racine
AVOCATS

Flash Info

10 mars 2021

Contrôle interne : Publication de l'arrêté du 25 février 2021

Publication de l'arrêté du 25 février 2021 visant à mettre à jour 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 (« ACPR ») et entrant en vigueur au 28 juin 2021[1].

L'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 (« **Arrêté** ») a été publié le 6 mars dernier.

L'Arrêté a été publié afin de mettre à jour 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 (« **l'Arrêté du 3 novembre 2014** ») pour prendre en compte certaines dispositions ayant été adoptées, dans un cadre international, et également européen. Une clarification est également opérée en ce qui concerne les différents niveaux de contrôle qui peuvent exister, et des précisions sont apportées pour les obligations devant être respectées tant en matière d'agrégation des données que de gestion du risque informatique.

Vous trouverez ci-après une description des principaux apports de ce texte.

[1] Par exception, l'article 241-2 nouveau de l'Arrêté du 3 novembre 2014 relatif à certaines informations arrêtées par le comité des nominations qui doivent être communiquées à l'ACPR est entré en vigueur le 7 mars 2021.

Sur l'organisation et les objectifs du contrôle interne :

L'Arrêté vient entériner l'existence de trois niveaux de contrôle distincts[2] à adapter selon la taille des entreprises assujetties, leur nature, et la complexité de leurs activités :

- Le premier niveau de contrôle est assuré par des agents exerçant des activités opérationnelles, qui identifient les risques induits par leur activité, et respectent les procédures et les limites fixées ;
- Le deuxième niveau de contrôle 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. 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. Ce deuxième niveau de contrôle est assuré par la fonction de vérification de la conformité et la fonction de gestion des risques ;
- 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 niveaux.

Concernant les contrôles de deuxième niveau, l'Arrêté insiste sur le fait que les agents dédiés[3] sont indépendants des unités qu'ils contrôlent. Enfin, les entreprises assujetties devront également désormais désigner un dirigeant effectif responsable de la cohérence et de l'efficacité de ce contrôle[4].

Sur le rôle du responsable de la fonction d'audit interne :

L'Arrêté apporte plusieurs éléments concernant le rôle du responsable de la fonction d'audit interne. En effet, les entreprises assujetties doivent désigner un responsable de la fonction d'audit interne, et doivent définir des procédures internes encadrant sa désignation et sa révocation. De plus, un dirigeant effectif devra être désigné afin de veiller à la cohérence et à l'efficacité du contrôle périodique assuré par la fonction d'audit interne. Les agents composant la fonction d'audit interne exerceront leurs missions de manière indépendante à l'égard de l'ensemble des entités et services qu'ils contrôlent[5].

De plus, des moyens affectés à la fonction d'audit interne devront être apportés pour pouvoir mener un cycle complet d'investigations de l'ensemble des activités sur un nombre d'exercice aussi limité que possible qui ne saurait excéder cinq ans[6]

[2] Article 12 modifié de l'Arrêté 3 novembre 2014
[3] Article 14 modifié de l'Arrêté du 3 novembre 2014
[4] Article 16 modifié de l'Arrêté du 3 novembre 2014
[5] Article 17 modifié de l'Arrêté du 3 novembre 2014
[6] Article 25 modifié de l'Arrêté du 3 novembre 2014

Sur le contrôle du risque de non-conformité par la fonction de vérification de la conformité :

Les entreprises assujetties doivent définir des procédures internes encadrant la désignation et la révocation de la fonction de vérification de la conformité[7]. Ce dernier ne pourra par ailleurs exercer aucune opération financière ou commerciale lorsqu'il n'est pas dirigeant effectif[8].

L'Arrêté précise également que lorsque la distinction entre le responsable de la fonction de vérification de la conformité et le responsable de la fonction de gestion des risques n'est pas justifiée (en raison de la taille, de la nature, et de la complexité des activités de l'entreprise assujettie), c'est le responsable de la fonction de gestion des risques qui sera chargé de veiller à la cohérence et à l'efficacité du contrôle du risque de non-conformité. Pour ce faire, il assure la coordination de tous les dispositifs qui concourent à l'exercice de la fonction de vérification de la conformité et de la fonction de gestion des risques[9].

Le responsable de la vérification de la conformité (ou une personne habilitée par ce dernier) interviendra également en cas d'opérations relatives à des nouveaux produits ou changements significatifs : il devra produire un avis écrit et systématique préalablement à l'exécution de ces opérations[10].

Enfin, l'Arrêté apporte des précisions sur les procédures permettant de garantir la séparation des tâches et de prévenir les conflits d'intérêts, en mentionnant leurs objets : ces procédures servent à recenser, évaluer, gérer et atténuer ou éviter les conflits d'intérêts avérés et potentiels au niveau de l'établissement et les intérêts privés du personnel qui pourraient avoir une incidence défavorable sur l'exercice de leurs attributions et responsabilités [11].

Concernant les systèmes de mesure des risques et procédures :

L'Arrêté mentionne les politiques concernant les données sur les risques : les établissements sont dans l'obligation d'en définir les politiques (à l'échelle du groupe le cas échéant), d'en régir la gestion, la qualité et l'agrégation. Des procédures doivent être mises en place concernant l'exactitude, l'intégrité, et l'exhaustivité des données sur les risques, ou encore une structure de données uniforme ou homogène pour identifier sans équivoque les données sur les risques. Les données agrégées sur les risques doivent être disponibles en temps utiles, et les capacités d'agrégation suffisamment adaptables pour répondre à des demandes ponctuelles[12].

Concernant la gestion de la continuité d'activité :

Un dispositif de gestion de la continuité d'activité validé par l'organe de surveillance et mis en œuvre par les dirigeants effectifs doit être mis en place, afin d'assurer la capacité à maintenir les services, notamment informatiques, des établissements assujettis de manière continue et à limiter leurs pertes en cas de perturbation grave[13].

[7] Article 28 modifié de l'Arrêté du 3 novembre 2014
[8] Article 29 modifié de l'Arrêté du 3 novembre 2014
[9] Article 32 modifié de l'Arrêté du 3 novembre 2014
[10] Article 35 modifié de l'Arrêté du 3 novembre 2014
[11] Article 38 modifié de l'Arrêté du 3 novembre 2014
[12] Article 104 modifié de l'Arrêté du 3 novembre 2014
[13] Article 215 modifié de l'Arrêté du 3 novembre 2014

Ce dispositif de gestion de la continuité d'activité doit inclure les éléments suivants :

a. Une procédure d'analyse quantitative et qualitative des impacts de perturbations graves sur les activités, tenant compte des liens de dépendance existant entre les différents éléments mis en œuvre pour chaque activité, notamment les actifs informatiques et les données ;
b. Un plan d'urgence et de poursuite de l'activité fondé sur l'analyse des impacts, qui indique les actions et moyens à mettre en œuvre pour faire face aux différents scénarios de perturbation des activités et les mesures requises pour le rétablissement des activités essentielles ou importantes ;
c. Un plan de reprise d'activité qui comporte des mesures d'urgence destinées à maintenir les activités essentielles ou importantes.

Concernant les nouveaux produits :

L'Arrêté renforce les exigences applicables concernant les nouveaux produits. En effet, il s'agira désormais de définir des politiques d'approbation des nouveaux produits et changements significatifs recouvrant (i) les nouveaux produits et services, (ii) les changements significatifs, pour cette entreprise ou pour le marché, à un produit, service ou processus existant et leurs systèmes associés, (iii) les opérations de croissance externe et interne ainsi que (iv) les transactions exceptionnelles. De plus, la fonction de gestion des risques devra produire, le cas échéant, une évaluation des risques selon des scénarios appropriés au regard de la significativité des risques induits par ces opérations[14].

Concernant l'externalisation :

Dorénavant, en cas de conclusion d'un contrat d'externalisation portant sur des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes ou lorsqu'une activité externalisée est devenue une prestation de service ou une tâche opérationnelle essentielle, l'entreprise assujettie devra en informer l'ACPR[15].

L'entreprise assujettie devra par ailleurs mettre à jour son registre des dispositifs d'externalisation, en distinguant les dispositifs d'externalisation portant sur des prestations de services ou des tâches opérationnelles essentielles ou importantes et les dispositifs d'externalisation d'autres activités[16].

Concernant la gestion du risque informatique :

L'Arrêté du 3 novembre 2014 comprend désormais un titre VI bis consacré à la gestion du risque informatique ainsi qu'un ensemble de définitions nouvelles : celles d' « actif informatique », de « système d'information », de « service informatique », de « risque informatique » et de « sécurité du système d'information »[17].

L'Arrêté définit les contours de la gestion du risque informatique. Les entreprises assujetties doivent établir leur stratégie en matière informatique afin de répondre aux objectifs de leur stratégie d'affaires. Les dirigeants effectifs et l'organe de surveillance doivent s'assurer que les ressources

[14] Article 221 modifié de l'Arrêté du 3 novembre 2014
[15] Article 232 modifié de l'Arrêté du 3 novembre 2014
[16] Article 238 modifié de l'Arrêté du 3 novembre 2014
[17] Article 10 modifié de l'Arrêté du 3 novembre 2014

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[18].

Les entreprises assujetties doivent organiser la gestion de leur risque informatique afin d'identifier le risque informatique auquel elles sont exposées, l'évaluer, adapter des mesures adéquates de réduction du risque informatique, y compris des contrôles, ainsi que surveiller l'efficacité de ces mesures et informer les dirigeants effectifs et l'organe de surveillance de leur bonne exécution[19].

Une politique de sécurité du système d'information doit être établie par les entreprises assujetties, pour déterminer 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. Elle doit être approuvée par les dirigeants effectifs et l'organe de surveillance[20].

Les entreprises assujetties doivent également organiser 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. Ces procédures couvrent notamment l'exploitation, la surveillance et le contrôle des systèmes et services informatiques. Elles sont complétées par un processus de détection et de gestion des incidents opérationnels ou de sécurité[21].

Enfin, Les entreprises assujetties disposent d'un cadre de conduite clair et efficace de leurs projets et programmes informatiques. Il est accompagné d'un processus de gestion de l'acquisition, du développement et de l'entretien des systèmes d'information, ainsi que par 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[22].

Auteurs

David Masson
Avocat Associé
dmasson@racine.eu

Sonia Oudjhani-Rogez
Avocat
soudjhanirogez@racine.eu

Lena Chemla
Avocat
lchemla@racine.eu

Maia Steffan
Avocat
msteffan@racine.eu

Jérémy Bouazis
Avocat
jbouazis@racine.eu

[18] Article 270-1 nouveau de l'Arrêté du 3 novembre 2014
[19] Article 270-2 nouveau de l'Arrêté du 3 novembre 2014
[20] Article 270-3 nouveau de l'Arrêté du 3 novembre 2014
[21] Article 270-4 nouveau de l'Arrêté du 3 novembre 2014
[22] Article 270-5 nouveau de l'Arrêté du 3 novembre 2014