boulevard de Berlaimont 14 – BE-1000 Bruxelles
tél. : +32 2 221 48 66
numéro d'entreprise : 0203.201.340
RPM Bruxelles
www.bnb.be

Banque Nationale Bank
DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Bruxelles, le 06 juillet 2021

Référence : NBB_2021_15

votre correspondant :
Thomas Plomteux
tél. : +32 2 221 21 97
thomas.plomteux@nbb.be

Orientations sur la sécurité et la gouvernance des technologies de l'information et de la communication

Champ d'application

- *Entreprises d'assurance et de réassurance de droit belge soumises à la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance (ci-après la « loi Solvabilité II ») (à l'exception des entreprises d'assurance visées aux articles 275, 276 ou 294 de la loi Solvabilité II précitée)*
- *Succursales agréées en Belgique d'entreprises d'assurance ayant leur siège social dans un pays tiers (pays qui n'est pas partie à l'accord sur l'Espace économique européen (EEE))*
- *Entités responsables d'un groupe d'assurance ou de réassurance de droit belge au sens des articles 339, 2°, et 343 de la loi Solvabilité II ou d'un conglomérat financier de droit belge au sens des articles 340, 1°, et 343 de la loi Solvabilité II*

Résumé/Objectif

La présente circulaire met en œuvre les orientations de l'Autorité européenne des assurances et des pensions professionnelles (ci-après l'« EIOPA ») sur la sécurité et la gouvernance des technologies de l'information et de la communication (EIOPA-BoS-20/600)[1] et sera d'application à partir du 6juillet 2021.

[1] Cf. https://www.eiopa.europa.eu/content/guidelines-information-and-communication-technology-security-and-governance_en.

Madame,
Monsieur,

I. Introduction et justification

Par la présente circulaire, la Banque nationale de Belgique (ci-après la « Banque ») indique que les orientations de l'EIOPA sur la sécurité et la gouvernance des technologies de l'information et de la communication sont intégrées dans sa pratique du contrôle. Ces orientations visent à assurer une gestion adéquate des technologies de l'information et de la communication (ci-après les « TIC ») et de la sécurité dans le secteur de l'assurance au sein de l'Union européenne, ainsi que des conditions de concurrence équitables en la matière. Ces orientations contiennent notamment des dispositions relatives à la gouvernance et à la stratégie, à la gestion des risques liés aux TIC et à la sécurité, à la sécurité de l'information, à la gestion des opérations de TIC, à la gestion des projets de TIC et du changement, ainsi qu'à la gestion de la continuité des activités.

La présente circulaire précise donc, dans le cadre de la gestion des risques liés aux TIC et à la sécurité, les attentes de la Banque en matière d'application des dispositions suivantes:

- la loi Solvabilité II, et en particulier l'article 42, § 1er concernant un système de gouvernance adéquat[2];
- le règlement délégué 2015/35 de la Commission européenne du 10 octobre 2014 complétant la directive 2009/138/CE du Parlement européen et du Conseil sur l'accès aux activités de l'assurance et de la réassurance et leur exercice, et en particulier les articles 258 à 260, 266, 268 à 271 et 274[3] du règlement délégué susmentionné.

2 Cet article renvoie notamment à:
- une structure de gestion adéquate basée, au plus haut niveau, sur une distinction claire entre la direction effective de l'entreprise d'assurance ou de réassurance d'une part, et le contrôle sur cette direction d'autre part, et prévoyant, au sein de l'entreprise, une séparation adéquate des fonctions et un dispositif d'attribution des responsabilités qui est bien défini, transparent et cohérent;
- des procédures efficaces d'identification, de mesure, de gestion, de suivi et de reporting interne des risques auxquels l'entreprise est ou pourrait être exposée, y compris la prévention des conflits d'intérêts;
- des fonctions de contrôle indépendantes, à savoir des fonctions-clés d'audit interne, de gestion des risques, etc. indépendantes adéquates;
- des mécanismes de contrôle et de sécurité dans le domaine informatique appropriés aux activités de l'entreprise;
- la mise en place de mesures adéquates de continuité de l'activité afin d'assurer le maintien des données et des fonctions critiques ou leur rétablissement le plus rapidement possible ainsi que la reprise dans un délai raisonnable de l'exercice des activités normales.

3 Ces articles renvoient notamment:
- à des exigences générales en matière de gouvernance pour les entreprises d'assurance et de réassurance, dont le fait qu'elles emploient un personnel possédant les aptitudes, les connaissances et l'expertise nécessaires ; le fait qu'elles se dotent de systèmes d'information qui produisent des informations complètes, fiables, claires, cohérentes, pertinentes et à jour ; le fait qu'elles préservent la sécurité, l'intégrité et la confidentialité des informations (article 258, paragraphe 1);
- au fait que les entreprises d'assurance et de réassurance établissent, mettent en œuvre et gardent opérationnelle une politique de continuité de l'activité (article 258, paragraphe 3);
- au fait que le système de gestion des risques comporte notamment une stratégie de gestion des risques clairement définie, des procédures en ce qui concerne le processus de prise de décision, des politiques écrites et des procédures et processus de reporting (article 259, paragraphe 1);
- aux domaines couverts par la gestion des risques, dont la gestion du risque opérationnel (article 260, paragraphe 1, point f));
- aux caractéristiques du système de contrôle interne (article 266);

II. Précisions relatives au champ d'application et à l'entrée en vigueur

Lorsque les orientations de l'EIOPA font référence aux « entreprises », elles sont applicables au champ d'application défini ci-dessus.

La présente circulaire sera d'application à partir du 6 juillet 2021.

Les orientations de l'EIOPA doivent être lues et appliquées ensemble avec les dispositions des circulaires suivantes:

- la circulaire coupole NBB_2016_31 en matière de système de gouvernance, dans la version modifiée du 5 mai 2020;
- la circulaire NBB_2020_018 du 5 mai 2020 concernant les recommandations de la Banque relatives à la sous-traitance de services en nuage (*cloud services*);
- la circulaire NBB_2015_32 du 18 décembre 2015, qui est applicable en particulier aux entreprises et groupes d'importance significative;
- la circulaire CBFA_2009_17 du 7 avril 2009, qui contient des dispositions complémentaires pour ce qui concerne la fourniture de services financiers via internet;
- la circulaire PPB 2005/2 du 10 mars 2005, qui contient des dispositions complémentaires pour ce qui concerne la gestion de la continuité des activités.

III. Orientations sur la sécurité et la gouvernance des technologies de l'information et de la communication

Définitions

En l'absence de définition dans les présentes orientations, les termes s'entendent tels qu'ils sont définis dans les actes législatifs visés dans l'introduction.

Les définitions suivantes s'appliquent aux fins des présentes orientations:

Propriétaire de ressources	Personne ou entité ayant la responsabilité et l'autorité d'un actif informatique.
Disponibilité	Propriété désignant la capacité d'accessibilité et d'utilisation à la demande (moment opportun) par une entité autorisée.
Confidentialité	Propriété selon laquelle les informations ne sont pas mises à la disposition ni divulguées à des personnes, entités, processus ou systèmes non autorisés.
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 d'information ciblant les systèmes TIC ou d'en faire un usage non autorisé.

- aux dispositions particulières concernant les fonctions, les lignes de reporting et la structure organisationnelle (article 268);
- aux missions et responsabilités de la fonction de gestion des risques (article 269), de la fonction de vérification de la conformité (article 270) et de la fonction d'audit interne (article 271);
- à l'établissement d'une politique écrite en matière de sous-traitance (article 274, paragraphe 1), aux devoirs et responsabilités lors du choix d'un prestataire de services pour toute activité ou fonction opérationnelle importante ou critique (article 274, paragraphe 3), à l'accord écrit entre l'entreprise d'assurance ou de réassurance et le prestataire de services (article 274, paragraphe 4), aux exigences imposées aux entreprises d'assurance ou de réassurance qui sous-traitent des fonctions ou activités opérationnelles importantes ou critiques (article 274, paragraphe 5).

Cybersécurité	Préservation de la confidentialité, de l'intégrité et de la disponibilité des informations et/ou des systèmes d'information par l'intermédiaire d'un dispositif de sécurité.
Actifs informationnels	Logiciels ou équipement informatique présents dans le système d'information de l'entreprise.
Projets de TIC	Tout projet, ou toute partie d'un projet, où les systèmes et services TIC sont modifiés, remplacés ou mis en œuvre.
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 cybernétiques ainsi que 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'informations et/ou d'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.
Actif d'information	Ensemble d'informations, tangibles ou non, qui mérite d'être protégée.
Intégrité	Propriété désignant l'exactitude et l'exhaustivité.
Incident opérationnel ou de sécurité	Un événement unique ou une série d'événements imprévus liés qui ont ou auront probablement un impact négatif sur l'intégrité, la disponibilité et la confidentialité des systèmes et services TIC.
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.
Tests de pénétration basés sur les risques (TLPT)	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.

Orientation 1 – Proportionnalité

1. Les entreprises devraient respecter les dispositions stipulées dans les présentes orientations de façon proportionnée eu égard à la nature, à l'ampleur et à la complexité des risques inhérents à leur activité.

Orientation 2 — Les TIC dans le cadre du système de gouvernance

2. L'organe d'administration, de gestion ou de contrôle (ci-après « l'AMSB ») devrait veiller à ce que le système de gouvernance des entreprises, 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.
3. L'AMSB devrait veiller à ce que les entreprises disposent d'un nombre d'employés suffisant, aux compétences adéquates, pour répondre à leurs besoins en termes opérationnels, de gestion des risques, et de mise en œuvre de la stratégie en matière de TIC. Par ailleurs, le personnel devrait recevoir régulièrement une formation adéquate sur la sécurité de l'information et les risques associés, ainsi que le prévoit l'orientation 13.
4. L'AMSB devrait veiller à ce que les ressources allouées soient suffisantes pour répondre aux besoins susmentionnés.

Orientation 3 – Stratégie en matière de TIC

5. L'AMSB 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.
6. La stratégie en matière de TIC devrait au moins définir:

   a) la façon dont les TIC des entreprises devraient évoluer afin de soutenir et mettre en œuvre leur stratégie globale, s'agissant notamment de l'évolution de la structure organisationnelle, des modèles commerciaux, 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 des prestataires de services;

   c) des objectifs clairs en matière de sécurité de l'information, dédiés aux systèmes de TIC ainsi qu'aux services, au personnel et aux processus des TIC.

7. Les entreprises devraient 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, selon le cas et lorsque cela présente un intérêt.
8. Les entreprises devraient 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 devrait être révisé et actualisé à intervalles réguliers.

Orientation 4 — Risques en matière de TIC et de sécurité dans le cadre du système de gestion des risques

9. L'AMSB 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 d'un rapport écrit régulier consacré au résultat du processus de gestion des risques qui sera adressé à l'AMSB.

10. Dans le cadre de leur système global de gestion des risques, les entreprises devraient, 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:

    a) les entreprises devraient 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;

    b) les entreprises devraient recenser et mesurer tous les risques liés aux TIC et à la sécurité pertinents auxquels elles sont exposées et classer les processus et activités, fonctions, rôles et ressources de leur entreprise identifiés (par exemple, ressources d'information et de TIC) en fonction du niveau de risque. Les entreprises devraient 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, devraient être identifiés;

    c) 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, devraient garantir que les exigences de protection qui en découlent sont cohérentes et exhaustives;

    d) l'évaluation des risques liés aux TIC et à la sécurité devrait 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;

    e) l'évaluation des risques liés aux TIC et à la sécurité devrait être réalisée et documentée à intervalles réguliers. Cette évaluation devrait également être effectuée en amont 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);

    f) en s'appuyant sur leur évaluation des risques, les entreprises devraient, 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 classement. Cela devrait inclure la définition de mesures destinées à gérer les risques résiduels restants.

11. Les résultats du processus de gestion des risques liés aux TIC et à la sécurité devraient être approuvés par l'AMSB et intégrés dans le processus de gestion du risque opérationnel dans le cadre de la gestion globale des risques dans les entreprises.

Orientation 5 - Audit

12. La gouvernance, les systèmes et les processus des entreprises concernant leurs risques en matière de TIC et de sécurité devraient faire l'objet d'un audit périodique, conformément au plan d'audit des entreprises[4], 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 à l'AMSB, en toute indépendance, une garantie de leur efficacité. La fréquence et les priorités de ces audits devraient être proportionnées aux risques concernés en matière de TIC et de sécurité.

Orientation 6 — Politique et mesures en matière de sécurité de l'information

13. Les entreprises devraient élaborer une politique écrite en matière de sécurité de l'information approuvée par l'organe de direction, qui devrait définir les principes et règles de haut niveau visant à protéger la confidentialité, l'intégrité et la disponibilité des informations des entreprises afin de soutenir la mise en œuvre de la stratégie en matière de TIC.

14. La politique devrait 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.

15. Ladite politique devrait 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, devrait également être communiquée et appliquée par les prestataires de services.

16. Sur la base de cette politique, les entreprises devraient établir et mettre en œuvre des procédures et 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 de sécurité de l'information devraient inclure, selon le cas, chacun des processus décrits dans les présentes orientations.

Orientation 7 - Fonction de sécurité de l'information

17. Les entreprises devraient 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 devraient garantir l'indépendance et l'objectivité de la fonction de sécurité de l'information en la séparant judicieusement des processus liés au développement et aux opérations de TIC. Cette fonction devrait rendre compte à l'AMSB.

4 Article 271 du règlement délégué.

18. De manière générale, il incomberait à la fonction de sécurité de l'information de:

a) soutenir l'AMSB dans la définition et le maintien de la politique de sécurité de l'information à l'intention des entreprises et contrôler son déploiement;

b) rendre compte à l'AMSB et la conseiller, de façon régulière et sur une base ad hoc, au sujet de l'état de la sécurité de l'information et son évolution;

c) suivre et examiner la mise en œuvre des mesures de sécurité de l'information;

d) veiller à ce que les exigences en matière de sécurité de l'information soient respectées lors du recours à des prestataires de services;

e) veiller à ce que tous les employés et prestataires de services qui accèdent à l'information et aux systèmes soient correctement informés de la politique de sécurité de l'information, par exemple au moyen de séances de formation et de sensibilisation à la sécurité de l'information;

f) coordonner l'examen des incidents opérationnels ou de sécurité et rendre compte des incidents pertinents à l'AMSB.

Orientation 8 — Sécurité logique

19. Les entreprises devraient définir, documenter et mettre en œuvre des procédures de contrôle d'accès logique ou de sécurité logique (gestion de l'identité et de l'accès) conformément aux exigences de protection visées dans l'orientation 4. Ces procédures devraient être mises en œuvre, appliquées, suivies et révisées périodiquement ; elles devraient également inclure des contrôles pour le suivi des anomalies. Ces procédures devraient, 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 devraient gérer les droits d'accès, y compris d'accès à distance, aux ressources d'information et à leurs systèmes de soutien selon le principe du « besoin d'en connaître ». Les utilisateurs devraient 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 devraient 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 une personne physique responsable ou à une tâche autorisée pour les actions qu'ils mènent dans les systèmes de TIC à tout moment;

c) droits d'accès privilégiés : les entreprises devraient mettre en œuvre des contrôles solides sur l'accès privilégié aux systèmes, en limitant strictement et en surveillant étroitement les comptes assortis de droits élevés d'accès aux systèmes (par exemple les comptes administrateur);

d) accès à distance : afin de garantir une communication sécurisée et de réduire les risques, l'accès administratif à distance à des systèmes de TIC ayant une importance critique devrait être accordé uniquement selon le « besoin d'en connaître » et lorsque des mesures d'authentification forte sont appliquées;

e) enregistrement des activités de l'utilisateur : les activités des utilisateurs devraient être enregistrées et surveillées de manière proportionnée au risque, ce qui inclut, au minimum, les activités des utilisateurs privilégiés. Les registres d'accès devraient être sécurisés afin de prévenir toute modification ou suppression non autorisée, et conservés durant une période proportionnée au niveau de criticité des fonctions « métiers », des fonctions « supports » et des actifs informationnels, sans préjudice des exigences de conservation définies dans le droit de l'UE ou le droit national. Les entreprises devraient 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 devraient 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 devraient être rapidement retirés;

g) réévaluation des accès : les droits d'accès devraient périodiquement être réexaminés afin 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 devraient être documentés de manière à faciliter la compréhension et l'analyse;

i) méthodes d'authentification : les entreprises devraient 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 devraient être proportionnées au niveau de criticité des systèmes de TIC, des informations ou des processus auxquels l'utilisateur accède. Au minimum, cela devrait inclure des mots de passe complexes ou des méthodes d'authentification plus fortes (comme l'authentification à deux facteurs), en fonction des risques pertinents.

20. L'accès aux données et aux systèmes de TIC via des applications devrait se limiter au minimum requis pour fournir le service concerné.

Orientation 9 — Sécurité physique

21. Les mesures de sécurité physique des entreprises (par exemple, la protection contre les pannes d'électricité, les incendies, les inondations et les accès physiques non autorisés) devraient 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.

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

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

Orientation 10 – Sécurité des opérations en matière de TIC

24. Les entreprises devraient 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 devraient inclure les mesures suivantes:

a) identification des vulnérabilités potentielles, qui devraient 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 en mettant à jour les définitions 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 d'information);

d) mise en œuvre de la protection des terminaux, incluant les serveurs, postes de travail et appareils mobiles. Les entreprises devraient évaluer si les terminaux sont conformes aux normes de sécurité qu'elles ont définies avant de lui 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 au repos et en transit (conformément à la classification des données).

Orientation 11 — Surveillance de la sécurité

25. Les entreprises devraient 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 devrait 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.

26. Pour effectuer cette surveillance, les entreprises devraient 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.

27. Les éléments récupérés par les dispositifs de surveillance devraient également permettre à l'entreprise d'analyser la nature des incidents opérationnels ou de sécurité, d'identifier des tendances et d'étayer les enquêtes internes.

Orientation 12 – Revues, évaluations et tests de la sécurité de l'information

28. Les entreprises devraient procéder à divers 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, les entreprises peuvent mener des analyses des faiblesses 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 de la sécurité physique.

29. Les entreprises devraient 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.

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

31. Les entreprises devraient 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 la menace) devraient être 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 devraient être effectués tous les ans.

32. Les entreprises devraient 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 mise en circulation d'applications critiques nouvelles ou fortement modifiées. Les entreprises devraient surveiller et évaluer les résultats des tests de sécurité et mettre à jour leurs mesures de sécurité en conséquence, sans retard injustifié dans le cas des systèmes de TIC ayant une importance critique.

Orientation 13 — Formation et sensibilisation à la sécurité de l'information

33. Les entreprises devraient établir des programmes de formation à la sécurité de l'information pour l'ensemble du personnel, y compris l'AMSB, 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. Les entreprises devraient veiller à ce que le programme de formation dispense régulièrement des formations à l'ensemble du personnel.

34. Les entreprises devraient veiller à ce que tous les membres du personnel, y compris l'AMSB, soient éduqués et sensibilisés régulièrement au risque de sécurité informatique afin de savoir comment réagir.

Orientation 14 – Gestion des opérations des systèmes d'information

35. Afin de suivre leur stratégie en matière de TIC, les entreprises devraient gérer leurs activités en s'appuyant sur la mise en œuvre des processus et procédures documentés en particulier pour les processus, procédures et opérations de TIC revêtant une importance critique. Ces documents devraient définir la manière dont les entreprises exploitent, surveillent et contrôlent les services et systèmes de TIC.

36. Les entreprises devraient 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.

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

38. Les entreprises devraient 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 devraient surveiller leurs actifs informatiques afin de vérifier s'ils sont bien pris en charge par leurs fournisseurs 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 prises en charge devraient être évalués et atténués. Les actifs informatiques inutilisés devraient être traités et éliminés.

39. Les entreprises devraient mettre en œuvre des processus de planification et de surveillance des performances 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.

40. Les entreprises devraient 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 besoins. Le périmètre et la fréquence des sauvegardes devraient 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 devraient être testées à intervalles réguliers.

41. Les entreprises devraient 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.

Orientation 15 — Gestion des incidents et des problèmes liés aux TIC

42. Les entreprises devraient 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.

43. Les entreprises devraient déterminer les critères et seuils appropriés pour classer un événement en tant qu'incident opérationnel ou de sécurité, ainsi que les indicateurs d'alerte proactive devant permettre la détection précoce desdits incidents.

44. Afin de minimiser l'impact d'événements indésirables et de permettre une reprise rapide des services, les entreprises devraient 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 devrait, à minima, établir:

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

b) les rôles et responsabilités inhérents à 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 – une entreprise devrait analyser les incidents opérationnels ou de sécurité qui ont été identifiés ou qui sont survenus en son sein et/ou à l'extérieur, et devrait 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:

i. 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;

ii. l'AMSB est informée 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.

e) 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;

f) 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;

ii. en temps utile, fournir des informations, notamment sur le signalement d'incidents, aux parties extérieures [par exemple les clients, d'autres acteurs au marché et les autorités de supervision pertinentes, le cas échéant et conformément à la réglementation applicable].

Orientation 16 – Gestion des projets de TIC

45. Les entreprises devraient mettre en œuvre une méthodologie de gestion de projet intégrant les exigences en matière de sécurité s'accompagnant d'un processus de gouvernance adéquat et d'un leadership pour la mise en œuvre des projets.

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

Orientation 17 — Acquisition et développement de systèmes de TIC

47. Les entreprises devraient 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 devrait être conçu selon une approche fondée sur les risques.

48. Avant l'acquisition ou le développement de systèmes, les entreprises devraient 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.

49. Les entreprises devraient veiller à ce que des mesures soient prises pour prévenir toute modification intentionnelle ou non des systèmes de TIC au cours de leur développement.

50. Les entreprises devraient 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.

51. Les entreprises devraient tester de manière appropriée les systèmes de TIC, les services de TIC et les mesures de sécurité de l'information afin de recenser les faiblesses, violations et incidents potentiels en matière de sécurité.

52. En complément les entreprises devraient garantir que les environnements de production sont séparés du développement, du test et des autres environnements ne relevant pas de la production.

53. Les entreprises devraient adopter des mesures afin de protéger l'intégrité du code source (le cas échéant) des systèmes de TIC. Elles devraient également documenter le développement, l'implémentation, 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.

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

Orientation 18 – Gestion des changements liés aux TIC

55. Les entreprises devraient 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 lors de modifications effectuées en urgence sur les TIC devraient pouvoir être tracés et notifiés a posteriori au propriétaire des ressources concerné en vue d'une analyse ex post.

56. Les entreprises devraient 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 concernés. Ces changements devraient respecter le processus officiel de gestion du changement des entreprises.

Orientation 19 – Gestion de la continuité des activités

57. Dans le cadre de la politique globale de continuité des activités des entreprises, il incombe à l'AMSB de définir et d'approuver la politique de continuité des activités TIC des entreprises. La politique de continuité des activités TIC devrait être communiquée de manière appropriée au sein des entreprises et devrait s'appliquer à l'ensemble du personnel concerné et, le cas échéant, aux prestataires de services.

Orientation 20 — Analyse de l'impact sur les activités (AIA)

58. Dans le cadre d'une bonne gestion de la continuité des activités, les entreprises devraient mener une analyse d'impact sur les activités afin d'évaluer l'exposition des entreprises 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 devrait 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'orientation 4.

59. Les entreprises devraient 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.

Orientation 21 – Planification de la continuité des activités

60. Les plans généraux de continuité des activités (PCA) des entreprises devraient tenir compte des risques significatifs susceptibles d'avoir une incidence négative sur les systèmes et services de TIC. Les plans devraient 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. Les entreprises devraient assurer une coordination appropriée avec les parties prenantes internes et externes, durant la mise en place de ces plans.

61. Les entreprises devraient mettre en place des PCA afin qu'elles puissent réagir de manière appropriée aux scénarios de défaillance potentiels et qu'elles puissent reprendre leurs activités dans la limite de la durée maximale d'interruption admissible (durée maximal 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 être perdues en cas d'incident à un niveau de service prédéfini).

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

Orientation 22 — Plans de réponse et de reprise

63. En fonction de l'analyse de l'impact sur les activités et des scénarios plausibles, les entreprises devraient définir des plans de réponse et de rétablissement. Ces plans devraient 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 de TIC et des données revêtant une importance critique pour les entreprises. Les plans de réponse et de rétablissement devraient viser à répondre aux objectifs de reprise des opérations des entreprises.

64. Les plans de réponse et de reprise devraient tenir compte à la fois des options de rétablissement à court terme et, lorsque cela est nécessaire, à long terme. Ces plans devraient 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.

65. Les plans devraient 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.

66. Dans le cadre des plans de réponse et de rétablissement, les entreprises devraient envisager et mettre en œuvre des mesures de continuité afin d'atténuer au minimum la défaillance des prestataires de services, qui revêtent une importance clé pour la continuité des services de TIC des entreprises (conformément aux dispositions des orientations de l'EIOPA relatives au système de gouvernance et des orientations relatives à la sous-traitance à des prestataires de services en nuage).

Orientation 23 - Mise à l'épreuve des plans

67. Les entreprises devraient 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 même que 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.

68. Les PCA devraient 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 temps de 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) devraient également être prises en compte.

69. Les tests relatifs aux PCA devraient 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).

70. Les résultats des tests devraient être documentés et toute lacune identifiée lors des tests devrait être analysée, résolue et communiquée auprès de l'AMSB.

Orientation 24 — Communication en situation de crise

71. En cas de perturbation ou d'urgence, et au cours de la mise en œuvre des PCA, les entreprises devraient 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 informées en temps utile et de façon appropriée.

Orientation 25 — Sous-traitance des services et des systèmes de TIC

72. Sans préjudice des orientations de l'EIOPA relatives à la sous-traitance à des prestataires de services en nuage, les entreprises devraient 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.

73. En cas de sous-traitance de fonctions critiques ou importantes, les entreprises devraient veiller à ce que les obligations contractuelles du prestataire de services (par exemple, contrat, accords de 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, 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, ainsi que ceux prévus par des plans d'urgence en cas d'interruption du service;

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

74. Les entreprises devraient surveiller le niveau de conformité de ces prestataires de services en matière de sécurité à travers les objectifs, les mesures et les niveaux de performance.

IV. Diffusion

Une copie de la présente circulaire est adressée au(x) commissaire(s), réviseur(s) agréé(s) de votre entreprise.

Je vous prie d'agréer, Madame, Monsieur, l'assurance de notre considération distinguée.

p.p. Pierre Wunsch
Gouverneur

Steven Vanackere
Vice-gouverneur