Tunis, le 13 Février 2024

**Circulaire de la Banque Centrale de Tunisie**
**N°2024-5 du 13 Février 2024**

**Objet** : Règles régissant l'activité de gestion des systèmes de paiement et de règlement-livraison de titres.

**Le Gouverneur de la Banque Centrale de Tunisie,**

Vu la loi organique n° 2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel,

Vu la loi n° 94-117 du 14 novembre 1994 portant réorganisation du marché financier, telle que modifiée et complétée par les textes subséquents,

Vu le code des sociétés commerciales, tel que modifié et complété par les textes subséquents,

Vu la loi n° 2005-51 du 27 juin 2005, relative au transfert électronique de fonds,

Vu la loi n° 2016-35 du 25 avril 2016, portant fixation du statut de la Banque Centrale de Tunisie et notamment ses articles 8, 17 et 42,

Vu la loi n°2016-48 du 11 juillet 2016, relative aux banques et aux établissements financiers,

Vu le décret-loi n°2023-17 du 11 mars 2023, relatif à la cybersécurité,

Vu le décret gouvernemental n° 2018-417 du 11 mai 2018, relatif à la publication de la liste exclusive des activités économiques soumises à autorisation et de la liste des autorisations administratives pour la réalisation de projets, les dispositions y afférentes et leur simplification tel que modifié et complété par le décret présidentiel n° 2022-317 du 8 avril 2022,

Vu l'arrêté du ministre des finances du 12 janvier 2016, portant visa du règlement du Conseil du Marché Financier relatif au dépositaire central de titres,

Vu l'avis n° 5 du comité de contrôle de la conformité du 9 février 2024, tel que prévu par l'article 42 de la loi n° 2016-35 du 25 avril 2016, portant fixation du statut de la Banque Centrale de Tunisie.

**Décide :**

# TITRE I : DISPOSITIONS GENERALES

**Article premier :** La présente circulaire a pour objet de fixer les règles régissant l'activité de gestionnaire de système de paiement et de système de règlement-livraison de titres, notamment celles relatives aux exigences minimales de gouvernance et de gestion des risques.

Elle a pour objectif de :

- Promouvoir des systèmes de paiement et de règlement-livraison de titres efficients, sécurisés et résilients à l'égard des risques notamment systémiques afin de faciliter le dénouement des transactions et de préserver la stabilité financière ;
- Protéger les participants des systèmes de paiement et de règlement-livraison de titres et leurs usagers ;
- Réhausser les capacités techniques et institutionnelles des systèmes nationaux de paiement et de règlement-livraison de titres en ligne avec les standards internationaux pour faciliter leur intégration aux systèmes de paiement régionaux ;
- Asseoir les conditions d'une concurrence saine, transparente et efficiente de l'activité de gestion des systèmes de paiement.

**Article 2 :** Au sens de la présente circulaire, on entend par :

- **Système de paiement :** Désigne l'ensemble d'instruments, de procédures, de règles, de plateformes techniques et de réseaux permettant le traitement, la compensation, le règlement et le transfert de fonds entre participants sur la base d'un engagement conventionnel avec le gestionnaire du système.
- **Système de règlement – livraison de titres :** Désigne l'ensemble complet de dispositions institutionnelles et de règles multilatérales prédéfinies

permettant la confirmation, la compensation et le règlement de transactions sur titres entre participants et ce, sur la base notamment du mécanisme de livraison contre règlement.

- **Compensation** : Fait de ramener à un solde unique les obligations entre participants au dispositif de compensation, réduisant ainsi le nombre et le montant des paiements nécessaires pour régler un ensemble de transactions.
- **Règlement Brut en Temps Réel :** Mécanisme de règlement en continu, sans compensation, des ordres de transfert de fonds ou de titres ou d'autres obligations entre participants au cas par cas, dès réception.
- **Règlement Net Différé :** Mécanisme de règlement net qui effectue le règlement d'obligations entre participants sur une base nette compensée à la fin d'un cycle de règlement prédéfini.
- **Mécanisme de livraison contre règlement :** un mécanisme de règlement de valeurs mobilières qui lie un transfert de titres et un transfert de fonds de manière à garantir que la livraison des titres intervienne si, et seulement si, le paiement correspondant ait lieu.
- **Gestionnaire de système :** désigne l'entité qui assure la gestion du système de paiement ou de règlement-livraison de titres, notamment à travers :
    - ✓ La mobilisation d'une infrastructure technique, dotée d'un dispositif de gestion des risques adéquat à l'activité du système, pour assurer le transfert de fonds ou de règlement sur titres issus du traitement et de la compensation, des obligations entre participants ;
    - ✓ La mise en place de règles de fonctionnement et des procédures normalisées adéquates au système ;
    - ✓ L'établissement de conditions formalisées d'adhésion au système géré.

- **Système d'importance systémique :** système dont le dysfonctionnement partiel ou total est susceptible de provoquer des perturbations de continuité d'activité ou de transmettre des difficultés aux participants ou dans le système financier de manière à impacter la stabilité financière.
- **Participant :** tout établissement dûment agréé ou habilité en vertu de la législation en vigueur à exercer des services financiers dont la prestation exige

la participation à un système de paiement ou de règlement-livraison de titres en respectant les règles qui régissent l'activité du système.

- **Participant direct :** participant qui se connecte directement au système pour effectuer ses opérations de compensation et de règlement.
- **Participant indirect :** participant qui fait appel à un participant direct pour lui assurer les opérations de compensation et de règlement.
- **Parties prenantes :** les parties prenantes du gestionnaire du système regroupent tous les acteurs qui participent à sa vie économique. Elles comprennent notamment l'autorité de régulation, les participants et les prestataires de services.
- **Administrateur indépendant :** est qualifié d'administrateur indépendant toute personne :
    - ✓ Ne détenant pas, elle-même, son conjoint, ses ascendants et descendants de premier degré, une participation directe ou indirecte dans le capital du gestionnaire du système, de ses filiales ou de ses participants ;
    - ✓ N'ayant pas fait partie des salariés du gestionnaire du système au moins au cours des 3 dernières années précédant sa désignation en qualité d'administrateur indépendant ;
    - ✓ N'agissant pas pour le compte d'un participant, d'un fournisseur ou d'un prestataire de service du gestionnaire du système ;
    - ✓ N'ayant pas de contrats de prestations conclus directement par lui-même ou par personne interposée avec le gestionnaire du système ou avec l'une des sociétés ayant des liens avec le gestionnaire du système.
- **Organe de direction :** directoire ou direction Générale du gestionnaire du système.
- **Conseil :** conseil de surveillance ou conseil d'administration du gestionnaire du système.
- **Dispositif à plusieurs niveaux de participation :** dispositif dont certains participants indirects font appel aux services fournis par d'autres participants

directs pour user des services centralisés d'un système de paiement ou d'un système de règlement-livraison de titres.

- **Règlement définitif :** extinction d'une obligation par transfert irrévocable et inconditionnel de fonds et/ou de titres.
- **Risque juridique :** risque de pertes en cas d'application de dispositions légales ou réglementaires non conformes aux prévisions ou en cas d'impossibilité de faire exécuter un contrat.
- **Risque d'activité :** détérioration potentielle de la situation financière du gestionnaire du système de paiement ou du système de règlement-livraison de titres liée à une baisse de ses recettes et/ou à l'augmentation de ses dépenses relatives à sa stratégie commerciale, qui entraînent une perte devant être imputée sur les fonds propres.
- **Risque opérationnel :** risque que des dysfonctionnements des systèmes d'information, des processus internes, des erreurs humaines ou des perturbations découlant d'événements extérieurs aboutissent à la réduction, à la détérioration ou à l'interruption des services fournis par un système de paiement ou de règlement-livraison de titres.
- **Risque informatique et cybernétique :** risque résultant d'une inadéquation ou d'une défaillance affectant l'organisation, le fonctionnement, le changement ou la sécurité du système d'information du système de paiement ou de règlement-livraison de titres. Ce risque fait partie du risque opérationnel.
- **Risques financiers :** risques de crédit et de liquidité.
- **Risque de crédit :** risque qu'un participant du système de paiement ou de règlement-livraison de titres ne s'acquitte pas intégralement d'une obligation financière à la date d'échéance ou ultérieurement.
- **Risque de liquidité :** risque qu'un participant du système de paiement ou de règlement-livraison de titres se trouve dans l'impossibilité de s'acquitter partiellement ou en totalité d'une obligation à son échéance. Le risque de liquidité ne signifie pas que le participant est insolvable, dès lors qu'il soit en mesure de s'acquitter de ladite obligation à une date ultérieure non spécifiée.

# TITRE II : AGREMENT POUR L'EXERCICE D'ACTIVITE DE GESTIONNAIRE DE SYSTEME DE PAIEMENT

## Chapitre premier : Des conditions d'agrément pour l'accès à l'activité de gestionnaire de système de paiement

**Article 3 :** Toute personne désirant exercer l'activité de gestionnaire de système de paiement doit, préalablement à l'exercice de son activité, obtenir un agrément à cet effet.

L'agrément pour l'exercice de l'activité de gestionnaire de système de paiement est accordé par la Banque Centrale de Tunisie, conformément aux conditions fixées par le décret présidentiel n° 2022-317 du 8 avril 2022 susvisé et par la présente circulaire, dont notamment :

- L'opportunité du système de paiement à gérer, ses perspectives à intégrer l'écosystème des paiements et ses capacités à répondre aux objectifs de stabilité financière et à la sécurité et l'efficacité du système national de paiement ;
- La structure du capital du gestionnaire du système de paiement notamment la qualité des actionnaires, directs et indirects, leur réputation, leurs capacités financières et leur prédisposition à promouvoir l'efficacité et la sécurité du système de paiement et à préserver la stabilité ;
- La soutenabilité du programme d'activité proposé par le gestionnaire du système de paiement. Le programme doit détailler le plan d'affaires, le business model en termes de services à fournir, des participants cibles, ainsi que des investissements projetés pour les infrastructures techniques et ses perspectives d'évolution ;
- Le niveau d'efficacité du système de paiement et sa capacité à développer une offre de services de paiement faciles à opérer par les usagers répondant aux besoins du marché et des opérateurs économiques ;
- L'adéquation des moyens financiers et humains mis à disposition du gestionnaire du système de paiement, y compris le capital et les ressources financières à allouer notamment aux investissements nécessaires en termes d'infrastructure technique pour assurer les équilibres financiers et faire face aux risques de défaut des participants ;

- L’approche du management des différents risques du système de paiement notamment la gouvernance de ces risques, les politiques, les procédures prévues et les mécanismes à mettre en place pour identifier, mesurer et maitriser ces risques conformément aux exigences de la présente circulaire ;
- Les capacités techniques et organisationnelles du système de paiement à assurer :
    - ✓ La sécurité, l’efficacité et la transparence des opérations et des données ;
    - ✓ La protection des actifs des participants et des usagers des services de paiement ;
    - ✓ La continuité de l'activité et, le cas échéant, le traitement des incidents de discontinuité par la mise en œuvre de plans d’urgence qui préservent la stabilité financière et la confiance des participants et des usagers ;
    - ✓ L’interconnexion avec tous les participants et les autres systèmes de paiement permettant l’interopérabilité des différents services qui sont rendus aux usagers.
- Le niveau de conformité du dispositif de gouvernance à déployer par le gestionnaire du système de paiement aux règles de gouvernance fixées par la présente circulaire ;
- La réputation, l’intégrité, la compétence et l'expérience des membres du conseil et de l’organe de direction ;
- La structure organisationnelle et administrative, les ressources humaines et le dispositif du contrôle interne du système de paiement et leur adéquation à l’activité et aux exigences d’efficacité et de sécurité ;
- Les politiques du système de paiement qui permettent un accès équitable, juste et transparent aux participants directs et indirects ainsi qu’aux autres systèmes de paiement conformément aux règles fixées par la présente circulaire ;
- L’accord de l'autorité compétente du pays d’origine pour :
    - ✓ Le gestionnaire du système de paiement au cas où il gère un autre système à l’étranger ;

- ✓ L'établissement financier dont le siège social est à l'étranger afin de participer au capital de la société gestionnaire du système de paiement à mettre en place.

**Article 4 :** Tout gestionnaire d'un système de paiement doit revêtir la forme d'une société anonyme.
Le capital de la société gestionnaire d'un système de paiement ne doit pas être inférieur à 10 millions de dinars Tunisiens.

**Article 5 :** Le gestionnaire de système de paiement ne peut exercer des activités autres que celles pour lesquelles il a été agréé qu'à titre exceptionnel et dans des proportions limitées par rapport à l'activité principale.

## Chapitre 2 : Des procédures d'octroi de l'agrément pour l'exercice de l'activité de gestionnaire de système de paiement

**Article 6 :** Toute personne qui désire obtenir l'agrément pour l'exercice de l'activité de gestionnaire de système de paiement doit soumettre à la Banque Centrale de Tunisie une demande au nom du Gouverneur, accompagnée d'un dossier tel que détaillé dans l'annexe I de la présente circulaire.

**Article 7 :** La Banque Centrale de Tunisie peut demander au requérant d'agrément dans un délai d'un mois à compter du dépôt de sa demande de lui fournir tous les renseignements et documents complémentaires nécessaires à l'instruction du dossier.

Toute demande d'agrément qui ne satisfait pas les renseignements et documents requis dans un délai de trois mois à compter de la date de sa demande par la Banque Centrale de Tunisie est considérée nulle.

La Banque Centrale de Tunisie rend sa décision d'agrément de principe ou de refus dans un délai maximum de quatre mois, à compter de la date de satisfaction de tous les renseignements et documents requis à cet effet.

Elle notifie au requérant de l'agrément le sort de sa demande et motive sa décision en cas de refus.

**Article 8 :** L'agrément de principe précise notamment la catégorie du système de paiement, la nature des opérations autorisées, la catégorie des participants, le capital initial, l'identité de l'actionnaire de référence et des principaux actionnaires

et fixe les conditions nécessaires à remplir pour l'octroi de l'agrément définitif, dont notamment :

- L'achèvement des procédures de constitution ;
- La mise à disposition des ressources nécessaires ;
- La confirmation de l'identité des membres du conseil et de l'organe de direction et des responsables de contrôle et de gestion des risques ;
- L'implémentation de l'infrastructure technique et logistique ;
- La mise en place des politiques, des procédures et des mécanismes opérationnels nécessaires au fonctionnement du système de paiement et toute autre exigence afférente pour garantir la satisfaction des conditions d'octroi de l'agrément.

Le requérant doit satisfaire les conditions prescrites dans l'agrément de principe dans un délai ne dépassant pas six mois à compter de la date de la notification de cet agrément. A titre exceptionnel, ce délai peut être prorogé de trois mois, sur demande motivée.

**Article 9 :** La Banque Centrale de Tunisie délivre l'agrément définitif, dans un délai de deux mois à compter de la réception d'une demande du requérant prouvant la satisfaction des conditions exigées dans l'agrément de principe.

Est considérée nulle toute demande d'agrément qui ne satisfait pas les renseignements et documents requis dans un délai d'un mois à compter de la date de sa demande par la Banque Centrale de Tunisie.

La Banque Centrale de Tunisie accorde l'agrément définitif ou rend d'une décision de refus dans un délai maximum de deux mois, à compter de la date de satisfaction de tous les renseignements et documents requis à cet effet.

**Article 10 :** La Banque Centrale de Tunisie est habilitée à prendre les mesures qu'elle juge nécessaires si :

- Le gestionnaire du système de paiement ne satisfait plus les conditions sur la base desquelles l'agrément a été octroyé ; et
- La continuité d'activité du système de paiement est de nature à porter atteinte à la stabilité financière.

## Chapitre 3 : Des changements de situations et des opérations d'externalisation dans l'exercice de l'activité de gestionnaire de système de paiement

**Article 11 :** Est soumis à l'agrément de la Banque Centrale de Tunisie tout changement dans l'un des éléments ou conditions sur la base desquels a été octroyé l'agrément pour exploiter et gérer un système de paiement et notamment :

- Tout changement que le gestionnaire du système de paiement envisage d'apporter à la catégorie du système de paiement ou à la nature de l'activité qui a été préalablement agréée ;
- Tout changement dans l'infrastructure technique approuvée pour l'activité d'un système de paiement, y compris sa modernisation, sa refonte ou son ouverture à l'interopérabilité avec d'autres systèmes de paiement, locaux ou étrangers ;
- Toute fusion entre gestionnaires de systèmes de paiement ;
- Toute suspension temporaire, partielle ou totale de l'activité du gestionnaire de système de paiement ;
- Le transfert d'actifs ou de passifs du gestionnaire du système de paiement qui entraîne un changement radical de sa structure financière ou un changement de catégorie ou de nature d'activité ;
- Tout changement du dispositif de gouvernance d'un gestionnaire de système de paiement sur le plan mode de gouvernance, structuration et personnes désignées ou habilitées pour gérer ce dispositif ;
- Les opérations d'externalisation, notamment techniques, ayant un impact sur la continuité de l'activité, la sécurité et le bon fonctionnement du système de paiement sur le plan efficacité et efficience.

**Article 12 :** L'agrément prévu par l'article précédent est accordé dans les délais et selon les conditions prévues à l'article 9 de la présente circulaire.

**Article 13 :** Le gestionnaire du système de paiement doit soumettre à la Banque Centrale de Tunisie avant sa signature toute convention d'externalisation.

**Article 14 :** Les opérations d'externalisation ne doivent pas :

- Déroger ou altérer les conditions dans lesquelles le gestionnaire du système de paiement satisfait les exigences de la présente circulaire ;

- Entrainer la délégation de la responsabilité du gestionnaire du système de paiement de se conformer à la présente circulaire ;
- Entrainer une modification dans la relation, les droits et les obligations du gestionnaire du système de paiement avec ses participants.

# TITRE III : DISPOSITIF DE GOUVERNANCE

## Chapitre premier : Obligations générales de gouvernance

**Article 15 :** Le gestionnaire du système doit se fixer des objectifs formalisés axés sur la sécurité et l'efficacité du système et qui soutiennent explicitement la stabilité du système financier et tiennent compte des intérêts des participants directs et indirects, de leurs clients et des autres parties prenantes.

Il doit se doter d'un dispositif formalisé, clair et transparent de gouvernance qui favorise la réalisation des objectifs cités à l'article premier de la présente circulaire.

**Article 16 :** Le gestionnaire du système doit mettre en place un dispositif de gouvernance qui définit notamment :

- Le mode de gouvernance ;
- Les structures de gouvernance, leurs compositions, leurs attributions, leurs règles de fonctionnement, les rapports entre elles ainsi qu'avec les entités opérationnelles ;
- Les politiques de gouvernance, y compris des niveaux clairs et directs de responsabilité et d'obligation de reddition de comptes ;
- Le dispositif de contrôle interne et de gestion des risques ainsi que les mécanismes destinés à assurer l'indépendance des fonctions de contrôle ;
- Les rapports du gestionnaire du système avec l'écosystème notamment avec les participants au système et les mesures susceptibles d'assurer un accès équitable et ouvert auxdits participants.

## Chapitre 2 : Les organes de gouvernance

**Article 17 :** Le conseil veille au fonctionnement efficace et sécurisé du système de manière à assurer sa pérennité et préserver la stabilité financière.

Il veille aussi à ce que la stratégie globale, les règles, les décisions et la conception du système tiennent compte de manière appropriée, des intérêts de ses participants, des usagers des services et des autres parties prenantes.

Il doit s'assurer que les moyens organisationnels, humains, financiers et techniques mis à disposition sont en adéquation avec ses missions.

**Article 18 :** Le conseil veille dans le cadre de l'exercice de ses missions à :

- Définir la stratégie du développement du système qui assure l'équilibre entre la performance et la maitrise des risques ;
- Mettre en place un dispositif de gouvernance adéquat à la nature, la complexité de ses activités et les risques qui y sont liés ;
- Mettre en place un dispositif de contrôle interne adéquat à l'activité du système, y compris des outils de surveillance visant à assurer l'efficacité et l'indépendance des fonctions de contrôle ;
- Définir et mettre en place un dispositif de gestion saine des risques permettant l'identification, le suivi et la maitrise des risques ;
- La cohérence de la politique informatique et de cybersécurité ainsi que la gestion saine du risque informatique et cybernétique ;
- Définir et mettre en œuvre des politiques appropriées de nomination, de rémunération et de succession des responsables des fonctions clés, notamment les fonctions de contrôle ;
- Définir et mettre en œuvre une politique de conformité ;
- Surveiller l'organe de direction dans la mise en œuvre effective de la stratégie du système et la conduite opérationnelle de ses activités ;
- Définir et mettre en œuvre des règles d'adhésion au système basées sur le principe de traitement juste et équitable des participants ;
- Définir et mettre en œuvre une politique de communication et de divulgation vis-vis des parties prenantes et du public.

**Article 19 :** Le conseil veille dans le cadre du suivi de l'organe de direction à :

- Apprécier les décisions prises par l'organe de direction dans la gestion du système ayant trait notamment à sa continuité, sa sécurité et son efficacité ;

- Contrôler la conformité des actions de l'organe de direction à la stratégie et aux politiques approuvées, notamment en matière de gestion des risques ;
- Définir des indicateurs quantitatifs et qualitatifs de suivi des performances du système.

**Article 20 :** Le gestionnaire du système doit veiller à ce que la composition du conseil soit adéquate à la nature des activités du système et garantisse une combinaison de compétences pluridisciplinaires en la matière.

Il doit veiller à ce que les membres du conseil disposent, outre les compétences managériales, des qualifications académiques et de l'expertise appropriées aux activités du système notamment dans les domaines de la finance, de l'audit et du management des risques, des technologies de l'information et de la sécurité informatique.

**Article 21 :** Le gestionnaire du système doit veiller à ce que la composition du conseil d'administration :

- Comporte au moins deux membres indépendants dont l'un dispose de solides qualifications en matière d'audit et de management des risques et l'autre dispose de solides qualifications dans les technologies de l'information et ce, outre une bonne expertise dans le domaine des paiements ; et
- Soit représentative des différentes catégories d'institutions participantes au système.

**Article 22 :** Le conseil veille à la mise en place d'une charte de bonne conduite signée par tous les membres du conseil en vertu de laquelle ils s'engagent notamment à :

- Ne pas occuper la même fonction dans un autre gestionnaire de système ou dans une entité liée à l'un des participants ;
- Ne pas cumuler la fonction de membre de conseil avec celle de membre de l'organe de direction du gestionnaire du système ou d'un autre gestionnaire de système ;
- Exercer leurs fonctions avec la diligence d'un entrepreneur avisé et d'un mandataire loyal ;
- Déclarer toute information ou situation pouvant induire une situation de conflit d'intérêts.

**Article 23 :** Le gestionnaire du système doit mettre en place un processus formalisé et transparent pour la désignation des membres du conseil.
Ce processus doit définir entre autres, des critères de sélection et d'évaluation des membres du conseil et de leur rotation au niveau des responsabilités au sein des comités visés par les dispositions de la présente circulaire.
Le processus de désignation des membres du conseil doit être communiqué à la Banque Centrale de Tunisie préalablement à son adoption.
Le gestionnaire du système est tenu, dans un délai ne dépassant pas dix jours de la date de désignation de tout membre au conseil, d'en informer la Banque Centrale de Tunisie qui s'assure que les conditions prévues à l'article 20 de la présente circulaire sont remplies.

**Article 24 :** La fréquence des réunions du conseil du gestionnaire du système doit tenir compte de la nature, de la diversité, de la complexité et du volume de l'activité du système. Cette fréquence doit être augmentée :

- Pour tout système classé d'importance systémique par décision de la Banque Centrale de Tunisie sur la base des critères qu'elle fixe à cet effet ;
- En cas de survenance d'événements exceptionnels pouvant, éventuellement, affecter négativement les conditions d'exploitation du système ;
- Lorsque le gestionnaire du système est appelé à pallier des insuffisances relevées par la Banque Centrale de Tunisie.

**Article 25 :** Le conseil procède régulièrement à l'auto-évaluation de ses performances globales, des performances de ses membres ainsi que des travaux de ses comités prévus par la présente circulaire.

L'exercice de l'auto-évaluation couvre notamment, les modalités de fonctionnement, l'assiduité et la contribution effective aux travaux ainsi que la pertinence et l'efficacité des recommandations et des décisions.

Les résultats de l'exercice d'auto-évaluation et les recommandations y afférentes doivent être consignés dans le rapport de gestion dont une copie est transmise à la Banque Centrale de Tunisie.

**Article 26 :** Le conseil doit créer un comité d'audit et des risques qui l'assiste dans la mise en place d'un dispositif efficace de contrôle interne et de gestion des risques. Le comité est chargé notamment de :

- Suivre la mise en place du dispositif de contrôle interne, en évaluer le bon fonctionnement et proposer le cas échéant des mesures correctrices ;
- S'assurer de la mise en œuvre de politiques, de procédures et de mécanismes efficaces et adéquats de gestion des risques permettant l'identification, la mesure et la maitrise de ces risques ;
- Analyser sur demande du conseil toute question spécifique en matière d'audit et des risques en émettant des appréciations et opinions sur le fonctionnement du système ;
- Informer le conseil de tout événement lié à l'audit ou aux risques susceptible de porter préjudice à la continuité, la sécurité et l'efficacité du système ;
- Donner son avis au conseil sur le rapport annuel et les états financiers et d'examiner les principaux rapports de contrôle interne avant leur transmission à la Banque Centrale de Tunisie ;
- Donner son avis sur les critères de nomination du ou des commissaires aux comptes et sur les programmes de contrôle et les résultats y afférents ;
- Suivre l'activité des organes chargés des fonctions de contrôle et de gestion des risques et donner son avis au conseil sur la nomination des responsables de ces organes ;
- Approuver les programmes d'audit annuels et trisannuels et leurs modifications ;
- Suivre les recommandations issues des missions d'audit interne et externe et les plans d'actions visant la régularisation des insuffisances soulevées dans les rapports d'audit ;
- Soumettre au conseil, à l'occasion de la tenue de ses réunions, un rapport d'activité du comité.

**Article 27 :** Le conseil doit créer un comité qui l'assiste dans le développement stratégique et technologique du système. Ce comité est chargé notamment de :

- Donner son avis sur les perspectives de développement stratégique du système et les projets y afférents ;
- Donner son avis sur le fonctionnement des infrastructures déployées, leurs performances et leur adéquation aux besoins des participants ;
- Appréhender les besoins et les prérequis de refonte et de modernisation de des infrastructures opérationnelles, projeter les investissements nécessaires et suivre les projets y afférents ;

- Informer le conseil de tout événement lié au développement stratégique et technologique susceptible de porter préjudice à la continuité, la sécurité et l'efficacité du système ;
- Suivre l'activité des entités internes chargées des fonctions d'exploitation et de développement des infrastructures du système ;
- Examiner les rapports et documents soumis au conseil relevant des attributions du comité ;
- Soumettre au conseil, à l'occasion de la tenue de ses réunions, un rapport d'activité du comité.

**Article 28 :** Le conseil doit veiller à ce que :

- Chaque comité soit composé d'au moins trois membres du conseil choisis parmi ceux ayant les qualifications et l'expertise les mieux adaptées à ses attributions ;
- Le comité d'audit et des risques soit présidé par le membre indépendant du conseil jouissant des qualifications solides et d'une expertise en matière d'audit et de gestion des risques ;
- Le comité du développement stratégique soit présidé par le membre indépendant du conseil jouissant des qualifications solides dans le domaine de technologies de l'information et d'une expertise métier dans les paiements ;
- Un membre du conseil ne soit pas membre dans plus d'un comité.

**Article 29 :** L'organe de direction veille dans le cadre de ses missions à une gestion saine et prudente du système. Il doit veiller notamment à :

- La conduite des activités du système en cohérence avec les orientations stratégiques arrêtées par le conseil ;
- La conformité du système aux exigences légales et réglementaires régissant son activité ;
- Assurer le bon fonctionnement du dispositif de contrôle interne et à l'efficacité et l'indépendance des fonctions de contrôle ;
- L'application de la politique de gestion des risques en s'engageant activement dans le suivi et la maîtrise de ces risques ;
- La mise en place d'une organisation adéquate aux activités du système et à une affectation optimale des ressources qui favorisent l'efficacité, la responsabilité et la transparence ;

- La communication au conseil et aux comités des reportings nécessaires pour la prise de décisions.

**Article 30 :** L'organe de direction doit alerter le conseil de tout fait important pouvant :

- Altérer la continuité des activités critiques du système ;
- Impacter la situation financière et le profil de risque du gestionnaire du système ;
- Provoquer un dysfonctionnement du système de contrôle interne et une aggravation des risques.

**Article 31 :** Le gestionnaire du système doit veiller à ce que les membres de l'organe de direction disposent des compétences académiques, de l'expertise et des qualifications managériales requises et appropriées aux activités de gestion du système qui leur permettent de s'acquitter convenablement de leurs responsabilités.

Le gestionnaire du système est tenu, dans un délai ne dépassant pas dix jours de la date de désignation d'un membre de l'organe de direction, d'en informer la Banque Centrale de Tunisie qui s'assure que les conditions prévues à l'alinéa précédent sont remplies.

## Chapitre 3 : Fonctions de contrôle

**Article 32 :** Le gestionnaire du système doit se doter des fonctions de contrôle en matière d'audit interne et de gestion des risques, y compris les risques informatiques, en rapport avec la taille, la nature et la complexité des activités du système et de son profil de risque.

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

**Article 33 :** Le gestionnaire du système doit s'assurer que le dispositif de gouvernance garantisse aux fonctions de contrôle interne et de gestion des risques l'indépendance, l'allocation des ressources qualifiées et suffisantes ainsi que l'accès aux comités et au conseil.

Il doit veiller en particulier à la séparation de la fonction de gestion du risque informatique des activités opérationnelles du système d'information et définir clairement les responsabilités qui lui sont assignées.

**Article 34 :** Le conseil et les comités d'appui du gestionnaire du système doivent se réunir périodiquement avec les responsables des fonctions de contrôle afin de suivre leurs travaux, de s'assurer de l'efficacité des processus de contrôle interne et de gestion des risques et de s'informer des manquements majeurs pouvant affecter le fonctionnement efficace et sécurisé du système.

**Article 35 :** La fonction de gestion des risques est chargée notamment :

- D'élaborer la politique de gestion des risques, y compris le risque cybernétique, et de veiller à la conformité des activités du système à cette politique ;
- D'élaborer une cartographie des risques et de mettre en œuvre des mécanismes d'identification, de mesure et de maitrise des risques ;
- De fournir un avis sur les décisions pouvant nourrir des risques préjudiciables au bon fonctionnement du système ;
- De signaler à temps au conseil, aux comités d'audit et risques et à l'organe de direction toute insuffisance du dispositif de gestion des risques pouvant porter préjudice au système.

**Article 36 :** La fonction d'audit interne est chargée notamment :

- De procéder à une évaluation rigoureuse, régulière et indépendante de l'efficacité des processus de contrôle interne et du dispositif de gestion des risques ;
- D'évaluer l'efficacité des fonctions de gestion des risques et de contrôle de la conformité ;
- De communiquer au conseil, aux comités, à l'organe de direction et aux structures de contrôles concernées les dysfonctionnements relatifs au dispositif de contrôle interne et de management des risques relevés ainsi que des mesures correctrices adéquates.

## Chapitre 4 : Politique de communication et de divulgation

**Article 37 :** Le gestionnaire du système doit adopter une politique de communication transparente permettant de divulguer, aux participants et au public, des informations pertinentes et actualisées sur les aspects significatifs de

l'activité du système. A cet effet, le gestionnaire du système doit créer une structure opérationnelle et des moyens logistiques de communication.

**Article 38 :** Le gestionnaire du système doit établir un rapport annuel d'activité destiné au public portant au moins sur :

- La structure de l'actionnariat, notamment les principaux actionnaires ;
- La composition du conseil, des comités d'appui et l'organisation du gestionnaire du système ;
- Une synthèse sur les travaux du conseil et des comités ;
- L'évolution des activités du système et un aperçu sur sa situation financière ;
- Les conditions de participation et de suspension ainsi que la liste des participants.

Ledit rapport doit être publié sur le site Web du gestionnaire du système.

**Article 39 :** Le gestionnaire du système veille, dans le cadre de sa politique de communication, à informer les participants des décisions ayant une incidence sur le bon fonctionnement du système et la stabilité financière.

# TITRE IV : DISPOSITIF DE GESTION DES RISQUES

**Article 40 :** Le gestionnaire du système veille à instaurer une gouvernance saine et efficace des risques auxquels il est exposé dans l'exercice de ses activités, afin d'assurer la sécurité et l'efficience du système et de préserver la stabilité financière.

Il doit se doter d'un dispositif solide et cohérent de gestion intégrée de tous les risques qu'il encourt notamment juridique, de crédit, de liquidité et opérationnel, lui permettant une gouvernance saine et une maitrise de ces risques.

Le dispositif susvisé doit tenir compte des risques significatifs que d'autres entités ayant des liens d'interdépendance avec le système lui font encourir. Il doit prévoir :

- Des outils appropriés de gestion de ces risques afin de limiter la prorogation des effets des perturbations au système, à ces entités, ainsi qu'au marché financier ;
- Des exigences aux participants et leur fournir des informations, pour qu'ils gèrent et maitrisent les risques qu'ils transmettent au système.

## Chapitre premier : Dispositif de gestion des risques juridiques et de non-conformité et règles de participation

**Article 41 :** Le gestionnaire du système doit se doter d'un dispositif efficace de gestion des risques juridiques et de non-conformité inhérents à ses activités. Il doit notamment se doter :

- D'une structure qui veille sur la conformité de ses activités à la réglementation en vigueur et sur la maitrise des risques juridiques ;
- De règles, procédures et contrats clairs et conformes à la réglementation qui permettent la protection des droits des participants à l'égard du défaut d'un ou de plusieurs d'entre eux et du risque d'invalidation, d'annulation ou mise en œuvre différée de ces règles et procédures.

**Article 42 :** Le gestionnaire du système doit veiller à ce que :

- La structure en charge des risques juridiques et de non-conformité soit dotée de ressources suffisantes et qualifiées ;
- Les règles, procédures et contrats définissent notamment les droits et obligations du système et de ses participants relatifs à l'accès au système, aux ordres de transfert de fonds et de titres et aux règles de gestion de défaut d'un ou plusieurs participants ;
- Les mesures d'atténuation des risques soient prévues.

**Article 43 :** Le gestionnaire du système doit définir et publier des critères de participation au système qui sont fondés sur une analyse des risques et qui permettent aux participants directs et indirects et, le cas échéant, à d'autres systèmes un accès ouvert à ses services.

Les conditions de participation au système doivent être justifiées en termes de sécurité et d'efficience du système et garantissent un accès équitable à tous les participants.

**Article 44 :** Le gestionnaire du système doit veiller à ce que le statut juridique du participant l'habilite à participer et qu'il dispose, des capacités technico-fonctionnelles d'intégration au système ainsi que des capacités organisationnelles appropriées en matière de gestion de risques.

Il doit s'assurer en permanence que ses conditions de participation sont respectées par les participants.

Il doit disposer de procédures clairement définies et publiées en matière de suspension et de sortie ordonnée d'un participant qui enfreint aux conditions de participation.

**Article 45 :** Le gestionnaire du système doit identifier, surveiller et gérer les risques importants découlant des dispositifs à plusieurs niveaux de participation. Il doit en particulier :

- Identifier les rapports de dépendance importants entre les participants directs et indirects susceptibles de l'affecter ;
- Identifier les participants indirects qui effectuent soit une part significative de transactions au niveau du système et/ou un niveau élevé des transactions par rapport à la capacité des participants directs au système ;
- Veiller à ce que ses règles, procédures et conventions lui permettent de collecter des informations de base sur les participants indirects afin de pouvoir gérer les risques inhérents à la participation à plusieurs niveaux ;
- Procéder régulièrement à l'examen des risques découlant des dispositifs à plusieurs niveaux de participation et prendre les mesures d'atténuation qui s'imposent.

## Chapitre 2 : Dispositif de défaut d'un participant

**Article 46 :** Le gestionnaire du système doit mettre en place des règles et des procédures efficaces et clairement définies pour gérer le défaut d'un participant. Il doit consigner les éléments nécessaires desdites règles au niveau de la convention de participation au système.

Ces règles et procédures doivent être conçues et testées de sorte que le gestionnaire du système puisse le cas échéant prendre en temps opportun des mesures qui garantissent la réalisation du règlement dans les délais et limiter les pertes et les tensions de liquidité afin de permettre au système de continuer à remplir ses obligations.

**Article 47 :** Le gestionnaire du système doit, pour la gestion du défaut de participant, définir et formaliser :

- Les conditions, notamment financières et/ou opérationnelles selon lesquelles un participant est considéré en défaut ;

- Les actions systématiques ou discrétionnaires à mettre en œuvre lorsqu'un défaut est déclaré, pour limiter son impact sur le système et les autres participants ;
- Les modalités de gestion des transactions à différents stades du traitement ;
- Les rôles, obligations et responsabilités des différentes parties.

**Article 48 :** Le gestionnaire du système doit communiquer à la Banque Centrale de Tunisie :

- Les conditions de participation, de suspension et de sortie ordonnée du système ;
- Les règles et procédures de gestion du défaut d'un participant ainsi que toutes les modifications qui y sont apportées.

Ces conditions, règles et procédures sont réputées approuvées si la Banque Centrale de Tunisie ne s'y oppose pas dans un délai d'un mois à compter de la date de leur communication.

## Chapitre 3 : Dispositif de gestion des risques financiers

**Article 49 :** Le gestionnaire du système doit se doter d'un dispositif solide de gestion des risques financiers, notamment de crédit et de liquidité, sur ses participants et sur d'autres entités avec lesquelles il entretient des rapports financiers ainsi que ceux découlant de ses processus de paiement, de compensation et de règlement-livraison de titres.

**Article 50 :** Le gestionnaire du système doit identifier les sources des risques financiers, mesurer et surveiller ses expositions et mettre en œuvre les mécanismes adéquats pour assurer une maitrise desdits risques. Il doit notamment :

- Disposer d'outils analytiques et opérationnels efficaces permettant de surveiller ses flux de règlement et d'évaluer les besoins de liquidité et de couverture du risque de crédit tout en procédant à des tests rigoureux de simulation de crise ;
- Mettre en place des règles et procédures explicites lui permettant de s'acquitter de ses obligations dans les délais fixés ou, au plus tard, le

lendemain, y compris celles découlant du défaut d'un ou de plusieurs participants ;
- Définir les règles et les processus à adopter pour reconstituer les liquidités en cas de crise.

**Article 51 :** Le gestionnaire du système doit adopter des mesures d'atténuation des risques financiers notamment par le recours sélectif à des conditions imposées aux participants, des limites d'exposition, des exigences de garantie ou un mécanisme de sécurisation préfinancé. Il doit veiller à ce que :

- Les mécanismes et les exigences adoptés soient proportionnels au profil de risque des participants et exercent l'impact le moins restrictif sur l'accès au système et sur la concurrence ;
- Les actifs acceptés en tant que garanties soient de qualité élevée et suffisamment liquides, tout en adoptant des pratiques de valorisation prudente.

**Article 52 :** Le gestionnaire d'un système opérant avec le règlement net différé dépourvu de toute garantie de règlement, même implicite, et dont les participants sont exposés à un risque financier découlant de ses processus de paiement ou de compensation, doit disposer d'actifs nets liquides suffisants pour pouvoir honorer, le jour même ou au plus tard le lendemain, au moins l'exposition résiduelle inhérente au défaut d'un participant.

**Article 53 :** Le gestionnaire du système doit veiller à ce que sa politique de placement soit compatible avec celle de gestion des risques et que ses placements soient de qualité élevée et suffisamment liquides.

**Article 54 :** Le gestionnaire d'un système de règlement-livraison de titres doit se conformer au principe de livraison contre règlement.

**Article 55 :** Le gestionnaire du système doit transmettre à ses participants un ensemble de données et d'indicateurs les aidant à mesurer et surveiller leurs expositions courantes dans le système. Il peut adopter des règles imposant aux participants de communiquer des informations pertinentes sur leurs expositions lui permettant d'appréhender leurs profils de risques.

**Article 56 :** Le gestionnaire du système doit se doter de procédures de communication, permettant à ses structures de gouvernance d'avoir une connaissance suffisante de son profil risque et des résultats de ses tests de

simulation et ce, afin de prendre les mesures qui s'imposent et de procéder à l'évaluation et, le cas échéant, à la mise à jour du dispositif de gestion des risques financiers.

**Article 57 :** Le gestionnaire du système doit soumettre au préalable à la Banque Centrale de Tunisie les mécanismes qu'il envisage de mettre en place pour l'atténuation de ses risques financiers.

## Chapitre 4 : Dispositif de gestion du risque d'activité

**Article 58 :** Le gestionnaire du système doit disposer de dispositif de gestion adéquat du risque d'activité lui permettant d'identifier, de surveiller et de maitriser ce risque, y compris les pertes dues à une mauvaise exécution de sa stratégie commerciale, à des flux de trésorerie négatifs ou à des charges d'exploitation inattendues et/ou excessivement importantes.

**Article 59 :** Le gestionnaire du système doit détenir des actifs nets liquides financés par les fonds propres lui permettant d'assurer la continuité de ses services si les pertes inhérentes au risque d'activité seraient constatées.

Les actifs nets liquides doivent correspondre au moins à six mois de charges d'exploitation courantes. Ils doivent être d'un niveau de qualité élevée et suffisamment liquides.

**Article 60 :** Le gestionnaire du système doit se doter d'un plan viable et approuvé par le conseil permettant, le cas échéant, la reprise d'activité ou une cessation ordonnée de ses services essentiels.

Il doit se doter aussi d'un plan viable de recapitalisation pour faire face à une éventuelle baisse de ses fonds propres en deçà du niveau requis. Ce plan doit être régulièrement actualisé, et soumis à la Banque Centrale de Tunisie avant son adoption.

## Chapitre 5 : Dispositif de gestion du risque opérationnel

**Article 61 :** Le gestionnaire du système doit se doter d'un dispositif solide de gestion du risque opérationnel approuvé par le conseil. Ce dispositif doit comprendre des politiques, des procédures, des outils et des contrôles appropriés permettant d'identifier, de surveiller et de maitriser ce risque pour assurer un fonctionnement efficace et sécurisé du système.

Le dispositif de gestion du risque opérationnel du système doit s'étendre aux risques nourris par les participants importants du système, les autres systèmes qui lui sont liés ainsi que les prestataires de services qui pourraient impacter son bon fonctionnement.

Le dispositif de gestion du risque opérationnel doit être examiné, audité et testé périodiquement et après tout changement significatif lié à l'activité ou à l'organisation.

**Article 62 :** Le dispositif de gestion du risque opérationnel à mettre en place doit couvrir notamment :

- L'identification des sources courantes et potentielles de ce risque et tenir compte de son évolution ;
- La définition des objectifs de fiabilité opérationnelle et la mise en œuvre des politiques et des outils appropriés ;
- La mise en œuvre de politiques de sécurité physique et de l'information pour contenir les vulnérabilités et menaces potentielles ;
- L'allocation de ressources humaines qualifiées et suffisantes avec une organisation adéquate et une affectation optimale de ces ressources ;
- Le développement d'un plan de continuité d'activité formalisé et régulièrement testé permettant la reprise de l'activité ;
- La définition claire des rôles et des responsabilités dans la gestion du risque opérationnel ;
- La mise en place de processus formels de conduite du changement et de gestion de projets pour atténuer le risque opérationnel résultant de modifications des opérations, des politiques, des procédures et des contrôles.
- La mise en place des plans appropriés pour s'adapter à toute éventuelle variation du volume d'activité ou évolution des spécificités techniques.

**Article 63 :** Le gestionnaire du système doit régulièrement surveiller, examiner et tester la capacité et les performances opérationnelles du système.

Les objectifs de fiabilité opérationnelle définis conformément à l'article 62 de la présente circulaire doivent comporter des mesures qualitatives et quantitatives de

performance opérationnelle du système qui servent de référence pour évaluer son efficience et son efficacité.

Ces objectifs doivent être revus régulièrement pour tenir compte des nouvelles évolutions technologiques et perspectives commerciales.

Le gestionnaire du système doit veiller à ce que le système dispose d'une capacité d'évolution adéquate pour atteindre ses objectifs opérationnels et pour supporter la montée en charge de ses activités.

Les performances opérationnelles du système doivent être communiquées régulièrement aux structures de gouvernance et aux participants.

**Article 64 :** Le gestionnaire du système doit définir des obligations opérationnelles et de continuité d'activité pour ses participants proportionnellement à leurs rôles et leur importance et ce, pour gérer les risques opérationnels qu'ils transmettent au système.

**Article 65 :** Le gestionnaire du système doit identifier et gérer les effets directs et indirects des risques de défaillance opérationnelle de ses prestataires de services externalisés sur la capacité du système à opérer de manière sécurisé et efficace. Il doit notamment :

- Prendre des mesures adaptées pour gérer le risque de dépendance vis-à-vis des prestataires grâce à des dispositifs contractuels et organisationnels appropriés ;
- Eviter la concentration de l'externalisation des opérations auprès d'un seul prestataire de service ;
- Disposer des moyens de contrôle de l'activité de ses prestataires de services lui permettant d'être en conformité permanente avec les exigences de la présente circulaire.

**Article 66 :** Le gestionnaire du système doit mettre en place un plan de continuité d'activité qui :

- Prend en compte les menaces internes et externes et identifie et évalue l'incidence de chacune ;
- Enonce clairement des objectifs de reprise des opérations critiques après interruption ;

- Définit des politiques et des procédures, y compris les mesures organisationnelles et techniques nécessaires pour rétablir l'exploitation ordinaire dans les délais impartis ;
- Définit le(s) point(s) de reprise des services critiques et la durée maximale d'interruption admissible (DMIA) du système ;
- Assigne les responsabilités pour la planification de la continuité de l'activité et affecte les ressources adéquates à cette planification ;
- Prévoit un site secondaire doté de ressources, de capacités et de fonctionnalités suffisantes ainsi que des effectifs appropriés pour assurer les services critiques et indispensables ;
- Prévoit un plan de communication avec les participants et les autres systèmes interdépendants.

**Article 67 :** Le plan de continuité d'activité doit être conçu de façon à permettre :

- La reprise des activités critiques dans la durée maximale d'interruption admissible ;
- D'effectuer les règlements avant la fin de la journée de la survenance de la perturbation.

**Article 68 :** Le plan de continuité d'activité doit, au moins une fois tous les deux ans, faire l'objet d'examen et de tests périodiques sur la base de divers scénarios de rupture d'activité.

Le personnel du gestionnaire du système doit être formé au déploiement du plan de continuité d'activité.

Le gestionnaire du système doit veiller à ce que les participants, les prestataires de services critiques et les systèmes qui lui sont liés participent auxdits tests et reçoivent une synthèse des résultats.

**Article 69 :** Le gestionnaire du système doit se doter de procédures et d'outils techniques adéquats qui permettent d'assurer :

- Le passage du système principal de production au système de secours ou inversement dans les délais impartis et sans perte de données traitées ;
- L'intégrité des messages et des données afférents aux opérations compensées ou réglées tout en garantissant leur traitement adéquat ;

- La confidentialité des données en conformité avec les exigences légales et réglementaires, en particulier à l'occasion de leur transfert ;
- L'enregistrement, la traçabilité et le stockage des données et des opérations à toutes les étapes de traitement, en particulier à l'entrée et à la sortie du système.

**Article 70 :** Le gestionnaire du système doit disposer de procédures exhaustives et formalisées pour enregistrer, analyser et résoudre tous les incidents opérationnels. Il doit en particulier :

- Veiller à la mise en place d'une procédure assurant la déclaration et l'enregistrement des incidents dans une base dédiée ;
- Mettre en place une piste d'audit permettant d'assurer la traçabilité des interventions et des opérations.

Il doit aussi formaliser, enregistrer et surveiller les interventions manuelles dans le système notamment à l'occasion de modifications de logiciels d'exploitation ou de paramétrage.

**Article 71 :** Le gestionnaire du système doit disposer de politiques efficaces de sécurité physique de ses locaux lui permettant :

- De contrôler et de restreindre l'accès à ses locaux ;
- D'évaluer et d'atténuer la vulnérabilité de ses locaux en cas d'attaques, d'intrusions et de catastrophes naturelles.

**Article 72 :** Le gestionnaire du système doit disposer de procédures, des règles de contrôles et des outils solides de sécurité de l'information, portant sur l'identification, l'évaluation et la gestion des menaces et des vulnérabilités portant atteinte à la sécurité de l'information.

Les données doivent être protégées notamment contre la perte, la fuite et l'accès non autorisé ainsi qu'à l'égard d'autres risques liés au traitement et à la gestion, tels que la négligence et la fraude.

Ces mesures de sécurité de l'information doivent respecter les normes de confidentialité, d'intégrité, de disponibilité, d'authentification et de non-répudiation.

**Article 73 :** Le dispositif de gestion du risque opérationnel doit être examiné, audité et testé périodiquement et après tout changement significatif dans le

système ou à la suite d'un incident majeur. Les procédures à appliquer, en cas de difficultés opérationnelles, doivent être validées et testées avec succès au moins une fois par an. Les rapports de tests et d'audit, y compris l'audit de la sécurité des systèmes d'information, doivent être communiqués à la Banque Centrale de Tunisie.

Le gestionnaire du système doit effectuer un audit de sécurité des systèmes d'information au moins une fois par an afin de s'assurer de la pertinence des dispositifs de sécurisation mis en place. Cet audit doit couvrir les prestataires de services auxquels il fait recours. Le gestionnaire du système doit exiger, auprès de ses prestataires auxquels il fait recours, un audit de sécurité de leurs systèmes d'information.

**Article 74 :** Le gestionnaire du système doit :

- Elaborer un rapport sur l'état des incidents importants et sur les modalités de reprise des services ou de réparation des anomalies ;
- Aviser la Banque Centrale de Tunisie des défauts de fonctionnement, d'interruption des activités du système, ainsi que de toute atteinte à la sécurité, à l'intégrité ou à la confidentialité des données et ce, sans préjudice des dispositions qui leur incombent en vertu de la législation et réglementation en vigueur.

# TITRE V : DISPOSITIONS TRANSITOIRES

**Article 75 :** Les dispositions du chapitre 2 du titre III relatives aux organes de gouvernance et du chapitre 1$^{er}$ du titre IV relatives au dispositif de gestion des risques juridiques et de non-conformité et règles de participation de la présente circulaire sont applicables au gestionnaire de système de règlement-livraison de titres tant qu'elles ne dérogent pas aux dispositions légales, réglementaires et statutaires régissant l'activité de dépositaire central de titres.

**Article 76 :** Les gestionnaires des systèmes de paiement exerçant leur activité avant l'entrée en vigueur de la présente circulaire doivent se conformer aux dispositions des articles 4 et 14 dans un délai ne dépassant pas la fin de l'année 2024.

**Article 77 :** Les gestionnaires des systèmes de paiement et du système de règlement-livraison de titres exerçant leur activité avant l'entrée en vigueur de la présente circulaire, doivent se conformer aux dispositions :

- Du titre III relatif au dispositif de gouvernance et du titre IV relatif au dispositif de gestion des risques, à l'exception des articles 51 et 52 du chapitre 3, dans un délai ne dépassant pas dix-huit (18) mois à partir de la date d'entrée en vigueur de la présente circulaire ;
- Des articles 51 et 52 du chapitre 3 du titre IV relatif au dispositif de gestion des risques dans un délai ne dépassant pas deux (2) ans à partir de la date d'entrée en vigueur de la présente circulaire.

**Article 78 :** Le gestionnaire du système de paiement ou du système de règlement-livraison de titres en exercice doit, dans un délai de 3 mois à partir de la date d'entrée en vigueur de la présente circulaire, transmettre à la Banque Centrale de Tunisie une feuille de route déclinant les actions et les mesures à entreprendre pour se conformer à ses dispositions.

**Article 79 :** La présente circulaire entre en vigueur à partir de sa date de publication.

**Le Gouverneur,**

**Marouane EL ABASSI**

**Annexe I à la circulaire n°2024-5 du 13 Février 2024 relative aux règles régissant l'activité de gestion des systèmes de paiement et de règlement-livraison de titres**

**LISTE DES DOCUMENTS ET INFORMATIONS CONSTITUTIFS DU DOSSIER DE DEMANDE D'AGREMENT DE CREATION D'UN SYSTEME DE PAIEMENT**

## 1- Informations sur l'actionnariat du gestionnaire du système de paiement

- Le formulaire « Demande d'agrément » signé par le requérant de l'agrément et comprenant les informations minimales suivantes : qualité, forme juridique et le cas échéant le groupe d'affiliation.
- Un formulaire « Déclaration sur l'honneur » signé par le requérant d'agrément attestant la fiabilité des informations et documents figurant dans le dossier d'agrément.
- Une liste exhaustive des actionnaires personnes physiques et morales qui détiennent des participations directes ou indirectes au capital de la société gestionnaire du système de paiement.
- Le pacte d'actionnaires, le cas échéant.
- Une note succincte sur les actionnaires précisant notamment l'organisation du groupe d'affiliation, ses activités, ses filiales, les participations qu'elles possèdent ainsi que l'expérience du requérant d'agrément dans le domaine d'activité objet de la demande d'agrément.
- Un formulaire « Identité de l'actionnaire » à remplir et à signer par chacun des actionnaires.
- Une copie de la pièce d'identité en cours de validité, le curriculum vitae à jour et un extrait du casier judiciaire délivré depuis moins de trois mois, des actionnaires personnes physiques du gestionnaire du système de paiement.
- Une lettre d'engagement des actionnaires pour la participation dans le capital du gestionnaire du système de paiement signée par les actionnaires.
- Les états financiers individuels et le cas échéant consolidés des trois dernières années, certifiés par les commissaires aux comptes pour les actionnaires personnes morales détenant directement et indirectement des actions dans le capital du gestionnaire du système de paiement.
- Une lettre d'engagement des actionnaires pour participer au capital du gestionnaire du système de paiement à agréer.

- Une copie de l'agrément délivré par l'autorité compétente du pays d'origine si le requérant de l'agrément est gestionnaire d'un système de paiement à l'étranger ou l'accord de ces autorités pour la société siégeant à l'étranger qui entend participer au capital du gestionnaire du système de paiement.

**2- Informations sur l'activité du système de paiement et les services à fournir :**

- Une description détaillée de l'activité à exercer par le système de paiement, de son écosystème, de l'opportunité de sa mise en place, ses fondements, son business model et ses rapports avec les participants et les autres systèmes de paiement.
- Description des participants cibles au système de paiement et des fournisseurs avec lesquels il est envisagé de conclure des conventions.
- Une description des politiques et procédures de travail et la technologie à utiliser couvrant, au moins, les éléments suivants :
    - ✓ Conditions de participation directe et indirecte au système ;
    - ✓ Mécanismes de paiement, de compensation et de règlement et leurs règles ;
    - ✓ Les règles de fonctionnement du système et les niveaux de service à fournir aux participants ;
    - ✓ Une analyse détaillée des risques et des mesures et mécanismes permettant de gérer et réduire les risques du système résultant du déficit de liquidité et d'insolvabilité des participants.
- Les mesures et mécanismes à mettre en place pour maitriser les risques de cyber-attaques et les risques opérationnels notamment techniques dont :
    - ✓ La sécurité des opérations à l'égard des risques d'interruption résultant de la défaillance du système ;
    - ✓ La conservation et le stockage des données du système et des participants en vue d'empêcher la divulgation non autorisée, l'usage abusif, la perte et le vol desdites données ainsi que les mesures pour se conformer aux exigences de la législation en vigueur.
- La convention ou les conventions types à conclure entre le gestionnaire du système de paiement et les participants directs et indirects.
- Politiques et procédures de collecte et de traitement des réclamations des participants au système.

### 3 – Business Model et programme d'activité

- Une lettre d'intention signée par le requérant d'agrément indiquant les motifs de la demande d'agrément.
- Les choix et les objectifs stratégiques en fonction de la catégorie du système de paiement à gérer et des participants directs et indirects au système.
- Une étude de marché, de l'environnement économique et financier du système de paiement à gérer et son positionnement sur le marché.
- La politique de tarification de participation au système de paiement à gérer et du bénéfice des services tenant compte du coût des investissements et des frais opératoires du système par rapport à ses caractéristiques techniques et organisationnelles, des conditions de concurrence et du coût des services de paiement aux usagers finaux.
- La politique de financement du système de paiement en termes de sources de financement et des conditions y afférentes en rapport avec les investissements programmés et l'évolution des charges opératoires pour assurer l'équilibre, optimiser la gestion de liquidité et couvrir en permanence les besoins en la matière.
- Une note sur le pilotage stratégique et opérationnel pour l'implémentation et la mise en production du système de paiement, notamment le planning de mise en œuvre et la feuille de route à cet effet.
- Un business plan sur 5 ans qui comprend :
    - ✓ Les hypothèses retenues pour l'élaboration du business plan et leurs impacts potentiels sur les projections financières sous forme d'indicateurs d'activité et de rentabilité sur une période de 5 ans ;
    - ✓ Des états financiers prévisionnels sur une période de 5 ans outre le détail des principales rubriques de ces états, selon une méthodologie décrivant des scénarii de base, optimiste et prudent ;
    - ✓ Des tests de sensibilité des hypothèses les plus importantes du programme d'activités pour le scénario de base et le plan d'action d'urgence.
- La politique de gestion des ressources humaines pour assurer l'adéquation de ces ressources au fonctionnement du système, notamment l'évolution du nombre d'agents, les modalités de recrutement ainsi que la politique de rémunération et de succession.

**4- Recours à l'externalisation de services auprès de prestataires :**

Fournir une description de la politique et des procédures de recours aux prestataires de services dans le cadre d'externalisation couvrant notamment :

- Les raisons du recours aux prestataires de services ainsi que l'étendue et la nature de services qui seront fournis par ceux-ci ;
- Les critères et les modalités de sélection et de contractualisation ;
- Les responsabilités et les obligations des parties ;
- Les méthodes de gestion et de suivi des activités des prestataires et les procédures de contrôle ;
- Les Projets de conventions qui seront conclus avec les prestataires de services.

**5- Moyens techniques et informatiques :**

- L'architecture technique utilisée :
  - ✓ Une description détaillée de l'architecture technique de l'infrastructure informatique utilisée pour fournir les services de compensation et de règlement et assurer le fonctionnement du système de paiement ;
  - ✓ Une description du dispositif de gouvernance, du système d'information et du dispositif de sécurité informatique en relation avec les dispositions applicables dans ce domaine, dont la protection des données personnelles ;
  - ✓ Une description du système d'information utilisé par les prestataires de services pour assurer le fonctionnement du système de paiement et le suivi du déroulement de ses opérations et services ;
- Caractéristiques techniques du système de paiement sur le plan fonctionnement et fourniture de services :
  - ✓ Une description du processus des services du système de paiement et les caractéristiques techniques de chaque service ;
  - ✓ Diagramme des flux de données indiquant les étapes du processus de compensation et de règlement ;
  - ✓ Description des mécanismes de suivi ainsi que des données à mettre à disposition des participants au système ;

- ✓ Description des exigences et des mesures de sécurité mises à la charge des participants.

- Description des rapports de communication et d'interconnexion avec les participants et l'environnement extérieur tout en spécifiant les exigences techniques, les mesures et les mécanismes de sécurité.
- Sécurité des moyens techniques :
  - ✓ Une description des procédures et outils de sécurité informatique en termes d'accès aux systèmes et aux données, d'intégrité du réseau, de pistes d'audit et d'archivage afin de garantir l'intégrité des données et des opérations, la disponibilité et la continuité des services et le suivi des processus et des flux ;
  - ✓ Description de l'hébergement et de la localisation des infrastructures informatiques et des centres de stockage des données, y compris le site géographique, les certificats d'audit de sécurité et de contrôle des sites ainsi que les mécanismes et mesures de sécurité des services fournis ;
  - ✓ Une description des méthodes et outils d'investigation, d'analyse des incidents d'exploitation pour anticiper, empêcher et corriger les défauts techniques et les cyber-risques.
- Le plan de continuité d'activité comportant notamment les renseignements suivants :
  - ✓ Les activités de base avec les objectifs de reprise de l'activité, y compris le calendrier prévu pour la reprise et les principales étapes, en particulier les actifs prioritaires à protéger, les délais maximums de rupture autorisée et le seuil maximal admissible de perte de données ;
  - ✓ Les moyens mis à disposition pour assurer la continuité de l'activité en cas d'interruption de service dus à des failles dans les systèmes clefs, la perte de données clefs, l'inaccessibilité aux locaux, l'indisponibilité d'hommes clefs ;
  - ✓ La fréquence à laquelle le requérant testera son plan de continuité d'activité de récupération en cas de sinistre, en communicant également le résultat de ces tests et indiquant la manière dont les résultats des tests seront pris en compte ;
  - ✓ Une description des mesures de réduction des risques qui seront approuvées par le demandeur de l'agrément en cas de résiliation du

contrat, assurant la mise en œuvre des opérations du système en cours ;

- ✓ Une description des mesures d'atténuation des risques à adopter par le requérant en cas de résiliation de la convention de prestation des services garantissant l'exécution des opérations en suspens au niveau du système et l'apurement des contrats en cours.

**6- Système de gouvernance, d'organisation et de contrôle interne**

- Le mode de gouvernance cible (direction générale et conseil d'administration ou directoire et conseil de surveillance).
- La composition envisagée du conseil d'administration ou du conseil de surveillance et des différents comités émanant de ces organes (notamment les comités spécialisés de stratégie, d'audit et des risques).
- Une liste nominative des membres du conseil d'administration ou du conseil de surveillance, y compris les membres indépendants et la direction générale (directeur général et directeur général adjoint) ou le directoire.
- Les statuts (ou le projet des statuts) de la société gestionnaire du système de paiement.
- Un curriculum vitae signé avec une pièce d'identité pour chaque membre du conseil indiquant de façon exhaustive le parcours académique et professionnel et un extrait du casier judiciaire daté de moins de trois mois.
- Une déclaration sur l'honneur signée par les membres du Conseil et de l'organe de direction attestant de la sincérité des informations fournies.
- La structure organisationnelle et administrative, les ressources humaines et le dispositif de contrôle interne du gestionnaire du système de paiement et son adéquation avec l'activité de ce système.
- Un rapport sur le dispositif de contrôle interne décrivant :
  - ✓ Les procédures adoptées pour les différentes opérations ;
  - ✓ Le rôle des structures de gouvernance ;
  - ✓ Les relations entre les différentes structures intervenantes ;
  - ✓ Les points et moyens de contrôle des trois niveaux notamment le contrôle permanant et périodique ;
  - ✓ L'organisation comptable et les modalités d'audit et d'examen de l'information financière et comptable.

- Un rapport décrivant le système mis en place pour lutter contre le financement du terrorisme et le blanchiment d’argent.

## MODELE DE DECLARATION SUR L'HONNEUR

Je soussigné(e) **[Prénom] [Nom]** demeurant **[Adresse]** atteste sur l'honneur de l'exactitude des informations et des documents présentés dans le dossier de demande d'agrément pour l'exercice d'activité de gestionnaire de système de paiement.

Fait pour servir et valoir ce que de droit.

**Date,**

Signature

**[Prénom] [Nom]**

## FORMULAIRE D'IDENTITE DE L'ACTIONNAIRE

Nom et prénom, ou dénomination sociale :

.....

Domicile ou siège social :

.....

Titulaire du document d'identité suivant :

CNI/Passeport n°.....délivré(e) à ..... le .....

Société inscrite au Registre National des Entreprises sous le n°.....

et représentée par .....