SECRÉTARIAT GÉNÉRAL

Notice relative aux modalités de mise en œuvre par les entreprises du secteur l'assurance et les organismes de retraite supplémentaire des orientations de l'Autorité européenne des assurances et pensions professionnelles relatives à la sécurité et à la gouvernance des technologies de l'information et de la communication (EIOPA-BoS-20/600).

(Version du 18/06/2021)

1. Présentation

Le présent document a pour objet d'assurer le respect des Orientations de l'Autorité européenne des assurances et pensions professionnelles (« AEAPP ») relatives à la sécurité et à la gouvernance des technologies de l'information.

La présente notice a pour objet de prévoir la mise en œuvre par les entreprises d'assurance ou de réassurance relevant du régime « Solvabilité II » mentionnés aux articles L. 310-3-1 du code des assurances, L. 211-10 du code de la mutualité ou L. 931-6 du code de la sécurité sociale ainsi qu'aux organismes de retraite professionnelle supplémentaire mentionnés aux articles L. 381-1 du code des assurances, L. 214-1 du code de la mutualité et L. 942-1 du code de la sécurité sociale (ci-après « les entreprises assujetties aux orientations de l'AEAPP ») des orientations de l'AEAPP relatives à la sécurité et la gouvernance des technologies de l'information et de la communication (EIOPA-BoS-20/600).

Ces orientations précisent notamment les diligences à effectuer par les organismes d'assurance et de réassurance afin de tenir compte de l'importance de la gestion du risque des nouvelles technologies de l'information et de sa prise en compte par la gouvernance. Les exigences en matière de gouvernance applicables aux ORPS sont similaires à celles relatives aux organismes d'assurance. La notice de l'ACPR du 17 décembre 2015 reprenant les orientations de l'AEAPP sur le système de gouvernance a ainsi été étendue aux ORPS dans la notice spécifique à ces organismes, publiée le 17 septembre 2018 par l'ACPR.

Dans cette même logique, il est attendu des ORPS qu'ils mettent en œuvre l'ensemble des orientations susmentionnées relatives à la sécurité et la gouvernance des technologies de l'information et de la communication.

Pour rappel, en application de la politique de transparence de l'ACPR, une notice a vocation à apporter des explications aux personnes contrôlées sur les modalités de mise en œuvre d'un texte réglementaire. Son contenu ne saurait toutefois épuiser toutes les questions soulevées par la mise en œuvre d'une orientation de l'AEAPP. Par ailleurs, la notice ne préjuge pas des décisions individuelles qui pourraient être prises par l'ACPR, sur la base des situations particulières qu'elle pourra être amenée à examiner.

Les orientations AEAPP ayant réaffirmé un principe d'application des mesures de gestion du risque informatique proportionnelle à la nature, à l'ampleur et à la complexité des risques inhérents à l'activité des entreprises assujetties concernées, les indications fournies par la Notice doivent être lues dans le respect de ce principe. À ce titre, l'ACPR tiendra compte de l'organisation interne des entreprises assujetties, de la nature, du périmètre et de la complexité des produits et services que ces entreprises fournissent ou comptent fournir.

La présente notice est applicable à compter du jour de sa publication au registre officiel de l'ACPR.

2. Champ d'application

L'ACPR entend se conformer pleinement aux orientations sur la sécurité et la gouvernance des technologies de l'information et la communication publiées le 12 octobre 2020 en version anglaise et le 6 février 2021 en version française.

L'ACPR s'attend à ce que les orientations auxquelles elle déclare se conformer soient mises en œuvre par les entreprises susvisées.

Définitions

1. 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.
2. 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.
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 informatiques	Logiciels ou équipements informatiques 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 informationnels	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

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

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.

L'AMSB devrait veiller à ce que les entreprises disposent d'un nombre d'employés suffisant qui doit être jugé de façon proportionnée eu égard à la nature, à l'ampleur et à la complexité des risques inhérents à leur activité.

Leurs compétences devraient être adéquates, pour répondre, en termes opérationnels, à leurs besoins, 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.

L'AMSB devrait veiller à ce que les ressources allouées soient suffisantes pour répondre aux besoins susmentionnés.

Orientation 3 – Stratégie en matière de TIC

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.

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 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 des prestataires de services etc.) 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.

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 lorsque cela présente un intérêt.

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

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 de manière régulière d'un rapport consacré au résultat du processus de gestion des risques à adresser à l'AMSB.

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 pertinents liés aux TIC et à la sécurité 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 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) ;

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 classification. Cela devrait 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 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

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, 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 points d'attention de ces audits devraient être proportionnés aux risques concernés en matière de TIC et de sécurité.

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

Les entreprises devraient élaborer une politique écrite en matière de sécurité de l'information approuvée par l'AMSB, qui devrait définir les principes et règles générales 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.

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.

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.

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, le cas échéant, chacun des processus décrits dans les présentes orientations.

Orientation 7 - Fonction de sécurité de l'information

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 fonctions opérationnelles en matière de TIC. Cette fonction devrait rendre compte à l'AMSB.

Il incomberait spécifiquement 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 et contrôler son déploiement ;

b) Rendre compte à l'AMSB 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 ;

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 et de sécurité et rendre compte des incidents pertinents à l'AMSB.

Orientation 8 — Sécurité logique

Les entreprises devraient 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'orientation 4. Ces procédures devraient être mises en œuvre, appliquées, suivies et révisées périodiquement ; elles devraient également inclure des contrôles visant à surveiller les 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 sous-jacents 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 tout moment à une personne physique responsable ou à une tâche autorisée pour les actions qu'ils mènent dans les systèmes de TIC ;

c) Droits d'accès privilégiés : les entreprises devraient 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'administrateur) ;

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 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 ; et

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 en jeu.

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

Orientation 9 — Sécurité physique

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.

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 formées et supervisées de manière adéquate. 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.

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

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 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 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 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).

Orientation 11 — Surveillance de la sécurité

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.

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.

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 de soutenir les investigations internes pour permettre de prendre des décisions éclairées.

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

Les entreprises devraient 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, les entreprises 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 de la sécurité physique.

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.

Les tests devraient 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 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 les risques) 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.

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 publication d'applications critiques nouvelles ou significativement 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
Les entreprises devraient établir des programmes de formation à la sécurité de l'information pour l'ensemble du personnel et des membres de 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.

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

Orientation 14 – Gestion des opérations des systèmes d'information
Les entreprises devraient 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 la manière dont elles exploitent, surveillent et contrôlent les systèmes et les services de TIC y compris critiques.

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.

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.

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 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 devraient être évalués et atténués. Les actifs informatiques inutilisés devraient être traités et éliminés.

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.

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 besoin. 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.

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

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.

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 proactifs devant permettre la détection précoce desdits incidents.

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, *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 – une entreprise devrait analyser les incidents opérationnels et 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 du marché et les autorités de supervision pertinentes, le cas échéant et conformément à la réglementation applicable].

Orientation 16 – Gestion des projets de TIC

Les entreprises devraient mettre en œuvre une méthodologie de gestion de projet propre aux TICs (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 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

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.

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.

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.

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.

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.

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.

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.

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

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 en urgence sur les TIC devraient pouvoir être tracés et notifiés a posteriori au propriétaire des ressources concernées en vue d'une analyse ex post.

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 sous-jacents. Ces changements devraient respecter le processus officiel de gestion du changement des entreprises.

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

Orientation 19 – Gestion de la continuité des activités

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)

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 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 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.

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
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.

Les entreprises devraient 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 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).

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, sont assurées.

Orientation 22 — Plans de réponse et de reprise
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.

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 ; et

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 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.

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'AEAPP 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
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.

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.

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).

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

Orientation 24 — Communication en situation de crise
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 informés en temps utile et de façon appropriée.

Orientation 25 — Sous-traitance des services et des systèmes de TIC
Sans préjudice des orientations de l'AEAPP 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.

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 ; 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 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 performanc