C I M A
CONFERENCE INTERAFRICAINE
DES MARCHES D'ASSURANCES

CONSEIL DES MINISTRES
DES ASSURANCES

REGLEMENT N° 010 /CIMA/PCMA/CE/SG/2024

RELATIF A LA SECURITE ET A LA GOUVENARNANCE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION ET AU PLAN DE CONTINUITE D'ACTIVITES DES ENTREPRISES D'ASSURANCES ET DE REASSURANCE

LE CONSEIL DES MINISTRES DES ASSURANCES,

Vu le Traité instituant une Organisation intégrée de l'Industrie des Assurances dans les Etats africains notamment en ses articles 6, 39, 40, 41 et 42 ;

Vu le Règlement n°0005/CIMA/PCMA/Ce/SG/2024 du Conseil des Ministres du 28 septembre 2009, modifiant et complétant le Code des assurances des Etats membres de la CIMA ;

Après avis du Comité des experts,

DECIDE :

TITRE I : DEFINITIONS ET GENERALITES

Article 1 : Définitions

Les définitions et dispositions du Code des assurances prévalent pour les termes non définis par le présent règlement.

Aux fins du présent règlement, on entend par :

- Actif informationnel	Ensemble d'informations, tangibles ou non, qui méritent d'être protégées.
- Actifs informatiques	Logiciels ou équipements informatiques présents dans le système d'information de l'entreprise.
- Confidentialité	Propriété selon laquelle les informations ne sont pas mises à la disposition ni divulguées à des personnes, entités, processus ou systèmes non autorisés.
- Conseil d'Administration (CA)	Organe de gouvernance qui détermine les orientations de l'activité de la société et veille à leur mise en œuvre.

- Cyberattaque	Tout type de piratage conduisant à une tentative offensive, malveillante de détruire, exposer, modifier, désactiver, voler ou obtenir un accès non autorisé à un actif informationnel ciblant les systèmes TIC ou d'enfaire un usage non autorisé. Les vecteurs généralement utilisés dont la liste n'est pas exhaustive sont : les programmes malveillants, l'attaque par déni de service distribué (DDOS), l'hameçonnage, l'attaque par injection de code SQL etc.
- Cybersécurité	Préservation de la confidentialité, de l'intégrité et de la disponibilité des informations et/ou des systèmes d'informations par l'intermédiaire d'un dispositif de sécurité.
- Disponibilité	Propriété désignant la capacité d'accessibilité et d'utilisation à la demande (moment opportun) par une entité autorisée.
- Incident opérationnel ou desécurité	Un événement unique ou une série d'événementsimprévus liés qui ont ou auront probablement un impact négatif sur l'intégrité, la disponibilité et la confidentialité des systèmes et services TIC.
- Intégrité	Propriété désignant l'exactitude et l'exhaustivité.
- Prestataire de services	Désigne un tiers exécutant au titre d'un accord de sous-traitance tout ou partie d'une procédure, d'un service ou d'une activité.
- Projets de TIC	Tout projet, ou toute partie d'un projet, où les systèmeset services TIC sont modifiés, remplacés ou mis en œuvre.
- Propriétaire de ressources	Personne ou entité ayant la responsabilité et l'autorité d'un actif informatique.
- Risque informatique et de sécurité	Risque de perte découlant d'une violation de la confidentialité, d'une défaillance de l'intégrité des systèmes et des données, de l'inadéquation ou de l'indisponibilité des systèmes et des données, ou de l'impossibilité de modifier les technologies de l'information dans un délai et pour des coûts raisonnables, lorsque l'environnement ou les exigences « métiers » changent (agilité). Cela inclut les risques de sécurité de l'information résultant de processus internes inadéquats ou défaillants, ou bien d'événements externes, y compris de cyberattaques ou d'une sécurité physique inadéquate.
- Sécurité de l'information	Préservation de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information et/ou de l'information. En outre, d'autres propriétés, telles que l'authenticité, la responsabilité, la non-répudiation et la

fiabilité, peuvent également être impliquées.

- Services de TIC — Services fournis par l'intermédiaire des systèmes de TIC et des prestataires de services à un ou plusieurs utilisateurs internes ou externes.
- Systèmes de TIC — Ensemble d'applications, de services, d'actifs informatiques, ou d'autres composantes de traitement de l'information, y compris l'environnement opérationnel.
- Tests de pénétration basés sur les risques — Tentative contrôlée de compromettre la cyber- résilience d'une entité en simulant les tactiques, les techniques et procédures des acteurs de la menace réelle. Ces essais s'appuient sur des renseignements ciblés sur les menaces et se concentrent sur les personnes, les processus et la technologie d'une entité, avec un minimum de connaissances préalables et d'impact sur les opérations.
- Vulnérabilité — Faiblesse, sensibilité ou faille d'un actif ou d'un logiciel qui est susceptible d'être exploitée par un ou plusieurs attaquants.

TITRE II : TECHNOLOGIES DE L'INFORMATION DE LA COMMUNICATION

Article 2 : Proportionnalité

Les entreprises d'assurances et de réassurance doivent respecter les dispositions stipulées dans le présent règlement de façon proportionnée eu égard à la nature, à l'ampleur et à la complexité des risques inhérents à leur activité.

Article 3 : TIC dans le cadre du système de gouvernance

Le Conseil d'Administration (CA) doit veiller à ce que le système de l'entreprise, notamment le système de gestion des risques et de contrôle interne, gère de manière adéquate les risques liés aux TIC et à la sécurité de l'information.

Le CA doit veiller à ce que l'entreprise se dote de compétences suffisantes (internes ou externes), eu égard à la nature, à l'ampleur et à la complexité des risques inhérents à leur activité.

Ces compétences doivent être adéquates, pour répondre, en termes opérationnels, aux besoins, de gestion des risques et de mise en œuvre de la stratégie en matière de TIC. Par ailleurs, le personnel doit recevoir régulièrement une formation adéquate sur la sécurité de l'information et les risques associés ainsi que le prévoit l'article 14 ci-dessous.

Le CA doit veiller à ce que les ressources allouées soient suffisantes pour répondre aux besoins susmentionnés.

Article 4 : Stratégie en matière de TIC 4

Le CA assume la responsabilité globale de définir, d'approuver, de superviser et de communiquer sur la mise en œuvre de la stratégie écrite en matière de TIC et de sécurité dans le cadre de la stratégie générale de l'entreprise.

La stratégie en matière de TIC doit au moins définir :

a) La façon dont les TIC doivent évoluer afin de soutenir et mettre en œuvre leur stratégie globale, s'agissant notamment de l'évolution de la structure organisationnelle, des modèles d'activité, du système de TIC et des principales dépendances à l'égard de prestataires de services ;

b) L'évolution de l'architecture des TIC, y compris les dépendances vis-à-vis desprestataires de services.

Les entreprises doivent veiller à ce que la stratégie en matière de TIC soit mise en œuvre, adoptée et communiquée en temps utile au personnel et aux prestataires de services concernés lorsque cela présente un intérêt.

Les entreprises doivent également instaurer un processus permettant de surveiller et de mesurer l'efficacité de la mise en œuvre de leur stratégie en matière de TIC. Ce processus doit être révisé et actualisé à intervalles réguliers.

Article 5 : Risques en matière de TIC et de sécurité dans le cadre du système de gestion des risques

Le CA a la responsabilité générale de mettre en place un système efficace de gestion des risques liés aux TIC et à la sécurité dans le cadre du système global de gestion des risques de l'entreprise. Cela inclut la détermination de la tolérance au risque face à ces risques, conformément à la stratégie de l'entreprise en matière de risques, ainsi que la rédaction de manière régulière d'un rapport consacré au résultat du processus de gestion des risques à adresser au CA.

Dans le cadre de leur système global de gestion des risques, les entreprises d'assurances et de réassurance doivent, s'agissant des risques liés aux TIC et à la sécurité (tout en définissant les exigences en matière de protection des TIC décrites ci-dessous), tenir compte à tout le moins, des éléments suivants :

c) Les entreprises d'assurances et de réassurance doivent établir et mettre régulièrement à jour une cartographie de leurs processus et activités, de leurs fonctions « métiers », de leurs rôles et de leurs ressources (par exemple, ressources d'information et de TIC) dans le but de déterminer leur importance et leurs interdépendances au regard des risques liés aux TIC et à la sécurité ;

d) Les entreprises d'assurances et de réassurance doivent recenser et mesurer tous les risques pertinents liés aux TIC et à la sécurité auxquels elles sont exposées et classer les processus et activités, fonctions, rôles etressources de leur entreprise, identifiés (par exemple, ressources d'information et de TIC) en fonction du niveau de risque. Elles doivent également évaluer les exigences de protection, à tout le moins, de la confidentialité, de l'intégrité et de la disponibilité de ces processus et activités, fonctions, rôles et ressources de l'entreprise (par exemple, ressources d'information et de TIC). Les propriétaires de ressources, auxquels il incombe de classer les ressources, doivent être identifiés ;

e) Les méthodes utilisées pour déterminer le niveau de risque ainsi que le niveau de protection requis, notamment en ce qui concerne les objectifs de protection de l'intégrité, de la disponibilité et de la confidentialité, doivent garantir que les exigences de protection qui en découlent sont cohérentes et exhaustives ;

f) L'évaluation des risques liés aux TIC et à la sécurité doit être effectuée sur la base des critères définis en matière de risques liés aux TIC et à la sécurité, en tenant compte du niveau de

risque des processus et activités, des fonctions, rôles et ressources de l'entreprise (par exemple, ressources d'information et de TIC), de l'ampleur des vulnérabilités connues et des incidents antérieurs ayant eu une incidence sur l'entreprise ;

g) L'évaluation des risques liés aux TIC et à la sécurité doit être réalisée et documentée à intervalles réguliers. Cette évaluation doit également être effectuée au préalable de tout changement majeur dans l'infrastructure, les processus ou les procédures affectant les processus et activités, les fonctions, les rôles et les ressources de l'entreprise (par exemple, les ressources d'information et de TIC) ;

h) En s'appuyant sur leur évaluation des risques, les entreprises d'assurances et de réassurance doivent, *a minima*, définir et mettre en œuvre des mesures permettant de gérer les risques liés aux TIC et à la sécurité qui ont été identifiés et de protéger les ressources d'information en fonction de leur classification. Cela doit inclure la définition de mesures destinées à gérer les risques résiduels restants.

Les résultats du processus de gestion des risques liés aux TIC et à la sécurité doivent être approuvés par le CA et intégrés dans le processus de gestion du risque opérationnel dans le cadre de la gestion globale des risques dans les entreprises d'assurances et de réassurance.

Article 6 : Audit

La gouvernance, les systèmes et les processus des entreprises d'assurances et de réassurance concernant leurs risques en matière de TIC et de sécurité doivent faire l'objet d'un audit périodique, conformément au plan d'audit des entreprises, par des auditeurs disposant des connaissances, des compétences et de l'expertise suffisantes en matière de risques liés aux TIC et à la sécurité de façon à fournir au CA, en toute indépendance, une garantie de leur efficacité. La fréquence et les points d'attention de ces audits doivent être proportionnés aux risques concernés en matière de TIC et de sécurité.

Les honoraires de cet audit réalisé par des entités externes pour le compte de l'entreprise d'assurance doivent être fixés à un montant raisonnable et justifié. Ce montant ne peut être supérieur à 20% des honoraires du commissaire aux comptes intervenant dans l'entité. La détention d'une certification pertinente à jour ou reconnaissance équivalente sur le système d'information par l'entreprise doit est prise en compte dans le cadre des travaux d'audit à effectuer et des honoraires. Sauf cas particulier justifié, ces interventions dont le rapport final doit être transmis à la DNA et au Secrétariat Général de la CIMA ne peuvent avoir une périodicité inférieure à trois (3) ans.

Article 7 : Politique et mesures en matière de sécurité de l'information

Les entreprises d'assurances et de réassurance doivent élaborer une politique écrite en matière de sécurité de l'information approuvée par le CA, qui doit définir les principes et règles générales visant à protéger laconfidentialité, l'intégrité et la disponibilité des informations des entreprises afin de soutenir la mise en œuvre de la stratégie en matière de TIC.

La politique doit inclure une description des principaux rôles et responsabilités en matière de gestion de la sécurité de l'information, définir les exigences applicables au personnel, ainsi qu'aux processus et aux technologies en matière de sécurité de l'information, en précisant que le personnel, à tous les niveaux, est responsable d'assurer la sécurité de l'information au sein des entreprises.

Ladite politique doit être communiquée au sein de l'entreprise et s'appliquer à l'ensemble du

personnel. Le cas échéant et s'il y a lieu, la politique relative à la sécurité de l'information, ou certaines parties de cette dernière, doit également être communiquée et appliquée par les prestataires de services.

Sur la base de cette politique, les entreprises doivent établir et mettre en œuvre des procédureset des mesures de sécurité de l'information plus spécifiques, visant notamment, à maîtriser les risques liés aux TIC et à la sécurité auxquels elles sont exposées. Ces procédures et mesures desécurité de l'information doivent inclure, le cas échéant, chacun des processus décrits dans le présent règlement.

Article 8 : Fonction de sécurité de l'information

Les entreprises d'assurances et de réassurance doivent instaurer, dans le cadre de leur système de gouvernance et conformément au principe de proportionnalité, une fonction de sécurité de l'information, dont les responsabilités seraient confiées à une personne désignée. Les entreprises doivent garantirl'indépendance et l'objectivité de la fonction de sécurité de l'information en la séparant judicieusement des processus liés au développement et aux fonctions opérationnelles en matièrede TIC. Cette fonction doit rendre compte au CA.

Il incombe spécifiquement à la fonction de sécurité de l'information de :

a) Soutenir le CA dans la définition et le maintien de la politique de sécurité de l'information et contrôler son déploiement ;

b) Rendre compte au CA et le conseiller, de façon régulière et sur une base *ad hoc*,au sujet de l'état de la sécurité de l'information et son évolution ;

Article 9 : Sécurité logique

Les entreprises d'assurances et de réassurance doivent définir, documenter et mettre en œuvre des procédures de contrôle d'accès logique et de sécurité logique (gestion de l'identité et de l'accès) conformément aux exigences de protection visées dans l'article 5 du présent règlement. Ces procédures doivent être mises en œuvre, appliquées, suivies et révisées périodiquement ; elles doivent également inclure des contrôles visant à surveiller les anomalies. Ces procédures doivent, au minimum, mettre les éléments suivants en œuvre (à ces fins, le terme « utilisateur » inclut les utilisateurs techniques) :

a) Besoin d'en connaître, principe du moindre privilège et séparation des fonctions : les entreprises doivent gérer les droits d'accès, y compris d'accès à distance, aux ressources d'information et à leurs systèmes sous-jacents selon le principe du « besoin d'en connaître ». Les utilisateurs doivent recevoir les droits d'accès minimum strictement requis pour exécuter leurs fonctions (principe du « moindre privilège »), c'est-à-dire pour prévenir tout accès non justifié à des données ou empêcher que l'allocation de droits d'accès combinés puisse servir à contourner les contrôles (principe de la « séparation des fonctions ») ;

b) Identification de l'utilisateur : les entreprises d'assurances et de réassurance doivent limiter, autant que possible, l'utilisation de comptes utilisateurs génériques et partagés et veiller à ce que les utilisateurs puissent être identifiés et associés à tout moment à une personne physique responsable ou à unetâche autorisée pour les actions qu'ils mènent dans les systèmes de TIC ;

c) Droits d'accès privilégiés : les entreprises d'assurances et de réassurance doivent mettre en œuvre des contrôles rigoureux sur l'accès privilégié aux systèmes, en limitant strictement et en surveillant étroitement les comptes assortis de droits d'accès élevés aux systèmes (par exemple les comptes d'administrateurs) ;

d) Accès à distance : afin de garantir une communication sécurisée et de réduire les risques, l'accès à distance à partir d'un compte administrateur à des systèmes de TIC ayant uneimportance critique doit être accordé uniquement selon le principe du « besoin d'en connaître » et lorsque des mesures d'authentification forte sont appliquées ;

e) Enregistrement des activités de l'utilisateur : les activités des utilisateurs doivent être enregistrées et surveillées de manière proportionnée au risque, ce qui inclut, au minimum,les activités des utilisateurs privilégiés. Les registres d'accès doivent être sécurisés afin de prévenir toute modification ou suppression non autorisée, et conservés durant une période minimale de dix (10) ans et proportionnelle au niveau de criticité des fonctions « métiers », des fonctions « supports » et des actifs informationnels, sans préjudice des exigences de conservation définies dans les textes de droit des pays membres de la CIMA. Les entreprises doivent utiliser ces informations pour faciliter l'identification et l'analyse d'activités anormales ayant été détectées dans la fourniture de services ;

f) Gestion des accès : les droits d'accès doivent être accordés, retirés ou modifiés en temps utile, selon des procédures d'approbation prédéfinies incluant le propriétaire fonctionnel des informations auxquelles l'utilisateur accède. Si l'accès n'est plus nécessaire, les droits d'accès doivent être rapidement retirés ;

g) Réévaluation des accès : les droits d'accès doivent périodiquement être réexaminésafin de veiller à ce que les utilisateurs ne possèdent pas de privilèges excessifs et à ce que les droits d'accès soient retirés/supprimés dès lors qu'ils ne sont plus requis ;

h) L'octroi, la modification et la révocation des droits d'accès doivent être documentésde manière à faciliter la compréhension et l'analyse ; et

i) Méthodes d'authentification : les entreprises d'assurances et de réassurance doivent appliquer des méthodes d'authentification suffisamment robustes pour assurer, de façon appropriée et efficace, que les politiques et procédures de contrôle d'accès sont respectées. Les méthodes d'authentification doivent être proportionnées au niveau de criticité des systèmes de TIC, des informations ou des processus auxquels l'utilisateur accède. Au minimum, cela doit inclure des mots de passe complexes ou des méthodes d'authentification plus fortes (comme l'authentification à deux facteurs), en fonction des risques en jeu.

L'accès aux données et aux systèmes de TIC *via des* applications doit se limiter au minimumnécessaire pour fournir le service concerné.

Article 10 : Sécurité physique

Les mesures de sécurité physique des entreprises d'assurances et de réassurance (par exemple, la protection contre les pannesd'électricité, les incendies, les inondations et les accès physiques non autorisés) doivent être définies, documentées et mises en œuvre pour protéger leurs locaux, leurs centres de données et les zones sensibles contre tout accès non autorisé et contre tous les dangers environnementaux.

L'accès physique aux systèmes de TIC doit être accordé uniquement aux personnes autorisées. L'autorisation doit être accordée en fonction des tâches et responsabilités de la personne concernée, en se limitant à des personnes formées et supervisées de manière adéquate. L'accès physique doit être régulièrement réexaminé afin de veiller à ce que les droits d'accès qui ne sont plus nécessaires soient rapidement retirés/supprimés.

Des mesures de protection adéquates contre les dangers environnementaux doivent être proportionnées à l'importance des bâtiments et au caractère critique des opérations ou des systèmes de TIC hébergés dans ces bâtiments.

Article 11 : Sécurité des opérations en matière de TIC

Les entreprises d'assurances et de réassurance doivent mettre en œuvre des procédures permettant de prévenir les incidents de sécurité (garantir la confidentialité, l'intégrité et la disponibilité des systèmes) et de minimiser l'impact de ces incidents sur la prestation des services informatiques. Ces procédures doivent inclure les mesures suivantes :

a) Identification des vulnérabilités potentielles, qui doivent être évaluées et résolues en garantissant que les systèmes de TIC sont à jour, y compris les logiciels fournis par les entreprises à leurs utilisateurs internes et externes, en installant les correctifs de sécurité essentiels, y compris incluant les mises à jour des antivirus, ou en mettant des contrôles compensatoires en œuvre ;

b) Mise en œuvre de configuration sécurisée de référence pour toutes les composantes revêtant une importance critique, telles que les systèmes d'exploitation, les bases de données, les routeurs ou les commutateurs ;

c) Segmentation réseau, systèmes de prévention des fuites de données et chiffrement du trafic du réseau (conformément à la classification des actifs informationnels) ;

d) Mise en œuvre de la protection des terminaux, incluant les serveurs, postes de travail et appareils mobiles. Les entreprises doivent évaluer si les terminaux sont conformes aux normes de sécurité qu'elles ont définies avant de leur accorder l'accès au réseau de l'entreprise ;

e) Mise en place de mécanismes de contrôle de l'intégrité des systèmes de TIC;

f) Chiffrement des données stockées et en transit (conformément à la classification des données).

g) Traitement et protection des données et des transactions, conformément à la loi régissant la protection des données à caractère personnel des Etats membres de la CIMA dans lequel elles exercent leurs activités.

Article 12 : Surveillance de la sécurité

Les entreprises d'assurances et de réassurance doivent établir et mettre en œuvre des processus et des procédures afin de surveiller en permanence les activités ayant une incidence sur la sécurité de l'information des entreprises. Cette surveillance continue doit couvrir au minimum les éléments suivants :

a) Les éléments d'origine externes et internes, en particulier concernant les fonctions métiers et support liés à la gestion des TIC ;

b) Les transactions réalisées par des prestataires de services, d'autres entités ou des utilisateurs internes ;

c) Les menaces potentielles internes et externes.

Pour effectuer cette surveillance, les entreprises doivent mettre en œuvre des dispositifs appropriés et efficaces de détection, de signalement et de réponse à des activités et comportements anormaux. Par exemple, pour détecter des intrusions physiques ou logiques, des vols ou altérations des données, ou encore des exécutions de codes malveillants ou l'exploitation de vulnérabilités matérielles ou logicielles.

Les éléments récupérés par les dispositifs de surveillance doivent également permettre à l'entreprise d'analyser la nature des incidents opérationnels ou de sécurité, d'identifier des tendances et de soutenir les investigations internes pour permettre de prendre des décisions éclairées.

Article 13 : Revues, évaluations et tests de la sécurité de l'information

Les entreprises d'assurances et de réassurance doivent procéder à diverses revues, évaluations et tests en matière de sécurité de l'information, afin d'assurer une identification efficace des vulnérabilités, au sens large, présentes au sein de leurs systèmes et services de TIC. Par exemple, elles peuvent mener des analyses d'écarts par rapport aux normes de sécurité de l'information, des examens de conformité, des audit internes et externes sur les systèmes d'information ou des examens dela sécurité physique.

Les entreprises d'assurances et de réassurance doivent établir et mettre en œuvre un cadre de test de la sécurité de l'information validant la solidité et l'efficacité des mesures de sécurité de l'information et veiller à ce que ce cadre tienne compte des menaces et des vulnérabilités décelées grâce à la surveillance des menaces et au processus d'évaluation des risques liés aux TIC et à la sécurité.

Les tests doivent être menés de manière sécurisée par des testeurs indépendants disposant des connaissances, des compétences et d'une expertise suffisante en sécurité de l'information.

Les entreprises d'assurances et de réassurance doivent tester les mesures de sécurité de manière récurrente. La portée, la fréquence et la méthode des tests (tels que les tests d'intrusion fondés sur les risques) doiventêtre proportionnées au niveau de risque identifié pour les processus et systèmes de l'entreprise.S'agissant de tous les systèmes de TIC ayant une importance critique, ces tests doivent être effectués tous les ans.

Les entreprises d'assurances et de réassurance doivent veiller à ce que les mesures de sécurité soient testées en cas de modification de l'infrastructure, des processus ou des procédures et si des changements sont apportés en raison d'incidents opérationnels ou de sécurité majeurs ou de la publication d'applications critiques nouvelles ou significativement modifiées. Elles doivent surveiller et évaluer les résultats des tests de sécurité et mettre à jour leurs mesures de sécuritéen conséquence, sans retard injustifié dans le cas des systèmes de TIC ayant une importance critique.

Article 14 : Formation et sensibilisation à la sécurité de l'information

Les entreprises d'assurances et de réassurance doivent établir des programmes de formation à la sécurité de l'information pour l'ensemble du personnel et des membres du CA, afin de s'assurer qu'ils soient formés à l'exécution de leurs tâches et responsabilités afin de limiter l'erreur humaine, le vol, la fraude,les abus ou les pertes. Elles doivent veiller à ce que le programme de formation dispense régulièrement des formations à l'ensemble du personnel.

Les entreprises d'assurances et de réassurance doivent veiller à ce que tous les membres du personnel soient formés et les membres du CA soient sensibilisés régulièrement au risque de sécurité informatique afin de savoir comment les traiter et y réagir. Elles doivent établir ces programmes de formation de façon proportionnée eu égard à la nature, à l'ampleur et à la complexité des risques inhérents à leur activité.

Article 15 : Systèmes et logiciels métiers

Les entreprises d'assurances et de réassurance doivent disposer d'un système automatisé de

gestion de l'activité d'assurance sur tous ses pans garantissant une confidentialité, intégrité et disponibilité des données et des informations en tout temps. Tous les processus devraient être automatisés dans la mesure du possible afin de limiter les risques de fraudes et de manipulations.

A ce titre, ce système doit couvrir au minimum les spécifications et fonctionnalités suivantes non exhaustives :

- Intégration du plan comptable des assurances ;
- Automatisation des rapprochements bancaires ;
- Gestion des immobilisations, intégrant les modalités d'évaluation de l'article 335-12 ;
- Édition de l'inventaire des actifs représentatifs de l'entreprises et des autres engagements règlementés ;
- Paramétrage des règles de congruence, de limitations globales et de dispersions (article 335-1 à 335-8 du Code des assurances) ;
- Paramétrage des tarifs des produits, notes techniques, des taux de commissions, les barèmes d'ouverture des sinistres ;
- Paramétrage spécifique du suivi des sinistres de grande ampleur avec automatisation de l'état C10D en non vie ;
- Enregistrement des contrats et des sinistres/prestations avec des informations exhaustives conformément respectivement aux dispositions des articles 414 et 415 du Code des assurances avec la possibilité d'extraction pour une analyse hors système ;
- Identification des polices souscrites par l'Etat et ses démembrements et gestion des traitements afférents ;
- À tout temps, le système doit être en mesure de présenter une image fidèle de la production, de l'état des sinistres/prestations ainsi que les états des règlements/arriérés à différents niveaux de granularité (global, branches, catégories, assurés, souscripteurs, par points de vente ou intermédiaires, etc.) ;
- Classification automatique des arriérés de primes ;
- Traitement automatisé des provisions techniques dans les conditions déterminées par les articles 334-2, 334-4, 334-6, 334-7, 334-8 à 334-13 du Code des assurances ;
- Gestion des intermédiaires d'assurance (et les commissions) et de la réassurance ;
- Historisation des opérations réalisées dans des journaux d'évènement ou pistes d'audit ;
- Génération automatique des données nécessaires à l'édition des états financiers, comptables et statistiques requis par le régulateur ;
- Accessibilité de la base de données des éditeurs de solutions par la société.

Article 16 : Gestion des opérations des systèmes d'information

Les entreprises d'assurances et de réassurance doivent gérer leurs opérations liées aux TIC conformément à leur stratégie en la matière. Pour ce faire, elles doivent se doter et mettre en œuvre des documents définissant lamanière dont elles exploitent, surveillent et contrôlent les systèmes et les services de TIC y compris critiques.

Les entreprises d'assurances et de réassurance doivent mettre en œuvre des procédures d'enregistrement et de surveillance des opérations de TIC ayant une importance critique afin de

détecter, analyser et corriger les erreurs.

Les entreprises d'assurances et de réassurance doivent tenir à jour un inventaire de leurs actifs informatiques. L'inventaire des actifs informatiques doit être suffisamment détaillé pour permettre d'identifier rapidement un actif informatique, son emplacement, sa classification de sécurité et son propriétaire.

Les entreprises d'assurances et de réassurance doivent surveiller et gérer le cycle de vie des actifs informatiques, afin de s'assurer qu'ils répondent toujours aux exigences « métiers » et aux exigences en matière de gestion des risques. Les entreprises doivent surveiller leurs actifs informatiques afin de vérifier s'ils sont bien pris en charge et maintenus par leurs éditeurs ou développeurs internes ou externes et à ce que tous les correctifs et mises à jour pertinents soient appliqués conformément au processus documenté. Les risques découlant des actifs informatiques obsolètes ou non pris en charge doivent être évalués et atténués. Les actifs informatiques inutilisés doivent être traités et éliminés.

Les entreprises d'assurances et de réassurance doivent mettre en œuvre des processus de planification et de surveillance desperformances et des capacités permettant de prévenir, détecter et résoudre tout problème de performance important dans les systèmes de TIC, ainsi que toute limite de capacité, dans un délai raisonnable.

Les entreprises d'assurances et de réassurance doivent définir et mettre en œuvre des procédures de sauvegarde et de restauration des données et des systèmes de TIC visant à assurer qu'ils peuvent être récupérés en cas de besoin. Le périmètre et la fréquence des sauvegardes doivent être définis conformément aux exigences de reprise des activités et en fonction de la criticité des données et systèmes de TIC, et analysés en fonction de l'évaluation des risques correspondante. Les procédures de sauvegarde et de restauration doivent être testées à intervalles réguliers.

Les entreprises d'assurances et de réassurance doivent veiller à ce que les sauvegardes des données et des systèmes de TIC soient stockées de façon sécurisée dans un ou plusieurs endroits suffisamment éloignés du site principal pour ne pas être exposés aux mêmes risques. Au moins une copie des données sauvegardées devrait être stockée dans l'espace CIMA et testées au travers de restaurations périodiques.

Article 17 : Gestion des incidents et des problèmes liés aux TIC

Les entreprises d'assurances et de réassurance doivent établir et mettre en œuvre un processus de gestion des problèmes et incidents afin, d'une part, de surveiller et consigner les incidents opérationnels et de sécurité et,d'autre part, de poursuivre ou rétablir les fonctions et processus « métiers » ayant une importance critique, après une perturbation.

Les entreprises d'assurances et de réassurance doivent déterminer les critères et seuils appropriés pour classer un événementen tant qu'incident opérationnel ou de sécurité, ainsi que les indicateurs d'alerte proactifs devantpermettre la détection précoce desdits incidents.

Afin de minimiser l'impact d'événements indésirables et de permettre une reprise rapide des services, les entreprises doivent établir des processus et des structures organisationnelles appropriés pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents opérationnels et de sécurité et pour veiller à ce que les causes originelles soient identifiées et éliminées afin d'empêcher la réapparition des incidents. Le processus de gestion des incidents et des problèmes doit, *a minima*, établir :

a) Les procédures visant à identifier, suivre, consigner, catégoriser et classer les incidents par ordre de gravité, en fonction de leur criticité pour les métiers ;

b) Les rôles et responsabilités selon les différents types d'incidents (par exemple les erreurs, les dysfonctionnements et les cyberattaques) ;

c) Les procédures de gestion des problèmes permettant d'identifier, d'analyser et de résoudre la cause originelle d'un ou de plusieurs incidents – l'entreprise d'assurance ou de réassurance doit analyser les incidents opérationnels et de sécurité qui ont été identifiés ou qui sont survenus en son sein et/ou à l'extérieur, et doit tenir compte des principaux enseignements tirés de ces analyses et mettre ses mesures de sécurité à jour en conséquence ;

d) Des plans de communication interne efficaces, y compris pour la notification des incidents et les procédures d'escalade - couvrant également les plaintes des clients relatives à la sécurité - afin d'assurer que :

e) Les incidents pouvant avoir une incidence négative importante sur les systèmes et services de TIC ayant une importance critique sont communiqués auprès des instances dirigeantes concernées ;

f) Le CA est informé des éventuels incidents importants de façon ponctuelle et, au minimum, est informée des conséquences des incidents, de la réponse qui leur est apportée et des contrôles supplémentaires à définir en conséquence.

g) Les procédures de réponse aux incidents visant à atténuer les conséquences des incidents et à faire en sorte que le service redevienne opérationnel et sécurisé dès que possible ;

h) Des plans de communication externe spécifiques pour les fonctions « métiers » et les processus revêtant une importance critique, afin de :

i) Collaborer avec les parties prenantes concernées pour répondre en toute efficacité et rétablir les activités suite à l'incident ;

j) En temps utile, fournir des informations, notamment sur le signalement d'incidents, aux parties extérieures (clients, autres acteurs du marché et les autorités de supervision pertinentes).

Article 18 : Gestion des projets de TIC

Les entreprises d'assurances et de réassurance doivent mettre en œuvre une méthodologie de gestion de projet propre aux TIC (tenant compte des exigences en matière de sécurité alignées sur les bonnes pratiques de marché et les normes professionnelles), s'appuyant sur un processus de gouvernance adéquat et une direction de projet ad hoc permettant de soutenir efficacement le déploiement de la stratégie en matière de technologies de l'information et de la communication à travers des projets dédiés.

Les entreprises d'assurances et de réassurance doivent surveiller les risques liés à leur portefeuille de projets de TIC de façons appropriée et les atténuer, en tenant également compte du fait que ces risques peuvent découlerdes interdépendances entre différents projets et des dépendances de plusieurs projets à l'égard des mêmes ressources et/ou expertises.

Article 19 : Acquisition et développement de systèmes de TIC

Les entreprises d'assurances et de réassurance doivent élaborer et mettre en œuvre un processus régissant l'acquisition, le développement et la maintenance des systèmes de TIC afin de garantir la confidentialité, l'intégrité, la disponibilité des données à traiter ainsi que le respect des exigences de sécurité définies. Ce processus doit être conçu selon une approche fondée sur les risques.

Avant l'acquisition ou le développement de systèmes, les entreprises d'assurances et de réassurance doivent veiller à ce que les exigences fonctionnelles et non fonctionnelles (y compris les exigences en matière de sécurité de l'information) et les objectifs techniques soient clairement définis.

Les entreprises d'assurances et de réassurance doivent veiller à ce que des mesures soient prises pour prévenir toutemodification malveillante intentionnelle ou non des systèmes de TIC au cours de leur développement.

Les entreprises d'assurances et de réassurance doivent avoir une méthodologie en place pour le test et l'approbation des systèmes de TIC, des services de TIC et des mesures de sécurité de l'information.

Les entreprises d'assurances et de réassurance doivent tester de manière appropriée les systèmes de TIC, les services de TICet les mesures de sécurité de l'information afin de recenser les faiblesses, violations et incidentspotentiels en matière de sécurité.

En complément, les entreprises d'assurances et de réassurance doivent garantir que les environnements de production sont séparés du développement, du test et des autres environnements ne relevant pas de la production.

Les entreprises d'assurances et de réassurance doivent adopter des mesures afin de protéger l'intégrité du code source (le caséchéant) des systèmes de TIC. Elles doivent également documenter le développement, l'implémentation et le fonctionnement et/ou la configuration des systèmes de TIC, de façon exhaustive, afin de réduire toute dépendance inutile à l'égard d'experts et de conserver la maitrise de la connaissance.

Les processus d'acquisition et de développement de systèmes de TIC des entreprises d'assurances et de réassurance doiventégalement s'appliquer aux systèmes de TIC développés ou gérés par les utilisateurs finaux desmétiers sans l'aval de la direction informatique (par exemple, les applications informatiques del'utilisateur final), en suivant une approche fondée sur les risques. Les entreprises doivent tenir un registre de ces applications soutenant les fonctions ou les processus « métiers » ayant une importance critique.

Article 20 : Gestion des changements liés aux TIC

Les entreprises d'assurances et de réassurance doivent établir et mettre en œuvre un processus de gestion des changements liés aux TIC afin de garantir que toutes les modifications apportées aux systèmes de TIC sont enregistrées, évaluées, testées, approuvées, implémentées et vérifiées de façon contrôlée. Les changements apportés en urgence sur les TIC doivent pouvoir être tracés et notifiés a posteriori au propriétaire des ressources concernées en vue d'une analyse ex post.

Les entreprises d'assurances et de réassurance doivent déterminer si les changements intervenant dans l'environnement opérationnel existant ont une incidence sur les mesures de sécurité existantes et nécessitent l'adoption de mesures supplémentaires afin d'atténuer les risques sous-jacents. Ces changements doivent respecter le processus officiel de gestion du changement des entreprises.

Ces processus doivent être conçus selon une approche fondée sur les risques.

Article 21 : Politique de continuité des activités

Le CA doit définir et approuver la politique globale de continuité des activités TIC de l'entreprise. La politique de continuité des activités TIC doit être communiquée de manière appropriée au sein des entreprises et doit s'appliquer à l'ensemble du personnel concerné et, le cas échéant, aux prestataires de services.

TITRE III : PLAN DE CONTINUITE DES ACTIVITES

Article 22 : Analyse de l'impact sur les activités (AIA)

Dans le cadre d'une bonne gestion de la continuité des activités, les entreprises d'assurances et de réassurance doivent mener une analyse d'impact sur les activités afin d'évaluer leur exposition à de graves perturbations de leurs activités et leurs répercussions potentielles, en termes quantitatifs comme qualitatifs, en utilisant des données internes et/ou externes et une analyse des scénarios. L'analyse de l'incidence sur les activités doit également tenir compte du caractère critique des fonctions « métiers », processus « supports », tiers et actifs informationnels identifiés et classifiés, ainsi que leurs interdépendances, conformément à l'article 5 du présent règlement.

Les entreprises d'assurances et de réassurance doivent veiller à ce que leurs systèmes et services de TIC soient conçus en fonction de leur analyse des impacts sur les activités (AIA) et alignés en conséquence, par exemple en assurant la redondance de certaines composantes ayant une importance critique afin de prévenir les perturbations découlant d'événements qui ont une incidence sur ces composantes.

Article 23 : Planification de la continuité des activités

Les plans généraux de continuité des activités (PCA) des entreprises d'assurances et de réassurance doivent tenir compte desrisques significatifs susceptibles d'avoir une incidence négative sur les systèmes et services deTIC. Les plans doivent soutenir les objectifs visant à protéger et, à restaurer si nécessaire la confidentialité, l'intégrité et la disponibilité de leurs processus « métiers », processus « supports » et actifs informationnels. Elles doivent assurer une coordination appropriée avec les parties prenantes internes et externes, durant la mise en place de ces plans.

Les entreprises d'assurances et de réassurance doivent mettre en place des PCA afin qu'elles puissent réagir de manière appropriée aux scénarios de défaillance potentielle et qu'elles puissent reprendre leurs activités dans la limite de la durée maximale d'interruption admissible (durée maximale au bout de laquelle un système ou processus doit être rétabli après un incident) et en fonction d'une perte de données maximale admissible (période maximale pendant laquelle des données peuvent êtreperdues en cas d'incident à un niveau de service prédéfini).

Les entreprises doivent envisager plusieurs scénarios différents dans leurs PCA, y compris des scénarios extrêmes mais plausibles et des scénarios de cyberattaques, et doit évaluer l'incidence potentielle de ces scénarios. En fonction de ces scénarios, les entreprises doivent décrire la façon dont la continuité des systèmes et services de TIC, ainsi que la sécurité de l'information au sein de l'entreprise, sont assurées.

Article 24 : Plans de réponse et de reprise

En fonction de l'analyse de l'impact sur les activités et des scénarios plausibles, les entreprises doivent définir des plans de réponse et de rétablissement. Ces plans doivent préciser les conditions pouvant déclencher l'activation des plans et des mesures à prendre pour assurer l'intégrité, la disponibilité, la continuité et la reprise, au minimum, des systèmes et services deTIC et des données revêtant une importance critique pour les entreprises d'assurances et de réassurance. Les plans de réponseet de rétablissement doivent viser à répondre aux objectifs de reprise des opérations des entreprises.

Les plans de réponse et de reprise doivent tenir compte à la fois des options de rétablissementà court terme et, lorsque cela est nécessaire, à long terme. Ces plans doivent au minimum :

a) Se concentrer sur le rétablissement des activités des services de TIC importants, des fonctions « métiers », des processus « support », des ressources d'information et de leurs interdépendances afin d'éviter toute incidence négative sur le fonctionnement de l'entreprise ;

b) Être documentés et mis à la disposition des unités « métiers » et « opérationnelles » et facilement accessibles en cas d'urgence, en plus d'inclure une définition claire des rôles et responsabilités ;

c) Être mis à jour en permanence conformément aux enseignements tirés des incidents, des tests, des nouveaux risques et nouvelles menaces identifiés, ainsi que des objectifs et priorités de reprise modifiés.

Les plans doivent également envisager des solutions alternatives si la reprise n'est pas possible à court terme en raison des coûts, des risques, de la logistique ou de circonstances imprévues.

Dans le cadre des plans de réponse et de rétablissement, les entreprises doivent envisager et mettre en œuvre des mesures de continuité afin d'atténuer au minimum la défaillance de prestataires de services, qui revêtent une importance clé pour la continuité des services de TICdes entreprises.

Article 25 : Mise à l'épreuve des plans

Les entreprises doivent tester leurs PCA et veiller à ce que les PCA relatifs aux fonctions « métiers », processus « supports » et activités opérationnelles d'importance critique, leurs fonctions, rôles et ressources d'entreprise (par exemple, les ressources d'information) de mêmeque leurs ressources de TIC et leurs interdépendances (y compris celles fournies par des prestataires de services) soient régulièrement testés en fonction de leur profil de risque.

Les PCA doivent être mis à jour à intervalles réguliers, en fonction des résultats des tests, des renseignements les plus récents sur les menaces et des enseignements tirés des événements précédents. Toute modification pertinente des objectifs de rétablissement (ce qui inclut le tempsde reprise admissible et le point de reprise admissible) et/ou les changements apportés aux processus et activités, aux fonctions, rôles et ressources de l'entreprise (par exemple, les ressources d'information et de TIC) doivent également être prises en compte.

Les tests relatifs aux PCA doivent démontrer que ces derniers sont en mesure d'assurer la continuité de l'activité jusqu'au retour à une situation normale ou tolérable d'un point de vue métier (selon un seuil de service ou de tolérance prédéfinie).

Les résultats des tests doivent être documentés et toute lacune identifiée lors des tests doitêtre analysée, résolue et communiquée au CA.

Article 26 : Communication en situation de crise

En cas de perturbation ou d'urgence, et au cours de la mise en œuvre des PCA, les entreprises d'assurances et de réassurance doivent veiller à disposer de mesures de communication efficaces en situation de crise, afin que toutes les parties concernées internes et externes, y compris les autorités compétentes, si cela est requis par la réglementation nationale, ainsi que les prestataires de services externes, soient informés en temps utile et de façon appropriée.

Article 27 : Sous-traitance des services et des systèmes de TIC

Les entreprises d'assurances et de réassurance doivent veiller à ce que, lorsque des services et des systèmes de TIC sont sous-traités, les exigences applicables au service TIC ou au système TIC soient respectées.

En cas de sous-traitance de fonctions critiques ou importantes, Elles doivent veiller à ce que les obligations contractuelles du prestataire de services (par exemple, contrat, accordsde niveau de service, clauses de résiliation dans les contrats concernés) comprennent à tout le moins les éléments suivants :

a) Des objectifs et mesures appropriés et proportionnés en matière de sécurité de l'information, y compris des exigences telles qu'un niveau minimal en matière de sécurité de l'information, des spécifications relatives au cycle de vie des données des entreprises d'assurances et de réassurance, des droits d'audit et d'accès, ainsi que toutes exigences concernant la localisation et le chiffrement des données, la sécurité du réseau et les processus de surveillance de la sécurité ;

b) Des accords de niveau de service, afin de garantir la continuité des services et des systèmes de TIC, ainsi que des objectifs de performances dans des circonstances normales, ainsique ceux prévus par des plans d'urgence en cas d'interruption du service ; et

c) Des procédures de traitement des incidents opérationnels et liés à la sécurité, notamment pour la déclaration et la remontée des informations.

Les entreprises d'assurances et de réassurance doivent surveiller le niveau de conformité de ces prestataires de services enmatière de sécurité à travers les objectifs, les mesures et les niveaux de performance.

TITRE IV : DISPOSITIONS TRANSITOIRES ET ENTREE EN VIGUEUR

Article 28 : Dispositions transitoires

Les entreprises d'assurances et de réassurance en activité à la date d'entrée en vigueur du présent règlement, disposent d'un délai de vingt-quatre (24) mois pour se conformer à ses dispositions.

Article 29 : Entrée en vigueur

Le présent règlement sera publié au journal officiel de la CIMA et entre en vigueur le premier jour du mois suivant la date de sa publication conformément à l'article 42 du Traité CIMA.

Fait à Abidjan, le 17 décembre 2024

Pour le Conseil des ministres,

Le Président

Conférence Interafricaine des Marchés d'Assurances - CIMA - Conseil des Ministres
Le Président

Adama COULIBALY