Quelles conséquences opérationnelles des nouvelles lignes directrices de l'ABE sur l'externalisation ?

Février 2019

L'ABE (autorité bancaire européenne) a ouvert en été 2018 une consultation portant sur une proposition de nouvelles lignes directrices relatives à l'externalisation. Ces lignes directrices remplaceront la précédente version, publiée en 2006, et auront vocation à s'appliquer tant aux établissements de crédit qu'aux entreprises d'investissement. Cette consultation s'étant terminée en septembre 2018, la publication des lignes directrices finalisée est désormais imminente. Les entités concernées peuvent sans attendre se préparer à leur entrée en application – prévue dès juin 2019 - en s'appuyant sur la version provisoire actuellement disponible.

Porteuse de risques, l'externalisation est déjà soumise à un cadre réglementaire exigeant

Du fait même de la souplesse que l'externalisation autorise, le régulateur fait le constat qu'elle est porteuse de nombreux risques : dilution de la responsabilité, délégation de fonctions essentielles à des entités de pays tiers situées hors du contrôle des régulateurs européens, perte de la vision globale de l'activité par les fonctions risque/ conformité et par les organes dirigeants, voire **perte de cette vision consolidée du risque par le régulateur lui-même.**

Afin de pallier ces différents risques, le régulateur a **défini et décliné au fil des années des principes directeurs afin d'encadrer ces accords d'externalisation.** Fixés dans les lignes directrices du CEBS (ex. ABE) de 2006, puis repris par la suite en droit national (notamment en France dans **l'arrêté du 3 novembre 2014),** ces principes directeurs sont au nombre de huit :

- Les fonctions stratégiques et relevant du cœur de métier ne peuvent être externalisées ;
- La responsabilité finale de la bonne gestion des risques associés à l'externalisation incombe à la direction de l'institution procédant à l'externalisation ;
- Une attention particulière doit être portée dès lors que l'entité externalise des activités stratégiques, i.e. activités d'une telle importance que tout problème dans la fourniture de ces activités pourrait avoir un effet significatif sur la capacité de l'institution à satisfaire aux exigences réglementaires, voire à poursuivre son activité ;
- Il ne devrait y avoir aucune restriction quant à l'externalisation d'activités non stratégiques ;
- L'externalisation doit s'inscrire dans une politique identifiée, incluant des plans d'urgence et des stratégies de sortie ;
- Les stratégies d'externalisation des institutions devraient leur permettre de faire face aux risques associés ;
- Tout accord d'externalisation devrait être l'objet d'un contrat officiel et détaillé ;
- Dans la gestion de ses relations avec le prestataire de service, l'institution devrait s'assurer de la mise en place d'un service level agreement.

Face à une nouvelle vague d'externalisation portée par la recherche de flexibilité et par l'open banking, l'ABE a ressenti le besoin d'un renforcement de la réglementation applicable

Depuis la publication de ces premières lignes directrices, **l'externalisation n'a cessé de se développer dans le secteur bancaire et financier,** pour des raisons multiples : recherche de flexibilité, baisse des coûts, et, plus récemment, **recherche de partenariats avec des fintechs afin d'acquérir de nouvelles technologies à moindre coût pour s'adapter à « l'open banking ».**

Le développement de **l'informatique en nuage** (*cloud computing)***,** qui apporte aux institutions bancaires et financières des solutions clef en main face à l'obsolescence et à la rigidité de leurs systèmes d'information, **pourrait également à l'avenir se porter vers les activités cœur,** et non plus seulement sur des activités périphériques, ce qui rend plus nécessaire leur encadrement.

En effet, malgré l'intérêt de ces solutions, elles portent avec elles des risques supérieurs aux systèmes d'information propriétaires, qu'il s'agisse de la confidentialité des données, de la difficulté pour l'entreprise déléguante d'exercer un contrôle réel, et surtout des faibles garanties de réversibilité et de préservation de l'intégrité des données en cas de défaillance du prestataire.

L'ABE cherche à inclure ces nouveaux acteurs et services dans le périmètre de sa supervision, via une extension considérable des notions « d'externalisation » et « d'activités critiques ».

Dans les lignes directrices actuellement en consultation, l'ABE propose une définition **extrêmement large** de l'externalisation, entendue comme « un arrangement de toute nature entre une entité et un fournisseur de service, par lequel ce fournisseur de service réalise un process, un service, une activité, ou une partie de ceux-ci, qui auraient autrement été réalisés par l'entité ».

Cette définition extensive pourrait être **facteur d'inquiétude pour les entités supervisées**, puisqu'elle ne comprend **aucune notion portant sur la durée ou la régularité de la prestation de service**, ce qui amènerait à soumettre toute prestation, y compris ponctuelle, aux **lourdes obligations de reporting, de suivi et de « testing » mises en place dans les lignes directrices.**

La notion d'activité « critique ou importante » est elle-même largement étendue, puisqu'elle comprend désormais « toute tâche opérationnelle réalisée par la fonction de contrôle interne », **contrairement à la définition antérieure où seules les activités directement liées à la fonction de contrôle étaient considérées comme critiques.** Dans la nouvelle définition, toutes les fonctions supports seraient désormais englobées, dès lors qu'elles s'appliquent à la fonction de risque et de contrôle interne.

Reporting, suivi et tests réguliers : de nouvelles contraintes pour garantir l'intégrité des fonctions externalisées.

Au-delà de l'extension du périmètre d'application de la réglementation, les nouvelles lignes directrices **renforcent les exigences relatives à la contractualisation des accords d'externalisation, à la transparence vis-à-vis du régulateur, à la gouvernance interne, au suivi et enfin aux conditions de dénonciation ou de résiliation des accords.**

La **contractualisation** doit ainsi désormais prévoir un certain nombre de **clauses obligatoires,** parmi lesquelles la possibilité pour l'entreprise d'accéder à tous moments à ses données (*notamment vis-à-vis des fournisseurs de services informatiques en nuage),* et de manière générale propres à garantir la possibilité pour l'entreprise délégante d'exercer un **contrôle effectif sur le prestataire.**

La **transparence** vis-à-vis du régulateur se matérialise par un **registre obligatoire de consignation de tous les accords d'externalisation de l'entreprise.** L'objectif affiché de ce registre est officiellement de permettre au régulateur de **monitorer le risque de concentration par un trop petit nombre d'acteurs** - notamment dans le domaine informatique **–** qui ferait courir un risque systémique à l'ensemble de la place financière en cas de défaillance.

Bien que le niveau de détail des informations à fournir varie en fonction du caractère critique ou non de l'activité, **on peut se demander néanmoins si l'objectif poursuivi justifie réellement que tous les accords d'externalisation – et non les seuls relatifs aux activités considérées comme critiques - doivent être consignée dans ce registre.** Une telle approche peut en effet être considérée comme en contradiction avec l'objectif de proportionnalité que l'ABE affirme poursuivre.

La clarification de la **gouvernance interne**, notamment en matière d'affectation des responsabilités, se matérialise quant à elle par la création d'une **fonction chargée de l'externalisation** (*outsourcing function*), pouvant être créée ex-nihilo ou rattachée à un cadre de haut niveau (*senior staff member*), directement responsable devant le comité de direction.

Enfin, l'objectif de **résilience** se matérialise par des obligations de **suivi** (via des KPI notamment) et surtout de **construction de plans de contingence visant à anticiper les cas de résiliation ou de défaillance.**

À cet égard, bien que l'objectif poursuivi paraisse tout à fait légitime et de nature à accroître le degré de préparation des institutions financières à de tels événements, on peut regretter **qu'il n'ait pas été fait de lien par le régulateur entre ces plans de contingence et les plans de redressement et de résolution bancaire déjà imposés par le FSB** (*Global Recovery and Resolution Plan)* **puis par l'Union européenne dans le cadre de l'Union bancaire**, ou encore avec les **plans de continuité d'activité,** généralisés dans le domaine bancaire et informatique**.** Il existera de fait un risque de redondance important entre ces différences réglementations.

De même, le nouveau registre, qui impose notamment de signaler toute externalisation de traitement de données personnelles à un prestataire externe, **parait sur ce point précis redondant avec le registre des traitements RGPD qui incluait déjà cette exigence.** La multiplication de registres se recoupant partiellement nous semble de nature à créer de nouvelles complexités dans la gestion des données, en particulier en termes de cohérence du rythme de mise à jour.

Enfin, l'absence de détail concret sur la réalisation des « tests » sur la solidité de ces plans de contingence laisse les entreprises dans **l'incertitude quant au degré d'investissement qui leur sera demandé.** Il existe en effet une grande différence entre la « simple » rédaction de plans théoriques visant à anticiper les cas de défaillance et la construction puis la réalisation fictive de cas de défaillance (de type « stress tests »), très onéreuse pour les entreprises concernées.

Les entités concernées doivent poursuivre le dialogue avec le régulateur afin d'éclaircir les modalités d'application des chapitres les plus sensibles

Le niveau d'impact des lignes directrices dans leur rédaction actuelle pourrait **grandement varier en fonction de l'interprétation qui sera faite de certaines notions clef :**

- **Sur l'extension du périmètre :** l'intégration dans la notion de « fonctions critiques ou importante » des tâches opérationnelles, dès lors qu'elles sont liées directement ou indirectement à la fonction contrôle, pourrait aboutir à **soumettre aux exigences les plus strictes des fonctions support n'ayant qu'un lien très lointain avec le métier cœur,** et dont le caractère « critique » reste par conséquent à prouver

- **Sur la proportionnalité des exigences imposées :** un grand nombre de dispositions seraient étendues à **toute forme d'externalisation, y compris ne portant pas sur des fonctions critiques ou importantes,** notamment l'obligation d'inscription dans le registre, qui s'appliquerait aux accords les plus mineurs. Reste à éclaircir également la question de savoir si cette exigence s'appliquerait également à des prestations ponctuelles.

Tout en continuant le dialogue avec le régulateur afin d'insister sur l'importance d'ajuster davantage le niveau d'exigence en fonction du risque effectif lié aux activités concernées, les entités doivent **étudier dès à présent les impacts sur les chantiers les plus lourds, notamment :**

- Engager une action de recensement de la totalité des accords d'externalisation en cours, sur la base du registre type proposé par l'ABE
- Envisager la mise à jour des contrats pour y intégrer les nouvelles clauses obligatoires
- Prévoir une revue des **plans de contingence** en cas de défaillance de leurs prestataires, le cas échéant en **adoptant une démarche cohérente avec les plans de redressement et de résolution existants**

Enfin, le coût accru de l'externalisation lié à ces nouvelles réglementations devra être intégré aux « business case » dans le cadre des dossiers d'arbitrages, en prenant notamment en compte **l'application plus aisée de ces règles aux cas d'externalisations intra groupe**, qui pourrait pousser davantage en faveur de ce type de solutions.

Henri O'Quin, Consultant Senior

AILANCY, cabinet de conseil indépendant spécialisé dans les métiers de la banque de la finance et de l'assurance vous accompagne pour relever vos enjeux métiers, accompagner vos réflexions et mener à bien vos projets de transformation.

Ailancy

32, rue de Ponthieu
75008 Paris
Tel : +33 (0)1 80 18 11 60
www.ailancy.com

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez la version électronique de notre étude en flashant ce QR code.

Retrouvez toutes nos publications sur www.ailancy.com/