Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Circulaire FINMA 2018/3 « *Outsourcing* – banques et assureurs »

Rapport sur l'audition concernant le projet de circulaire qui s'est déroulée du 6 décembre 2016 au 31 janvier 2017

21 septembre 2017

Laupenstrasse 27
3003 Berne
Tél. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

Table des matières

Eléments essentiels

1. La FINMA a mené une audition sur le projet de circulaire 2018/3 « *Outsourcing* – banques et assureurs » entre le 6 décembre 2016 et le 31 janvier 2017. Cette révision a mis à jour les exigences prudentielles relatives aux projets d'externalisation et les a concrétisées dans une circulaire commune destinée aux banques/négociants en valeurs mobilières et aux entreprises d'assurance.

2. La révision de l'ancienne circulaire de la FINMA 2008/7 « *Outsourcing* – banques » repose sur l'idée d'une réglementation davantage basée sur des principes. Les établissements peuvent organiser la mise en œuvre des exigences relatives aux externalisations afin de prendre en compte les différents modèles d'affaires et les risques correspondants. Cette approche basée sur des principes a encore été sensiblement renforcée par rapport à la version présentée à l'audition, et la responsabilité individuelle des établissements est mise en évidence. On renonce à apporter des précisions dans des foires aux questions (FAQ) ou d'autres aides à l'interprétation.

3. En plus des banques/négociants en valeurs mobilières et des assurances, de nombreuses entreprises indirectement concernées par la circulaire se sont exprimées lors de l'audition. Dans l'ensemble, les participants à cette dernière reconnaissent la nécessité d'avoir des exigences prudentielles appropriées pour les externalisations et une gestion adéquate du risque. De même, le besoin d'actualiser les dispositions existantes en raison des évolutions (technologiques) des dernières années n'est guère contesté. Les critiques formulées par les participants à l'audition portaient sur les points suivants :

    - une circulaire commune aux banques et aux entreprises d'assurance est inadéquate, car les modèles d'affaires et les bases légales diffèrent ;

    - la notion de « caractère essentiel » devrait être modifiée. De plus, il conviendrait de ne pas supprimer l'annexe présentant des exemples de prestations essentielles (sécurité juridique) et d'exclure de la circulaire les opérations de moyens de paiement (et pas uniquement celles de cartes de crédit) ;

    - l'égalité de traitement des externalisations au sein ou en dehors d'un groupe est disproportionnée ;

    - les exigences relatives aux transferts à l'étranger sont trop strictes, en particulier l'information préalable de la FINMA, la preuve expresse de l'exercice des droits de contrôle et la possibilité d'accéder à tout moment aux données en Suisse ;

- les restrictions concernant l'externalisation de la gestion du risque et de la *compliance* vont trop loin ; des externalisations complètes devraient être possibles au moins au sein d'un groupe ;

- de manière générale, les exigences relatives aux droits de contrôle sont excessives et ne sont pas neutres du point de vue technologique (notamment dans le contexte d'une externalisation en nuage [*cloud outsourcing*]) ;

- les exigences portant sur le contrat, le choix, l'instruction et le contrôle ne reposent pas suffisamment sur des principes ;

- l'application de la circulaire révisée aux relations d'*outsourcing* existantes des banques constitue un effet rétroactif illicite et une inégalité de traitement par rapport aux entreprises d'assurance. De manière générale, il faudrait également prévoir un délai transitoire supérieur à deux ans pour la mise en œuvre des nouvelles exigences ;

- selon les avis émanant du secteur de l'assurance, la disposition d'exception énoncée au Cm 46 de la version présentée à l'audition devrait être supprimée ;

- de façon générale, la circulaire ne devrait pas concerner les transferts à des infrastructures des marchés financiers, car celles-ci sont déjà soumises à une réglementation stricte ; une obligation d'informer préalablement la FINMA suffirait ;

- il n'existe aucune base légale pour les dispositions spécifiques aux banques d'importance systémique et ces prescriptions sont contraires aux normes internationales.

4. Dans la version finale de la circulaire, la FINMA a tenu compte de beaucoup de ces critiques :

   - la circulaire ne comprend plus aucune explication concernant les banques d'importance systémique ;

   - le délai transitoire a été prolongé et porté à cinq ans ;

   - la définition du caractère essentiel repose davantage sur des principes ; elle a été complétée par une auto-évaluation relevant de la responsabilité individuelle ;

   - les conditions d'une externalisation de la gestion du risque et de la *compliance* ont été précisées ;

- un complément basé sur des principes indique que le contexte du groupe peut être pris en compte lors d'un *outsourcing* interne ;

- la preuve du droit de contrôle à l'étranger et l'exigence selon laquelle les contrôles doivent être délégués à un prestataire organisé selon le droit suisse sont supprimées. Il incombe toutefois aux assujettis de veiller à garantir les droits de contrôle même en cas de transfert à l'étranger ;

- l'obligation d'annonce des banques en cas de transfert de grandes quantités de données d'identification des clients a été supprimée.

5. La circulaire entre en vigueur le 1er avril 2018.

Liste des abréviations

CFB	Commission fédérale des banques
CID	*Client Identifying Data* (données d'identification du client)
CSF	Conseil de stabilité financière
LB	Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargne (RS 952.0)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1)
LSA	Loi fédérale du 17 décembre 2004 sur la surveillance des entreprises d'assurance (loi sur la surveillance des assurances, RS 961.01)
OB	Ordonnance du 30 avril 2014 sur les banques et les caisses d'épargne (RS 952.02)
OLPD	Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (RS 235.11)
OS	Ordonnance du 9 novembre 2005 sur la surveillance des entreprises d'assurance privées (RS 961.011)
Solvabilité II	Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II), JO L 335 du 17.12.2009, p. 1

1 Introduction

La FINMA a mené une audition sur la révision de la Circ.-FINMA 2018/3 « *Outsourcing* – banques et assureurs » entre le 6 décembre 2016 et le 31 janvier 2017. L'information concernant l'audition a été publiée sur le site Internet de la FINMA. En plus des banques et des assurances, auxquelles est destinée la circulaire, des entreprises indirectement concernées par cette dernière (notamment en qualité de partenaires d'externalisation des banques ou des assurances) se sont exprimées sur le projet présenté à l'audition. Le présent rapport récapitule de manière générale les prises de position reçues des participants à l'audition, celles des banques/négociants en valeurs mobilières, des assurances et des tiers étant rassemblées dans des rubriques distinctes.

2 Prises de position reçues

Les personnes et les institutions suivantes (mentionnées par ordre alphabétique) ont participé à l'audition et ne se sont pas opposées à la publication de leur prise de position :

- ARIZON Sourcing SA (Arizon)
- Association des banques étrangères en Suisse (AFBS)
- Association Suisse d'Assurances (ASA)
- Association Suisse d'Audit Interne (ASAI)
- Association suisse des banquiers (ASB)
- Association suisse des télécommunications (asut)
- Assura SA (ASS)
- Credit Suisse (CS)
- economiesuisse
- EXPERTsuisse (ES)
- GI KARTAC du secteur des paiements (KAR)
- Homburger (HOM)
- HSBC Private Bank (Suisse) SA (HSBC)
- Laux Lawyers SA (LAUX)
- Leonteq Securities AG (LEO)
- MS Amlin SA (Amlin)
- Oberson Abels SA (OB)
- Raiffeisen Suisse société coopérative (RAI)
- Santésuisse (SAN)
- Schweizerischer Verband Unabhängiger Effektenhändler (SVUE)

- SIX Group SA (SIX)
- Société suisse du droit de la responsabilité civile et des assurances (SDRCA)
- Swico
- Swiss Payment Association (SPA)
- Swiss Re (SRZ)
- Swisscom (Suisse) SA (SCOM)
- swissICT (SICT)
- UBS SA (UBS)
- Union des Banques Cantonales Suisses (UBCS)
- Visana Services AG (VIS)
- Zurich Compagnie d'Assurances SA (ZIC)

3 Résultats de l'audition et évaluation par la FINMA

3.1 Généralités

Prises de position des banques / négociants en valeurs mobilières

La majorité des participants à l'audition sont favorables au maintien d'une réglementation basée sur des principes. Dans le même temps, de nombreuses dispositions détaillées et la conservation ou l'extension de la liste des exceptions sont demandées. Par ailleurs, plusieurs participants à l'audition déplorent que la circulaire prévoit un renforcement des exigences dans différents domaines, notamment concernant l'égalité de traitement des transferts externes et internes, les exigences supplémentaires pour les banques d'importance systémique ainsi que les transferts à l'étranger. Cette critique est due à la grande importance que revêtent les externalisations.

L'UBCS regrette que le principe de proportionnalité ne soit pas appliqué de manière cohérente dans le projet et que des exceptions et des allégements doivent également être accordés à des banques plus grandes (catégorie 3 en particulier) en cas de modèle d'affaires conservateur, peu complexe et comportant peu de risques.

Enfin, certains participants à l'audition dénoncent le fait que des conditions analogues pour les banques et les assureurs soient parfois réglementées différemment (par ex. effet rétroactif ; cf. également le point 3.8). Ils estiment que les entreprises d'assurance bénéficient parfois d'une réglementation plus souple, ce qui engendre des distorsions de la concurrence et une charge réglementaire accrue pour les banques.

Prises de position des assureurs

L'ASA pense que la réglementation commune proposée par la FINMA pour les banques et les assureurs ne se justifie ni sur le plan technique ni au niveau de la systématique du droit. Contrairement aux banques, l'externalisation de certaines fonctions d'une entreprise d'assurance est soumise à des bases légales spécifiques : art. 4 al. 2 let. j LSA en relation avec l'art. 5 al. 2 LSA, qui prévoit une obligation d'approbation des plans d'exploitation, et art. 47 LSA, qui impose une obligation de renseigner et d'annoncer. En revanche, les banques ne devraient pas soumettre leurs projets d'*outsourcing* à l'approbation préalable de la FINMA. Compte tenu des conditions-cadres légales et du contexte différents, l'ASA est d'avis que les conditions relatives au secteur de l'assurance devraient être fixées dans une circulaire séparée « *Outsourcing* – assureurs ».

ASS, la SDRCA, ZIC et SRZ déplorent que la circulaire se traduise à de nombreux égards par un renforcement des exigences ou par un accroissement de la charge administrative et des coûts, alors que les risques inhérents à une externalisation ne le justifient que partiellement. Ce renforcement ne s'appuie sur aucune raison objective. Par conséquent, les exigences relatives à une externalisation auprès d'une autre société du groupe devraient être plus souples. Cela vaut également pour les relations entre le siège et une succursale. L'approche basée sur des principes devrait être mise en œuvre de manière cohérente.

Prises de position des tiers

De manière générale, la plupart des participants à l'audition saluent la concrétisation des conditions prudentielles des projets d'*outsourcing* et le maintien d'une pratique prudentielle basée sur des principes. De plus, HOM est explicitement favorable à la libéralisation des possibilités d'externalisation pour les entreprises d'assurance. En outre, la majorité des participants se félicitent de l'abandon des exigences relatives à la protection des données et, partant, d'une meilleure orientation clientèle pour éviter les doublons avec le droit correspondant. Par exemple, SCOM se réjouit de la clarification des rapports entre le droit de la surveillance, le droit civil et le droit pénal, qui était nécessaire à ses yeux, car cela contribue à la sécurité juridique.

Plusieurs participants à l'audition soulignent que les nouvelles exigences de l'*outsourcing* doivent présenter une flexibilité accrue pour ne pas entraver les solutions innovantes (par ex. solutions en nuage). Selon la SPA, les petites banques notamment devraient avoir la possibilité d'élaborer elles-mêmes leurs chaînes de création de valeur en faisant appel, par exemple, à des sociétés de fintech.

SIX demande que les prestations essentielles à la place financière qui sont proposées, par exemple, par une infrastructure des marchés financiers en

Suisse soient exclues du champ d'application de la circulaire. En particulier, les pouvoirs étendus d'instruction, de directive et de contrôle prévus par le projet empêchent, dans les faits, l'élaboration et la fourniture de prestations rationalisées et standardisées par un seul prestataire.

Les avis divergent quant à l'harmonisation des exigences posées aux banques et aux assurances au sein d'une même circulaire.

Appréciation

La circulaire révisée précise et harmonise autant que possible les exigences prudentielles relatives aux projets d'*outsourcing* des banques et des entreprises d'assurance. Davantage basée sur des principes, l'approche tient compte des différences entre le secteur bancaire et celui de l'assurance ainsi que de la grande diversité des établissements correspondants. Dans le même temps, la responsabilité individuelle des établissements est mise en avant en cas d'externalisation.

La requête concernant une exception généralisée ou une exemption de certaines exigences pour les infrastructures des marchés financiers qui agissent en tant que prestataires d'*outsourcing* ou qui proposent des prestations à l'ensemble de la place financière n'est pas retenue, car elle créerait une inégalité de traitement vis-à-vis des autres prestataires. De plus, la focalisation accrue sur la situation spécifique à un établissement permet de mieux prendre en considération les organisations centralisées.

Conclusion

L'orientation sur des principes et la responsabilité individuelle des établissements sont encore renforcées.

3.2 Exigences supplémentaires pour les banques d'importance systémique

Prises de position des banques / négociants en valeurs mobilières

Pendant l'audition, UBS, CS, l'ASB, Raiffeisen et l'UBCS ont critiqué de manière parfois virulente les exigences supplémentaires posées aux externalisations des banques d'importance systémique (Cm 3, 6, 15 et 16, 43 à 45 et 48 du projet présenté à l'audition).

L'ASB, qui représente les établissements concernés, souligne d'un point de vue formel que la capacité de liquidation des banques d'importance systémique ne devrait pas être abordée dans une circulaire sur l'*outsourcing*, mais devrait être déterminée dans le plan d'urgence des établissements financiers correspondants.

Appréciation

Les conditions du maintien des fonctions d'importance systémique des banques d'importance systémique en présence d'une menace d'insolvabilité sont énoncées à l'art. 9 al. 2 let. d LB en relation avec les art. 60 ss OB. Les banques ou groupes bancaires d'importance systémique doivent non seulement s'assurer du maintien des fonctions d'importance systémique, mais également veiller à la poursuite des prestations nécessaires à cet effet.

Les banques ou groupes bancaires d'importance systémique obtiennent ces prestations de différentes façons : grâce à des sociétés du groupe ou à des tiers, grâce à des domaines d'activité internes à la banque ou en combinant ces possibilités. Compte tenu de la diversité des modèles de prestations utilisés par les banques d'importance systémique, il est préférable de définir les conditions-cadres spécifiques par banque ou groupe bancaire d'importance systémique plutôt que d'adopter une réglementation générale abstraite dans la circulaire « *Outsourcing* ». Les dispositions concernant les banques d'importance systémique dans le projet de circulaire sont donc supprimées. Nonobstant ce qui précède, les banques d'importance systémique doivent indiquer dans leur plan d'urgence dans quelle mesure l'externalisation des prestations est compatible avec l'objectif de ce plan (maintien des fonctions d'importance systémique) et montrer que cette externalisation n'entrave pas une restructuration ou une liquidation ordonnée en cas d'insolvabilité. Ce faisant, elles doivent tenir compte non seulement de la circulaire « *Outsourcing* », mais également des lois et exigences de surveillance essentielles à l'étranger (art. 61 al. 1 let. g OB) ainsi que des normes internationales correspondantes.

La FINMA renonce donc à transposer de manière abstraite sa pratique dans une circulaire à l'aide d'exigences spécifiques aux externalisations des banques d'importance systémique, notamment car le nombre d'établissements concernés est faible et les questions correspondantes peuvent être résolues au cas par cas dans le cadre de l'approbation des plans d'urgence.

Conclusion

Les dispositions supplémentaires concernant les banques d'importance systémique dans le projet présenté à l'audition (Cm 3, 6, 15 et 16, 43 à 45 et 48) sont purement et simplement supprimées.

La FINMA définira au cas par cas, dans le cadre de la planification d'urgence, les exigences relatives à l'externalisation de prestations par les banques d'importance systémique en tenant compte de l'organisation spécifique de la fourniture des prestations.

3.3 Structure et concepts (Cm 1 à 7)

Prises de position des banques / négociants en valeurs mobilières

L'ASB et UBS suggèrent de préciser que la circulaire n'entend pas réglementer la capacité de liquidation en tant que telle. Celle-ci est déjà régie par l'art. 9 al. 2 let. d LB et il n'existe aucune base légale pour des exigences plus étendues.

Se référant à la définition d'*outsourcing*, certains participants à l'audition exigent que seul le caractère essentiel d'une prestation soit déterminant et que le complément « tout ou partie » soit dès lors supprimé. Par ailleurs, il faudrait ajouter que seules les externalisations au sens de la circulaire sont concernées. En outre, plusieurs participants déplorent que l'expression « activité commerciale » soit trop vaste ; ils souhaitent que seules les prestations présentant un lien (direct) avec une activité soumise à autorisation ou intrinsèque d'une banque soient assujetties à la circulaire.

La SVUE regrette que le rapport explicatif se focalise sur le caractère indépendant au détriment de la durabilité. En revanche, l'UBCS aimerait que l'indépendance soit davantage clarifiée.

De plus, l'UBCS propose d'exposer explicitement, à titre complémentaire et au sens d'un catalogue négatif, les structures qui ne constituent pas un *outsourcing* en vertu de la circulaire en raison de leurs conditions-cadres spécifiques (par ex. sur la base d'un droit contraignant ou en cas d'exceptions ou d'incidents).

Concernant la définition du caractère essentiel des externalisations, la plupart des participants à l'audition critiquent une formulation, selon eux, trop générale des différents types de risque, qui omet également de préciser leur matérialité (par ex. en relation avec l'importance du risque ou du dommage [SVUE et LEO] et les répercussions négatives en cas d'exécution déficiente [UBS]). Cela étendrait le champ d'application de la circulaire, car presque toutes les prestations devraient dès lors être considérées comme essentielles. A cet égard, RAI cite également les sociétés de révision, qui auront probablement tendance à classer davantage de fonctions comme essentielles.

Par ailleurs, selon l'ASB et l'UBCS, l'énumération des prestations essentielles qui est proposée au Cm 5 est trop générale, manque de cohérence et couvre donc de facto toutes les activités d'une banque. Concrètement, les exemples cités – par d'autres participants également comme CS – portent sur les expressions « informatique » et « conservation des données ». Enfin, plusieurs participants à l'audition pointent d'éventuelles incohérences ou contradictions dans la définition des données d'identification du client entre le rapport explicatif et la circulaire. De nombreux participants préconisent de

conserver l'ancienne annexe avec des exemples plutôt que d'intégrer une énumération directement dans la circulaire.

L'UBCS ne comprend pas pourquoi le caractère essentiel devrait être présenté différemment au niveau des banques d'une part et des assurances d'autre part.

Prises de position des assureurs

Sur le plan terminologique, l'ASA recommande de parler de « fonctions » externalisées (comme à l'art. 4 LSA) au lieu de « prestations ». Par conséquent, le terme « prestataire » devrait également être remplacé par « fournisseur ».

La SDRCA suggère d'évaluer le caractère essentiel en tenant compte non seulement de la nature, de la taille et de l'étendue de la prestation dans son ensemble, mais également en relation avec la taille de la fonction complète.

SAN et, par analogie, ASS partent du principe que les prestations qui ne sont pas énumérées expressément dans la circulaire ne relèvent pas de son champ d'application. De plus, ces deux participants à l'audition estiment qu'il existe une incohérence au niveau de la terminologie : la version française de la circulaire utilise l'expression « fonction essentielle », alors que l'art. 4 al. 2 let. j LSA parle de « fonction importante ». SAN et ASS renvoient également à un passage de la page 8 du rapport explicatif, selon lequel un *outsourcing* se voit conférer un caractère essentiel si, dans le cadre d'une externalisation, le prestataire obtient accès aux CID. On ignore si cette définition étendue s'applique aussi aux assureurs.

L'ASA propose de définir le caractère essentiel comme suit : « Pour ce qui est des entreprises d'assurance, sont réputées essentielles toutes les fonctions qui ont un impact essentiel sur les risques liés à l'exploitation d'une entreprise d'assurance. » L'ASA énumère ensuite toute une série de fonctions essentielles, dont la révision interne. En revanche, il serait inapproprié d'intégrer forfaitairement l'informatique dans les prestations essentielles, car les fonctions informatiques sont très vastes et très variées. Au demeurant, l'ASA souhaite une énumération exhaustive des fonctions essentielles afin d'assurer la sécurité juridique. SRZ émet un avis similaire.

Prises de position des tiers

Concernant l'article sur le but, ES propose de le compléter pour prendre en compte la protection des données et des secrets. Selon la SPA et le KAR, cet article devrait notamment indiquer que la circulaire explique et concrétise les exigences prudentielles auxquelles doivent répondre les externalisations.

Plusieurs participants à l'audition suggèrent d'ajouter « au sens de la circulaire » dans la définition de l'*outsourcing* afin de la limiter aux externalisations qui sont pertinentes au niveau prudentiel. HOM suggère de préciser que seuls les transferts à une autre personne morale, mais pas ceux à des succursales (ou, au plus, à des succursales étrangères), sont concernés par la circulaire. Sinon, le champ d'application de cette dernière serait très vaste.

Pour ce qui est du caractère essentiel, l'ASAI conseille de renoncer au rapport entre externalisation et caractère essentiel et de tenir compte à la place de la nature, de la taille et de l'étendue de la prestation par rapport à l'ensemble de la fonction. De plus, certains participants souhaitent préciser le terme « partie » en ce sens que les externalisations partielles relèveraient de la circulaire uniquement si des éléments ou contenus essentiels sont concernés.

En outre, SCOM et l'asut demandent une clarification afin que les prestations qui ne peuvent « théoriquement » pas être fournies par l'établissement (par ex. télécommunications, poste, etc.) soient explicitement exclues du champ d'application de la circulaire. Plusieurs participants exigent également que les critères déterminant le caractère essentiel lors d'une externalisation de CID soient précisés, car la circulaire et le rapport explicatif divergent sur ce point.

Certains participants arguent que les fonctions « informatique » et « conservation des données », notamment, sont définies de manière trop générale dans les exemples cités de prestations essentielles et que des précisions sont indispensables, sous peine que toutes les prestations ayant un lien avec l'informatique ne doivent être considérées comme étant soumises à la circulaire. Par ailleurs, beaucoup réclament le retour de l'ancienne annexe avec des exemples ou refusent sa suppression, principalement pour assurer la sécurité juridique. En particulier, le catalogue négatif devrait absolument être conservé, selon SIX par exemple.

Enfin, ES demande que les déclarations du rapport explicatif sur l'accomplissement des tâches de manière indépendante soient reprises dans la circulaire, y compris la présomption d'indépendance pour les tâches essentielles.

Appréciation

La garantie de la capacité de liquidation est supprimée de l'article sur le but de la circulaire, car la capacité d'assainissement et de liquidation doit être assurée indépendamment d'une externalisation. Cela signifie également que cette dernière ne doit pas mettre en péril ou empêcher la capacité d'assainissement et de liquidation. Ce point est particulièrement important en cas de transfert à l'étranger.

Par ailleurs, la définition des *outsourcings* a été limitée à ceux au sens de la circulaire. De plus, la terminologie de cette dernière a été adaptée de sorte que l'on parle désormais de l'externalisation de fonctions (et non plus de prestations). Il n'y a aucune modification sur le fond. Concernant la requête émise lors de l'audition en vue d'une précision ou d'une suppression de la formulation « … remplir [...] tout ou partie d'une prestation... », on peut retenir que l'externalisation partielle d'une fonction ne saurait être réputée essentielle que si une partie essentielle est transférée.

Le caractère « durable » n'est pas expliqué de manière plus détailléedans le rapport explicatif. Par nature, un *outsourcing* se caractérise par une certaine pertinence temporelle. Des transferts uniquement brefs ou temporaires ne sont dès lors pas réputés durables. Cela correspond à la pratique précédente, sur laquelle on peut s'appuyer en la matière.

Eu égard aux nombreux feed-back reçus lors de l'audition, la définition du caractère essentiel a été remaniée en profondeur et simplifiée. A cet égard, la circulaire repose davantage sur des principes, et la détermination du caractère essentiel des prestations externalisées relève dans une large mesure de la responsabilité des établissements. Ceux-ci doivent en particulier se baser sur les objectifs et les prescriptions des lois sur la surveillance des marchés financiers.

Pour les banques, la pratique précédente est conservée, mais l'on renonce sciemment à énumérer des exemples de fonctions essentielles en raison de la nouvelle approche. Par rapport au rapport explicatif, il convient de préciser la présomption du caractère essentiel en relation avec les grandes quantités de CID[1] : si, dans le cadre d'une externalisation, un prestataire obtient un accès à de grandes quantités de CID (et pas uniquement à quelques-uns), cet *outsourcing* se voit conférer un caractère essentiel.

Pour les assurances, le concept de « grandes quantités de CID » n'est pas utilisé de la même façon et n'a pas la même signification en raison du modèle d'affaires différent. Dans le secteur de l'assurance, pour évaluer le caractère essentiel des données des assurés, il convient d'examiner dans quelle mesure les intérêts de ces derniers sont affectés.

En l'espèce, cela implique le maintien de la pratique précédente, tout en considérant désormais la gestion du risque et la *compliance* comme des fonctions essentielles à l'aune de l'art. 96 al. 4 OS : sont réputées essentielles en vertu de l'art. 4 al. 2 let. j LSA toutes les prestations de services qui sont indissociablement liées à l'exploitation d'une entreprise d'assurance, telles que la production (développement des produits, distribution, souscrip-

[1] Le concept de « grandes quantités de CID » est défini au Cm 53 de l'annexe 3 de la Circ.-FINMA 08/21 « Risques opérationnels – banques » comme étant la « quantité de CID qui, rapportée au nombre total des comptes/à la taille totale du portefeuille de particuliers, est significative ».

tion), la gestion du portefeuille (gestion des polices), le règlement des sinistres (traitement des prestations), la comptabilité (comptabilité financière et *controlling* financier), le placement et la gestion de fortune ainsi que l'informatique (traitement de l'information et des données).

Conclusion

Dans la circulaire, le caractère essentiel est davantage basé sur des principes. Sa concrétisation est spécifique à un établissement et devrait dès lors incomber à ce dernier. Les établissements assument donc une responsabilité accrue dans l'évaluation du caractère essentiel. Toute autre précision découle de la pratique relative à la surveillance des banques et des assurances.

On parle désormais de « fonctions » (externalisées) et non plus de « prestations ». Il n'y a aucune modification sur le fond.

3.4 Champ d'application (Cm 8 à10)

Prises de position des banques / négociants en valeurs mobilières

Concernant le champ d'application, plusieurs participants à l'audition ont demandé de préciser que les succursales étrangères des banques et négociants en valeurs mobilières ayant leur siège en Suisse ne sont pas soumises à la circulaire. UBS souligne que ces succursales sont assujetties aux exigences du droit local correspondant.

En revanche, l'ASB souhaite d'autres clarifications relatives au champ d'application en général et, en particulier, à l'applicabilité aux sociétés du groupe tenues de consolider[2] ainsi qu'aux succursales suisses des établissements étrangers. Si ces dernières procédaient à une externalisation, la circulaire s'appliquerait uniquement lorsqu'une autre entité juridique fournit la prestation, mais pas lorsque celle-ci est réalisée au sein de la même entité juridique.

La plupart des participants à l'audition critiquent l'abandon des allégements en cas d'externalisations intragroupe ou la suppression des privilèges d'un groupe dans le projet présenté à l'audition. L'ASB et l'UBCS estiment que cette réglementation méconnaît la réalité d'un groupe, au sein duquel certaines prestations sont généralement fournies à l'ensemble du groupe par des entités spécifiques à ce dernier. De plus, il faut expressément autoriser des droits de contrôle provisoires en relation avec la création de sociétés communes[3] en qualité de prestataires d'*outsourcing* (par analogie à la circu-

[2] L'ASB propose donc à cet égard de modifier le tableau des destinataires.

[3] Groupe au sens de l'art. 3*c* LB.

laire de la FINMA 2008/7 « Outsourcing – banques », Cm 9). Sinon, des entreprises communes faisant office de prestataires d'*outsourcing* (SIX-SIS par ex.) seraient privées de secteurs d'activité essentiels et leur existence serait menacée.

CS mentionne lui aussi la disproportion de la suppression, car l'on ne tient ainsi pas compte de la situation concrète au sein des groupes concernés. Il demande donc que les allégements suivants soient prévus : analyse du risque avant la conclusion du contrat (Cm 23), examen des capacités professionnelles et des ressources (Cm 24), prise en compte des coûts de transition et de changement (Cm 25), approbation préalable requise en cas de recours à des sous-traitants (Cm 40).

Prises de position des assureurs

SAN et VIS souhaitent que les petites et moyennes entreprises d'assurance des catégories de surveillance 5, 4 et 3 ainsi que les entreprises qui ont externalisé toute l'exécution des affaires d'assurance auprès d'une société de prestations interne au groupe soient exclues du champ d'application de la circulaire. De même, contrairement à d'autres branches relevant des assurances privées (responsabilité civile et choses), les assureurs complémentaires maladie ne devraient pas être assujettis à la circulaire. Par ailleurs, le champ d'application de cette dernière ne devrait pas englober les intermédiaires d'assurance, car ceux-ci ne sont pas mandatés directement par les assureurs, mais jouissent d'une relation contractuelle avec le preneur d'assurance éventuel.

Par analogie, la SDRCA souhaite que l'application de la circulaire soit fortement réduite si une succursale suisse externalise des fonctions auprès du siège à l'étranger et inversement. Au demeurant, ces externalisations ne devraient pas être considérées comme de l'*outsourcing*. En outre, des simplifications devraient être possibles en cas d'externalisation auprès d'une filiale à 100 % de l'entreprise d'assurance. Par analogie à la Circ.-FINMA 08/7 en vigueur, SRZ entend préciser que les externalisations effectuées par les succursales étrangères d'une entreprise d'assurance ayant son siège en Suisse relèvent des dispositions du droit local.

Amlin demande que les exigences de cette circulaire ne s'appliquent pas aux *outsourcings* intragroupe réalisés en Suisse et dans l'Union européenne (UE) par des (ré)assureurs.*Prises de position des tiers*

D'après SIX, la suppression des privilèges accordés aux groupes ne devrait pas compliquer davantage, sans nécessité apparente, le recours éprouvé à des sociétés du groupe centralisées en qualité de prestataires (par ex. risques, informatique, etc.), d'autant que dans le cas de SIX, celles-ci sont également assujetties à la surveillance consolidée de la FINMA.

Concernant le champ d'application, certains participants critiquent le fait que toutes les règles de l'*outsourcing* externe s'appliquent aux transferts internes ou demandent d'y renoncer. Certains allégements devraient au moins être conservés.

Appréciation

Les groupes et les conglomérats sont supprimés du champ d'application de la circulaire. En tant qu'entités économiques, ils ne sont pas partie prenante dans un contrat d'externalisation. Il convient cependant de tenir compte à l'échelle du groupe des risques liés à une externalisation en termes de consolidation ; il est renvoyé à cet effet aux exigences légales de la surveillance des groupes et des conglomérats (cf. art. 64 ss et art. 72 ss LSA et art. 191 OS ou art. 3*f* al. 2 LB).

La critique selon laquelle les externalisations des succursales suisses ne constitueraient pas un *outsourcing* sur le plan juridique ne saurait être recevable. En l'espèce, l'interprétation prudentielle prime celle du Code des obligations : ces succursales sont soumises à la surveillance de la FINMA et cette dernière doit pouvoir vérifier si la fourniture des prestations est conforme au droit de la surveillance. Les externalisations d'une entreprise suisse auprès de sa filiale ou succursale étrangère relèvent également du champ d'application de la circulaire. Il est en effet important de savoir, en termes de sous-traitance, si une fonction essentielle est de nouveau externalisée par l'intermédiaire de cette filiale ou succursale étrangère.

En revanche, l'externalisation (primaire) de fonctions essentielles par une filiale ou succursale étrangère d'un établissement ayant son siège en Suisse n'est pas soumise au champ d'application de la circulaire, car son contrôle incombe à l'autorité de surveillance étrangère compétente.

De nombreux participants ont critiqué la suppression des privilèges accordés aux groupes dans la version présentée à l'audition. Ils ont été entendus en ce sens qu'un nouveau chiffre marginal basé sur des principes a été introduit. Il précise que la situation du groupe doit être prise en compte (cf. ch. 3.6.2). Ce chiffre marginal peut également s'appliquer aux organisations centralisées et aux entreprises communes en vertu du Cm 9 de la Circ.-FINMA 08/7.

En termes de risques, on ne saurait exclure toute une catégorie d'entreprises d'assurance (par ex. assureurs complémentaires maladie selon la LSA) du champ d'application de la circulaire. De plus, la base légale énoncée à l'art. 4 al. 2 let. j LSA prévoit que cette disposition s'applique à *toutes* les entreprises d'assurance, ce qui va à l'encontre d'une réglementation d'exception. Ces bases doivent donc également s'appliquer lorsqu'une entreprise d'assurance transfère des fonctions essentielles à des intermédiaires.

Les allégements préconisés par plusieurs participants à l'audition en cas d'externalisations intragroupe ou entre une succursale et son siège sont pris en considération dans la reformulation du Cm 22. D'autres allégements ne sont pas judicieux. Dans la surveillance des assurances, cela correspond au demeurant à la pratique antérieure.

Conclusion

Les groupes financiers et les conglomérats financiers sont supprimés du champ d'application de la circulaire. Les exigences relatives à la prise en compte des risques à l'échelle du groupe, y compris ceux découlant d'*outsourcings*, résultent des prescriptions existantes sur la surveillance des groupes et des conglomérats. Conformément à la pratique précédente, les externalisations des succursales suisses continuent de relever du champ d'application de cette circulaire.

Les succursales et filiales étrangères d'établissements ayant leur siège en Suisse ne sont pas assujetties à la circulaire, mais au droit local respectif.

3.5 Admissibilité (Cm 11 à 20)

3.5.1 Dispositions communes (Cm 11 à 14)

Prises de position des banques / négociants en valeurs mobilières

Plusieurs participants critiquent la formulation du Cm 12 de la version présentée à l'audition, selon laquelle les fonctions qui englobent la prise de décisions stratégiques ne peuvent pas être externalisées. Par exemple, RAI estime que cette formulation est vague. De plus, CS considère que la prise de décisions stratégiques ressort déjà du terme « haute direction ». L'ASB et UBS pensent par ailleurs qu'il faudrait revoir l'interdiction d'externaliser les décisions relatives à l'acceptation et à la rupture de relations d'affaires, car cela pourrait constituer un obstacle en cas d'automatisation[4].

Des participants à l'audition déplorent les exigences concernant l'externalisation de la gestion du risque et de la *compliance*. CS et UBS demandent que les tâches opérationnelles soient entièrement externalisables pour les banques de toutes les catégories de surveillance. En outre, l'expression « tâches purement opérationnelles » devrait être précisée. Par principe, RAI, l'ASB et HSBC rejettent toute restriction en cas d'externalisation intragroupe. L'UBCS souhaite également que le Cm 14 de la version présentée à l'audition soit étendu aux établissements de la catégorie de surveillance 3.

[4] En l'espèce, elles citent l'exemple d'un logiciel tiers qui décide automatiquement de l'acceptation d'une relation d'affaires.

Prises de position des assureurs

L'ASA et ASS saluent la nouvelle possibilité d'externaliser toutes les fonctions essentielles, car cela équivaut à une libéralisation de la pratique en vigueur dans le secteur de l'assurance, qui permettait au plus le transfert de deux fonctions essentielles sur trois. L'ASA estime cependant que les restrictions sont encore trop élevées.

Plusieurs participants à l'audition demandent la suppression complète du Cm 13, voire du Cm 14 également. Ils soulignent que la révision interne peut être externalisée en vertu de la Circulaire FINMA 2017/2 « Gouvernance d'entreprise – assureurs ». Les trois fonctions de contrôle que sont la révision interne, la gestion du risque et la *compliance* devraient être traitées de la même manière. L'externalisation totale de la gestion du risque et de la *compliance* auprès d'une autre entité au sein du même groupe d'assurance devrait également être possible. Même la directive Solvabilité II prévoit des exigences plus souples pour un transfert à une autre société du groupe par rapport à une externalisation complète auprès d'un tiers, notamment car l'entreprise a les moyens d'exercer ses droits d'examen et de contrôle, ce qui réduit les risques correspondants. Par analogie à la réglementation de Solvabilité II, SRZ suggère d'envisager la nomination d'un « responsable de fonction » par l'entreprise pour chaque fonction de contrôle afin de garantir une évaluation et une gestion appropriées des risques pertinents du point de vue de l'entreprise.

VIS se demande quelles tâches de conduite de la direction seraient considérées comme « centrales » et ce que l'on entend par « fonctions qui englobent la prise de décisions stratégiques ». SAN propose de préciser l'expression « relations d'affaires », tandis que l'ASA et, par analogie, ASS souhaitent supprimer le passage correspondant.

Prises de position des tiers

En référence à Solvabilité II, l'ASAI demande qu'une fonction puisse être externalisée dans son ensemble. De même, des transferts complets à des sociétés du groupe devraient être possibles. La SPA et KARTAC souhaitent que les entreprises de toutes les catégories de surveillance puissent externaliser entièrement les tâches opérationnelles de *compliance*.

Appréciation

La FINMA prend acte des critiques formulées par la plupart des participants à l'audition sur l'externalisation de la gestion du risque et de la *compliance*. La nouvelle formulation des conditions au Cm 9 repose davantage sur des principes, tout en tenant compte du principe de proportionnalité : en tant qu'instances de contrôle indépendantes, le contrôle des risques et la fonction de *compliance* des entreprises des catégories de surveillance 1 à 3 ne

peuvent pas être externalisés. Les fonctions correspondantes doivent demeurer dans l'entreprise et être organisées de manière à pouvoir piloter et surveiller le domaine externalisé, les exigences concrètes découlant, pour les assurances, de l'art. 96 al. 4 OS et, pour les banques, de la Circulaire FINMA 2017/1 « Gouvernance d'entreprise – banques ». Par ailleurs, les entreprises des catégories de surveillance 4 et 5 peuvent se contenter de nommer à la direction un responsable qui veillera à l'évaluation et à la gestion appropriées des risques pertinents des fonctions externalisées du point de vue de l'entreprise. Les établissements de toutes les catégories de surveillance peuvent externaliser les tâches opérationnelles de gestion du risque et de *compliance*.

S'il existe une gestion du risque ou une *compliance* au niveau du groupe, les entités juridiques peuvent exploiter les synergies correspondantes. Cependant, il incombe au conseil d'administration et à la direction de l'entité juridique respective de veiller à un contrôle adéquat des risques au niveau de cette entité juridique et à la prise en compte des risques du sujet de droit dans la gestion du risque et la *compliance* locales.

Conclusion

Les conditions d'externalisation de la gestion du risque et de la *compliance* ou des instances de contrôle correspondantes (contrôle des risques et fonction de *compliance*) sont davantage basées sur des principes.

Le Cm 14 de la version présentée à l'audition est supprimé.

3.5.2 Banques (Cm 15 et 16)

Les exigences supplémentaires pour les banques d'importance systémique ont été supprimées (cf. ch. 3.2 ci-dessus à ce sujet).

3.5.3 Entreprises d'assurance (Cm 17 à 20)

Prises de position des banques / négociants en valeurs mobilières

L'UBCS ne comprend pas pourquoi des règles différentes s'appliquent aux banques et aux assurances. Par exemple, le Cm 12 réglemente pour les banques l'exigence fondamentale d'un droit des sociétés et de la surveillance fonctionnel ainsi que d'une gouvernance d'entreprise conforme aux normes internationales. Il n'existe aucune raison manifeste de ne pas appliquer cette règle aux assurances.

Prises de position des assureurs

L'ASA et SRZ proposent de modifier le Cm 17 de la version présentée à l'audition afin que l'externalisation des fonctions de contrôle ne soit pas uniquement possible de manière restreinte.

L'ASA souhaite ajouter au Cm 19 « indépendamment des branches d'assurance pour lesquelles les captives bénéficient d'un agrément ».

Prises de position des tiers

D'après LAUX, l'externalisation partielle de prestations (par ex. certains aspects de l'« informatique ») serait soumise à autorisation pour les assurances. LAUX estime que cela constituerait un changement de pratique et serait contraire à l'art. 4 al. 2 let. j LSA, selon lequel seul un transfert de l'informatique en tant que fonction complète (au sens d'une « scission ») requiert une autorisation.

Appréciation

On peut opposer à la critique de l'UBCS sur l'égalité de traitement que les dispositions du Cm 12 de la version présentée à l'audition s'appliquent tant aux banques qu'aux assurances. Les autres dispositions des nouveaux Cm 10 à 13 portent sur des questions spécifiques aux entreprises d'assurance.

Concernant la proposition de l'ASA et de SRZ (l'externalisation des fonctions de contrôle ne devrait pas être uniquement restreinte), il est renvoyé au ch. 3.5.1.

Pour ce qui est du complément suggéré par l'ASA au Cm 19 de la version présentée à l'audition, il convient de préciser que les captives d'assurance directe sont soumises en tant que telles à cette disposition, comme l'indique déjà expressément la formulation de cette dernière.

Conclusion

Les conditions relatives à l'admissibilité des externalisations pour les entreprises d'assurance sont conservées.

3.6 Exigences pour les entreprises externalisatrices (Cm 21 à 45)

3.6.1 Inventaire des prestations de services externalisées (Cm 21 et 22)

Prises de position des banques / négociants en valeurs mobilières

RAI et l'UBCS estiment de manière générale que les exigences relatives à l'inventaire vont trop loin. Ce dernier devrait se limiter aux principaux aspects (fournisseurs et contrat) ainsi qu'aux prestations externalisées ou les établissements devraient uniquement veiller à documenter de manière adéquate les prestations externalisées. De plus, l'ASB et l'AFBS demandent que le formulaire de saisie J du plan d'exploitation soit identique pour les assurances afin que celles-ci et les banques soient soumises aux mêmes exigences.

Plusieurs participants à l'audition soulignent que le terme « auxiliaires » est inapproprié et disproportionné, car il englobe également les collaborateurs du prestataire, par exemple. Mieux vaudrait parler de « sous-traitants ».

Par ailleurs, CS souhaite une uniformisation ou, du moins, une précision des termes « prestataire » et « fournisseur » ainsi que, de manière générale, une adaptation à la terminologie de l'art. 61 al. 1 let. f. OB. HSBC et l'UBCS aimeraient que l'expression « organe responsable au sein de l'entreprise » soit précisée. On pourrait en effet penser qu'il doive toujours s'agir du même organe ou d'un organe central, ce qui ne serait pas opportun.

Prises de position des assureurs

Plusieurs participants à l'audition souhaitent que l'inventaire se limite aux prestations *essentielles* externalisées, car le recensement de toutes les prestations serait disproportionné. De plus, l'utilisation du terme « auxiliaire » est critiquée.

L'ASA et ASS aimeraient par ailleurs que le Cm 22 de la version présentée à l'audition soit supprimé, car il est disproportionné, selon elles, de considérer la moindre modification de l'inventaire comme un changement du plan d'exploitation.

Prises de position des tiers

Concernant l'inventaire, l'ASAI pense que les exigences devraient également s'appliquer aux externalisations non essentielles, car c'est la seule façon de garantir un pilotage par la direction et une surveillance par le conseil d'administration. Cette thématique est néanmoins déjà abordée au Cm 27.

En revanche, ES et Arizon demandent que l'inventaire se limite aux prestations essentielles. La SPA et KARTAC aimeraient en outre une formulation plus ouverte qui permettrait de recourir à d'autres instruments comparables (par ex. base de données des contrats).

Plusieurs participants critiquent l'utilisation du terme « auxiliaire ». De plus, il est suggéré que seuls figurent dans l'inventaire les tiers auprès desquels une prestation (partielle) essentielle a été externalisée, mais pas ceux qui fournissent des prestations interchangeables[5] ou non essentielles (LAUX). SICT et Arizon[6] soulignent que le critère de l'indépendance[7] ou l'octroi d'une certaine marge de négociation sont décisifs dans les relations avec des sous-traitants.

Appréciation

La FINMA prend acte de la critique concernant le terme « auxiliaire », qui est remplacé par « sous-traitant ». Il faut déterminer si la contribution des sous-traitants doit être qualifiée d'essentielle au sens de la circulaire en vue de leur inclusion éventuelle dans l'inventaire. Etant donné que des activités répétitives ou interchangeables peuvent être essentielles, ces critères ne sont en l'espèce pas déterminants en soi.

Concernant l'inventaire, les exigences se limitent à la description de la fonction externalisée, au fournisseur (y compris les sous-traitants), au bénéficiaire et à l'unité responsable au sein de l'entreprise. Elles semblent être suffisamment basées sur des principes et offrent une marge de manœuvre suffisante lors de l'application. Pour les assurances, le formulaire de saisie J du plan d'exploitation sera adapté en vertu de ces conditions.

L'inventaire doit comprendre les externalisations considérées comme essentielles au sens de cette circulaire. En raison des principes généraux de la documentation, il va cependant de soi que les assujettis documenteront également à leur niveau les externalisations qui ne sont pas essentielles au regard de la circulaire.

Pour ce qui est du Cm 22 de la version présentée à l'audition, il convient de préciser que l'inventaire fait partie intégrante du formulaire de saisie J du plan d'exploitation et constitue une annexe sans surbrillance. Cette présentation dudit formulaire J indique clairement que l'inventaire et ses modifications ne sont pas en soi soumis à l'obligation d'annonce et d'approbation. Cette dernière concerne davantage les éléments désignés expressément comme tels dans le formulaire J (surlignage bleu foncé).

---

[5] Par exemple : fournisseurs de matières premières (prestations standardisées et automatisées).

[6] Arizon estime également que la mention du terme « auxiliaire » est partiellement en contradiction avec le Cm 4 (indépendance) de la version présentée à l'audition.

[7] SICT cite notamment les prestations de logistique ou de maintenance informatique parmi les externalisations dépendantes.

Conclusion

L'inventaire des fonctions externalisées comprend les externalisations essentielles au sens de cette circulaire. Les sous-traitants qui fournissent des fonctions essentielles doivent également y figurer.

Au demeurant, la version de la circulaire présentée à l'audition est conservée.

3.6.2 Choix, instruction et contrôle du prestataire (Cm 23 à 28)

Prises de position des banques / négociants en valeurs mobilières

CS, l'ASB et UBS exigent une adaptation ou une explication des exigences précises régissant l'apport d'une prestation de services préalablement à la conclusion du contrat. Il faut indiquer clairement que seule une charge proportionnée est requise pour la documentation et que la formulation, qui a été complétée par rapport à la Circ.-FINMA 08/7, n'implique aucune nouvelle norme ni aucune exigence fondamentalement plus étendue. En outre, les réflexions économiques ne sont pas pertinentes en droit de la surveillance.

Pour ce qui est des obligations de documentation, la plupart des participants à l'audition sont tout aussi critiques vis-à-vis de la formulation sur le choix du prestataire. Par exemple, la SVUE estime qu'une remarque plus brève et plus générale sur la sélection professionnelle répondrait davantage aux objectifs.

En particulier, de nombreux participants à l'audition déplorent également la mention des risques de concentration. Selon Arizon notamment, des prestations provenant d'un seul fournisseur sont plus sûres et plus solides, car les processus correspondants sont souvent interdépendants. D'après l'ASB, les risques de concentration ne constituent pas en soi un inconvénient, car ils peuvent contribuer, entre autres, à réduire les coûts et la complexité. En outre, plusieurs participants soulignent que la gestion des risques de concentration au sein d'un groupe est déjà abordée à l'art. 2bis al. 1 let. b LB et dans les plans d'urgence et que les exigences devraient dès lors s'appliquer – si nécessaire – aux seuls transferts externes. UBS considère que des économies d'échelle doivent encore pouvoir être réalisées grâce à une consolidation des prestataires. Enfin, l'UBCS est d'avis que cette exigence ne saurait se traduire par un risque de concentration illicite qui découlerait d'externalisations des banques d'importance systémique auprès du même prestataire (par ex. ServCo).

En outre, les participants à l'audition déplorent en majorité que l'accent soit mis sur les coûts de transition et de changement. Pour l'ASB et UBS, il s'agit d'aspects ou de critères économiques qui ne sont pas pertinents en droit de la surveillance et qui n'ont aucun intérêt public en termes de réglementation.

Selon CS, l'UBCS et RAI, un prestataire ne peut pas garantir, au sens de la LB, qu'il pourra offrir durablement la prestation de services. L'expression doit donc être supprimée ou modifiée. Par ailleurs, il convient de préciser dans quelle mesure les exigences vont au-delà d'une analyse générale des risques. Enfin, l'ASB et l'UBCS, notamment, estiment que la phrase « la réintégration ordonnée de la prestation de services externalisée doit être garantie » ne peut pas être mise en pratique.

D'après l'ASB et UBS, il en va de même pour le droit de donner des instructions. Il serait plus judicieux que les prestataires doivent contribuer aux adaptations contractuelles nécessaires au respect des prescriptions réglementaires.

Prises de position des assureurs

L'ASA, la SDRCA et SRZ souhaitent que le Cm 23 soit précisé en ce sens qu'il faille réaliser une *évaluation conforme à l'importance de l'externalisation*. En outre, cette évaluation intégrerait uniquement des réflexions économiques et opérationnelles *essentielles* ainsi que les risques et les opportunités qui leur sont liés. En revanche, SAN et ASS demandent que ce chiffre marginal soit supprimé.

SRZ exige que le Cm 24 de la version présentée à l'audition ne s'applique pas aux externalisations intragroupe. Compte tenu des compétences requises et des coûts, il est opportun dans un groupe de mettre certaines tâches ou fonctions (par ex. informatique, sécurité de l'information) à la disposition de toutes les sociétés du groupe de manière centralisée. SRZ renvoie également à la directive Solvabilité II, qui reconnaît que les exigences relatives au choix d'un prestataire interne au groupe sont généralement moins élevées.

L'ASA propose plusieurs modifications du Cm 25. Lors de la décision statuant sur l'*outsourcing* et du choix du prestataire, « *tous les coûts allant de la transition à une éventuelle réintégration* » doivent être pris en compte. Il convient de supprimer la disposition selon laquelle le prestataire doit garantir qu'il pourra offrir durablement la prestation de services. Quant à la dernière phrase, elle devrait être complétée par « *ou le transfert à un tiers* ». La SDRCA souhaite des adaptations similaires.

L'ASA, la SDRCA et SRZ suggèrent que le Cm 27 soit, dans l'ensemble, davantage axé sur les risques, et proposent la formulation « conformément aux risques liés à l'externalisation ». SAN et VIS considèrent que cette disposition n'est pas nécessaire tant que le prestataire interne au groupe est soumis à la même haute surveillance et à la même direction opérationnelle que l'entreprise d'assurance concernée. ASS souligne que les *risques* liés à l'*outsourcing* doivent faire l'objet de la surveillance, et non les prestations.

Certains participants à l'audition conseillent de supprimer le Cm 28 ou de l'intégrer au Cm 26.

Prises de position des tiers

Concernant la documentation en général et l'analyse du risque en particulier, l'ASAI préconise une approche basée sur les risques qui tienne compte du risque de l'externalisation spécifique. Des allégements devraient être prévus pour les externalisations intragroupe (conformément à Solvabilité II) ou pour les transferts internes en Suisse.

Selon SIX, la formulation relative à l'analyse du risque doit être adaptée ; en revanche, les réflexions économiques et opérationnelles ne devraient pas figurer dans des exigences prudentielles.

Plusieurs prises de position critiquent le fait que les risques de concentration doivent être pris en compte dans le choix du prestataire. De manière générale, l'expression devrait être clarifiée et précisée. Une externalisation de processus partiels ou de systèmes informatiques auprès de plusieurs prestataires (pour tenter de respecter les exigences) pourrait se traduire par une fragmentation qui augmenterait les risques d'interface et, de manière générale, les risques opérationnels.

Pour ce qui est de l'exigence d'une réintégration ordonnée d'une prestation externalisée, l'ASAI et Arizon demandent que la possibilité d'un transfert à un autre fournisseur soit également une option suffisante. A cet égard, certains participants à l'audition déplorent la prise en compte des coûts de transition et de changement en arguant que ces aspects purement économiques ne sont pas pertinents du point de vue prudentiel.

Concernant l'extension du système de contrôle interne à la prestation externalisée, SCOM demande que la situation financière du fournisseur soit surveillée et évaluée régulièrement, en plus des prestations. L'ASAI suggère que les risques essentiels liés à l'externalisation soient identifiés quelles que soient leurs catégories ou classifications (selon le concept-cadre de la gestion du risque). En revanche, la SPA et KARTAC estiment que les exigences relatives à la surveillance et au contrôle des risques sont très élevées et qu'elles pourraient annihiler les avantages d'un *outsourcing*.

Appréciation

La critique des participants à l'audition a été entendue en ce sens que le nouveau Cm 22 permet de tenir compte de la situation du groupe pour les transferts internes. Concernant les exigences désormais énoncées aux Cm 16 à 21 (et 32 à 35 ; cf. ch. 3.6.8), l'ancrage au sein d'un groupe peut être considéré dans la mesure où il est prouvé que les risques habituellement liés à une externalisation n'existent pas dans le contexte du groupe ou

que certaines exigences ne sont pas pertinentes ou sont réglementées autrement.

Dès lors, dans ce contexte, on peut par exemple tenir compte du fait que la procédure de sélection d'un prestataire interne ne doive pas être aussi complète que pour un prestataire externe, en particulier lorsque la qualité de service du prestataire interne est connue. En outre, une participation majoritaire permet, en général, d'exercer dans les faits une plus forte influence sur le prestataire que sur une entreprise extérieure.

Le Cm 16 (Cm 23 de la version présentée à l'audition) est précisé en ce sens que les réflexions économiques et opérationnelles essentielles doivent être prises en compte dans l'analyse du risque.

L'exigence selon laquelle les risques de concentration doivent être considérés lors du choix d'un prestataire est conservée. Elle n'implique en soi aucune restriction lors de la sélection, mais permet d'intégrer les risques éventuels dans l'évaluation.

Une précision est apportée au Cm 18 (Cm 25 de la version présentée à l'audition), l'accent étant mis sur les possibilités et les conséquences d'un changement de prestataire et non, comme dans la version précédente, sur les coûts qui y sont liés. Au Cm 20 (Cm 27 de la version présentée à l'audition), le terme « immédiatement » est remplacé par « rapidement ». Le temps de réaction peut ainsi être défini de manière appropriée en fonction du risque.

Il a été souligné lors de l'audition que l'utilisation du terme « garantie » n'était pas opportune en relation avec des externalisations. Il convient de préciser à cet égard que le prestataire et l'entreprise assujettie doivent tous deux offrir la garantie d'une fourniture de prestations irréprochable. Dans le domaine de l'assurance, cela figure au demeurant à l'art. 14 al. 3 LSA.

Conclusion

Concernant les exigences énoncées aux Cm 16 à 21 et 32 à 35, l'ancrage au sein d'un groupe peut être considéré dans la mesure où il est prouvé que les risques habituellement liés à une externalisation n'existent pas ou que certaines exigences ne sont pas pertinentes ou sont réglementées autrement.

Par ailleurs, certaines formulations des Cm 16 à 21 ont été légèrement adaptées ou sont davantage axées sur les risques, conformément aux feedback des participants à l'audition.

3.6.3 Responsabilité (Cm 29)

Prises de position des banques / négociants en valeurs mobilières

L'UBCS estime que la seconde phrase du Cm 29 de la version présentée à l'audition n'apporte aucune valeur ajoutée et peut dès lors être supprimée.

Prises de position des assureurs

L'ASA souhaite la suppression de la dernière phrase du Cm 29.

Prises de position des tiers

Selon l'ASAI, la prescription sur la responsabilité devrait se limiter au choix diligent, à l'instruction et à la surveillance de la prestation.

Appréciation

L'externalisation n'exonère pas l'entreprise de sa propre responsabilité concernant la direction du domaine externalisé, raison pour laquelle le Cm 23 (Cm 29 de la version présentée à l'audition) est conservé.

Conclusion

La seconde phrase du Cm 23 est conservée.

3.6.4 Sécurité (Cm 30 et 31)

Prises de position des banques / négociants en valeurs mobilières

Se référant aux externalisations déterminantes pour la sécurité qui sont mentionnées au Cm 30, l'UBCS demande que la qualité des exigences en matière de sécurité soit précisée. De même, HSBC souhaite que des définitions clarifient ces points.

Certains participants à l'audition considèrent que les prescriptions sur le dispositif de sécurité vont trop loin. Ils soulignent en particulier l'impossibilité de couvrir tous les cas d'urgence prévisibles. Selon l'ASB et UBS, la formulation suggère en outre une certaine proximité avec le plan d'urgence des banques d'importance systémique en vertu de l'art. 9 al. 2 let. d LB.

Enfin, LEO demande que les Cm 30 et 31 de la version présentée à l'audition soient permutés. Le premier s'applique uniquement aux prestations d'importance systémique, alors que le dernier vaut par analogie pour toutes les banques et tous les négociants en valeurs mobilières.

Prises de position des assureurs

L'ASA souhaite compléter le Cm 30 afin que les exigences en matière de sécurité puissent s'appuyer sur des normes reconnues. L'entreprise doit contrôler le respect de ces exigences. La SDRCA suggère toutefois qu'un contrôle centralisé effectué, par exemple, par une fonction à l'échelle du groupe suffise ; il ne devrait dès lors pas impérativement être exécuté par l'entreprise d'assurance proprement dite.

Concernant le Cm 31, l'ASA propose une formulation selon laquelle l'entreprise d'assurance et le prestataire définissent des normes minimales de continuité des affaires pour les externalisations ayant une incidence sur les clients.

Prises de position des tiers

L'ASAI pense que des contrôles au sein du groupe devraient pouvoir être réalisés par un organe central (en référence au Cm 30). Pour ES, il n'est pas clair ce que l'on entend exactement par externalisations déterminantes pour la sécurité.

Plusieurs participants à l'audition demandent que les exigences concernant le dispositif de sécurité s'appuient davantage sur la gestion de la continuité des affaires (*Business Continuity Management* BCM) et sur celle des niveaux de service (*Service Level Management*). Pour KARTAC et la SPA, le dispositif de sécurité élaboré conjointement par l'entreprise externalisatrice et le prestataire va trop loin, car il requiert notamment une obligation de diligence plus élevée qu'en l'absence d'*outsourcing*.

Appréciation

En cas d'externalisations déterminantes pour la sécurité, les exigences en matière de sécurité doivent être mises en œuvre concrètement en fonction de l'établissement, de l'activité externalisée, des risques spécifiques ainsi que des systèmes ou technologies utilisés. Elles doivent être adéquates (c'est-à-dire *state of the art*), ce qui nécessite une évaluation au cas par cas. Dans ce contexte et en vertu du principe de neutralité technologique, la FINMA renonce sciemment à définir des normes spécifiques.

Les exigences relatives au dispositif de sécurité (nouveau Cm 25) sont adaptées de sorte que celui-ci permette en cas d'urgence (et non pas, comme dans la version présentée à l'audition, *dans tous les cas d'urgence prévisibles*) la continuité de la fonction externalisée. Les établissements définissent eux-mêmes la taille et la couverture du dispositif de sécurité dans le cadre de leur analyse du risque. A cet égard, il faut prendre en compte les

exigences minimales en matière de BCM selon l'autorégulation de l'ASA ou de l'ASB[8].

Conclusion

Aucune norme spécifique n'est définie à dessein pour les exigences en matière de sécurité. La définition et la mise en œuvre de ces dernières doivent intervenir en fonction de l'établissement et des risques liés à l'externalisation.

Les exigences portant sur le dispositif de sécurité ont été légèrement remaniées.

3.6.5 Secret des affaires et secret professionnel, protection des données

Prises de position des banques / négociants en valeurs mobilières

La plupart des participants à l'audition saluent la distinction opérée entre les exigences prudentielles de la FINMA et les dispositions du droit de la protection des données, ou peuvent au moins la comprendre. L'ASB et l'UBCS craignent que cette distinction n'implique un rôle plus important du préposé fédéral à la protection des données et à la transparence (PFPDT) pour les aspects des externalisations qui touchent au droit de la protection des données. Il est donc primordial d'établir une coordination entre la FINMA et le PFPDT pour éviter toute norme divergente, en particulier en matière de secret bancaire et de protection des données[9]. Par conséquent, les dispositions en vigueur sur le secret bancaire dans la Circ.-FINMA 08/7 (Cm 37 à 39) devraient être reprises dans la circulaire révisée, principalement pour assurer la sécurité juridique. Enfin, le principe 5 « Secret des affaires et secret professionnel, protection des données » devrait figurer intégralement dans la nouvelle circulaire, car il traduit clairement les attentes de la FINMA. La révision en cours de la LPD ne justifie pas la suppression de ce principe.

HSBC propose, par exemple, de reprendre les Cm 37 à 39 de la Circ.-FINMA 08/7. Cela permettrait à la FINMA de définir les exigences techniques pour la sécurité des données dans les banques.

Prises de position des assureurs

Aucune.

[8] Cf. les chiffres des recommandations de l'ASA et de l'ASB en matière de BCM qui sont considérés comme standards minimaux dans la Circ.-FINMA 2008/10 « Normes d'autorégulation reconnues comme standards minimaux ».

[9] Selon l'UBCS, les obligations légales de garder le secret auxquelles sont soumises les banques en vertu du secret bancaire (art. 47 LB), notamment, sont sensiblement plus strictes que les règles de la LPD.

Appréciation

La suppression des dispositions sur la protection des données et le secret bancaire est maintenue. Elle découle de la délimitation entre les exigences prudentielles de la surveillance des marchés financiers et les exigences ancrées dans le droit public et dans le droit privé (en particulier la LPD) ainsi que du lien entre l'art. 47 LB et le droit pénal (cf. art. 6 al. 1 et art. 7 al. 1 let. b LFINMA).

L'annexe 3 de la circulaire de la FINMA 2008/21 « Risques opérationnels – banques » reste déterminante pour le traitement des données électroniques des clients par les banques.

Conclusion

La suppression des anciennes dispositions de la Circ.-FINMA 08/7 sur la protection des données (cf. ses Cm 31 à 33, 36 et 37 à 39) est maintenue.

3.6.6 Audit et surveillance (Cm 32 à 35)

Prises de position des banques / négociants en valeurs mobilières

Certains participants à l'audition, dont l'ASB et l'UBCS, critiquent l'exigence d'un droit de regard et d'examen intégral, permanent et sans entraves, car celui-ci pourrait contrevenir à d'éventuelles règles juridiques locales contraires et contraignantes ou à des circonstances particulières qui découleraient de faits concrets. Pour des questions d'efficacité, des partenaires d'*outsourcing* ne peuvent ou ne veulent pas accorder un droit de regard et d'examen complet à chaque entreprise. Le droit de regard direct devrait donc pouvoir être exclu du contrat et remplacé, par exemple, par une consultation et une vérification incombant à la société d'audit du prestataire. UBS indique qu'un droit de regard et d'examen « permanent » est disproportionné, car l'entreprise contrôlée doit pouvoir se préparer.

Les infrastructures en nuage sont citées à titre d'exemple. Il s'agit fréquemment de grands centres de calculs répartis géographiquement, dont l'exploitation est fortement automatisée et que de nombreux clients peuvent utiliser simultanément. Dans ces circonstances, l'exigence d'une inspection sur place par l'entreprise externalisatrice, sa société d'audit et la FINMA ne répond pas à l'objectif et n'est pas réalisable, tant en raison des spécificités techniques que pour des questions de sécurité.

Selon RAI et l'ASB, le Cm 33 constitue une ingérence dans la stratégie de contrôle de l'auditeur prudentiel et requiert des activités d'audit allant au-delà de la circulaire de la FINMA 2013/3 « Activités d'audit ». La possibilité unique de se reposer sur l'organe de révision du prestataire restreint les variantes de contrôle de la société d'audit prudentiel. En outre, RAI suggère

que les activités d'audit puissent également être réalisées par la révision interne du groupe en cas d'externalisations intragroupe.

D'après l'ASB, rien n'explique pourquoi les activités d'audit déléguées doivent être exécutées par un organe de révision organisé selon le droit suisse.

Enfin, CS, l'ASB et l'UBCS demandent de préciser qu'un transfert à l'étranger ne doit pas compliquer de manière disproportionnée la surveillance par la FINMA. En effet, toute externalisation de ce type complique la surveillance dans une certaine mesure. Pour l'UBCS, la formulation actuelle s'apparente à une interdiction factuelle.

Prises de position des assureurs

Aux Cm 32 et 33, l'ASA propose de supprimer l'exigence d'un organe de révision « organisé selon le droit suisse ». Elle suggère également d'apporter le complément suivant : *« L'entreprise peut s'appuyer en plus sur le rapport de contrôle du fournisseur, à condition que ce rapport ait été établi selon la norme ISAE 3402, type II, ou une norme similaire. »*

La SDRCA et, par analogie, SRZ estiment souhaitable d'accorder des allégements concernant le droit de regard et d'examen intégral et permanent, en particulier en relation avec des fournisseurs d'infrastructures en nuage, sous peine que l'accès à ces solutions en nuage ne soit considérablement compliqué ou que le droit de regard correspondant ne soit guère applicable de manière judicieuse.

SAN demande que l'octroi d'un droit de regard et d'examen (contractuel) intégral par des tiers en faveur de la FINMA soit supprimé au Cm 32.

L'ASA, SRZ et la SDRCA souhaitent que le Cm 34 soit complété afin qu'une externalisation ne complique pas « de manière significative » la surveillance par la FINMA. Ces participants arguent qu'un transfert à l'étranger s'accompagne implicitement de complications en raison des compétences territoriales.

Enfin, l'ASA suggère de compléter le Cm 35 en ce sens qu'un prestataire non assujetti à la surveillance de la FINMA devra s'engager contractuellement envers l'entreprise à « mettre à disposition, à l'attention de la FINMA, » tous les renseignements et documents relatifs au domaine d'activités transféré. Cette proposition entend prendre en compte le fait que le droit étranger interdit parfois de fournir directement ces informations à la FINMA.

Prises de position des tiers

LAUX, SICT, la SPA et KARTAC considèrent que les exigences sur les droits de contrôle sont trop élevées et détaillées. En outre, le terme « permanent » n'est pas neutre sur le plan technologique, en particulier en ce qui concerne les solutions en nuage. Selon SICT et LAUX, un droit de regard et d'examen interprété de manière trop large pourrait notamment engendrer des problèmes de sécurité pour les infrastructures à utilisateurs multiples ou mettre en péril la sécurité et les secrets des autres utilisateurs de la même infrastructure. Les exigences devraient donc être abaissées ou complétées[10] en tenant compte de cet aspect (sécuritaire).

De manière générale, SICT considère que les déclarations sur les solutions en nuage sont appropriées, car selon son appréciation, de nombreuses applications actuelles en nuage ne seraient de toute manière pas concernées par la circulaire en raison de leur manque d'indépendance.

L'ASAI estime que la révision interne devrait être explicitement indiquée comme la détentrice du droit d'examen. De plus, il faudrait préciser à quels rapports se réfère le Cm 35.

Appréciation

L'exigence selon laquelle le domaine externalisé doit pouvoir être examiné de manière permanente, intégrale et sans entraves aussi bien en Suisse qu'à l'étranger est conservée. Elle repose, tout comme son interprétation, sur le principe de la neutralité technologique et sur l'égalité de traitement quant à l'obligation de respecter la circulaire : toutes choses étant égales par ailleurs, la réglementation ne doit pas décider des moyens et, en particulier, des technologies que les établissements utilisent dans leurs activités. Inversement et dans le cadre d'*outsourcings*, les établissements qui externalisent des tâches (par ex. auprès d'une infrastructure en nuage) ne doivent pas être soumis à des exigences moins strictes que ceux qui exécutent ces mêmes tâches en leur sein. En particulier, une surveillance efficace par la FINMA et les activités d'audit nécessaires en la matière ne doivent pas être entravées dans les faits, voire empêchées par des externalisations (cf. Cm 28). La fonction externalisée doit donc présenter le même statut prudentiel que les fonctions exécutées en interne.

Les termes « permanent », « intégral » et « sans entraves » doivent cependant être interprétés selon le principe de proportionnalité. Pour ce qui est du caractère « permanent », des activités d'audit peuvent être réalisées en accordant un temps de préparation approprié. Le terme « intégral » se rap-

[10] « …, des réserves objectivement justifiées étant autorisées pour protéger des intérêts légitimes (maintien de la sécurité, obligations de confidentialité vis-à-vis de tiers et lutte contre les entraves excessives à l'activité opérationnelle). »

porte uniquement aux faits pertinents sur le plan prudentiel. Enfin, l'expression « sans entraves » ne se limite qu'aux activités ou fonctions externalisées par l'établissement et implique de respecter les secrets d'affaires de tiers. Un complément restrictif ajouté dans la circulaire souligne désormais que les droits d'examen doivent être accordés *pour la prestation externalisée*. En informatique en particulier, la présence sur place (par ex. dans un centre de calcul) n'est pas impérative dans tous les cas. Il est donc envisageable d'exercer le droit de regard à distance.

La requête de nombreux participants à l'audition qui souhaitent la suppression de l'obligation d'une délégation des activités d'audit aux seuls organes de révision organisés selon le droit suisse a été entendue. En la matière, il ne doit pas s'agir de l'organe de révision mandaté pour le contrôle des comptes ; il importe davantage qu'il soit dûment qualifié pour l'audit correspondant. Toutefois, même en cas de délégation des activités d'audit, la société d'audit prudentiel continue d'assumer la responsabilité finale quant à la confirmation du respect de la circulaire.

La proposition selon laquelle la révision interne du groupe pourrait effectuer les activités d'audit en cas d'externalisations intragroupe ne saurait être acceptée en raison de considérations liées à l'indépendance.

Conclusion

Par principe, la fonction externalisée doit présenter le même statut prudentiel que les fonctions exécutées en interne.

L'exigence de droits d'examen permanents, intégraux et sans entraves est conservée, les termes devant cependant être interprétés de manière proportionnée, à l'aune des explications précédentes.

Désormais, les activités d'audit ne doivent plus impérativement être déléguées à un organe de révision organisé selon le droit suisse. De plus, il ne doit pas s'agir de l'organe de révision mandaté par le prestataire pour le contrôle des comptes.

3.6.7 Transfert à l'étranger (Cm 36 à 38)

Prises de position des banques / négociants en valeurs mobilières

CS demande de préciser au Cm 36 qu'aucune autorisation préalable de la FINMA n'est nécessaire pour apporter la preuve des droits de contrôle.

CS, UBS, l'ASB et l'UBCS émettent des réserves générales sur la preuve de ces droits à l'étranger au moyen d'avis de droit, car cela n'est guère l'usage dans la pratique. La FINMA devrait plutôt établir une liste des pays dans les-

quels la preuve est présumée apportée[11]. L'UBCS considère que cette exigence s'apparente à une interdiction factuelle des transferts à l'étranger. Aucune exigence autre que celles des Cm 136.2 ss de la Circ.-FINMA 08/21 « Risques opérationnels – banques » ne devrait être posée.

La plupart des participants à l'audition rejettent l'obligation d'une information préalable en cas de transfert à l'étranger de données d'identification des clients. Plusieurs estiment qu'il s'agit d'une charge administrative supplémentaire inutile. De plus, l'AFBS ignore quelles informations devraient être fournies et si le transfert serait réalisable sous réserve de l'approbation de la FINMA.

Par ailleurs, des participants déplorent que l'expression « grandes quantités de données d'identification des clients » ne soit pas définie de manière plus précise. En outre, des doutes subsistent quant au caractère essentiel de ces données.

CS et RAI critiquent le fait que le Cm 38 n'indique pas clairement les types d'accès autorisés (accès à distance, réplication des données, etc.). L'exigence éventuelle d'une réplication des données engendrerait des coûts énormes.

Enfin, certains participants contestent le fait qu'en parlant de « capacité d'assainissement et de liquidation », la FINMA étende à tous les établissements bancaires des concepts propres à la réglementation des grandes banques.

Prises de position des assureurs

L'ASA et SRZ demandent la suppression du Cm 36. La preuve que les droits de contrôle peuvent être exercés et appliqués de manière suffisante est déjà fournie avec l'obligation contractuelle énoncée au Cm 32. Seuls des faits passés ou présents peuvent être prouvés. Un événement futur ne peut pas l'être ; il peut tout au plus être présenté comme probable ou crédible. Au demeurant, cette preuve ne doit pas être apportée en vertu de Solvabilité II.

L'ASA demande que le champ d'application du Cm 37 de la version présentée à l'audition soit limité aux banques.

Par ailleurs, l'ASA et SRZ critiquent la formulation du Cm 38. Le lieu de stockage des données concernées n'est pas pertinent pour la capacité d'assainissement et de liquidation de l'entreprise en Suisse, alors que la possibilité d'y accéder (depuis la Suisse) l'est. Il n'existe aucune raison objective d'imposer un stockage dans ce pays. Les conditions correspondantes sont disproportionnées. Tel qu'il est formulé, le projet implique une réplication des

[11] Selon l'UBCS, base analogue à l'art. 7 LPD par ex.

données en Suisse qui serait bien trop chère, si tant est qu'elle soit réalisable. Cette prescription exclut dans la pratique le recours à l'informatique en nuage (*cloud computing*).

ASS exige que les dispositions, formalistes à ses yeux, des Cm 32 à 38 de la version présentée à l'audition soient assouplies.

Prises de position des tiers

L'ASAI et HOM demande que l'exigence concernant la preuve des droits de contrôle soit supprimée, car les assureurs font déjà l'objet d'une surveillance directe en la matière (approbation des modifications du plan d'exploitation). De plus, cette exigence dépasse celle de Solvabilité II. KARTAC et la SPA estiment que la preuve préalable des droits de contrôle va trop loin et engendre de facto une interdiction des transferts à l'étranger.

La plupart des participants à l'audition rejettent l'obligation d'une information préalable en cas de transfert à l'étranger de grandes quantités de données d'identification des clients. Si cette exigence devait être conservée, l'ASAI et ES estiment nécessaire d'apporter au moins des précisions sur le chiffrage/secret bancaire, le sens de données d'identification des clients, etc. Enfin, ES se demande si les établissements peuvent procéder à l'externalisation après avoir rempli l'obligation d'informer ou s'ils doivent attendre une quelconque confirmation de la FINMA.

Plusieurs participants à l'audition exigent que l'accès aux données en Suisse ne s'apparente pas à une obligation de stocker les données (de manière redondante) dans ce pays, car cela annihilerait les avantages des externalisations.

Appréciation

L'obligation d'apporter préalablement la preuve des droits de contrôle à l'étranger est supprimée. Cela ne dispense toutefois pas les établissements de clarifier ces droits de manière appropriée en cas de transfert à l'étranger. Comme auparavant, l'établissement externalisateur doit veiller à ce que les droits de contrôle restent garantis même lors de ces transferts. L'exigence formelle d'une preuve préalable est en revanche caduque.

On renonce également à l'obligation d'une information préalable en cas de transfert à l'étranger de grandes quantités de données d'identification des clients, comme le souhaitaient les participants à l'audition. La description de la prestation externalisée ou l'indication du fournisseur (en vertu du nouveau Cm 14) dans l'inventaire à actualiser régulièrement doivent permettre de déterminer si de grandes quantités de données d'identification des clients sont transférées à l'étranger. En cas de besoin, la FINMA peut demander cet inventaire aux banques dans le cadre de son activité de surveillance.

En cas d'*outsourcing* transfrontalier, il est primordial pour les banques et les entreprises d'assurance que l'accès, la lisibilité et l'exploitation opérationnelle de toutes les données pertinentes pour la surveillance demeurent possibles à tout moment en Suisse en dépit de l'externalisation. Le terme « information », qui contrairement à la version présentée à l'audition est désormais utilisé, englobe notamment les caractéristiques liées à la lisibilité et à l'exploitation opérationnelle. Ces exigences sont neutres sur le plan technologique et axées sur des principes.

Accès aux informations au sens du Cm 31 pour les entreprises d'assurance

Dans la pratique de la surveillance des assurances, cette exigence peut être mise en œuvre, par exemple, en établissant une structure appropriée qui garantira, en cas d'assainissement et de liquidation, que les informations nécessaires seront disponibles et que les prétentions émises par des requérants pourront être identifiées et réglées. Concernant une externalisation en nuage, des « solutions en nuage privées » (*private cloud*), notamment, sont envisageables.

Dans l'intérêt de la surveillance et de la protection des assurés, toutes les données concernant ces derniers ainsi que les données pertinentes pour la fortune liée et l'ensemble du *reporting* à la FINMA sont particulièrement importantes. L'endettement est déterminé sur la base des comptes statutaires. En l'espèce, un assainissement et une liquidation doivent être possibles en Suisse. Sur le plan prudentiel, cela découle non seulement d'une bonne gestion du risque (art. 22 LSA) ou gestion de la continuité des affaires, mais également de manière implicite de plusieurs autres normes du droit de la surveillance des assurances (art. 53 al. 1 LSA et art. 54*a* al. 1 LSA, ce dernier énonçant que les créances d'assurés qui peuvent être constatées au moyen des livres de l'entreprise d'assurance sont réputées produites d'office en cas de faillite.) Cette disposition implique que la FINMA puisse effectivement accéder aux données lors de la procédure de faillite afin de les consulter et de les traiter (traitement de l'information).

Le mandataire général conserve les documents relatifs au portefeuille suisse d'assurance au siège de l'ensemble des affaires suisses et tient les livres et registres qui s'y rapportent. Sur demande motivée, la FINMA peut autoriser que certains documents soient conservés dans un autre lieu (cf. art. 19 OS). L'art. 19 OS doit être interprété de telle sorte que cette exigence s'applique uniquement aux entreprises d'assurance ayant leur siège en Suisse.

Accès aux informations au sens du Cm 31 pour les banques / négociants en valeurs mobilières

Eu égard aux bases prudentielles moins marquées dans le domaine de la surveillance des banques, on renonce à une description détaillée de la mise

en œuvre des exigences par les établissements bancaires. L'accès aux informations nécessaires à l'assainissement ou à la liquidation doit être garanti depuis la Suisse ; en d'autres termes, les données doivent être disponibles et lisibles sans aucune restriction depuis ce pays, même en cas de faillite. Il incombe aux établissements assujettis de veiller au respect de ce principe grâce à des mesures appropriées.

Conclusion

On renonce à l'obligation d'une preuve préalable des droits de contrôle en cas de transfert à l'étranger. Nonobstant ce point, en vertu du droit de la surveillance, les établissements externalisateurs sont tenus de garantir les droits de contrôle (et la possibilité effective d'une vérification).

L'obligation d'informer prévue pour les banques dans la version présentée à l'audition en cas de transfert à l'étranger de grandes quantités de données d'identification des clients est supprimée.

Le principe selon lequel l'accès aux informations nécessaires à l'assainissement et à la liquidation doit être possible à tout moment en Suisse est conservé.

La surveillance des assurances comprend des dispositions spécifiques aux exigences de « tenue des livres » en Suisse (cf. art. 19 OS).

3.6.8 Contrat (Cm 39 à 45)

Prises de position des banques / négociants en valeurs mobilières

CS et l'UBCS demandent que les exigences de documentation soient plus faibles pour les externalisations intragroupe (par ex. SLA).

L'utilisation de l'expression « personne auxiliaire » suscite à nouveau de vastes critiques (tout comme au Cm 21 du projet présenté à l'audition ; cf. les arguments exposés au ch. 3.6.1). Plusieurs participants à l'audition indiquent que l'approbation préalable des sous-traitants n'est pas applicable en pratique et souhaitent dès lors sa suppression ou sa limitation aux seuls cas dans lesquels le sous-traitant fournit des prestations essentielles.

Prises de position des assureurs

L'ASA, SRZ, la SDRCA, SAN et, par analogie, ASS exigent la suppression de l'obligation d'approbation lors du recours à des sous-traitants au Cm 40. Concernant le transfert des obligations et des garanties du prestataire aux sous-traitants, la formulation utilisée devrait être davantage axée sur les risques et mieux prendre en compte la proportionnalité. La formulation du projet dépasse le cadre d'une gestion nécessaire et judicieuse du risque

ainsi que les exigences de Solvabilité II. Elle n'est pas réalisable, du moins dans le domaine informatique/l'informatique en nuage, ou conduit pratiquement à exclure toute solution novatrice pour les assureurs.

Pour ce qui est du Cm 41, l'ASA souhaite une formulation précise qui se focalise exclusivement sur les chiffres marginaux mentionnés et non sur l'ensemble de la circulaire. Toutes les obligations issues de cette dernière ne peuvent pas être transférées aux sous-traitants. Selon l'ASA, le Cm 42 devrait être supprimé, car la disposition est inutilement formaliste.

Prises de position des tiers

Il est demandé de manière presque unanime que le terme « sous-traitant » soit utilisé à la place de « personne auxiliaire ». De même, plusieurs participants à l'audition soulignent que l'approbation préalable ou l'obligation d'approbation en cas de recours à des sous-traitants n'est pas applicable en pratique. Il devrait également être possible de réglementer cet aspect de manière contractuel pour le recours à tous les futurs sous-traitants ou, par exemple, de convenir d'une obligation d'annonce ultérieure. Il faudrait au moins assouplir cette exigence en la limitant, par exemple, aux activités essentielles du contrat. De plus, l'asut et SCOM estiment que l'obligation d'approbation et celle de transfert des obligations et garanties sont judicieuses uniquement lorsque le tiers a accès à de grandes quantités de données d'identification des clients[12] ou lorsque le recours à un tiers par le prestataire constitue en soi une externalisation essentielle au sens de la circulaire.

Appréciation

On renonce à utiliser le terme « auxiliaire » dans toute la circulaire. De plus, le Cm 33 (Cm 40 de la version présentée à l'audition) est complété comme le souhaitent les participants à l'audition en ce sens que l'obligation d'une approbation préalable s'applique uniquement si le prestataire externalise (à son tour) des parties essentielles à un sous-traitant.

Concernant les exigences énoncées aux Cm 32 à 35, l'ancrage au sein d'un groupe peut être considéré dans la mesure où il est prouvé que les risques habituellement liés à une externalisation n'existent pas ou que certaines exigences ne sont pas pertinentes ou sont réglementées autrement. Ainsi, des exigences plus faibles en matière de documentation sont possibles dans le contexte d'un groupe par exemple, si les contenus n'ont pas fait l'objet de négociations contractuelles formelles, contrairement à l'usage lorsqu'un contrat est conclu avec un prestataire externe.

[12] Selon l'asut, il ressort du rapport explicatif que la FINMA met l'accent sur les grandes quantités de données d'identification des clients et considère leur externalisation comme essentielle.

Conclusion

On renonce systématiquement au terme « auxiliaire ». L'exigence concernant la réserve d'approbation pour le recours à des sous-traitants se limite aux cas dans lesquels ces sous-traitants fournissent une part essentielle de la fonction (au sens de la circulaire).

Par ailleurs, la situation du groupe peut être prise en compte dans les Cm 32 à 35 (par ex. pour l'exigence de documentation de l'accord contractuel).

3.7 Conditions et exceptions

Prises de position des banques / négociants en valeurs mobilières

L'ASB salue la réglementation sur les conditions et les exceptions. Elle souhaite cependant des estimations de la FINMA quant aux prestations spécifiques qui pourraient ou non être considérées comme essentielles.

Prises de position des assureurs

L'ASA déplore que la formulation du Cm 46 soit aussi ouverte. Ce chiffre marginal devrait définir des critères spécifiques et être complété par des exemples. SAN est certes favorable à une réglementation des exceptions, mais pense également que la formulation est trop ouverte. Selon SAN et VIS, ce chiffre marginal permettrait aux entreprises d'assurance et aux prestataires qui relèvent de la même haute direction et de la même direction opérationnelle d'être entièrement ou partiellement exemptés de l'application de la circulaire, à condition que cette structure ne soit pas exclue de manière générale de son champ d'application.

Prises de position des tiers

Aucune.

Appréciation

Des exceptions ou l'ajout d'autres conditions peuvent être décidés au cas par cas, comme le prévoit déjà la Circ.-FINMA 08/7. La nouvelle approche concernant la définition du caractère essentiel des externalisations confère aux établissements une responsabilité individuelle plus grande en la matière.

Dans le secteur de l'assurance, l'art. 4 al. 2 let. j LSA restreint fortement la possibilité d'accorder des exceptions.

Conclusion

La possibilité de définir des exceptions est maintenue.

3.8 Dispositions transitoires

Prises de position des banques / négociants en valeurs mobilières

Certains participants à l'audition critiquent l'application de la circulaire révisée aux relations d'*outsourcing* existantes et la considèrent comme un effet rétroactif illicite. Les fournisseurs risquent de ne plus accepter les contrats adaptés et, dans le pire des cas, de résilier l'externalisation. De même, le délai transitoire de deux ans pour adapter les relations d'*outsourcing* existantes est jugé trop court. En particulier, il devrait être sensiblement prolongé ou la mise en œuvre devrait être repoussée si l'effet rétroactif est conservé.

Prises de position des assureurs

L'ASA souhaite apporter une précision au Cm 49 afin que la circulaire ne s'applique pas aux externalisations réalisées *avant* son entrée en vigueur. De plus, il faut indiquer expressément qu'en l'espèce, les modifications du plan d'exploitation relèvent de l'art. 4 al. 2 let. j LSA. Sur le fond, de nombreux autres participants à l'audition demandent des adaptations similaires.

Prises de position des tiers

Certains participants déplorent le bref délai transitoire de deux ans et, de manière générale, l'effet rétroactif pour les banques, qu'ils jugent disproportionné.

Appréciation

La FINMA estime proportionné d'adapter les relations d'*outsourcing* qui préexistent aux nouvelles exigences dans un délai raisonnable. En outre, du point de vue de la surveillance et en vertu du principe de l'égalité de traitement, le fait que ces *outsourcings* soient soumis pendant encore des années à d'autres conditions que les externalisations réalisées après l'entrée en vigueur de la circulaire révisée serait difficilement justifiable.

Les participants à l'audition soulignent cependant à raison que la mise en œuvre de nouvelles exigences matérielles requiert suffisamment de temps et de ressources. Il en est tenu compte. La circulaire entrera en vigueur le 1er avril 2018, un délai transitoire de cinq ans s'appliquant aux *outsourcings* préexistants des banques.

Aucun délai transitoire n'est nécessaire pour les assurances, car il n'y avait pas de circulaire correspondante jusqu'à présent et la circulaire révisée codifie dans une large mesure la pratique déjà établie. Il est donc justifié que les modifications du plan d'exploitation intègrent une adaptation à la nouvelle circulaire. Cette adaptation s'effectuera donc progressivement.

Conclusion

La circulaire entrera en vigueur le 1er avril 2018. Elle vaut également pour les relations d'*outsourcing* préexistantes des banques, mais un délai transitoire porté à cinq ans à compter de l'entrée en vigueur est accordé en la matière.

Concernant les entreprises d'assurance, la circulaire s'applique dès son entrée en vigueur aux autorisations initiales ainsi qu'aux modifications du plan d'exploitation.

4 Suite de la procédure

La Circ.-FINMA 18/3 « *Outsourcing* – banques et assureurs » entrera en vigueur le 1er avril 2018.