ROYAUME DU MAROC

acaps
Autorité de Contrôle des Assurances et de la Prévoyance Sociale

Rabat, le 2 0 DEC 2023

P.IN.05/2023

INSTRUCTION RELATIVE A LA GESTION DES RISQUES CYBER

Le Président de l'Autorité,

Vu la loi n° 17-99 portant code des assurances promulguée par le dahir n° 1-02-238 du 25 rejeb 1423 (3 octobre 2002) telle qu'elle a été modifiée et complétée ;

Vu la loi n° 64-12 portant création de l'Autorité de contrôle des assurances et de la prévoyance sociale promulguée par le dahir n° 1-14-10 du 4 joumada I 1435 (6 mars 2014), notamment son article 19 ;

Vu l'instruction n°P.IN.02/2021 du 04 Février 2021 relative au système de gouvernance,

Décide

L'objet de la présente instruction est de fixer les principes devant être considérés par les entreprises d'assurances et de réassurance pour la gestion des risques cyber. Ces principes concernent la stratégie et la gouvernance de l'entreprise, le système de gestion des risques et la sous-traitance ainsi que la veille, le partage de l'information et la sensibilisation.

Chapitre I - Dispositions générales

Article 1

La présente instruction s'applique aux entreprises d'assurances et de réassurance et ce, sans préjudice des dispositions de la loi n° 05-20 relative à la cybersécurité qui restent applicables à celles désignées en tant qu'infrastructures d'importance vitale en application de l'article 16 de ladite loi.

Article 2

Au sens de la présente instruction, on entend par :

- **Cybersécurité :** l'ensemble de mesures, procédures, concepts de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies permettant à un système d'information de résister à des évènements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessibles.

- **Système d'information :** un ensemble organisé de ressources telles que le personnel, les matériels, les logiciels, les données et les procédures qui permettent de collecter, de classifier, de traiter et de diffuser de l'information sur un environnement donné.

- **Actif informationnel :** toute ressource ayant de la valeur pour l'entreprise, tels que le matériel, le logiciel, la donnée ou la procédure qui composent le système d'information.

- **Incident de cybersécurité :** Un ou plusieurs événements indésirables ou inattendus liés à la sécurité des systèmes d'information et présentant une forte probabilité de compromettre les activités d'une entreprise d'assurance et de réassurance, ou de menacer la sécurité de ses systèmes d'information.

- **Cybermenace :** Une action qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.

Article 3

L'entreprise d'assurances et de réassurance, désignée ci-après « entreprise », intègre les risques cyber dans son système de gouvernance, en tenant compte de la nature, du volume et de la complexité de ses activités.

Article 4

L'entreprise met en place un dispositif de gestion des risques cyber qui comprend la stratégie, la politique, les procédures et le processus de reporting à même de lui permettre de soutenir la sécurité opérationnelle de l'entreprise et la disponibilité, l'intégrité et la confidentialité des données des assurés et des tiers ainsi que d'éviter toute atteinte à sa réputation. Ce dispositif est revu et mis à jour régulièrement pour garantir son efficacité.

Chapitre II - Stratégie et Gouvernance

Article 5

Le conseil d'administration ou le conseil de surveillance de l'entreprise désigné ci-après « Conseil » établit la stratégie de cybersécurité en tenant compte de son appétence au risque. La stratégie énonce clairement les principes à considérer et les objectifs à atteindre en matière de cybersécurité.

Article 6

Le Conseil approuve la politique de l'entreprise en matière de gestion des risques cyber et veille à sa mise en œuvre.

Cette politique couvre notamment les éléments suivants :

- La description des objectifs en matière de cybersécurité qui doivent notamment être cohérents avec la stratégie commerciale de l'entreprise ;

- Les exigences relatives aux personnes, aux processus et aux technologies nécessaires à la gestion des risques cyber et à la communication en temps opportun des incidents de cybersécurité ;
- Les interactions avec les différentes parties prenantes (les intermédiaires d'assurances, les assurés, les prestataires de services, les tiers ...).

Article 7

Le Conseil assure une surveillance efficace de la gestion des risques cyber. Il s'assure notamment que :

- Les responsabilités de l'identification, le suivi et la gestion des risques cyber sont bien définis et attribués de la manière la plus appropriée dans la structure organisationnelle de l'entreprise ;
- Des ressources adéquates, des compétences et expertises suffisantes sont consacrées à la gestion des risques cyber ;
- Des mesures appropriées sont mises en place pour garantir la sensibilisation et l'engagement de l'ensemble du personnel de l'entreprise en matière de cybersécurité.

Le Conseil s'assure également qu'il a accès à des informations pertinentes lui permettant de prendre des décisions éclairées en matière de cybersécurité. Il s'assure en particulier de la cohérence du profil de risque de l'entreprise au regard de son niveau de tolérance aux risques cyber et de ses objectifs commerciaux.

Article 8

La Direction Générale ou le Directoire de l'entreprise désigné ci-après « organe de direction » fournit au Conseil des propositions en vue de la définition de la stratégie et de la politique de l'entreprise en matière de cybersécurité.

L'organe de direction présente au Conseil des informations suffisantes et pertinentes de manière à lui permettre de prendre des décisions en temps utile concernant ces risques.

Il est chargé de la mise en œuvre du dispositif de cybersécurité.

Article 9

L'entreprise désigne un responsable chargé de l'application du dispositif de cybersécurité et de la coordination en la matière. Ledit responsable possède l'expertise et les connaissances requises, jouit de l'indépendance et dispose des ressources nécessaires pour mener à bien sa mission.

Article 10

L'entreprise procède, conformément au plan d'audit fixé par le Conseil, au moins une fois tous les trois (3) ans à un audit externe indépendant de son dispositif de cybersécurité, réalisé par des prestataires experts en la matière. Toutefois, l'entreprise peut substituer l'audit externe précité par un audit effectué en interne et ce, après accord de l'Autorité.

Une copie dudit rapport d'audit est communiquée à l'Autorité au plus tard quinze (15) jours après sa validation par le Conseil.

Chapitre III – Système de gestion des risques

Article 11

L'entreprise traite les risques cyber dans son système global de gestion des risques, conformément à l'appétence aux risques définie par le Conseil.

Le dispositif de cybersécurité, mis en place par l'entreprise conformément à l'article 4 ci-dessus, doit lui permettre d'anticiper, détecter, répondre, contenir et se rétablir des éventuels incidents de cybersécurité.

Article 12

L'entreprise classifie ses actifs informationnels et ses systèmes d'information selon leur niveau de sensibilité aux risques cyber. A cet effet, elle veille notamment à :

- Dresser et maintenir à jour une cartographie de ses actifs informationnels et de ses systèmes d'information en tenant compte des interconnexions avec d'autres systèmes internes et externes ainsi que des dépendances vis à vis des prestataires de services ;
- Effectuer une évaluation des risques des actifs et des systèmes précités et les classifier en termes de criticité pour orienter la priorisation des efforts en matière de détection, de protection, de réponse et de reprise.

L'entreprise arrête des procédures d'habilitation des personnes pouvant accéder aux informations classifiées et des conditions d'échange, de conservation ou de transport de ces informations.

Article 13

L'entreprise met en place des contrôles et des moyens adéquats pour se protéger contre les risques cyber et les gérer dans le cadre des niveaux de tolérance fixés par l'organe de direction. A ce titre, elle veille notamment à :

- Mettre en œuvre des technologies et des processus proactifs pour protéger ses actifs informationnels et ses systèmes d'information en fonction de la criticité et de la classification qui leur sont attribuées. En particulier, ces technologies et processus doivent permettre de protéger les données lorsqu'elles sont au repos ou en transit ;
- Assurer une gestion active des risques cyber pouvant provenir des tiers, notamment par le biais de contrôles lui permettant de vérifier qu'ils ont mis en œuvre des mesures appropriées la protégeant contre les risques cyber.

Article 14

L'entreprise met en place des processus de surveillance systématique pour détecter rapidement les incidents de cybersécurité et évaluer périodiquement l'efficacité des contrôles existants. Ces processus sont revus en permanence pour suivre les évolutions et le niveau de sophistication des cybermenaces.

Article 15

L'entreprise teste d'une manière approfondie son dispositif de cybersécurité. Elle peut se baser à cet effet sur des évaluations de vulnérabilité, la simulation de scénarios d'incidents et des tests d'intrusion.

L'analyse des résultats des tests est exploitée en vue de corriger les faiblesses et les insuffisances éventuelles du dispositif de cybersécurité.

Article 16

L'entreprise met en place des plans de réponse et de rétablissement lui permettant de reprendre ses activités en toute sécurité. Ces plans doivent permettre de soutenir les objectifs de protection de la confidentialité, de l'intégrité et de la disponibilité des actifs informationnels ou des systèmes d'information.

Les plans de réponse et de rétablissement doivent être intégrés au plan de continuité de l'activité de l'entreprise (PCA). Ils doivent être testés au moins une fois par an et faire l'objet d'une révision, le cas échéant.

Article 17

L'entreprise met en place des plans de communication avec les parties prenantes internes et externes (assurés, partenaires commerciaux, autorités compétentes ...) afin d'assurer une communication appropriée et en temps opportun en cas d'incident de cybersécurité. Elle veille en particulier à adopter un plan de communication qui favorise une réponse rapide et une atténuation des risques, dans l'intérêt de l'activité de l'entreprise et des autres parties prenantes.

Chapitre IV – Sous-traitance de la gestion des systèmes d'information

Article 18

Outre les dispositions de l'instruction n°P.IN.02/2021 relative au système de gouvernance, portant sur la sous-traitance des fonctions importantes ou critiques, lorsqu'une entreprise sous-traite la gestion de ses systèmes d'information, elle veille à ce que le contrat de sous-traitance précise les éléments ci-après :

- Les objectifs et les mesures de sécurité techniques et organisationnelles permettant de protéger les systèmes d'information ainsi que les processus de surveillance de cette sécurité ;
- Les objectifs de performances des services aussi bien dans des circonstances normales qu'en situation de crise ;

- Les mesures permettant de garantir la continuité des services en cas d'incident ;
- Les procédures de traitement des incidents de sécurité, en particulier des cas de violation de données ;
- Les conditions de réversibilité permettant d'assurer la reprise partielle ou complète du système d'information ;
- Les exigences de sécurité à observer en cas de recours du prestataire de service à la sous-traitance (cas de chaine de sous-traitance) ;
- Les modalités de déroulement des audits de sécurité, le cas échéant, par l'entreprise d'assurance ou par ses auditeurs externes.

Chapitre V – Veille, partage de l'information et sensibilisation

Article 19

L'entreprise assure une veille continue sur les vulnérabilités et les développements technologiques en matière de cybersécurité afin de pouvoir faire face efficacement aux incidents de cybersécurité aussi bien dans leurs formes connues que nouvelles.

Article 20

L'entreprise veille à échanger avec les parties prenantes les informations pertinentes en matière de cybersécurité sur les menaces, les vulnérabilités, les incidents et les réponses, afin de contribuer au renforcement des défenses et la limitation des dommages et d'élargir l'apprentissage en la matière.

Article 21

L'entreprise veille à assurer des formations et des actions de sensibilisation sur la cybersécurité au profit de ses employés et des personnes ayant accès à ses systèmes d'information. L'entreprise prévoit en particulier des formations personnalisées pour les personnes ayant accès à des données critiques ou sensibles ou ceux dotés d'accès à haut privilèges sur les systèmes d'information.

Chapitre VI- Entrée en vigueur

Article 22

La présente instruction entre en vigueur le premier janvier 2024.

Président de l'Autorité de Contrôle des Assurances
et de la Prévoyance Sociale

Signé : M. Abderrahim Chahbi