financiers.

5.5 Gestion des Créances

- ✓ Enregistrement des cessions de créances ;
- ✓ Génération du tableau d'amortissement des créances titrisées ;
- ✓ Génération du tableau d'écoulement des créances ;
- ✓ Enregistrement et suivi des sûretés, garanties et accessoires attachés aux créances ;
- ✓ Enregistrement et suivi des instruments financiers à termes ;
- ✓ Enregistrement et suivi du recouvrement des créances ;
- ✓ Enregistrement des rechargements.

5.6 Gestion de la tarification

- ✓ Paramétrage des taux à facturer pour les différentes commissions (gestionnaire de créance, dépositaire, ...).

5.7 Gestion des titres émis

- ✓ Définition et sauvegarde des caractéristiques des titres adossés aux créances ;
- ✓ Enregistrement des émissions de titres adossés aux créances et génération du tableau d'amortissement prévisionnel de ces titres ;
- ✓ Génération du tableau d'écoulement des émissions de titres adossés aux créances avec une périodicité mensuelle, trimestrielle, semestrielle ou annuelle.

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

5.8 Gestion de la trésorerie du FCTC

- ✓ Paramétrage et suivi du Compte spécialement affecté ;
- ✓ Enregistrement et suivi des emprunts d'espèces et emprunts subordonnés ;
- ✓ Enregistrement et suivi des disponibilités (dépôt à vue, bons et obligations du Trésors, etc.) ;
- ✓ Paramétrage de l'ordre d'affectation des sommes perçues ;
- ✓ Calcul des frais de fonctionnement à chaque paiement des porteurs de titres ;
- ✓ Calcul des intérêts courus sur les comptes financiers (DAT, dépôt à vue rémunéré, etc.) à chaque paiement des porteurs de titres ;
- ✓ Validation de la distribution calculée pour les porteurs de titres ;
- ✓ Paiement des porteurs de titres.

5.9 Gestion de la comptabilité

- ✓ Paramétrage du plan comptable ;
- ✓ Paramétrage des opérations et des journaux ;
- ✓ Ouverture et clôture d'exercice ;
- ✓ Edition du journal ;
- ✓ Edition de la balance générale (à six colonnes au moins) et du grand livre ;
- ✓ Edition des états financiers.

Si le logiciel de la SG-FCTC n'intègre pas un module de comptabilité, il devra avoir une interface entre ce logiciel et le logiciel de gestion de la comptabilité, afin de réduire les opérations manuelles de déversement des écritures.

Article 6 : Spécifications de sécurité des logiciels de gestion métier des SGI, des BTCC, des SGO et des SG-FCTC

Les logiciels de gestion des SGI, des BTCC, des SGO et des SG-FCTC doivent comporter les spécifications de sécurité listées ci-après :

6.1 Piste d'audit

La piste d'audit doit être configurée sur les logiciels de gestion afin de garantir l'enregistrement des actions effectuées par les utilisateurs de ces logiciels et de garantir ainsi leurs traçabilités. De plus, l'accès à cette piste d'audit doit être correctement restreint, de sorte à être non accessible aux utilisateurs privilégiés tels que les administrateurs des logiciels.

6.2 Authentification des utilisateurs

L'accès aux logiciels doit se faire via une authentification des utilisateurs. Celle-ci devra empêcher les personnes non autorisées d'accéder aux logiciels.

6.3 Prohiber l'accès simultané avec le même compte utilisateur

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

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

6.4 Profils utilisateurs

Chaque logiciel 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 sont conformes aux attributions des utilisateurs au sein de la SGI et des sociétés de gestion.

6.5 Changement de mot de passe à la première connexion

Lorsque l'authentification est basée sur le code utilisateur et le mot de passe, ce dernier doit être changé lors de la première connexion.

6.6 Déconnection automatique des utilisateurs après un temps d'inactivité

Les logiciels 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.

6.7 Paramétrage des mots de passe (longueur, complexité, durée, historique, verrouillage)

Dans les cas d'authentification basée sur le couple code utilisateur-mot de passe, les mots de passe des logiciels doivent être paramétrables de sorte à définir les valeurs des paramètres suivants :

- longueur du mot de passe. La longueur minimale recommandée est de huit (08) caractères ;
- complexité du mot de passe (au moins une majuscule, au moins une minuscule, au moins un caractère spécial, au moins un caractère alphanumérique) ;
- durée maximale du mot de passe. La durée recommandée est de quatre-vingt-dix (90) jours ;
- verrouillage des comptes après un nombre de tentatives de connexions. Au maximum trois (03) tentatives sont recommandées.

6.8 Cryptage ou hachage des fichiers/tables des mots de passe

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

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

SECTION III : SECURITE DU SYSTEME D'INFORMATION DES SGI, DES BTCC, DES SGO ET DES SG-FCTC

Article 7 : Gouvernance et gestion des risques

Les Conseils d'Administration et les Directions Générales des SGI, des BTCC, des SGO et des SG-FCTC devront prendre des actions pour surveiller les risques technologiques et veiller à ce que leur fonction informatique soit en mesure de soutenir leurs stratégies et objectifs.

Ils devront 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 la sécurité informatiques, 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'assurer que son contenu reste pertinent, compte tenu de l'évolution de la technologie ainsi que des risques qui y sont associés.

Article 8 : Politique de sécurité informatique

Les SGI, les BTCC, les SGO et les SG-FCTC doivent posséder une politique de sécurité informatique adaptée à leur activité et à leur infrastructure informatique propre et comportant au minimum les rubriques ci-après :

- responsabilité en matière de sécurité du Système d'Information ;
- conception et modification des applications ;
- sécurité physique des équipements ;
- sécurité des accès (en interne et à distance) à l'infrastructure informatique ;
- sécurité des données ;
- gestion des comptes utilisateurs, des accès et des révocations ;
- gestion des accès à la salle des serveurs ;
- gestion de l'antivirus ;

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

- directives aux collaborateurs en matière d'utilisation des biens informatiques ;
- report des incidents de sécurité ;
- formation et sensibilisation des utilisateurs sur la sécurité informatique.

Cette politique doit être validée par la Direction Générale et communiquée à tous les utilisateurs du Système d'Information (employé, prestataire).

Article 9 : Plan de Continuité d'Activités

Les Sociétés de Gestion et d'Intermédiation, les Banques Teneurs de Comptes et Conservateurs ainsi que les Sociétés de Gestion d'OPCVM et de FCTC doivent veiller à ce que leur organisation, leurs systèmes et leurs procédures soient conçus pour maintenir leurs fonctions critiques ou les rétablir le plus rapidement possible afin de remplir leurs obligations de préservation des intérêts et des droits de leurs clients. L'élaboration d'un plan de continuité d'activités comprenant un plan de secours informatique s'avère obligatoire. Il doit permettre de faire face à des interruptions sérieuses et non planifiées des activités, résultant notamment de pannes informatiques, d'attaques informatiques et de cybercriminalité, d'incident, de destruction totale ou partielle et/ou l'inaccessibilité des bâtiments opérationnels, de perturbations sociales importantes, de sabotages, d'actes de terrorisme, de catastrophes naturelles, de dégât des eaux ainsi que de la défaillance de services d'utilité publique (télécommunications, électricité, gaz naturel, ...).

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 l'entreprise et l'efficience des contrôles d'atténuation pour des risques existants ;
- une définition de la stratégie de continuité d'activités ;
- l'élaboration (mise en œuvre de la stratégie) du plan 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.

Le site de reprise doit être géographiquement distinct et suffisamment éloigné du site principal afin d'atténuer le risque qu'un même sinistre touche les deux sites.

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

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 une journée de données.

Après la survenance d'un désastre, lors de la séance de négociation, qui l'empêcherait de poursuivre ses activités de négociation, la SGI dispose de quatre (4) heures pour transmettre les ordres de ses clients. Pour se faire, elle pourra se rendre à l'antenne nationale de bourse ou utiliser tout autre moyen à sa disposition.

Une copie du plan de continuité d'activités doit être conservée dans un lieu sécurisé, à l'extérieur du site principal de la SGI, la BTCC ou de la société de gestion.

Périodiquement et au moins une (1) fois par an, le plan doit être testé afin de vérifier son efficacité. 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 10 : Sauvegarde et restauration des données

Les données des Sociétés de Gestion et d'Intermédiation, des Banques Teneurs de Comptes et Conservateurs ainsi que des Sociétés de Gestion d'OPCVM et de FCTC doivent être sauvegardées de sorte à les rendre disponibles au besoin. La disponibilité des données sauvegardées est un élément crucial pour la reprise des activités informatiques en cas de sinistre. De même, les tests de restauration doivent permettre de s'assurer de la réutilisabilité des sauvegardes effectuées.

Pour atteindre les objectifs de sauvegarde et de restauration des données, les Sociétés de Gestion et d'Intermédiation, les Banques Teneurs de Comptes et Conservateurs ainsi que les Sociétés de Gestion d'OPCVM et de FCTC doivent rédiger une procédure de sauvegarde et de restauration des données. Cette procédure, validée par la Direction Générale, doit contenir les rubriques non exhaustives suivantes :

- définition des données sauvegardées (Base de Données, fichiers d'application, système, ...) ;
- fréquence de sauvegarde ;
- type de sauvegarde (sauvegarde complète, incrémentale, différentielle) ;
- support de sauvegarde ;
- rétention des données sauvegardées ;
- sauvegarde externe des données ;
- restauration des données.

La fréquence de sauvegarde des données doit être de vingt-quatre (24) heures au plus.

Une copie des données sauvegardées, doit être externalisée, conservée sur un site secours sécurisé (contrôle d'accès physiques et logiques stricts protégeant les données).

Périodiquement et au moins une (1) fois par an, les tests de restauration doivent être effectués. Ces tests de restauration doivent permettre de vérifier la capacité

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

à récupérer les données sauvegardées en évaluant la fiabilité des supports de sauvegarde.

Article 11 : Accès à l'infrastructure informatique

Les SGI, les BTCC, les SGO et les SG-FCTC doivent prendre les mesures de sécurité nécessaires pour prévenir les accès non autorisés à leur infrastructure informatique en interne ou à distance. L'accès à l'infrastructure informatique doit s'appuyer sur des solutions d'authentification solides qui permettent, avec un degré d'assurance très élevé, de vérifier l'identité des utilisateurs. Elles doivent utiliser à cet égard des passerelles contrôlées entre internet et leur 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. Elles doivent 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.

Enfin, les SGI, les BTCC, les SGO et les SG-FCTC doivent accorder une attention nécessaire à la sécurisation adéquate de leurs applications, de leurs bases de données et de leurs systèmes d'exploitation.

Article 12 : Gestion des incidents

La gestion des incidents constitue l'un des processus critiques de la gestion des services informatiques. Elle doit être effectuée sur une base continue afin de restaurer le plus rapidement possible un service informatique normal après un incident et d'avoir un impact minimal sur les opérations des Sociétés de Gestion et d'Intermédiation, des Banques Teneurs de Comptes et Conservateurs, ainsi que des Sociétés de Gestion d'OPCVM et de FCTC. Pour mener à bien la gestion des incidents, les SGI, les BTCC, les SGO et les SG-FCTC doivent disposer d'une procédure de gestion d'incidents. Cette procédure, validée par la Direction Générale, 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.

Cette procédure doit être rigoureusement appliquée afin d'identifier et de répondre à tous les incidents en contrôlant leurs impacts à des niveaux acceptables. 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

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

mise en œuvre doit être transmis annuellement, au mois de janvier, au Conseil Régional de l'Épargne Publique et des Marchés Financiers (CREPMF).

Enfin, tout incident majeur doit être systématiquement communiqué au CREPMF.

Article 13 : Gestion des changements aux systèmes de production

Les SGI, les BTCC et les sociétés de gestion doivent 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 sécurités.

Ce processus doit être régi par une procédure de gestion des changements. Cette procédure validée par la Direction Générale, doit inclure les principales étapes suivantes :

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

Cette procédure doit être rigoureusement appliquée afin de s'assurer que la mise en œuvre des changements permet d'atteindre les objectifs de l'entreprise.

Par ailleurs, conformément à la règlementation du marché financier régional, tout changement concernant le logiciel de gestion métier doit être soumis à l'approbation préalable du CREPMF.

Article 14 : Gestion des prestataires de services

Les prestataires jouent un rôle important dans la gestion des systèmes et des processus des SGI, des BTCC, des SGO et des SG-FCTC. Une sélection minutieuse et un contrôle des prestataires sont essentiels pour minimiser les risques de sécurité auxquels elles pourraient être confrontées. Celles-ci doivent mettre en œuvre des mesures pour répondre aux menaces de sécurité qui peuvent survenir au cours de leurs 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, elles devront utiliser les pratiques suivantes :

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

- effectuer une diligence raisonnable (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 niveaux 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 les prestataires de services donnent l'accès à toutes les parties de leurs systèmes, opérations, documentation et installations afin de procéder à tout examen (évaluation, vérification de la conformité) à des fins réglementaires. De plus, l'engagement de prestataires ne devrait pas empêcher le Conseil Régional de l'Épargne Publique et des Marchés Financiers (CREPMF) d'évaluer les risques informatiques des acteurs du marché, qui comprendraient l'inspection des systèmes et installations des prestataires. À cet égard, les acteurs doivent veiller à ce que les accords contractuels avec les prestataires, dans le cadre d'une externalisation de la fonction informatique, reconnaissent l'autorité du CREPMF pour effectuer toute évaluation ;
- veiller à ce que l'utilisation de prestataires, l'externalisation des systèmes informatiques, n'entraînent pas un affaiblissement ou une dégradation des contrôles internes des SGI, des BTCC, des SGO et des SG-FCTC. Ces dernières, restent en définitive responsables de toute violation de leurs données financières et de celles de leurs clients. Elles doivent exiger des prestataires de services qu'ils appliquent rigoureusement des procédures et contrôles de sécurité afin de protéger la confidentialité et la sécurité des informations sensibles ou confidentielles telles que leurs données financières et celles de leurs 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 ;
- élaborer et appliquer des procédures pour mettre fin à l'accès des prestataires de services aux systèmes dès la résiliation ou l'expiration du contrat ;
- vérifier, pour les SGI, les BTCC, les SGO et les SG-FCTC ayant leurs données externalisées (données hébergées chez des prestataires), la capacité du prestataire de services à récupérer les systèmes et les services informatiques externalisés en étant conformes aux délais acceptables de

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

reprise des activités (RTO : Recovery Time Objective) avant de conclure tout accord avec les fournisseurs de services. Aussi, à la résiliation ou à l'expiration du contrat, elles doivent avoir le pouvoir contractuel et les moyens de retirer ou de détruire rapidement les données stockées dans les systèmes et les sauvegardes des prestataires de services.

Article 15 : Journalisation et droit d'accès à la piste d'audit

Les logiciels de gestion métier, les Bases de Données et les Systèmes d'Exploitation 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 applications de gestion métier, sur la Base de Données et le Système d'Exploitation des applications de gestion métier pour chaque SGI, BTCC, SGO et SG-FCTC.

Les logs générés par cette journalisation doivent être sécurisés (protégés contre toute modification) et archivés de manière adéquate afin de garantir leur intégrité et leur qualité de pièces probantes. Ces logs doivent être uniquement accessibles par le contrôle interne. Enfin, ils 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 16 : Surveillance et réalisation d'examen en matière de sécurité

Les SGI, les BTCC, les SGO et les SG-FCTC doivent étroitement surveiller le personnel ayant des privilèges d'accès élevés à leurs systèmes, car il possède les connaissances et les ressources nécessaires pour contourner les contrôles implémentés dans ces systèmes et les procédures de sécurité.

Elles doivent adopter les contrôles et pratiques suivants :

- mettre en œuvre des mécanismes d'authentification forts 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 consignées ;
- 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 Responsable du contrôle interne des SGI, des BTCC, des SGO et des SG-FCTC devra effectuer des contrôles (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

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org
TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org

semestre (les mois de janvier et juillet), les rapports de ces contrôles doivent être transmis au Conseil Régional et conservés par les SGI, les BTCC, les SGO et les SG-FCTC.

------oOo------

Avenue Joseph ANOMA
01 B.P. 1878 Abidjan 01/Côte d'Ivoire
Site web : http://www.crepmf.org

TEL.: (225) 20 21 57 42 / 20 31 56 20
Fax: (225) 20 33 23 04
Email:sg@crepmf.org