SECRÉTARIAT GÉNÉRAL

Notice relative à la gestion du risque informatique pour les entreprises du secteur de la banque, des services de paiement et des services d'investissement

(Version du 07 juillet 2021)

Table des matières

CHAMP

1. La présente Notice s'adresse aux entreprises du secteur de la banque, des services de paiement et des services d'investissement visées par l'arrêté du 3 novembre 2014 relatif au contrôle interne (ci-après « les entreprises assujetties »).

Présentation

2. Par cette Notice, l'Autorité de contrôle prudentiel et de résolution (ACPR) souhaite apporter des explications à propos des nouvelles dispositions relatives à la gestion du risque informatique introduites par l'arrêté modificatif du 25 février 2021[1] dans l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (ci-après « l'arrêté »). Ces évolutions ont pour effet de mettre le cadre règlementaire français en conformité avec les orientations de l'Autorité bancaire européenne (ABE) EBA/GL/2019/04 sur la gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité (ci-après « les orientations ABE »).

3. Les orientations ABE ont souligné que le risque informatique devait être pleinement pris en compte dans le dispositif général de gestion des risques. C'est pourquoi les nouvelles dispositions ont été intégrées à l'arrêté relatif au contrôle interne et renvoient aux dispositifs de gouvernance, de contrôle interne et de gestion des risques. Avec les modifications apportées à l'arrêté, l'ACPR est conforme aux orientations ABE, à la fois par les dispositions générales relatives au contrôle interne, et par les nouvelles dispositions introduites spécifiquement pour renforcer la maîtrise du risque informatique.

4. La Notice vise à clarifier les modalités de mise en œuvre des nouvelles dispositions de l'arrêté. Elle replace ainsi les éléments sur la gestion du risque informatique dans le contexte général du contrôle interne et de la gestion des risques. Elle se réfère pour cela aux principes figurant dans les orientations ABE, en les précisant en tant que de besoin.

5. Le cas échéant, certaines explications fournies par la Notice ont pu être nourries par les bonnes pratiques présentées dans le Document de Réflexion sur le risque informatique en date du 28 janvier 2019.

6. Les bonnes pratiques recommandées par l'ANSSI sont également encouragées par l'ACPR, et la Notice les mentionne donc ponctuellement.

[1] Arrêté du 25 février 2021 modifiant l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.

7. Les orientations ABE[2] et les nouvelles dispositions réglementaires françaises[3] ayant réaffirmé un principe d'application des mesures de gestion du risque informatique proportionnelle à la taille et à la complexité des entreprises assujetties concernées, les indications fournies par la Notice doivent être lues dans le respect de ce principe. Au titre de l'arrêté, l'ACPR tiendra compte de la taille, du volume d'activités, des implantations ainsi que de la nature, de l'échelle et de la complexité des risques inhérents au modèle d'entreprise et aux activités des entreprises assujetties. En outre, au titre des orientations ABE, dont l'approche est similaire, elle 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.

8. Le thème de l'externalisation n'est pas particulièrement développé dans la Notice, dans la mesure où les dispositions en la matière ne sont pas propres à la gestion du risque informatique. En revanche, l'ACPR rappelle, en accord avec l'article 237 de l'arrêté, que les entreprises assujetties qui externalisent tout ou partie de leur service informatique, demeurent pleinement responsables du respect de toutes les obligations qui leur incombent au titre de l'arrêté.

[2] Section 1.1 des orientations ABE : « *Tous les établissements financiers devraient respecter les dispositions stipulées dans les présentes orientations d'une façon qui, d'une part, soit proportionnée à la taille et à l'organisation interne des établissements financiers, à la nature, la portée et la complexité des produits et services que ces établissements fournissent ou comptent fournir et au risque qu'ils présentent, et qui, d'autre part, tienne compte de ces facteurs.* »

[3] Article 4 de l'arrêté : « *Les entreprises assujetties veillent à mettre en place un contrôle interne en adaptant l'ensemble des dispositifs prévus par le présent arrêté, ainsi que, le cas échéant, par les dispositions européennes directement applicables, à la taille, au volume de leurs activités, aux implantations ainsi qu'à la nature, à l'échelle et à la complexité des risques inhérents à leur modèle d'entreprise et à leurs activités*. »

Section 1 : GOUVERNANCE ET DISPOSITIF DE GESTION DU RISQUE INFORMATIQUE

Chapitre Ier : Gouvernance

Point 1 : stratégie informatique

Premier alinéa de l'article 270-1 de l'arrêté (cf. §4 à 6 des orientations ABE)

Le premier alinéa de l'article 270-1 de l'arrêté dispose que « *les entreprises assujetties établissent leur stratégie en matière informatique afin de répondre aux objectifs de leur stratégie d'affaires* ». Cette disposition pose ainsi le principe selon lequel les moyens informatiques mis en œuvre doivent répondre aux besoins de l'entreprise, ou du groupe auquel elle appartient, pour la réalisation de ses activités, ce qui inclut les besoins de ses clients. La stratégie informatique est ainsi partie intégrante de la stratégie générale de l'entreprise. À défaut, le risque serait que la fonction informatique s'engage dans des choix qui ne serviraient pas au mieux les intérêts de l'entreprise assujettie.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- La stratégie informatique définit, en accord avec les équipes « métier » ou sous leur conduite, les objectifs d'évolution du système d'information à court et moyen termes, donc sur plusieurs années, et les moyens pour les atteindre.
    - ✓ À titre de bonne pratique, la stratégie informatique devrait reposer sur un processus formalisé permettant de recueillir les besoins des « métiers » et des « fonctions » utilisateurs du système d'information sur plusieurs années, tout en y incluant les besoins propres à l'évolution et au maintien en condition des systèmes informatiques eux-mêmes (obsolescence, capacité, etc.).

- Outre les besoins de l'entreprise, la stratégie informatique prend en compte, sur plusieurs années, les évolutions du système d'information nécessaires au maintien des capacités des systèmes informatiques, et vise à assurer la maîtrise des dépendances vis-à-vis de prestataires et un niveau élevé de sécurité.
- Les dirigeants effectifs sont responsables de la définition, de la validation, de la mise en œuvre et du suivi de cette stratégie au titre de leur responsabilité générale sur la bonne marche de l'entreprise et de la maîtrise des risques, donc également du risque informatique. Cela permet également de renforcer les engagements pris au titre de la stratégie informatique et de veiller à ce qu'ils soient atteints.
- L'organe de surveillance approuve la stratégie informatique et veille par la suite à sa bonne mise en œuvre.
- La stratégie informatique tient compte des besoins de continuité d'activité de l'entreprise assujettie.
- La stratégie informatique se décline en plans d'action permettant d'atteindre les objectifs qu'elle fixe et repose sur des processus permettant de vérifier l'efficacité de sa mise en œuvre.

- ✓ À titre de bonne pratique, un plan d'action stratégique est assorti notamment d'objectifs de mise en œuvre, de délais et périodes de mise en place, de critères de succès, de ressources, d'une estimation des coûts ainsi que d'une évaluation des risques. Les différentes actions sont idéalement hiérarchisées en fonction des priorités stratégiques auxquelles elles répondent.

- Le plan d'action stratégique est communiqué à toutes les personnes concourant à celui-ci, y compris les prestataires lorsque cela est nécessaire, et fait l'objet d'une réévaluation périodique.
  - ✓ À titre de bonne pratique, la revue annuelle de la stratégie informatique est encouragée**,** sauf si l'évolution de l'environnement informatique incite à choisir une fréquence différente. Par exemple, le changement de modèle d'affaires, la mise en place de nouvelles technologies ou le remplacement d'un prestataire de service essentiel peuvent justifier le choix de révisions plus fréquentes.

- La mise en œuvre du plan d'action fait l'objet d'un pilotage pour s'assurer de la réalisation des objectifs fixés, anticiper toute difficulté et procéder en cas de besoin à des ajustements.

Point 2 : adéquation des ressources allouées

Second alinéa de l'article 270-1 de l'arrêté (cf. §3 des orientations ABE)

Le second alinéa de l'article 270-1 de l'arrêté dispose que « *les dirigeants effectifs et l'organe de surveillance s'assurent que les ressources allouées à la gestion des opérations informatiques, à la sécurité du système d'information, ainsi qu'à la continuité d'activité sont suffisantes pour que l'entreprise assujettie remplisse ses missions* ». Dans la continuité des dispositions relatives à l'établissement d'une stratégie, l'arrêté impose ainsi que l'entreprise assujettie alloue des moyens financiers, humains et techniques suffisants pour pouvoir mettre en œuvre son système d'information dans de bonnes conditions de fonctionnement et de sécurité, conformément à ses objectifs stratégiques. La responsabilité en incombe aux dirigeants effectifs de manière permanente et continue et à l'organe de surveillance, à l'occasion de l'approbation de la stratégie par ce dernier ainsi qu'au titre des *reportings* qui lui sont faits. L'article 270-1 va au-delà des dispositions de l'article 216[4] consacré à la maîtrise du risque opérationnel, en ce sens qu'il traite de l'ensemble des ressources (financières, mais aussi humaines et techniques) utilisées pour assurer les différents types d'opérations informatiques, et non pas uniquement celles relatives à la maîtrise du risque au sens strict.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les tableaux de bord synthétisant l'activité informatique (qu'il s'agisse de la conduite opérationnelle des services existants ou de la fourniture de nouveaux services) et l'évaluation des risques associés transmis aux dirigeants effectifs sont suffisamment clairs, compréhensibles et compris pour permettre des prises de décisions adaptées au profil de risque de l'entreprise assujettie.

- Les équipes en charge des opérations informatiques et de la sécurité informatique disposent d'effectifs en nombre suffisant ayant les compétences requises en les maintenant à jour par des formations ou des certifications.

[4] Article 216 de l'arrêté : « *Les entreprises assujetties se dotent des moyens adaptés à la maîtrise des risques opérationnels, y compris juridiques*. »

- ✓ À titre de bonne pratique, il est souhaitable de formaliser la politique de gestion des ressources humaines en charge des opérations informatiques, dont la dimension technique est forte par nature, en précisant la répartition cible des effectifs internes et externes, ainsi que les fonctions clés pour lesquelles il est dans la mesure du possible préférable de conserver en interne une expertise suffisante. Elle peut être complétée par une politique de gestion des compétences définissant les objectifs de formation du personnel, en particulier via des certifications professionnelles, complétées par des formations aux évolutions technologiques et métier.

- Dans le cadre du budget annuel de l'établissement, approuvé par l'organe de surveillance, les dirigeants effectifs allouent de façon claire et suffisante des lignes budgétaires correspondant aux missions mentionnées à l'article 270-1.
  - ✓ À titre de bonne pratique, la mise en cohérence entre le processus de définition de la stratégie informatique et celui de définition du budget informatique est encouragée pour ne pas créer de décalage. Aussi, il est préférable que les projets et la maintenance bénéficient chacun pour leur part d'une allocation budgétaire spécifique et bien identifiée, de façon à éviter les effets d'éviction. En outre, compte tenu du cycle de vie des programmes/projets informatiques, la combinaison entre une approche pluriannuelle permettant d'allouer des enveloppes globales pour les programmes de grande ampleur et une approche annuelle pour définir le budget de l'année à venir, constitué à la fois de la quote-part des grands programmes sur l'année considérée et des projets de taille plus modeste mais prioritaires, facilite le pilotage budgétaire d'ensemble. En pratique, il est préférable que tous les acteurs concernés soient associés au processus budgétaire, même si les arbitrages ultimes sont opérés par la direction générale.

Point 3 : responsabilité des dirigeants effectifs lors du recours aux prestataires

Articles 237 et 238 de l'arrêté (cf. §33 et 42 des orientations ABE EBA/GL/2019/02)

Le a) de l'article 237 de l'arrêté dispose que « *l'externalisation n'entraîne aucune délégation de la responsabilité des dirigeants effectifs* », ce qui vaut pour les services informatiques externalisés comme pour toutes les autres prestations externalisées. Cette disposition pose ainsi le principe selon lequel l'externalisation de services informatiques ou autres tâches opérationnelles informatiques essentielles ou importantes, nonobstant leur dimension technique, doit faire l'objet d'un pilotage effectif au plus haut niveau des entreprises assujetties. L'article 237 porte sur l'externalisation en général, mais s'applique aussi bien sûr en matière informatique. À cet égard, l'ACPR appelle l'attention des entreprises assujetties sur le fait que la définition de l'externalisation indiquée dans les orientations de l'ABE sur l'externalisation (EBA/GL/2019/02), ainsi que la définition française des « *prestations de services ou autres tâches opérationnelles essentielles ou importantes* », peuvent inclure des situations de souscriptions de services informatiques auprès de prestataires[5] dès lors que celles-ci correspondent aux critères d'importance requis. La responsabilité générale des dirigeants effectifs impose qu'ils soient attentifs aux risques qui pourraient résulter des prestations informatiques fournies par des prestataires externes. À défaut, le risque serait que les responsables s'aperçoivent trop tardivement, notamment à l'occasion d'un problème grave avec le prestataire, de l'importance de la dépendance de l'entreprise assujettie vis-à-vis d'un tiers, et n'aient alors pas correctement précisé les obligations propres à chaque partie prenante. Pour cela, les dirigeants

[5] À la différence des achats ponctuels, qui sont hors champ (achat de matériel ou de logiciel par exemple)

effectifs doivent pouvoir s'appuyer sur des outils de gestion du risque d'externalisation, tels que ceux requis par l'article 238 de l'arrêté qui renvoie notamment à une « *évaluation du risque encouru préalablement à la signature du contrat* », une « *politique formalisée de contrôle des prestataires externes* » et à un « *registre des dispositifs d'externalisation en vigueur* ».

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les dirigeants effectifs valident la politique d'externalisation, y compris dans ses dimensions relatives à l'externalisation d'opérations informatiques. Cette politique est soumise à l'approbation de l'organe de surveillance. Elle précise les conditions de recours aux prestataires externes (y compris intragroupe), principalement pour les prestations de services ou d'autres tâches opérationnelles, notamment de nature informatique, qualifiées d'essentielles ou importantes. Selon l'importance et la sensibilité des activités, elle prévoie en outre dans quelle mesure les dirigeants effectifs et l'organe de surveillance participent au processus de décision et d'approbation du recours à ces prestataires, et de terminaison de ces prestations.

- Les choix d'externalisation sont fondés sur des analyses de risque produites par les équipes du contrôle.

- Le registre des contrats d'externalisation visé à l'article 238 permet de disposer d'une vision consolidée des contrats négociés avec les prestataires et d'en effectuer le suivi en termes de maîtrise des risques.

    - ✓ À titre de bonne pratique, pour les activités externalisées les plus sensibles, il peut être utile qu'un comité de pilotage en charge du suivi des niveaux de service soit présidé par le responsable de la fonction informatique, voire par un représentant à haut niveau de l'entreprise assujettie.

Chapitre 2 : Contrôle interne du risque informatique

Point 4 : 1er niveau de contrôle permanent du risque informatique

Articles 12 et 270-2 de l'arrêté (cf. §10, 13, et partiellement 17 à 23 des orientations ABE)

Le a) de l'article 12 de l'arrêté dispose que « *le premier niveau de contrôle interne est assuré par des agents exerçant des activités opérationnelles* » et que « *ces agents identifient les risques induits par leur activité et respectent les procédures et les limites fixées* ». Concernant le risque informatique, ce premier niveau de contrôle implique toutes les unités en charge des opérations informatiques, c'est-à-dire des processus de conception, de développement, de gestion, de surveillance et de sécurité des systèmes d'information, y compris s'agissant des services informatiques fournis par des prestataires. Ces unités sont désignées comme constituant la « fonction informatique » dans les orientations ABE[6], concept repris ci-après pour simplifier le propos. Il est à noter que l'arrêté utilise les termes « premier niveau de contrôle permanent » alors que les orientations de l'ABE sur la gouvernance interne

[6] Plus précisément, les orientations ABE utilisent « fonction de TIC » (technologies de l'information et de la communication).

(EBA/GL/2021/05) utilisent le concept de « 1ère ligne de défense ». Cette différence n'emporte pas de conséquence dans la mesure où les unités désignées comme la « fonction informatique » constituent la première ligne de défense et doivent réaliser les contrôles de premier niveau pour la bonne maîtrise des risques liés à leurs tâches. Il doit également être noté que les textes ne prescrivent aucune organisation particulière aux entreprises assujetties. Ainsi, les opérations précitées peuvent être confiées à une même unité (« direction informatique » par exemple) ou à plusieurs (par exemple si chaque « métier » dispose de ses équipes informatiques). Il est également courant que ces opérations incluent les tâches de conception, d'équipement, de configuration, de suivi et d'intervention en matière de sécurité informatique. Ces opérations de sécurité doivent être distinguées des tâches de contrôle de deuxième niveau qui incombent à une fonction de contrôle (cf. point 5). Si l'entreprise assujettie place ces tâches opérationnelles de sécurité sous la responsabilité d'un « responsable de la sécurité des systèmes d'information » (RSSI), lui-même placé sous l'autorité hiérarchique du responsable de la fonction informatique, son indépendance ne pourra être considérée comme établie et il conviendra qu'une fonction de contrôle indépendante, en charge de contrôles de deuxième niveau, soit chargée d'assurer une revue de ces dispositifs.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Au titre de la maîtrise des risques liés à ses opérations, la fonction informatique identifie les différents types de risque informatique auxquels elle peut être confrontée. Cette identification, prenant généralement la forme d'une cartographie des risques, se conforme à la cartographie générale des risques établie par la fonction de gestion des risques afin de permettre la bonne appréciation du risque informatique dans la gestion globale des risques de l'entreprise assujettie.
- La fonction informatique évalue ses risques afin de décider des mesures efficaces de maîtrise du risque et les maintenir dans les limites fixées par l'entreprise assujettie compte tenu de son appétit pour le risque. Elle veille également à ce que les projets et changements relatifs aux systèmes et services informatiques soient conformes aux obligations réglementaires applicables et aux procédures définies par l'entreprise assujettie.
- La fonction informatique assure un suivi des mesures de maîtrise et en rend compte aux responsables du deuxième niveau de contrôle permanent ainsi qu'aux dirigeants effectifs et à l'organe de surveillance, selon un niveau de détail adapté au rôle de chacun d'entre eux.

Point 5 : 2e niveau de contrôle permanent du risque informatique

Articles 12, 14, 15, 23, 224 et 270-2 de l'arrêté (cf. §11 et 13 des orientations ABE, et §173 des orientations ABE EBA/GL/2021/05)

Le b) de l'article 12 de l'arrêté dispose que « *le deuxième niveau de contrôle interne est assuré par des agents au niveau des services centraux et locaux, exclusivement dédiés à la gestion des risques y compris le risque de non-conformité* », que « *dans le cadre de cette mission, ces agents vérifient notamment que les risques ont été identifiés et gérés par le premier niveau de contrôle selon les règles et procédures prévues* », et enfin que « *ce deuxième niveau de contrôle est assuré par la fonction de vérification de la conformité et la fonction de gestion des risques* […] *ou par une ou plusieurs unités indépendantes dédiées au deuxième niveau de contrôle* ». Le 2e alinéa de l'article 14 de l'arrêté dispose que « *les agents exerçant des contrôles de deuxième niveau sont indépendants des unités qu'ils*

contrôlent ». Appliquées à la gestion du risque informatique, ces dispositions imposent que les fonctions de gestion des risques et de la conformité, ainsi que d'autres unités indépendantes de contrôle interne si les entreprises assujetties en disposent (par exemple une unité spécialisée sur la sécurité informatique), jouent le rôle de la « 2e ligne de défense » contre le risque informatique, dans le cadre du contrôle permanent du risque opérationnel. Cette obligation vaut également pour la sécurité de l'information, dont il importe qu'elle ne soit pas laissée tout entière à la discrétion de la « 1ere ligne de défense ». À défaut, le contrôle interne permanent du risque informatique ne serait assuré que par un seul niveau de contrôle, et ce risque ne serait alors pas contrôlé de la même façon que les autres risques opérationnels alors qu'il en représente pourtant une dimension majeure. De même, les dirigeants effectifs et l'organe de surveillance ne bénéficieraient pas, le cas échéant, d'une analyse indépendante le concernant, remettant en cause leur capacité à prendre des décisions éclairées en matière de gestion du risque informatique. En pratique, cela signifie que le deuxième niveau de contrôle permanent du risque informatique contrôle l'efficacité et la pertinence des actions de maîtrise du risque réalisées par le premier niveau de contrôle permanent.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les responsables des fonctions de contrôle de deuxième niveau, comme la fonction de gestion des risques ou la fonction de conformité, s'assurent de la bonne intégration du cadre de gestion du risque informatique, y compris en matière de sécurité informatique, notamment la définition de l'appétit pour le risque et la cartographie du risque, dans le dispositif global de gestion des risques de l'entreprise assujettie.
- Le contrôle de deuxième niveau du risque informatique est confié à une fonction indépendante (des unités en charge du contrôle de premier niveau), comme la fonction de gestion des risques ou la fonction de conformité, ou une autre unité indépendante dédiée à ce type de contrôle. Cela s'applique donc également à la sécurité informatique, qui doit faire l'objet de contrôles de deuxième niveau en plus des contrôles de premier niveau.
- S'agissant de la sécurité informatique, il convient de souligner que la réglementation amène donc les entreprises assujetties à mettre en œuvre des équipes distinctes et indépendantes (par leur rattachement hiérarchique) pour la mise en œuvre des contrôles de premier et de deuxième niveau. Il ne peut donc s'agir d'une seule et même équipe confiée par exemple au RSSI :
    a. Si l'entreprise assujettie choisit de confier le contrôle de premier niveau au RSSI en le rattachant à un responsable opérationnel (responsable de la fonction informatique ou responsable des opérations par exemple), celui-ci jouera alors un rôle opérationnel (par exemple la mise en œuvre de solutions de sécurité) et assurera la responsabilité des contrôles de premier niveau. Dans cette situation, il conviendra alors que l'entreprise assujettie se dote d'une équipe spécialisée de contrôle de deuxième niveau, au sein d'une fonction de contrôle, disposant de l'autorité et de la compétence nécessaire.
    b. Si l'entreprise assujettie confie au RSSI une responsabilité de contrôle de deuxième niveau, celui-ci ne peut alors être en charge d'activités opérationnelles ni être rattaché au responsable de la fonction informatique. Son indépendance ne saurait être réputée acquise que s'il répond hiérarchiquement au responsable d'une fonction de contrôle de deuxième niveau, ou est considéré comme tel et dispose des mêmes attributs de

responsabilité (notamment pouvoir être entendu à sa demande par l'organe de surveillance, en cohérence avec l'article 23 de l'arrêté).

- Comme pour les autres risques, les responsables des fonctions de contrôle de deuxième niveau, comme la fonction de gestion des risques ou la fonction de conformité, rendent compte de l'efficacité de ce cadre aux dirigeants effectifs et à l'organe de surveillance.
- L'appétit pour le risque informatique, y compris en matière de sécurité informatique, ainsi que les limites globales de risques afférentes mentionnés à l'article 224 de l'arrêté sont fixés par les dirigeants effectifs et approuvés par l'organe de surveillance, sur proposition du responsable de la fonction de gestion des risques.

Point 6 : cadre de gestion du risque informatique

Article 270-2 de l'arrêté (cf. §10 à 13, puis 15 à 24 des orientations ABE)

L'article 270-2 de l'arrêté recense les grands axes qui constituent la gestion du risque informatique. Les indications relatives aux attributions des deux premières « lignes de défense » telles qu'exposées aux points 4 et 5 ci-dessus précisent en quoi le contrôle permanent y contribue. Les entreprises assujetties doivent ainsi mettre en place un cadre de gestion du risque informatique applicable à l'ensemble de leurs processus informatiques internes ainsi qu'à ceux réalisés par leurs prestataires, en conformité avec leur cadre de gestion du risque opérationnel.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- L'entreprise assujettie tient à jour un inventaire de ses actifs informatiques, permettant d'apprécier leur niveau d'importance pour la bonne gestion des processus informatiques (notamment le traitement des incidents opérationnels et de sécurité, la gestion des changements, la conformité aux standards techniques et la gestion de l'obsolescence des composants en fin de vie). Cet inventaire comprend notamment les informations suivantes :
    - pour les différentes activités opérationnelles, de support ou de contrôle de l'entreprise assujettie (c'est à dire ses processus), les actifs informatiques et les données qui sont utilisés, ainsi que les liens de dépendance entre eux
    - les caractéristiques des actifs, notamment leur classification de sécurité, leur propriétaire, leur emplacement, et leur configuration
    - les systèmes d'information et les personnels et prestataires intervenant dans la réalisation des processus, y compris les personnes responsables des actifs informatiques ou des données.
- L'entreprise assujettie classe selon leur niveau d'importance ses processus, ainsi que les actifs informatiques et les données qui y sont rattachés. La classification tenant compte notamment des objectifs de confidentialité, d'intégrité et de disponibilité et est revue lors des évaluations de risque.
- L'entreprise assujettie évalue au moins annuellement le risque informatique pouvant affecter ses processus, ainsi que les actifs informatiques et les données qui y sont rattachés. Cette évaluation peut être plus fréquente en cas de modifications apportées aux activités ou à l'environnement informatique (nouvelles applications, fonctionnalités, services, recours à des prestations *Cloud*…) ou à la suite d'incidents opérationnels ou de sécurité significatifs.

- L'entreprise assujettie surveille en permanence les menaces et vulnérabilités pouvant affecter ses processus, ainsi que les actifs informatiques et les données qui y sont rattachés. Cette surveillance donne lieu à une mise à jour des scénarios d'analyse de risque.
- L'entreprise assujettie informe du résultat de ces actions ses dirigeants effectifs et son organe de surveillance, qui, le cas échéant, réagissent en prenant les dispositions nécessaires.

Point 7 : gestion du risque informatique porté par les prestataires

Articles 234 et 270-2 de l'arrêté (cf. §7, 8 et 9 des orientations ABE et §33 des orientations ABE EBA/GL/2019/02)

L'article 234 de l'arrêté requiert que les trois « lignes de défense » du contrôle interne contrôlent les activités externalisées. Appliquées à la gestion du risque informatique, ces dispositions posent le principe selon lequel l'externalisation de services informatiques doit faire l'objet d'un contrôle permanent et périodique dans le même objectif que les activités internes des entreprises assujetties. À défaut, les dirigeants effectifs ne pourraient pas s'appuyer sur des moyens de contrôle pertinents pour piloter l'externalisation des opérations informatiques, et les entreprises assujetties s'engageraient avec des prestataires sans en maîtriser les risques. Il s'agit ainsi pour les entreprises assujetties de s'assurer de l'efficacité du dispositif de gestion du risque informatique prévu à l'article 270-2 quand elles ont recours à des prestataires, y compris lorsque ceux-ci sont des entités de leur groupe, qu'il s'agisse de prestations externalisées ou de souscriptions de services informatiques.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les entreprises assujetties identifient, évaluent, surveillent et gèrent tous les risques auxquels elles sont ou pourraient être exposés dans le cadre d'accords conclus avec des prestataires de services informatiques, qu'il s'agisse d'accords d'externalisation ou de souscriptions de services informatiques.
- Les contrats et les accords de niveau de service conclus avec ces prestataires précisent notamment :
    - les situations d'externalisation « en chaîne », c'est-à-dire le recours par le prestataire à un ou plusieurs autres prestataires de « nième rang », y compris les situations dans lesquelles l'entreprise assujettie doit l'autoriser au préalable pour s'assurer que cela ne crée pas un risque qu'elle ne pourrait maîtriser
    - l'emplacement des sites de production, et des données gérées pour l'entreprise
    - les obligations relatives au cycle de vie des données (les sauvegardes par exemple)
    - des objectifs et mesures en matière de sécurité des systèmes d'information, notamment les exigences en matière de chiffrement des données, de sécurité des réseaux et de surveillance des incidents
    - des procédures de traitement des incidents opérationnels ou de sécurité, en particulier concernant la remontée puis la communication d'informations
    - au moins pour l'externalisation de services informatiques essentiels ou importants, les dispositifs de continuité d'activité mis en œuvre par le prestataire.

- ✓ À titre de bonne pratique, il est souvent utile que les entreprises assujetties disposent de clauses types, validées par leurs services juridiques, pour leur permettre de toujours disposer de contrats conformes à la règlementation et préserver leurs intérêts.

- Les entreprises assujetties veillent à ce que les prestataires respectent les engagements pris dans les contrats et les accords de niveau de service.

  - ✓ À titre de bonne pratique, des comités de suivi et de pilotage conjoints entre l'entreprise assujettie et les prestataires peuvent être organisés pour permettre de veiller à la qualité de la prestation fournie. Le cas échéant, il est souhaitable que le comité de pilotage soit présidé par un responsable de l'entreprise assujettie dont le niveau hiérarchique est défini en fonction de la sensibilité de l'activité externalisée. Par ailleurs, un processus d'escalade auprès des services informatiques ou de la direction générale en cas de dégradation de la qualité de service ou de la relation d'affaires apparaît préférable pour gagner en réactivité.

- Les entreprises assujetties veillent à introduire des clauses de réversibilité dans les contrats relatifs aux prestations de services ou autres tâches opérationnelles essentielles ou importantes qui prévoient un délai de prévenance de l'entreprise assujettie suffisant avant la cessation du contrat par le prestataire, ainsi que l'engagement de ce dernier d'aider l'entreprise assujettie à basculer vers un autre prestataire, à récupérer toutes ses données, et à détruire les informations détenues pour l'entreprise cliente après le changement de prestataire.

Point 8 : audit interne du risque informatique

Articles 12, 16 et 25 de l'arrêté (cf. §11, puis 25 à 27 des orientations ABE)

Le c) de l'article 12 de l'arrêté dispose que « *le troisième niveau de contrôle est assuré par la fonction d'audit interne composée d'agents au niveau central et, le cas échéant, local distincts de ceux réalisant les contrôles de premier et deuxième niveau.* » Le dernier alinéa du même article précise que « *le troisième niveau de contrôle assure, au moyen d'enquêtes, le contrôle périodique de la conformité des opérations, du niveau de risque effectivement encouru, du respect des procédures, de l'efficacité et du caractère approprié* » du travail effectué par le contrôle permanent. Appliquées à la gestion du risque informatique, ces dispositions posent le principe selon lequel les équipes de l'audit interne ou de l'inspection interne jouent le rôle de la « troisième ligne de défense » contre le risque informatique, dans le cadre du contrôle interne du risque opérationnel (contrôle périodique). À défaut, le dispositif de contrôle interne du risque informatique serait insuffisant. En pratique, la fonction d'audit interne assure le contrôle périodique au moyen d'enquêtes sur les processus informatiques permettant d'en vérifier l'efficacité, la bonne exécution, la conformité et la sécurité. Elle vérifie également la bonne application et la conformité du cadre de gestion du risque informatique (donc aussi les actions conduites par la ou les fonction(s) de contrôle de deuxième niveau responsable de la gestion du risque informatique).

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- La fonction d'audit dispose d'une méthodologie appropriée pour le contrôle du risque informatique, y compris dans ses dimensions de sécurité informatique. L'univers d'audit

permet bien de couvrir les unités composant la fonction informatique, ainsi que la ou les fonctions de contrôle de deuxième niveau en charge du risque informatique.

- Les cycles d'audit consacrés au risque informatique ne peuvent excéder la périodicité prévue à l'article 25 de l'arrêté. Il est en outre rappelé que des délais plus courts peuvent s'appliquer à des « systèmes d'information d'importance vitale »[7], ce qui peut aussi faire figure de bonne pratique pour l'audit d'autres systèmes d'information.
- Les cycles d'audit informatique sont établis selon les dispositions de l'article 25 de l'arrêté en intégrant les objectifs annuels des dirigeants effectifs et des orientations de l'organe de surveillance.
- Le traitement des constats relevés pendant ces audits fait l'objet d'un suivi formel, la clôture effective des constatations d'audit étant contrôlée dans le délai convenu, et le contrôle étant cohérent avec le niveau de risque.
- Afin d'assurer son indépendance, la fonction d'audit est constituée d'agents disposant de connaissances, compétences et expertise avérées en matière de gestion du risque informatique (à défaut, le recours à des ressources d'audit disponibles au sein de l'entreprise assujettie mais non consacrées à l'audit informatique reste envisageable), complété si besoin par les services d'un prestataire.
- Les entreprises assujetties de taille modeste qui ne disposent pas d'effectifs suffisants pour la réalisation d'audits spécialisés sur les sujets de risque informatique se font assister par des cabinets d'audit externes disposant de ces compétences.

[7] Définis par l'article L.1332-6-1 du code de la Défense comme les « *systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* ».

Section 2 : GESTION DES OPERATIONS INFORMATIQUES

La Section 2 renvoie à l'article 270-4 de l'arrêté (cf. §50 à 60 des orientations ABE)

Chapitre 1er : Principes fondant la gestion des opérations informatiques

Point 9 : processus et procédures documentés de gestion des opérations

L'article 270-4 de l'arrêté dispose que « *les entreprises assujetties organisent leurs processus de gestion des opérations informatiques conformément à des procédures à jour et validées, dont l'objectif est de veiller à ce que les services informatiques répondent aux besoins de l'entreprise assujettie et de ses clients.* » Il dispose en outre que ces procédures « *couvrent notamment l'exploitation, la surveillance et le contrôle des systèmes et services informatiques* ». Ces dispositions posent ainsi le principe selon lequel les opérations informatiques sont documentées et que les procédures qui les encadrent sont approuvées par les dirigeants effectifs. À défaut, le risque serait la mise en œuvre incohérente de ces opérations, au détriment du bon fonctionnement de l'entreprise assujettie.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les services informatiques fournis aux utilisateurs sont adaptés à leurs besoins.
    - ✓ À titre de bonne pratique, les entreprises assujetties sont encouragées à :
        - suivre une méthodologie partagée par l'ensemble des parties prenantes pour recueillir et valider les exigences fonctionnelles formulées par les utilisateurs
        - s'assurer que les exigences techniques qui imposent des contraintes à la prise en compte des besoins fonctionnels sont connues des utilisateurs et admises par eux
        - veiller à ce que les administrateurs techniques prennent en compte au plus tôt, dans la conception et la réalisation de nouveaux services, les exigences techniques propres à l'exploitation des systèmes et réseaux.
- Les opérations informatiques s'appuient de préférence sur des processus automatisés (normalement plus stables et fiables dès lors qu'ils ont été correctement vérifiés), afin de limiter au maximum les traitements manuels (qui doivent donc faire l'objet de vérifications approfondies et régulières).
- Les opérations informatiques font l'objet d'une surveillance régulière fondée sur des procédures visant à détecter, analyser et corriger les erreurs qui affectent ces opérations. La détection est réalisée par le personnel d'exploitation en charge du suivi de la production mais peut également être effectuée par des équipes spécialisées, pour une meilleure capacité de réaction. La surveillance des opérations s'appuie sur des outils de détection qui doivent couvrir l'ensemble des équipements afin de garantir un pilotage exhaustif.
    - ✓ À titre de bonne pratique, les outils de détection devraient :
        - répertorier des anomalies déjà rencontrées afin de bénéficier d'une surveillance plus automatique
        - être installés à différents niveaux du système d'information pour permettre d'identifier tous types de dysfonctionnements techniques, avant même la survenance d'un incident (par exemple, repérer des temps de réponse

anormalement longs permet d'anticiper une interruption du système d'information).

- Les entreprises assujetties veillent à la cohérence, cohésion et concision de leur système d'information en suivant un plan d'architecture applicatif et technique rationnel.
    - ✓ À titre de bonne pratique, les entreprises assujetties mettent en œuvre une démarche d'urbanisation visant à maîtriser l'organisation de leur système d'information. Elles se fixent des objectifs visant à sa simplification de manière à éviter toute croissance désordonnée et autres difficultés de gestion.

Point 10 : gestion du cycle de vie des actifs informatiques

Les procédures relatives à la gestion des opérations requises par l'article 270-4 de l'arrêté supposent également que les entreprises assujetties définissent une politique de gestion du cycle de vie de leurs actifs informatiques et s'assurent qu'ils répondent en permanence aux besoins des utilisateurs et aux exigences de la gestion du risque. Cet objectif tient compte des solutions informatiques mises en œuvre (par exemples les services de *Cloud*).

L'ACPR appelle l'attention des entreprises assujetties sur le fait que cette politique inclut normalement la gestion des correctifs et des mises à jour, et traite et évalue les risques liés à l'obsolescence des actifs.

Point 11 : processus de planification et de surveillance des performances

Les procédures relatives à la gestion des opérations requises par l'article 270-4 de l'arrêté « *dont l'objectif est de veiller à ce que les services informatiques répondent aux besoins de l'entreprise assujettie et de ses clients* », supposent aussi que les entreprises assujetties mettent en œuvre des processus de surveillance et de gestion de la bonne performance de leurs systèmes informatiques pour en accroître suffisamment à l'avance la capacité et ne pas compromettre l'augmentation de leur usage.

L'ACPR appelle l'attention des entreprises assujetties sur le fait que ces processus méritent d'être formalisés dans des procédures opérationnelles, qui permettent également aux administrateurs des systèmes de suivre de manière rigoureuse les différentes opérations en situation de service normal et de service dégradé.

- ✓ À titre de bonne pratique, les entreprises assujetties sont encouragées à veiller à ce que les niveaux de service soient formalisés dans des conventions de service avec les unités utilisatrices. Ces conventions précisent les critères de suivi et le niveau de satisfaction attendu pour les services, à la fois en termes de qualité et de disponibilité. Les unités utilisatrices internes à l'entreprise mais responsables des services rendus aux clients externes (site web, applications mobiles par exemple) devraient exercer le même rôle pour faire valoir le niveau de service rendu à la clientèle. La formalisation des niveaux de service attendus apparaît nécessaire pour mesurer l'atteinte des besoins des utilisateurs ainsi que l'existence d'indicateurs permettant de suivre les engagements et de prendre des actions de correction. Par ailleurs, il est préférable que ces conventions indiquent également le niveau de sécurité attendu.

Point 12 : procédures de sauvegarde et de restauration des données et des systèmes d'information

Les procédures de gestion des opérations, de même que le processus de gestion des incidents opérationnels ou de sécurité, visés à l'article 270-4 de l'arrêté, supposent que les entreprises assujetties définissent et mettent en œuvre des procédures de sauvegarde et de restauration des données et des systèmes d'information.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Ces procédures permettent de récupérer les données et les systèmes en cas de besoin.
- Ces procédures sont issues d'une analyse de risque et sont cohérentes avec les besoins des métiers.
- Le périmètre et la fréquence des sauvegardes sont définis conformément aux exigences de reprise des activités et au niveau de criticité des données et des systèmes d'information.
- Les procédures de sauvegarde et de restauration sont testées régulièrement, et une bonne pratique consiste à ce que la durée entre chaque test n'excède pas un an.
- Les sauvegardes des données et des systèmes d'information sont stockées de façon sécurisée à un endroit suffisamment éloigné ou protégé du site principal et ne sont pas exposées aux mêmes risques, y compris de compromission de sécurité.

Chapitre 2 : gestion des incidents opérationnels ou de sécurité

Point 13 : procédures de détection, classification et réponse aux incidents informatiques

L'article 270-4 de l'arrêté dispose que les entreprises assujetties complètent leur processus de gestion des opérations informatiques par « *un processus de détection et de gestion des incidents opérationnels ou de sécurité* ». Cette disposition pose notamment le principe selon lequel les entreprises assujetties établissent et mettent en œuvre un processus de gestion des incidents afin de surveiller et consigner les incidents opérationnels et de sécurité liés au système d'information. À défaut, le risque serait d'être dans l'incapacité de réagir avec efficacité à ces évènements, et donc d'en subir les conséquences sur une période prolongée, voire d'être dans l'incapacité de les surmonter.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance d'établir :

- Des procédures visant à identifier, recenser, classifier et suivre ces incidents en fonction de leur importance pour elles-mêmes et leurs clients.
- Les rôles et responsabilités des différents intervenants pour chaque type d'incidents.
- Des procédures permettant d'identifier, d'analyser et de résoudre les principales causes et facteurs déclencheurs ou aggravant des incidents.
- Des plans de communication internes incluant la notification des incidents significatifs à l'organe de surveillance.

- Des plans de communication externes.
- Des procédures de gestion de la continuité d'activité, telles que précisées dans la Section 5 ci-après.

Section 3 : GESTION DES PROJETS INFORMATIQUES ET DES CHANGEMENTS

La Section 3 renvoie à l'article 270-5 de l'arrêté (cf. §37 puis §61 à 76 des orientations ABE)

Chapitre 1er : Gestion des projets informatiques

Point 14 : processus de gouvernance des projets informatiques

L'article 270-5 de l'arrêté dispose que « *les entreprises assujetties disposent d'un cadre de conduite clair et efficace de leurs projets et programmes informatiques* ». Cette disposition pose ainsi le principe selon lequel la gestion des projets informatiques est organisée de façon efficace et méthodique. À défaut, le risque serait que certains projets soient gérés sans pilotage des preneurs de décision, et sans prise en compte de l'environnement général de l'entreprise et des autres projets parallèles, pouvant entraîner des désorganisations, voire des incidents divers.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance :

- D'évaluer et veiller à la maîtrise des risques liés à leurs projets.
- D'établir par écrit un cadre de gestion des projets informatiques qui impose au minimum que chacun de ces projets fasse l'objet :
  - d'un exposé des objectifs, du calendrier et de ses étapes
  - ✓ À titre de bonne pratique, un dispositif de communication auprès des différents acteurs impliqués peut être mis en place pour réduire les risques d'incompréhension, susceptibles de générer des erreurs ou retards. De façon générale, l'utilisation d'une méthodologie de conduite de projets est encouragée pour favoriser le bon enchaînement des différentes étapes de réalisation après vérification de la qualité des livrables. En particulier, le processus de mise en production doit être rigoureux : la planification des déploiements logiciels et matériels est d'autant plus efficace qu'elle s'appuie sur des procédures formalisées qui visent à garantir un niveau satisfaisant de disponibilité. Ce processus devrait également s'appuyer sur un calendrier de changement regroupant ces procédures anticipant non seulement les périodes où le personnel expérimenté est présent, mais aussi celles où il est absent afin de prévoir, le cas échéant, que des experts qualifiés soient mobilisables en astreinte et des responsables joignables en cas d'anomalie.
  - d'un exposé des rôles et responsabilités des personnes concourant à sa mise en œuvre
  - d'une évaluation des risques par les différentes unités chargées des normes de gestion informatique et de sécurité, ainsi que par le responsable de la fonction de gestion des risques ou par le responsable de la conformité, ou par le responsable d'une fonction indépendante de contrôle dédiée au risque informatique (2ème « ligne de défense »)
  - ✓ À titre de bonne pratique, des comités assurant le suivi des travaux et favorisant la coordination des acteurs peuvent être mis sur pied pour faciliter le suivi des délais, des coûts et de la qualité ainsi que la prise de décision. Les projets les plus importants peuvent être suivis par un sponsor chargé de veiller à leur bon déroulement.

- d'une vigilance particulière concernant les interdépendances avec d'autres projets, les ressources partagées et les éventuelles situations de blocage liées à ces adhérences.

- D'adopter un cadre de gestion de projets informatiques compatible avec les éléments précédents y compris en mode « agile » (méthode de type *Scrum* par exemple).

Point 15 : gestion des risques des projets informatiques

Il résulte des dispositions de l'article 270-2 de l'arrêté sur l'identification et l'évaluation du risque et du point 14 que les exigences de sécurité des projets informatiques dépendent d'une analyse de risque menées par les deux niveaux de contrôle permanent.

À ce titre, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les équipes chargées des projets informatiques disposent d'une expérience suffisante et des qualifications appropriées pour les mener.
- L'état d'avancement des projets informatiques majeurs et les risques qui leur sont associés font l'objet d'un suivi régulier par les dirigeants effectifs et l'organe de surveillance, chacun pour leur rôle respectif.

Chapitre 2 : Acquisition et développement des systèmes informatiques

Point 16 : processus d'acquisition, de développement et d'entretien des systèmes informatiques

L'article 270-5 de l'arrêté dispose que le cadre de conduite des projets et programmes informatiques est « *accompagné d'un processus de gestion de l'acquisition, du développement et de l'entretien des systèmes d'information* […] *garantissant que les modifications apportées aux systèmes informatiques sont enregistrées, testées, évaluées, approuvées et implémentées de façon contrôlée* ». Cette disposition pose ainsi le principe selon lequel l'organisation interne des entreprises assujetties en matière de conduite de projet s'applique également, et pour les mêmes raisons, à ce type particulier de modifications. À défaut, le risque serait l'échec de l'intégration de la nouvelle acquisition au sein du système d'information, ou l'échec du développement envisagé.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Il est important que ce processus intègre :
    - une analyse et une validation par la direction de la ou des unité(s) utilisatrice(s) concernée(s) des exigences fonctionnelles et non-fonctionnelles des systèmes informatiques (en s'assurant que les contraintes à la prise en compte des besoins fonctionnels sont connues des utilisateurs et admises par eux), y compris les objectifs de sécurité, avant l'acquisition ou le développement
    - des mesures permettant de garantir l'intégrité des systèmes informatiques durant leur développement, leur intégration et leur mise en production
    - une méthodologie permettant de tester et valider la conformité des systèmes informatiques aux besoins de l'entreprise assujettie avant leur mise en service, tenant

compte de l'importance et de la sensibilité des actifs et processus métiers impliqués, étant entendu que l'environnement de test doit être le plus comparable possible à l'environnement de production

- ✓ À titre de bonne pratique, les tests de non régression sur le périmètre concerné par ces évolutions, fondés sur la méthodologie documentée des tests, sont encouragés pour éviter les effets de bords non désirés.
  - des procédures d'évaluation continue des systèmes informatiques et des services informatiques en cours de développement ou d'acquisition, et notamment de leur sécurité, pour identifier d'éventuelles vulnérabilités
  - la stricte séparation entre les environnements informatiques de production et les autres environnements, notamment ceux dédiés aux développements ou aux tests, accompagnée d'une restriction des accès, pour assurer les mêmes exigences d'intégrité et de confidentialité des données de production lorsque celles-ci sont utilisées dans d'autres environnements que les environnements de production
  - la documentation du développement, de l'implémentation, du fonctionnement, de la configuration et de l'exploitation de leurs systèmes informatiques.

- Ces dispositions s'appliquent également aux systèmes ou services informatiques développés et gérés par leurs utilisateurs sans recours aux unités chargées de la gestion des opérations informatiques (« *end-user computing* »)[8]. Ceux-ci devraient être proscrits pour des applications sensibles de l'entreprise assujettie (par exemple, pour les modèles de calcul de risque). Ils doivent en outre être inscrits dans un registre tenu à jour lorsqu'ils concourent à des activités essentielles ou importantes (par exemple, les solutions utilisées pour produire des *reportings* règlementaires ou calculer des modèles de risque). Ce registre doit être considéré comme un élément de contrôle interne.
  - ✓ À titre de bonne pratique, ce registre peut classer ces systèmes ou services particuliers selon le niveau de risque qui leur est associé. Il contient des informations permettant d'identifier leurs utilisateurs et propriétaires, la ou les version(s) en cours d'utilisation, les données traitées, les systèmes de secours, les solutions d'archivage, ainsi que leurs dépendances à d'autres systèmes ou services de cette nature ou au reste du système d'information. Enfin, de façon complémentaire au suivi des « *end-user computing* » permis par le registre, le contrôle régulier de leurs droits d'accès est encouragé.

Chapitre 3 : Gestion des changements informatiques

Point 17 : processus de gestion des changements informatiques

L'article 270-5 de l'arrêté dispose que le cadre de conduite des projets et programmes informatiques est « *accompagné d'un processus de gestion des changements informatiques garantissant que les modifications apportées aux systèmes informatiques sont enregistrées, testées, évaluées, approuvées et implémentées de façon contrôlée* ». Cette disposition pose ainsi le principe selon lequel l'organisation interne des entreprises assujetties en matière de conduite de projet s'applique également, et pour les mêmes raisons, aux changements informatiques en général, de façon

[8] À défaut d'être réintégrés dans la gestion habituelle des systèmes et services opérée par la fonction informatique

proportionnée à leur ampleur, et sans que le recours à des processus de gestion des changements automatisés ne conduise à diminuer le contrôle des changements opérés. À défaut, le risque serait que les changements soient réalisés sans pilotage et entraînent alors un non-alignement entre les besoins fonctionnels et le système d'information qui doit y répondre.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Le processus de gestion des changements prévoit des procédures particulières pour opérer des changements nécessaires en situation d'urgence tout en conservant des mesures de protection appropriées.
  - ✓ À titre de bonne pratique, ce processus peut définir les typologies de changement, y compris donc les changements standards et les changements urgents, pour corriger les anomalies graves de fonctionnement. Aussi, il est préférable qu'il intègre une description des traitements opérés distinguant les différentes phases, notamment l'enregistrement, l'évaluation des impacts, la classification, la priorisation, les étapes de validation, la planification, les tests, les conditions de retour arrière, ainsi que les différentes versions (« *releases* »). Pour les changements les plus importants, des recettes fonctionnelles et techniques exhaustives et formalisées sont encouragées de façon à vérifier leur caractère adéquat.
- Les entreprises assujetties identifient, en continu, les conséquences des changements sur les mesures existantes de sécurité du système d'information et adoptent des mesures complémentaires nécessaires pour couvrir les éventuels nouveaux risques induits par ces changements.

Section 4 : SECURITE DU SYSTÈME D'INFORMATION

La Section 4 renvoie à l'article 270-3 de l'arrêté (cf. §28 à 49 des orientations ABE)

Chapitre 1er : Politique de sécurité du système d'information

Point 18 : principes et contenu de la politique de sécurité du système d'information

L'article 270-3 de l'arrêté dispose que « *les entreprises assujetties établissent par écrit une politique de sécurité du système d'information qui détermine les principes mis en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité de leurs informations et des données de leurs clients, de leurs actifs et services informatiques* ». Il dispose également que « *cette politique est fondée sur une analyse des risques et approuvée par les dirigeants effectifs et l'organe de surveillance* ». Ces dispositions posent ainsi le principe selon lequel la sécurité du système d'information des entreprises assujetties est clairement définie et documentée de façon à avoir une référence pour chaque opération concernant directement ou indirectement la sécurité, validée à haut niveau pour garantir une bonne articulation au sein de l'ensemble de l'organisation et fondée sur les risques pour veiller à son caractère adéquat vis-à-vis des opérations menées. À défaut, le risque serait la démultiplication de références de sécurité potentiellement sans cohérence, ce qui serait facteur de vulnérabilités donc de sécurité insuffisante, ou pénalisant pour les opérations des entreprises assujetties.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- La politique de sécurité du système d'information est conforme aux principes de gouvernance et de gestion du risque informatique.
- La politique de sécurité précise les rôles et responsabilités en matière de sécurité pour l'ensemble du personnel et des prestataires intervenants dans les locaux ou utilisant le matériel de l'entreprise.
- La politique de sécurité prend en compte la sécurité des données (incluant la protection des données personnelles) et des traitements dès la conception des systèmes informatiques (principe connu sous le nom de « *Security by design* », et « *Privacy by design* » pour le cas particulier des données personnelles).
- La politique de sécurité couvre l'ensemble des processus et des actifs informatiques ou des données en tenant compte de leur niveau d'importance et de sensibilité, établis lors du processus d'évaluation des risques.
- La politique de sécurité est mise à jour en fonction des résultats du processus d'évaluation des risques, ou quand des évolutions importantes ont été apportées au système d'information.
- La politique de sécurité couvre les phases de stockage, d'échange ou d'utilisation des données.
- La politique de sécurité fixe les grandes orientations des mesures de sécurité précisées ci-après et renvoie pour chacune à des procédures détaillées.
- Les entreprises communiquent la politique de sécurité du système d'information à tout leur personnel et à tous les prestataires qui accèdent à leur système d'information.

Chapitre 2 : Sécurité physique et logique

Point 19 : principes de la sécurité physique

Le 2e alinéa de l'article 270-3 de l'arrêté dispose qu'« *en application de leur politique de sécurité du système d'information, les entreprises assujetties formalisent et mettent en œuvre des mesures de sécurité physique […] adaptées à la sensibilité des locaux, des actifs et services informatiques, ainsi que des données* ». Cette disposition pose ainsi le principe selon lequel la sécurité du système d'information commence par des mesures ou parades tangibles adéquates, visant tant à prévenir les risques à caractère accidentel (« sécurité » au sens strict) que les actes malveillants (le mot « sureté » est parfois utilisé dans ce contexte). À défaut, les locaux des entreprises assujetties seraient trop accessibles et exposés, les mettant en situation de vulnérabilité non maitrisable.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Ces mesures incluent un examen régulier des droits d'accès et des dispositifs de surveillance mis en place, pour s'assurer que seul le personnel dont les responsabilités et les qualifications le justifient ait accès de façon surveillée aux emplacements permettant d'accéder au système d'information ou à des informations sensibles.
- L'entreprise assujettie met en œuvre une protection différenciée par zonage pour tenir compte de la sensibilité des différents locaux.
    - ✓ À titre de bonne pratique, le zonage distingue notamment les espaces accessibles au public de ceux restreints aux employés ou les zones critiques. Des procédures strictes encadrent les conditions d'accès aux différentes zones, reposant sur des dispositifs de protection périmétrique (clôtures, barrières, sas d'entrée, contrôle par badge, etc.) et de détection d'intrusion (vidéo-surveillance, alarmes, etc.), proportionnés au besoin de protection. Ainsi, les actifs physiques les plus critiques, tels que les serveurs, les postes d'administration, les équipements réseaux, les équipements électriques, ou encore les clés, devraient bénéficier d'une protection renforcée par des dispositifs de sécurité complémentaires et spécifiques (par exemple, cage autour des serveurs, fermeture des baies, vidéo-surveillance spécifique). Les incidents de sécurité qui affectent les locaux des entreprises assujetties méritent de faire l'objet de journaux d'évènements conservés pendant une durée suffisante pour pouvoir mener à bien toutes les investigations utiles, dans le respect de la réglementation sur la protection des données personnelles et du droit au respect de la vie privée.
- Le site et les locaux choisis minimisent l'exposition aux dangers dans la mesure du possible, l'analyse de risques reflète la prise en compte des risques environnementaux et les mesures contre les catastrophes naturelles et autres dangers issus de l'environnement de l'entreprise sont adaptées à l'importance et à la sensibilité des locaux, des opérations informatiques qui y sont réalisées et des systèmes informatiques qu'ils hébergent.
    - ✓ À titre de bonne pratique, il est préférable d'interdire l'entreposage de matières inflammables dans les locaux.
- Les bâtiments, particulièrement leurs salles de production informatique, sont pourvus de dispositifs de détection des évènements accidentels susceptibles de détériorer les systèmes informatiques (inondation ou incendie par exemple) et d'extinction des incendies.

- ✓ À titre de bonne pratique, les dispositifs d'extinction sont paramétrés pour éviter les déclenchements intempestifs susceptibles d'endommager les matériels, et sont activables à distance par l'équipe de surveillance des installations.

Point 20 : principes de la sécurité logique

Le 2e alinéa de l'article 270-3 de l'arrêté dispose qu'« *en application de leur politique de sécurité du système d'information, les entreprises assujetties formalisent et mettent en œuvre des mesures de sécurité […] logique adaptées à la sensibilité des locaux, des actifs et services informatiques, ainsi que des données* ». Cette disposition pose ainsi le principe selon lequel la sécurité du système d'information repose également sur des mesures constituées de dispositifs adéquats de protection par logiciel, visant à gérer les identités et les accès. À défaut, le système d'information des entreprises assujetties serait trop exposé aux actes malveillants, et en particulier aux cyber-attaques, alors que ces dernières sont sans cesse plus sophistiquées.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties pour qu'elles appuient leurs mesures de sécurité logique sur les principes et modalités suivants :

- L'enrôlement/désenrôlement : attribution à l'utilisateur de droits sur le système d'information au moment de sa prise de fonction, ces droits lui étant automatiquement retirés lorsqu'il la quitte.
  - ✓ À titre de bonne pratique, pour faciliter la mise en œuvre de ce principe, la définition *a priori* des profils (métiers et techniques) pour uniformiser et faciliter l'attribution de droits unitaires, et la mise en place de processus maintenant la cohérence entre le système de gestion des accès et le système des ressources humaines sont encouragées. Dans la mesure du possible, la durée des contrats des prestataires est prise en compte de façon à bloquer les accès rapidement au terme de leur prestation.
- Le besoin d'en connaître : quelles que soient ses accréditations, chaque utilisateur n'est autorisé à accéder qu'aux informations pour lesquelles le bénéfice de l'accès lui est explicitement accordé.
- Le moindre privilège : chaque utilisateur accède aux ressources en ayant uniquement les droits nécessaires à l'exercice de ses fonctions.
  - ✓ À titre de bonne pratique, les droits d'administration ne sont accordés que lorsque l'administrateur effectue une tâche d'administration du système.
- La séparation des tâches : les responsabilités liées à une activité importante ou sensible sont réparties entre plusieurs unités, de façon à ce que l'infraction à la politique de sécurité mise en place soit nécessairement le fait d'une entente intentionnelle et provoquée.
- N'autoriser qu'après avoir authentifié : tous les accès à des ressources doivent être contrôlés à chaque fois que nécessaire, même si une authentification initiale a été réalisée, tenant compte du contexte et du risque, et si besoin par une authentification de plus haut niveau.
  - ✓ À titre de bonne pratique, l'accès à une page privée d'un site Web ne doit pas supposer par défaut que l'utilisateur est passé auparavant par la page d'authentification. Ce principe permet de simplifier les modèles de sécurité pour chaque composant et favorise la conception d'architectures modulaires. Elle n'est pas un frein à l'ergonomie

si les protocoles de sécurité permettant de propager les authentifications sont correctement mis en œuvre.

Point 21 : application des principes de sécurité logique

Le respect des principes de sécurité logique précédemment mentionnés permet notamment de suivre et contrôler l'utilisation des ressources informatiques en fonction des besoins, et en conformité avec la réglementation sur la protection des données personnelles et le droit au respect de la vie privée.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Il doit être possible d'imputer les actions effectuées par les utilisateurs. À cette fin les comptes génériques et les comptes partagés ne sont utilisés que de manière :
    - exceptionnelle
    - justifiée dans la politique de sécurité
    - encadrée (avec un dispositif permettant de remonter, *in fine*, à la personne ayant utilisé le compte partagé)
    - et surveillée (les identifiants des comptes désactivés ne doivent pas être réattribués à de nouveaux utilisateurs pour garantir la bonne imputabilité des actions dans le temps).
- L'entreprise assujettie contrôle les droits d'accès privilégiés et leurs modalités d'accès à distance.
- L'entreprise assujettie enregistre les activités des utilisateurs des systèmes informatiques, en particulier celles des utilisateurs privilégiés. Elle définit les modalités de stockage et d'accès de ces enregistrements pour permettre la détection d'anomalies.
- L'entreprise assujettie contrôle l'ajout, la suppression et la modification des droits d'accès, y compris les responsabilités et les rôles de chaque intervenant dans ce processus.
- L'entreprise assujettie définit les modalités de vérification périodique (« circularisation ») des droits d'accès.
    - ✓ À titre de bonne pratique, la vérification des droits d'accès est au moins annuelle.
- L'entreprise assujettie applique différents modes d'authentification en fonction du niveau de sensibilité des systèmes, des données ou des processus.
    - ✓ À titre de bonne pratique, ces modes d'authentification incluent au minimum des règles de complexité et de mise à jour des mots de passe. Les situations les plus sensibles requièrent des solutions d'authentification forte, telle que l'authentification à deux facteurs. C'est tout particulièrement le cas pour la connexion au système d'information depuis l'extérieur des locaux de l'entreprise.
- L'entreprise assujettie s'assure que la protection des moyens d'authentification (mots de passe, tokens…) fait l'objet d'une sensibilisation du personnel ainsi que de contrôles réguliers.

Chapitre 3 : Sécurité des opérations informatiques

Point 22 : mesures de sécurisation des systèmes et services informatiques

Les mesures de sécurité requises par l'article 270-3 de l'arrêté supposent également que les entreprises assujetties formalisent et mettent en œuvre des procédures pour prévenir, identifier et traiter les problèmes de sécurité de leurs systèmes et services informatiques. Pour cela, les entreprises assujetties sont invitées à se référer aux guides et recommandations de sécurité informatique publiés par l'ANSSI et à les mettre en œuvre de manière proportionnée et raisonnée[9].

Concernant les dispositions précitées, l'ACPR appelle en particulier l'attention des entreprises assujetties sur l'importance :

- D'un maintien en condition de sécurité des logiciels et des micrologiciels par application des correctifs de sécurité ou de mesures compensatoires.
    - ✓ À titre de bonne pratique, il est recommandé d'utiliser des versions toujours soutenues par les éditeurs et fabricants et d'appliquer les correctifs relatifs aux vulnérabilités les plus graves dans les plus brefs délais. À défaut, des mesures compensatoires sont mises en place pour limiter la capacité d'exploitation des vulnérabilités existantes.
- De la mise en œuvre de configurations de référence sécurisées pour les équipements matériels et de la vérification de l'intégrité des configurations des serveurs.
    - ✓ À titre de bonne pratique, cela vise le durcissement des configurations par la limitation au strict nécessaire des logiciels ainsi que des fonctionnalités des équipements (se référer pour cela aux guides de l'ANSSI).
- De la segmentation des réseaux en zones distinctes composées de systèmes ayant des besoins de sécurité homogènes, en évitant donc les réseaux sans mécanisme de cloisonnement (réseaux « à plat ») qui facilitent la propagation d'une attaque. Cette segmentation peut être physique (pare-feu physique) ou logique (pare-feu logiciel virtualisé et/ou VLAN[10]).
    - ✓ À titre de bonne pratique, une segmentation typique comporte au moins quatre zones de sécurité réseaux (une zone « démilitarisée » exposée à Internet avec filtrage externe et interne / des réseaux internes bureautiques / des réseaux pour la production informatique type centres de données / un réseau dédié à l'administration des équipements informatiques). Elle peut en outre être complétée par des dispositifs de rupture protocolaire et de déport de serveurs (applications « multi-tiers »). En principe, le filtrage du trafic réseau entre ces différentes zones est réalisé sur la base d'une cartographie documentée des flux strictement nécessaires réalisée *a priori*, qui est contrôlée au moins annuellement. Ces recommandations sont également applicables lors du recours à des prestations *Cloud* « *Infrastructure as a Service* » (IaaS).
- De la protection des équipements réseaux et des terminaux d'accès.

[9] https://www.ssi.gouv.fr/administration/bonnes-pratiques/

[10] Pour « réseau local virtuel » (« *Virtual Local Area Network* » en anglais)

- ✓ À titre de bonne pratique, pour améliorer la résilience du système, le déploiement des outils de sécurité de fournisseurs distincts entre différents équipements, par exemple entre les passerelles et les équipements utilisateurs, est encouragé. Par ailleurs, la conformité d'un terminal d'accès aux normes de sécurité de l'entreprise est vérifiée avant d'autoriser sa connexion au réseau de celle-ci.

- De la protection des données, notamment par le chiffrement des flux et des données stockées et de leur support en fonction de leur niveau de sensibilité, et la mise en œuvre de solutions de prévention des pertes de données.

  - ✓ À titre de bonne pratique, il est recommandé de s'informer sur les produits évalués par l'ANSSI lors du choix du dispositif. Par ailleurs, cette protection est encouragée également pour les supports ayant stocké des données, qui doivent être considérés au même niveau de sensibilités que les données qu'ils ont stockées. Ainsi, les équipements nomades tels qu'ordinateurs portables, tablettes et smartphones méritent de disposer d'un contrôle empêchant le démarrage ainsi que l'accès sans authentification. L'existence d'une procédure décrivant la gestion de la fin de vie des supports d'information (y compris le remplacement par des prestataires ou fournisseurs dans le cadre de la garantie) est encouragée.

Chapitre 4 : Surveillance de la sécurité

Point 23 : détection des incidents et réponses appropriées

Ce point renvoie aussi à l'article 270-4 de l'arrêté

L'article 270-4 de l'arrêté prévoit que les entreprises assujetties organisent la gestion de leurs opérations informatiques et disposent de procédures pour l'exploitation, la surveillance et le contrôle des systèmes et services informatiques. Ces procédures « *sont complétées par un processus de détection et de gestion des incidents opérationnels ou de sécurité* ». L'objectif de cette détection est de pouvoir repérer au plus tôt un incident et de réagir de manière appropriée. Ainsi, les entreprises formalisent et mettent en œuvre des procédures de surveillance continue de la sécurité de leur système d'information. Il s'agit d'un élément fondamental du dispositif de résilience opérationnelle permettant le déclenchement éventuel du processus de gestion de crise (cf. Section 5).

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance d'assurer :

- L'exhaustivité et la réactivité des détections, que ce soient des intrusions physiques dans leurs locaux, des accès non autorisés à leurs systèmes informatiques ou une utilisation inappropriée de leurs services informatiques.

  - ✓ À titre de bonne pratique, la totalité du système d'information est couvert (à défaut, ses éléments communiquant avec Internet et ses composants sensibles). La surveillance des transactions suspectes dans les applications, les outils d'administration, les bases de données ou tout autre environnement sensible est faite en temps réel pour permettre une plus grande réactivité face aux attaques.

- L'adéquation des moyens techniques et humains permettant ces détections.

  - ✓ À titre de bonne pratique, il est préférable de disposer d'outils automatiques de recueil et d'analyse de traces et d'une équipe de surveillance pour les exploiter (tel un

« *Security Operating Centre* » – SOC), idéalement mobilisée 24 heures sur 24 et 7 jours sur 7, toute l'année. Les traces recueillies sont alors horodatées, archivées, et protégées contre toute tentative de modification. Les événements surveillés comprennent :

- Les connexions inhabituelles au système d'information (connexions à des horaires ou dates inhabituels comme des vacances, ubiquité des connexions, accès depuis des machines ou des adresses Internet nouvelles, etc.)
- Les anomalies lors de l'authentification des utilisateurs externes (clients, prestataires ou partenaires) et internes
- Les comportements anormaux des clients utilisant des sites transactionnels (gestion de compte en ligne par exemple)
- Les opérations suspectes de paiement ou de transfert de titres
- Les fonctions de copie ou de suppression de masse sur les bases de données sensibles
- Les fonctions d'élévation de privilèges sur les systèmes et bases.

- La mise en œuvre d'une veille permanente relative aux menaces qui pourraient affecter la sécurité de leur système d'information. Cette veille inclut une surveillance des fuites de données ou de la présence de logiciels malveillants et sert à l'amélioration continue des dispositifs de surveillance des entreprises assujetties, notamment sur les plans technologique et organisationnel.

Chapitre 5 : Évaluation de la sécurité et sensibilisation

Point 24 : évaluation de la sécurité du système d'information

Ce point renvoie aussi à l'article 270-2 de l'arrêté

L'article 270-2 de l'arrêté précise que, dans le cadre de la gestion de leur risque informatique, les entreprises assujetties doivent « *surveiller l'efficacité* [des] *mesures* [adéquates de réduction du risque informatique] *et informer les dirigeants effectifs et l'organe de surveillance de leur bonne exécution* ». L'objectif est de vérifier la pertinence et l'efficacité des mesures de sécurité appliquées au système d'information. Pour cela, les entreprises assujetties définissent un cadre de test de la sécurité du système d'information, qui tient compte des menaces pesant sur leurs activités et des particularités de leur système d'information.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance des points suivants :

- La mise en place d'une documentation sur les méthodes d'évaluation et la justification des choix effectués.

- La pertinence des tests en fonction des objectifs recherchés.

  ✓ À titre de bonne pratique, les tests peuvent notamment prendre les formes suivantes :

  - Des revues de conformité et d'analyses d'écarts à des normes ou des standards de sécurité
  - Des audits internes et externes sur la sécurité des systèmes informatiques, y compris sur les mesures de sécurité physique
  - Des analyses de codes sources

- Des exercices annuels de gestion de crise « cyber »[11]
- Des tests d'intrusion dans les systèmes informatiques essentiels ou importants qui peuvent être, selon les cas, des tests d'intrusion fondés sur une recherche préalable des menaces (« TLPT », *Thread-led penetration test*).

- Le cadre de test doit en particulier garantir :
  - L'expertise des équipes chargées des tests
  - L'assurance que les testeurs sont séparés des équipes en charge de la mise en œuvre des mesures de sécurité
  - La récurrence des tests de sécurité dont la périodicité est définie au regard des risques et de la sensibilité des systèmes évalués
  - La prise en compte dans le programme des tests des changements apportés aux systèmes informatiques dans la logique du point 17 de cette Notice.

- La mise à jour des dispositifs de sécurité du système d'information en fonction des résultats de ces tests.
  - ✓ À titre de bonne pratique, dans le cas de tests d'intrusion, il est recommandé de valider la correction des vulnérabilités identifiées par le test initial par un deuxième test mené dans des conditions similaires d'indépendance entre le testeur et l'unité en charge de la remédiation.

Point 25 : formation et sensibilisation en matière de sécurité informatique

Le troisième alinéa de l'article 270-3 de l'arrêté dispose que « *les entreprises assujetties mettent également en œuvre un programme de sensibilisation et de formations régulières, soit au moins une fois par an, à la sécurité du système d'information au bénéfice de tous les personnels et des prestataires externes, et en particulier de leurs dirigeants effectifs* ». Cette disposition est justifiée par le fait que les individus interagissant avec le système d'information, soit au moment de sa conception et de sa mise en œuvre, soit ensuite lors de son utilisation, peuvent être eux-mêmes, en raison de leurs erreurs ou négligences, un vecteur de risque de dysfonctionnement ou d'atteinte à la sécurité. À défaut d'actions de sensibilisation suffisantes, les entreprises assujetties sont exposées à de multiples vulnérabilités graves et facilement exploitables pour leur nuire, en particulier quand les utilisateurs disposent de droits privilégiés. Concernant ses prestataires, l'article 270-3 implique seulement que l'entreprise assujettie s'assure qu'un programme de sensibilisation et de formation équivalent est mis en œuvre de leur côté, et que ses prestataires puissent participer aux exercices de sensibilisation qu'elle mène pour son propre personnel (dans les limites prévues par le droit du travail).

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur les points suivants :

- Les programmes de sensibilisation et de formation touchent l'ensemble du personnel de l'entreprise assujettie. Ces programmes sont renforcés pour les agents fortement exposés en termes de sécurité informatiques (par exemple, les administrateurs des éléments du système informatique, utilisateurs engageant des opérations de décaissement). Il existe également des

[11] L'ANSSI a publié un guide d'organisation des exercices de gestion de crise « cyber » qui peut être consulté pour cela.

actions adaptées pour les dirigeants effectifs et, à titre de bonne pratique, pour les membres de l'organe de surveillance.

- ✓ À titre de bonne pratique, des tests de simulation d'attaques de type « hameçonnage » (« *phishing* ») peuvent être organisés pour tester la bonne compréhension de ces enseignements et la maîtrise des comportements. Le résultat de ces exercices a vocation à être analysé pour permettre, si besoin, la mise en place d'actions de formation supplémentaire.

- L'efficacité de ces programmes est vérifiée, et leur révision prend en compte les nouvelles menaces et les éventuelles lacunes constatées.

Section 5 : GESTION DE LA CONTINUITE DES ACTIVITES

La Section 5 renvoie à l'article 215 de l'arrêté (cf. §77 à 91 des orientations ABE)

Point 26 : principes fondant le cadre de gestion de la continuité d'activité

Le premier alinéa de l'article 215 de l'arrêté dispose que « *les entreprises assujetties établissent un dispositif de gestion de la continuité d'activité […] ».* Cette exigence vise à ce que les entreprises puissent maintenir leurs services de manière continue et limiter leurs pertes en cas de perturbation grave. Cette disposition est générale, et couvre donc à la fois les activités générales de l'entreprise, mais aussi les services informatiques qui les soutiennent.

Le dispositif de continuité d'activité doit couvrir toutes les situations de perturbation, y compris celles causées par des cyber–attaques, non seulement celles affectant la disponibilité des services informatiques, mais aussi la confidentialité ou l'intégrité des systèmes et données. Ce dispositif doit donc déterminer les moyens informatiques nécessaires et leur modalité de mise en œuvre pour faire face aux perturbations et rétablir son service habituel.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance d'assurer :

- La formalisation des politiques et des procédures pour la coordination, le pilotage et la prise de décision en cas de perturbation.
- La définition claire des rôles et responsabilités pour les situations de gestion de crise.
- L'implication des dirigeants effectifs et leur validation, pour garantir l'alignement de la continuité avec la stratégie de l'entreprise.

Point 27 : analyse d'impact sur l'activité

Le a) de l'article 215 de l'arrêté précise que le dispositif de continuité d'activité comprend « *une procédure d'analyse quantitative et qualitative des impacts de perturbations graves sur leurs activités […] ».* Cette disposition pose ainsi le principe selon lequel la continuité d'activité suppose un processus préparatoire documenté et adapté au profil de risque des entreprises assujetties, donc une bonne connaissance du système d'information et de ses fonctions essentielles. Les entreprises assujetties évaluent grâce à cette procédure les impacts pour fonder leur dispositif de gestion de la continuité d'activité, en prenant en compte toutes les données disponibles, y compris publiques. L'analyse d'impact est étendue aux situations de cyber attaques, donc couvre non seulement la disponibilité, mais aussi l'intégrité et la confidentialité des systèmes et des données. À défaut, les dispositifs du plan d'urgence et de poursuite d'activité, ainsi que du plan de reprise d'activité, pourraient ne pas répondre de façon adéquate aux objectifs de continuité d'activité donc aux orientations données par l'organe de surveillance.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance d'assurer :

- La prise en compte, par les entreprises, de l'importance et de la sensibilité de leurs activités opérationnelles, de support ou de contrôle.

- ✓ À titre de bonne pratique, il est souhaitable que les personnes « clés » soient identifiées pour garantir qu'elles seront mobilisables en cas de crise.

- L'intégration dans le périmètre de l'analyse des actifs informatiques ou des données qui sont utilisés et des prestataires concernés, ainsi que les liens de dépendance existant entre les différents éléments mis en œuvre pour chaque activité.

- La définition des priorités de maintien des activités de l'entreprise et la pertinence des estimations des ressources humaines, immobilières, techniques et financières nécessaires.

- La mise en place d'objectifs de durée maximale d'interruption admissible (DMIA) des activités et de durée de perte de données maximale admissible (PDMA), auxquels doivent se conformer les systèmes et services informatiques. À ce titre :

    - La redondance des équipements est un moyen possible pour assurer une bonne disponibilité
    - La DMIA se traduit pour les équipes de production en un « *recovery time objective* » – RTO qui définit le délai maximal de reprise
    - La PDMA se définit au travers d'un « *recovery point objective* » – RPO, qui exprime la durée maximale admise entre un incident et la date de sauvegarde des données la plus récente.

Point 28 : plan d'urgence et de poursuite d'activité (PUPA)

Le b) de l'article 215 de l'arrêté précise que le dispositif de continuité d'activité comprend « *un plan d'urgence et de poursuite de l'activité fondé sur l'analyse des impacts […] ».* Selon le n) de l'article 10 de l'arrêté, il s'agit d'un « *ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant, de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes de l'entreprise assujettie, puis la reprise planifiée des activités et à limiter ses pertes* ». Le PUPA, parfois encore appelé plan de continuité d'activité (PCA), pose le principe selon lequel l'entreprise assujettie doit prendre des mesures visant à faire en sorte que son activité soit maintenue en toute circonstance, ne serait-ce qu'en mode dégradé. Les scénarios de crise afférents sont ainsi de nature diverse, avec des faits générateurs pas nécessairement d'origine informatique, et il convient donc d'anticiper également les situations de cyber-attaques.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur :

- L'implication des dirigeants effectifs dans la définition du plan, qui doit en outre être conforme aux orientations données par l'organe de surveillance.

- La mise à jour au moins annuelle du plan en fonction du résultat des tests mentionnés ci-après, de l'évolution des menaces, ou de la modification des objectifs de DMIA des activités et de durée de la PDMA.

- L'importance de définir :

    - Les actions et moyens à mettre en œuvre pour faire face aux différents scénarios de perturbation des activités, y compris des cas de dysfonctionnements informatiques et de cyberattaques, afin de protéger ou de rétablir la confidentialité, l'intégrité et la disponibilité des activités opérationnelles, de support ou de contrôle, ainsi que des actifs informatiques ou les données.

- Les scénarios de crise, qui doivent répondre à tous les types d'impact (disponibilité, intégrité, confidentialité)
- Les mesures requises pour le rétablissement des activités essentielles ou importantes dans le respect des objectifs de durée maximale d'interruption admissible des activités et de durée maximale admissible de perte de données
- Les modalités de maintien ou de rétablissement de la continuité des systèmes et services informatiques, ainsi que de la sécurité du système d'information.

Point 29 : plan de reprise d'activité (PRA)

Le c) de l'article 215 de l'arrêté précise que le dispositif de continuité d'activité comprend « *un plan de reprise d'activité qui comporte des mesures d'urgence destinées à maintenir les activités essentielles ou importantes ».* Le PRA, encore parfois appelé « plan de secours informatique » (PSI), vise principalement à assurer la continuité des systèmes et services informatiques. Conformément aux dispositions réglementaires, il est important qu'il inclue un volet consacré à la reprise d'urgence des activités les plus essentielles, même en mode dégradé. Le PRA se conforme aux besoins des « métiers » et autres « fonctions » utilisateurs du système d'information. Cela signifie qu'il répond aux objectifs de continuité des activités formulés dans l'analyse d'impact, ainsi qu'aux mesures de poursuite des activités inscrits dans le PUPA.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance des points suivants :

- Les situations où le PRA ne répond pas aux objectifs de continuité fixés par les métiers et fonctions utilisateurs du système d'information doivent faire l'objet d'un arbitrage par les dirigeants effectifs.
- Le PRA comporte des mesures d'urgence destinées à maintenir, ne serait-ce qu'en mode dégradé, les activités essentielles ou importantes de l'entreprise assujettie, notamment ses services de paiement.
- Les solutions de secours informatique reposent sur différents sites fonctionnant soit en partage de charge de production, chacun pouvant supporter une charge suffisante pour compenser la perte d'un ou de plusieurs autres sites. Si les solutions reposent sur différents sites dont l'un seulement est actif à la fois, ces centres sont suffisamment éloignés pour disposer d'approvisionnements électriques et de télécommunication différents. Ils ne sont pas exposés aux mêmes risques environnementaux, comme indiqué au point 20. Si tel était le cas du fait de leur proximité, un autre site plus éloigné est nécessaire pour disposer de réelles capacités de production dans tous les scénarios d'indisponibilité.
- Le PRA est documenté et mis à jour conformément aux enseignements tirés d'incidents ou de tests.
- Le PRA comporte des solutions organisationnelles alternatives aux solutions informatiques si la reprise n'est pas possible à court terme en raison des coûts, des risques, de la logistique ou de circonstances imprévues.

Point 30 : tests du dispositif de gestion de la continuité d'activité

Le cinquième alinéa de l'article 215 de l'arrêté dispose que « *les entreprises assujetties testent périodiquement leur dispositif de gestion de la continuité d'activité, notamment leurs services informatiques […] ».* Cette disposition, qui en rappelle d'autres sur la gestion des changements, des opérations ou de la sécurité, renvoie aussi au principe selon lequel tout dispositif ne peut être considéré comme abouti s'il n'est pas testé. Les activités opérationnelles, de support ou de contrôle, essentielles ou importantes, ainsi que leurs actifs informatiques ou l'accès aux données, doivent donc être testés au moins annuellement. Ces tests tiennent compte de leurs liens de dépendance, y compris avec des prestataires. À défaut, l'obsolescence de ce dispositif ou son caractère inapproprié par rapport aux objectifs qui lui sont fixés ou à l'environnement dans lequel il est installé, ne seraient pas détectés, ce qui pourrait entraver les capacités de continuité d'activité en cas de perturbation majeure.

Concernant les dispositions précitées, l'ACPR appelle l'attention des entreprises assujetties sur l'importance des points suivants :

- Le test de poursuite des activités doit mobiliser, selon différents scénarios d'indisponibilité, les ressources humaines et immobilières nécessaires au maintien des activités essentielles ou importantes.
- Le test des dispositifs de continuité informatique doit pouvoir être déclenché, soit en totalité pour l'ensemble du système d'information, soit par partie ou application. Si l'exploitation est répartie sur au moins deux sites fonctionnant en partage de charge (mode « actif-actif »), il importe que chacun des sites puisse supporter la charge totale de fonctionnement en cas d'indisponibilité d'un ou de plusieurs sites.
- Le test conduit à utiliser l'environnement de secours en situation réelle par les équipes métiers pendant une période suffisamment significative et sur un périmètre représentatif de leurs activités critiques (notamment pour permettre le déroulement des travaux de fins de période comme une fin de semaine ou de mois).
    - ✓ À titre de bonne pratique, la période de bascule doit inclure des périodes d'utilisation habituelle des services informatiques, ainsi que des pics d'activité. Elle doit être suffisamment longue pour permettre le rétablissement de l'environnement nominal.
- Le test inclut les services fournis par des prestataires ou des partenaires (une autre entreprise assujettie par exemple).
- Le test donne lieu à un rapport écrit destiné aux dirigeants effectifs et identifiant les défauts observés.

Point 31 : communication de crise

Ce point renvoie aussi à l'article 270-4 de l'arrêté

Le point 13 de la Notice explique que, dans le cadre du processus de gestion des incidents opérationnels ou de sécurité prévu par l'article 270-4 de l'arrêté, il est important pour les entreprises assujetties de disposer de plans de communication de crise internes et externes en cas de perturbation grave. Cela s'explique par le besoin d'informer sans délai et de manière appropriée les parties prenantes à leurs activités dans ces situations, donc de pouvoir réagir efficacement lors d'une crise. Cela contribue donc aux objectifs de continuité d'activité, en préparant l'établissement à diffuser des messages appropriés à sa clientèle et aux autres parties concernées. À défaut, une communication mal maitrisée est susceptible d'accroitre la gravité d'une situation de crise.

À ce titre, l'ACPR appelle l'attention des entreprises assujetties sur l'importance :

- De préparer et valider à l'avance les plans de communication de crise (notamment, identification des personnes qui auront la responsabilité de communiquer, préparation des messages à diffuser, et procédures d'escalade de l'information), en fonction des scénarios de crise.
- De tester régulièrement ces plans de communication, et de les corriger si le résultat du test le justifie.