Guide « Contrôle interne »

*Les informations contenues dans ce **guide « Contrôle interne »** sont uniquement publiées à titre informatif et n'ont pas vocation à être exhaustives, ni à lier l'ACPR dans ses relations avec les personnes soumises à son contrôle. Elles ont pour objet d'expliquer de manière pédagogique le cadre réglementaire relatif au contrôle interne applicable aux sociétés de financement, établissements de monnaie électronique, établissements de paiement et organismes d'assurance relevant du régime dit « Solvabilité II ». Ces informations sont simplement destinées à aider les porteurs de projet désireux de déposer un dossier de demande d'autorisation auprès de l'ACPR. En aucun cas, elles ne préjugent de la décision de l'ACPR sur les dossiers individuels.*

Table des matières

A. Cadre réglementaire pour les activités bancaires et de paiement

Les sociétés de financement, les établissements de monnaie électronique, les établissements de paiement et les PSIC doivent disposer d'un système adéquat de contrôle interne leur permettant de mesurer les risques et la rentabilité de leurs activités (articles L. 511-55, L. 522-6, L. 522-14 et L. 526-27 du Code monétaire et financier).

Ce dispositif de contrôle interne qui doit être adapté à la nature et au volume de leurs activités, à leur taille, à leurs implantations et aux risques de différentes natures auxquels ils sont exposés, doit comprendre notamment (article 3 de l'arrêté du 3 novembre 2014) :

- Une organisation claire des rôles et responsabilités des dirigeants,
- Un système de contrôle des opérations et des procédures internes ;
- Une organisation comptable et du traitement de l'information ;
- Des systèmes de mesure des risques et des résultats ;

Mis en ligne le 6 janvier 2022

- Des systèmes de surveillance et de maîtrise des risques ;
- Un système de documentation et d'information à l'attention des dirigeants, de l'organe de surveillance et de l'ACPR ;
- Une organisation de la gestion du risque informatique ;
- Et également un dispositif de surveillance des flux d'espèces et de titres pour les sociétés de financement.

En application des articles 258 à 266 de l'arrêté du 3 novembre 2014 modifié[1], les établissements de monnaie électronique, les établissements de paiements, les PSIC et les sociétés de financement sont tenus de remettre, chaque année à l'ACPR, un rapport annuel de contrôle interne (RACI).

Nota bene : Les établissements de monnaie électronique à agrément simplifié et les établissements de paiement à agrément simplifié ne sont pas soumis aux dispositions relatives au contrôle interne prévues par l'arrêté du 3 novembre 2014 modifié (article 274 dudit arrêté).

Les autres références à retenir :

- Le règlement n° 575/2013 du 26 juin 2013 du Parlement européen et du Conseil concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement ;
- Le règlement (UE) n° 1024/2013 du 15 octobre 2013 confiant à la BCE des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit ;
- Les orientations de l'ABE sur la gouvernance interne (EBA/GL/2017/11), applicables depuis le 30 juin 2018, en particulier le titre V « Cadre et mécanismes de contrôle interne » et le titre II « Rôle et composition de l'organe de direction et des comités » ;
- Les orientations de l'ABE sur l'évaluation du risque lié aux technologies de l'information et de la communication (« TIC ») dans le cadre du processus de contrôle et d'évaluation prudentiels (EBA/GL/2017/05), applicables depuis le 1er janvier 2018 ;
- Les orientations de l'ABE sur les tests de résistance des établissements (EBA/GL/2018/04), applicables depuis le 1er janvier 2019 ;
- Les orientations de l'ABE relatives à l'externalisation (EBA/GL/2019/02), applicables depuis le 30 septembre 2019 ;
- Les orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité (EBA/GL/2019/04), applicables depuis le 30 juin 2020.
- L'arrêté du 6 janvier 2021 relatif au dispositif et au contrôle interne en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et de gel des avoirs et d'interdiction de mise à disposition ou d'utilisation des fonds ou ressources économiques.

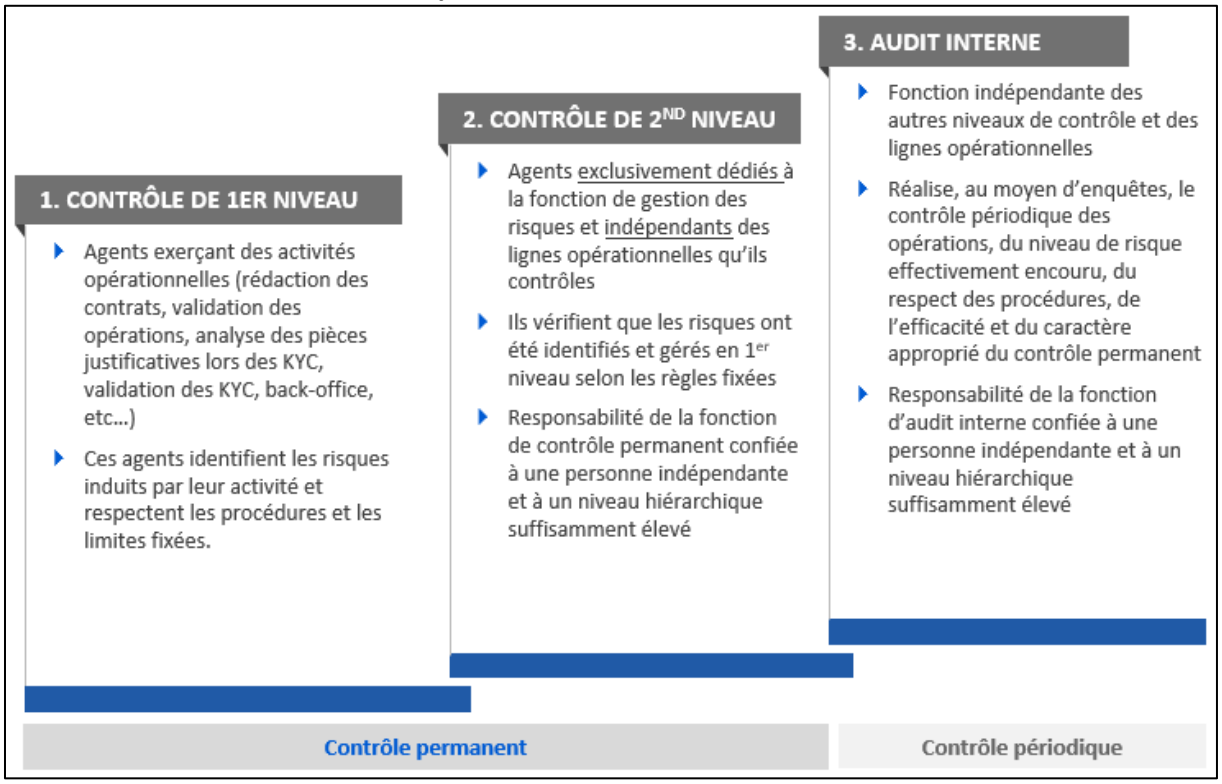
[1] L'arrêté du 3 novembre 2014 modifié, relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'ACPR, prévoit la mise en œuvre de mesures de sécurité minimales dans les processus de prise de décision et de gestion de l'activité courante. Il met en place des normes de gestion internes, qualitatives et s'applique à la fois sur base sociale et consolidée. Il participe à la prévention des difficultés d'un établissement en l'obligeant à adopter un dispositif de contrôle interne adapté à sa taille et ses activités de nature à réduire ses risques.

B. Illustrations sur les modalités de mise en œuvre

1. Structuration du contrôle interne

Le contrôle interne se décompose en trois niveaux de contrôle.

Schéma récapitulatif sur les trois niveaux de contrôle



2. Cartographie des risques et plan de contrôle permanent et périodique

La cartographie des risques permet d'identifier tous les risques auxquels la société fait face, d'évaluer ces risques (scoring), de les mesurer et de les piloter au moyen d'un outil de gestion qui doit être opérationnel. C'est une démarche continue qui nécessite l'actualisation de la cartographie.

Le dispositif de cartographie des risques doit être suffisamment détaillé. Le plan de contrôle qui contribue à la maitrise des risques doit être adapté à l'impact identifié. La cartographie des risques et le plan de contrôle sont interdépendants et évoluent de concert.

Exemples de risques :

- Les risques opérationnels :
    - Les fraudes internes et externes (la fausse déclaration, le vol commis par des employés, les détournements des procédures, etc.) ;
    - Les pratiques en matière RH (la formation inadaptée, la contestation salariale, le non-respect de la règlementation relative à la santé, l'absence de personne clé, etc.) ;
    - Les pratiques commerciales (la mauvaise commercialisation incluant les pratiques commerciales trompeuses et l'absence de remise de la documentation pré-contractuelles ou contractuelles, l'inadéquation des processus de vente, l'inexécution

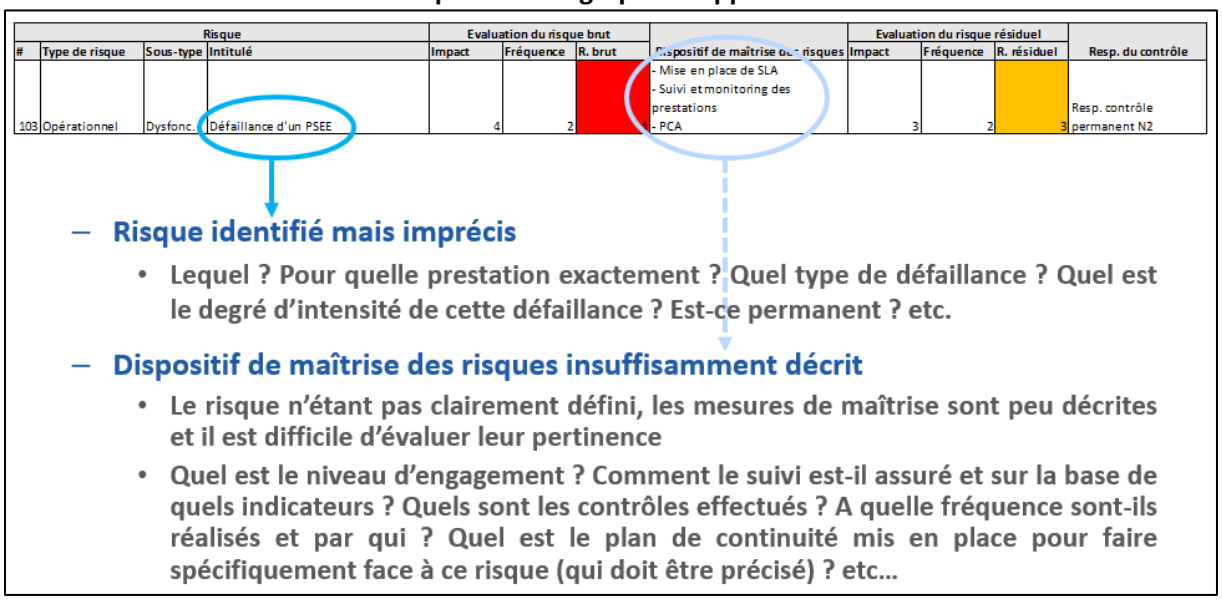
ou la mauvaise exécution des engagements contractuels, la gestion des réclamations des clients, etc.) ;
    - Le dommage aux actifs matériels (terrorisme, vandalisme, inondation, incendie, etc.) ;
    - L'interruption de l'activité et le dysfonctionnement des systèmes (la défaillance d'un PSEE, etc.) ;
    - L'exécution ou la livraison défaillante (accès non autorisé à des comptes de la clientèle, documentation légale ou contractuelle incomplète, litiges avec un PSEE, etc.).

- Les risques informatiques :
    - Inadéquation des ressources informatiques, la perte ou la corruption des données, plan de sauvegarde informatique inadapté, exécution de requête frauduleuse sur les API bancaires, gestion des habilitations inadaptée, manipulation non autorisée des données, protection physique inadéquate, défaillance des systèmes de contrôle des accès, défaillance dans la gouvernance des PSEE en matière de SSI, etc.

- Les risques de non-conformité, les risques de réputation, les risques comptables, etc.

Le plan de contrôle est à adapter aux risques identifiés.

Exemple de cartographie à approfondir



3. Contrôle des fonctions externalisées

Le principe général qui structure le recours à l'externalisation est que les établissements qui externalisent des prestations essentielles, critiques ou importantes demeurent pleinement responsables du respect de toutes les obligations qui leur incombent (communiqué de presse ACPR du 22/07/2021).

L'arrêté du 3 novembre 2014 ainsi que les orientations de l'ABE relatives à l'externalisation (EBA/GL/2019/02) encadrent l'externalisation notamment par les sociétés de financement, les établissements de monnaie électronique, les établissements de paiement et les PSIC..

Les orientations de l'ABE sont applicables à tous les schémas d'externalisation mis en place à partir du 30 septembre 2019, sauf pour les dispositions relatives aux accords de coopération qui s'appliquent

au 31 décembre 2021 (paragraphe 63 (b) des orientations susvisées). Tous les accords d'externalisation existants doivent donc être complétés conformément aux orientations avant le 31 décembre 2021.

Pour la définition des tâches opérationnelles essentielles ou importantes, il faut se référer à l'article 10 r) de l'arrêté du 3 novembre 2014.

Pour la définition des fonctions critiques ou importantes, il faut se référer à la section 4 des orientations de l'ABE relatives à l'externalisation (EBA/GL/2019/02).

Les articles 11, 12 et 234 de l'arrêté du 3 novembre 2014 prévoient la mise en place d'une fonction de contrôle interne (permanent et périodique) couvrant les activités externalisées. Les orientations de l'ABE relatives à l'externalisation (EBA/GL/2019/02) précisent les modalités de surveillance que devraient mettre en place les établissements, comprenant notamment la mise en place de normes d'exécution conformes à leurs politiques.

Si vous avez recours à des prestataires et que vous leur avez confié des fonctions critiques ou importantes, le registre les concernant comporte les informations listées au point 55 des orientations de l'ABE relatives à l'externalisation (EBA/GL/2019/02).

Nota bene : Pour le contrôle des IOBSP, la position 2013-P-01 de l'ACPR apporte plus de précisions sur l'application de 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'ACPR.

4. Points de contrôle spécifiques aux agents de PSP

Les prestataires de services de paiement (« PSP » - définis à l'article L. 521-1 du Code monétaire et financier) agréés sont responsables vis-à-vis des tiers des actes de tout agent qu'ils mandatent (article L. 523-3, al.1er Code monétaire et financier).

En ce sens, les PSP sont tenus de contrôler et de suivre les activités de leurs agents (article L. 522-14 du Code monétaire et financier). De manière similaire, le PSP contrôle la bonne application par l'agent des procédures LCB-FT et de gel des avoirs (article 28 de l'arrêté du 6 janvier 2021).

Les PSP doivent ajuster leurs contrôles aux activités de l'agent. Ils doivent mettre en place un plan de contrôle sur pièces et sur place (article L. 523-3, al. 2e Code monétaire et financier).

Exemples de questions à se poser :

- Dans quelle mesure l'agent exerce-t-il un contrôle sur les flux ?
- Quels sont les risques associés à la clientèle de l'agent ?
- Quels sont les risques associés à l'activité de l'agent ?
- Quelles tâches seront déléguées à l'agent ?
- Quel système de reporting doit être mis en place par le prestataire de services de paiement pour qu'il contrôle cette activité ?
- Quels sont les effets de la commercialisation d'une offre via un agent sur la rentabilité ?
- Dans quelle mesure le PSP maîtrise-t-il la commercialisation de l'offre par l'agent ?
- L'agent est-il bien inclus dans les programmes de formation ?
- Le client est-il bien conscient que l'agent agit au nom et pour le compte du prestataire de services de paiement ? Comment ?

Les principaux points de contrôle d'un agent de PSP sont les suivants :

- Gouvernance et organisation :
  - Organisation globale ;
  - Dispositif de maîtrise des risques, de contrôle interne et de conformité ;
  - Cartographie des risques ;
  - Politique et procédure de protection des données personnelles, etc.

- Gestion des risques :
  - Procédure comptable ;
  - Procédure de reporting ;
  - Gestion de l'externalisation ;
  - Procédure pour les nouveaux produits, etc.

- Risques liés aux instruments de paiement :
  - Description du produit ou des produits (volumétrie, clientèle, flux financier, flux de données, traçabilité, etc.) ;
  - Gestion des risques « produit » et sécurité des moyens de paiement ;
  - Gestion des demandes clients, des réclamations et des demandes d'exercice de droit ;
  - Politique commerciale et de distribution ;
  - Données sensibles et données personnelles, etc.

- PUPA[2] et remontée des incidents :
  - PUPA ;
  - Plan et test PUPA ;
  - Procédure de remontée des incidents, etc.

- Risques TIC et sécurité des systèmes informatiques :
  - Dispositif de sécurité des SI ;
  - PSSI ;
  - Monitoring des SI ;
  - Habilitations ;
  - Architecture ;
  - Formation ;
  - Inventaire des actifs, etc.

C. Cadre réglementaire pour les activités d'assurance

Les organismes d'assurance et de réassurance doivent se doter d'un système de contrôle interne. Les principales exigences en la matière sont définies dans les articles suivants pour les organismes soumis à Solvabilité II :

- Article L. 354-1 à L. 354-3 du Code des assurances ;
- Article R. 354-4 du Code des assurances ;
- Article 258 du règlement délégué n° 2015/35 ;
- Article 266 et suivants du règlement délégué n° 2015/35.

1. Objectif du contrôle interne

[2] Plan d'urgence et de poursuite de l'activité

Selon l'article R. 354-4 du Code des assurances, le système de contrôle interne comprend au minimum des procédures administratives et comptables, un cadre de contrôle interne, des dispositions appropriées en matière d'information et une fonction Vérification de la conformité.

L'objectif du système de contrôle interne est d'assurer (i) le respect du cadre législatif et réglementaire auquel est soumis l'organisme d'assurance, (ii) l'efficacité et l'efficience de ses opérations et (iii) la disponibilité des informations financières et non financières, ainsi que leur fiabilité.

À ce titre, les responsables de fonctions clés, en charge de la conformité, de la gestion des risques, de l'actuariat et de l'audit interne, sont directement impliqués dans l'évaluation et la mise en œuvre du système de contrôle interne.

2. Moyens mis en œuvre

Le système de contrôle interne s'appuie sur des politiques écrites et des procédures développées par l'organisme d'assurance. Ces dispositifs décrivent l'ensemble des moyens, des comportements et des actions adaptées à l'organisme contribuant à la maîtrise des opérations et des risques, et à l'utilisation efficiente de ses ressources.

Ce système doit permettre à l'organisme de prendre en compte de manière appropriée les risques significatifs auxquels il est exposé, qu'ils soient opérationnels, financiers ou de conformité.

Les politiques écrites suivantes sont en particulier attendues (article 258 du règlement délégué n° 2015/35) :

- Politique de gestion des risques ;
- Politique de contrôle interne ;
- Politique d'audit interne ;
- Politique d'externalisation ;
- Politique de continuité de l'activité ;
- Politique de rémunération.

Le contrôle interne se décompose en trois niveaux de contrôle :

- Le contrôle de premier niveau (effectué par les opérationnels) ;
- Le contrôle de deuxième niveau (effectué par les services de contrôle interne ou un service non impliqué dans l'activité opérationnelle) ;
- Le contrôle de troisième niveau (effectué par l'audit interne).

3. Points de vigilance

L'ACPR s'attache à vérifier la bonne adéquation des règles et procédures avec la règlementation et la bonne application de ces dernières par l'entreprise d'assurance. Elle vérifie notamment les points suivants :

(i) Politiques écrites

Les principales politiques écrites doivent être transmises dans le cadre de la demande d'agrément.

Post-agrément, ces politiques sont évolutives et peuvent être complétées au fur et à mesure du développement de l'activité afin de les rendre plus opérationnelles, sous réserve que ces évolutions soient validées par les instances de gouvernance concernées. Certaines politiques peuvent également être complétées par des procédures spécifiques. Les politiques écrites doivent être revues une fois par an par les instances de gouvernance concernées (Article R. 354-1 du Code des assurances), afin de confirmer que celles-ci sont toujours pertinentes ou afin de les adapter.

(ii) Politique de gestion des risques et définition de seuils d'alerte par catégorie de risque

La politique de gestion des risques définit des seuils d'alerte par catégorie de risque (Article R.354-3 du Code des assurances). La détermination des seuils d'alerte doit être cohérente avec le profil de risque de la société.

En cas de franchissement de seuils d'alerte, il convient de décrire les mesures d'atténuation des risques qui seraient mises en œuvre par la société. Dans la pratique, en matière de solvabilité, le seuil d'alerte doit être supérieur à une couverture de 100% du capital de solvabilité requis.

En effet, les organismes d'assurance doivent détenir à tout moment les fonds propres éligibles couvrant le SCR (Article L.352-1 du Code des assurances) et le MCR (Article L.352-5 du Code des assurances). En cas de non couverture du capital de solvabilité requis ou de risque de sous-couverture dans les trois prochains mois, la société doit en informer immédiatement l'ACPR et lui soumettre un plan de rétablissement (Article L.352-7 du Code des assurances).

À ce titre, il est nécessaire de fixer des seuils de couverture du SCR/MCR supérieurs à 100% dans le cadre du système de gestion des risques, afin d'assurer une « gestion saine et prudente » de la société (Article L.354-1 du Code des assurance).

(iii) Externalisations

La société doit déclarer l'ensemble des externalisations de fonctions critiques ou importantes (renvoi vers le site de l'ACPR).

En application de l'instruction n° 2020-I-09, la société est tenue de fournir le « formulaire de notification d'une externalisation d'activité ou de fonction importante ou critique ou d'évolution importante concernant cette externalisation » à l'ACPR. Le recours à des prestataires d'hébergement de données doit en particulier être signalé.
L'ACPR examine la nature des conventions signées (en vérifiant notamment la durée de la convention, les clauses de réversibilité, les droits d'accès aux informations et d'audit, etc.), le formulaire d'externalisation et s'informe si des audits du prestataire ont été réalisés ou sont prévus.

(iv) Cartographie des risques

Le système de contrôle interne comprend une cartographie des risques de la société.

Cette cartographie doit être suffisamment complète pour pouvoir appréhender les principaux risques ou les accumulations de risques auxquels l'organisme est exposé. À ce titre, le système de contrôle interne interagit avec la fonction de gestion des risques, puisque le calcul de l'intensité des risques prend en compte les effets d'atténuation permis grâce aux contrôles mis en œuvre.

(v) Anomalies/incidents

La société assure le recensement centralisé des anomalies ou incidents, dans le cadre de son système de contrôle interne.

(vi) Plan de conformité

La société doit disposer d'un plan de conformité validé par le conseil d'administration ou l'organe assimilé.

Le plan de conformité détaille les activités prévues pour la fonction de vérification de la conformité, lesquelles couvrent tous les domaines d'activité pertinents de l'entreprise d'assurance ou de réassurance et leur exposition au risque de conformité (article 270 du règlement délégué (UE) 2015/35 de la Commission du 10 octobre 2014 complétant la directive Solvabilité 2). Cette fonction doit être confiée à un responsable clairement identifié au sein du système de gouvernance de l'organisme. La fonction de vérification de la conformité a notamment pour objet de conseiller les dirigeants effectifs ainsi que le conseil d'administration ou le conseil de surveillance sur toutes questions relatives au respect des dispositions législatives, règlementaires et administratives afférentes à l'accès à l'activité d'assurance et de réassurance et à leur exercice (Article R. 354-4-1 du Code des assurances).

(vii) LCB-FT

Une attention particulière au plan de contrôle relatif à la LCB/FT (articles L561-32, R561-38-3 et R562-1 du code monétaire et financier et articles 13 et 16 de l'arrêté du 6 janvier 2021).