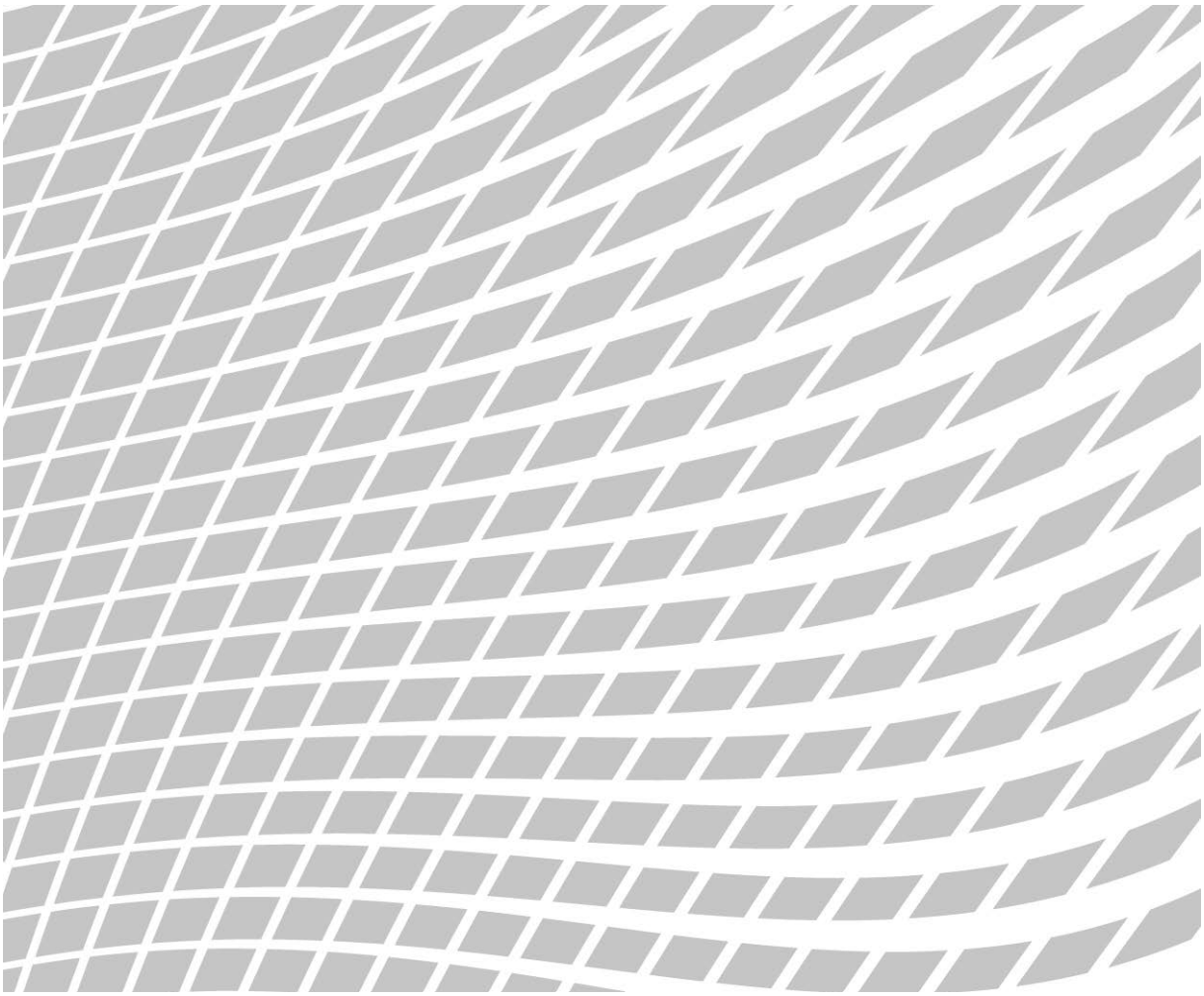
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

6 décembre 2016

Circulaire 2017/xx « *Outsourcing* – banques et assureurs »

Rapport explicatif



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 circulaire 2008/7 « O*utsourcing* – banques » a été entièrement révisée et vaut désormais tant pour les banques que pour les entreprises d'assurance.

2. L'ensemble des exigences de la présente circulaire doivent être satisfaites même en cas d'externalisations internes au groupe, ce qui est conforme à la pratique en vigueur pour les entreprises d'assurance mais constitue une nouveauté pour les banques.

3. Le transfert de prestations de services critiques à des banques appartenant au même groupe financier n'est dorénavant plus autorisé pour les banques d'importance systémique. Ces dernières doivent par ailleurs s'assurer qu'un transfert ne sera pas préjudiciable à la continuité des prestations de services critiques en cas d'insolvabilité (imminente). Des exigences renforcées sont donc définies pour les contrats d'*outsourcing* portant sur des prestations de services critiques.

4. Conformément à la pratique en vigueur des entreprises d'assurance mais nouvellement pour les banques, un inventaire des prestations de services externalisées doit être établi.

5. Les anciennes dispositions de la circulaire dont la teneur avait trait au droit de la protection des données ainsi que les exigences concernant l'information des clients ont été supprimées afin d'éviter tout doublon avec la loi sur la protection des données.

6. En cas de transferts à l'étranger, il faut désormais garantir qu'il soit possible d'avoir accès à tout moment, en Suisse, à l'ensemble des données nécessaires à un assainissement ou à une liquidation.

7. L'annexe qui donnait des exemples d'externalisations entrant ou non dans le champ d'application de la circulaire a été supprimée. Les principaux exemples sont désormais évoqués dans le corps même de la circulaire.

Liste des abréviations

CFB	Commission fédérale des banques
CID	*Client identifying data* (données d'identification du client)
CSF	Conseil de stabilité financière
LB	Loi du 8 novembre 1934 sur les banques et les caisses d'épargne (RS 952.0)
LPD	Loi du 19 juin 1992 sur la protection des données (RS 235.1)
LSA	Loi du 17 décembre 2004 sur la surveillance des entreprises d'assurance (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)

1 Contexte

Dans le sillage de la mondialisation, de la numérisation et de l'intensification de la répartition du travail, les *outsourcings* (externalisations) n'ont cessé de gagner en importance ces dernières années. Ils permettent notamment de simplifier les processus, de réduire les coûts et de profiter des compétences de prestataires tiers (notamment dans le domaine informatique) lorsqu'elles ne sont pas disponibles au sein de l'entreprise. Dans le même temps, il convient pour les banques, les négociants en valeurs mobilières et les entreprises d'assurance de s'assurer, au niveau prudentiel, que les exigences visant une organisation appropriée sont satisfaites, les risques limités et qu'une surveillance efficace s'exerce même sur les domaines d'activités externaliséfs.

C'est dans ce but qu'en août 1999, la CFB a publié la circulaire 99/2 « *Outsourcing* – banques ». Cette circulaire a été soumise à une révision partielle pour la dernière fois en 2002 (Circ.-CFB 2002/2, aujourd'hui Circulaire FINMA 2008/7 « O*utsourcing* - banques »).

Dans le domaine de la surveillance des assurances, les exigences concernant les *outsourcings* n'étaient pas, jusqu'alors, définies au niveau des circulaires. Conformément à l'art. 4 al. 2 let. j en relation avec l'art. 5 al. 2 LSA, les entreprises d'assurance doivent, dans le cadre du plan d'exploitation, soumettre pour approbation à la FINMA, les informations et les documents concernant les contrats ou autres accords en vertu desquels des fonctions essentielles de l'entreprise d'assurance seraient externalisées. Les exigences encadrant l'*outsourcing* étaient jusqu'à présent précisées dans les explications relatives au plan d'exploitation, au sens d'une communication de la pratique[1]. La Communication FINMA 63 (2014) concrétisait le transfert de fonctions essentielles à des intermédiaires par des entreprises d'assurance.

La circulaire 2017/xx « *Outsourcing* - banques et assureurs » vise à concrétiser, en une seule et même circulaire, les exigences prudentielles concernant les projets d'*outsourcing* des banques comme des entreprises d'assurance.

Depuis la publication de la Circ.-FINMA 08/7, le CSF a édité des lignes directrices pour améliorer la continuité des prestations de services critiques en cas de crise (lignes directrices du CSF) qui sont déterminantes pour les *outsourcings.* Les mesures qu'elles contiennent visent le maintien des fonctions d'importance systémique en cas d'insolvabilité (imminente) et donc, l'amélioration de la résistance aux crises des banques d'importance systémique. [2]

[1] Cf. www.finma.ch > Autorisation > Assurances > Plan d'exploitation

[2] FSB « Guidance on Arrangements to Support Operational Continuity in Resolution », 18 août 2016

2 Besoin de régulation et objectifs

Le principal objectif de la révision est de conserver en matière d'*outsourcings* la pratique prudentielle fondée sur les principes et de l'harmoniser, autant qu'il est permis et approprié, au niveau des banques et des entreprises d'assurance. Ce faisant, il convient de s'assurer que les externalisations n'auront pas d'effet préjudiciable sur les clients, les créanciers, la stabilité du marché financier, ni encore sur une activité de surveillance efficace.

En référence aux lignes directrices du CSF, il faut imposer aux banques d'importance systémique des exigences renforcées en rapport avec le transfert de prestations de services critiques. Il faut notamment s'assurer que les *outsourcings* n'auront pas d'effet préjudiciable en cas de restructuration ou de liquidation et qu'ils sont pris en compte dans le cadre du plan d'urgence. Il s'agit par ailleurs de définir les exigences correspondantes afin de concrétiser les prescriptions légales fixées pour le plan d'urgence.

Les dispositions de la Circ.-FINMA 08/7 qui avaient matériellement pour objet des questions relevant du droit de la protection des données disparaissent de la circulaire avec cette révision. Les doublons ainsi que d'éventuelles divergences ou difficultés de délimitation entre les dispositions prudentielles de la circulaire et les dispositions légales sur la protection des données seront ainsi évités à l'avenir.

Enfin, il convient d'actualiser les concepts importants et la terminologie, de condenser la circulaire et de l'aligner sur la pratique actuelle de la FINMA. En partie caduque, l'annexe à la Circ.-FINMA 08/7 est supprimée. Les principaux exemples sont désormais évoqués dans le corps même de la circulaire.

3 Structure

La structure de la circulaire précédente est conservée. L'extension du champ d'application aux entreprises d'assurance implique toutefois que les sections II (concepts) et IV (admissibilité) de la circulaire traitent séparément des entreprises d'assurance et des banques (cf. à ce sujet le chiffre 4.1 ci-après). A ces exceptions près, les dispositions de la présente circulaire sont applicables aux banques comme aux entreprises d'assurance.

Pour ce qui est de l'admissibilité des *outsourcings*, la différence fondamentale réside dans le fait que les externalisations déterminantes pour le plan d'exploitation sont soumises à autorisation dans le cas des entreprises d'assurance (art. 4 al. 2 let. j en relation avec l'art. 5 al. 2 LSA), alors que pour les banques, il n'y a pas d'obligation légale d'autorisation pour les externalisations. Contrairement aux entreprises d'assurance, pour lesquelles il n'existe actuellement aucun champ d'audit spécifique aux externalisations en vertu de la circulaire FINMA 2013/3 « Activités d'audit », les sociétés d'audit des banques doivent contrôler les externalisations. Ici transparaît la différence d'approches entre la surveillance des banques où prévaut la surveillance indirecte et la surveillance des assurances, où la surveillance directe est prépondérante.

4 Commentaire des dispositions

4.1 Structure et concepts

Dans le cadre de la révision totale de la circulaire, la partie consacrée aux définitions ou concepts a été remaniée et adaptée à la pratique prudentielle actuelle de la FINMA. Matériellement, il n'en résulte aucun durcissement de la pratique prudentielle.

Un ***outsourcing*** au sens de la présente circulaire s'entend dans une acception large. Selon l'ancienne interprétation déjà, il n'était pas nécessaire qu'un domaine d'activités, entendu au sens d'une unité autonome sur le plan organisationnel, soit externalisé pour qu'il y ait *outsourcing*. Il n'est pas déterminant non plus qu'il s'agisse d'une tâche d'entreprise qui relève typiquement ou spécifiquement des banques ou des entreprises d'assurance. Ce point de vue n'aura éventuellement son importance que lors de l'appréciation du caractère essentiel. Le fait qu'une prestation de services ait d'abord été fournie par l'établissement externalisateur ou qu'elle ait été apportée dès le début par un prestataire tiers n'est pas non plus pertinent pour la qualification en tant qu'*outsourcing*.

Pour que le prestataire puisse être considéré comme accomplissant les tâches externalisées **de manière indépendante** (Cm 4), l'entreprise doit lui laisser un champ d'action significatif et lui transférer les compétences nécessaires. Lorsqu'un prestataire accomplit une tâche essentielle, son activité est, en cas de doute, présumée indépendante.

Enfin, l'applicabilité de la présente circulaire n'est pas influencée par le fait que le transfert intervienne au sein d'un groupe d'entreprises (par ex. de la société mère à sa filiale ou entre deux filiales) ou à un prestataire externe qui n'a sinon aucune autre relation avec l'établissement externalisateur (cf. au sujet du champ d'application le ch. 4.2 ci-après).

La circulaire traite exclusivement des externalisations **essentielles**. Le caractère essentiel n'est pas une notion qui peut être définie uniformément pour les banques et pour les entreprises d'assurance. L'exigence correspondante au sein des banques s'est en effet développée à partir de la pratique de surveillance de la FINMA et était jusqu'à présent consignée dans la Circ.-FINMA 08/7 alors que dans le cas des entreprises d'assurance, les fonctions essentielles au sens de l'art. 4 al. 2 let. j LSA renvoient aux fonctions qui sont impérativement présentes dans une entreprise d'assurance.

4.1.1 Banques (Cm 5 et 6)

Les critères servant à juger de ce caractère essentiel (Cm 5 et 6) sont fondés sur des principes et reposent sur une prise en compte des risques au sens du droit de la surveillance.

Les prestations de services dans les domaines de la logistique (restauration et cantine, sécurité des bâtiments, prestations générales de service et de soutien, etc.) et des ressources humaines (décompte des salaires, de la rémunération et des bonus des collaborateurs, occupation de forces de travail temporaires, etc.) qui ne sont pas déterminantes ni pour les affaires bancaires ni pour celles des négociants en valeurs mobilières continueront à ne pas être considérées comme essentielles. La participation à

des systèmes de traitement et de paiement des valeurs mobilières[3], les relations avec les banques correspondantes, les livraisons physiques de monnaie et les transports de valeurs, l'approvisionnement des distributeurs de billets, l'acquisition et la maintenance de logiciels ou tout projet ou mandat de développement de logiciels, les opérations de cartes de crédit, les encaissements ainsi que le conseil juridique et fiscal ne relèvent pas non plus de la circulaire.

Si, dans le cadre d'une externalisation, le prestataire obtient un accès aux CID[4], cet *outsourcing* se voit conférer un caractère essentiel.

4.1.2 Entreprises d'assurance (Cm 7)

Le Cm 7 définit les fonctions essentielles dans le secteur de l'assurance. La gestion du risque et la *compliance* sont désormais considérées comme des fonctions essentielles. Cela mis à part, la description présentée au Cm 7 correspond à la pratique actuelle de la FINMA.

La notion de caractère essentiel intègre une composante quantitative qu'il convient d'évaluer indépendamment du transfert des fonctions d'entreprise. Pour juger du caractère essentiel de la fonction partielle, il faut examiner si son transfert affecterait les intérêts des assurés. Cette appréciation dépend, d'une part, de la taille du domaine externalisé et, d'autre part, de l'étendue de la marge de manœuvre laissée au prestataire. Ainsi, une simple relation de mandat dans laquelle l'entreprise d'assurance se réserve le droit d'émettre des directives au cas par cas ne constitue pas une externalisation au sens de la circulaire. Par exemple, l'attribution d'un mandat à un cabinet d'avocats afin qu'il procède au règlement de différents cas de sinistres ne peut pas être qualifiée de détachement d'une fonction d'entreprise. En revanche, il en va autrement de l'externalisation systématique du règlement des recours (en tant que sous-fonction de la fonction clé qu'est le règlement des sinistres).

Sont par conséquent soumises à l'obligation d'autorisation les situations dans lesquelles le prestataire exerce plusieurs fonctions essentielles pour un portefeuille d'assurance et où l'entreprise d'assurance apparaît uniquement ou majoritairement comme le porteur du risque. Une telle externalisation revêt un caractère essentiel lorsque le nombre et la structure des polices ou encore la distribution des produits peuvent mettre en péril la solvabilité de l'entreprise d'assurance, affecter les intérêts des clients ou compliquer la surveillance de la FINMA. Voir à ce sujet la Communication FINMA 63 (2014).

[3] Alors que la participation à des systèmes de traitement et de règlement des valeurs mobilières ne relève pas de la circulaire, il existe différentes formes de participation ou d'aménagements technico-opérationnels de l'accès au système. D'éventuelles dispositions opposables aux participants à ces systèmes qui régissent justement les aménagements de l'accès au système sont du seul ressort des exploitants de ces systèmes.

[4] Le concept de « Grandes quantités de CID » est défini au Cm 53 de l'annexe 3 de la Circ.-FINMA 2008/21 « 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 ».

4.2 Champ d'application (Cm 8 à 10)

Sur le plan matériel, la circulaire est applicable aux *outsourcings* au sens du Cm 4 qui doivent être qualifiées d'essentielles conformément aux Cm 5 à 7.

Pour ce qui est des banques, le champ d'application de la circulaire est étendu dans la mesure où les exceptions à certaines dispositions prévues par la circulaire pour les externalisations entre parties proches, c'est-à-dire dans le cadre d'*outsourcings* internes au groupe (cf. Cm 6 à 11 de la Circ.-FINMA 08/7), ont été supprimées. Par principe, les externalisations internes au groupe ne doivent pas être traitées avec une diligence moindre, ni soumises à une surveillance moins intense de la part de la banque ou de l'entreprise d'assurance. Les exceptions notamment valables jusqu'à présent comme la libération de l'obligation de contracter (principe 9, Circ.-FINMA 08/7) ne sont plus défendables du point de vue du risque et ne seront donc plus retenues à l'avenir.

Concernant les entreprises d'assurance, le champ d'application correspond à la pratique actuelle. Restent notamment qualifiés d'externalisations le transfert d'activités par la succursale suisse d'une entreprise étrangère auprès du siège principal ou d'une autre entité de l'entreprise d'assurance, ainsi que tout transfert des fonctions d'une entreprise d'assurance à une de ses succursales.

L'externalisation de la révision interne ne relève pas du champ d'application de la présente circulaire. Il fait l'objet des circulaires FINMA relatives à la gouvernance d'entreprise[5].

4.3 Admissibilité

4.3.1 Dispositions communes (Cm 11 à 14)

Les banques et les entreprises d'assurance sont par principe autorisées à externaliser toute fonction à condition que les exigences de la présente circulaire (cf. Cm 21 à 45) soient remplies. Pour ce qui est de la surveillance des assurances, cela constitue une libéralisation par rapport à l'ancienne pratique qui autorisait l'externalisation de deux des trois fonctions clés (production, gestion du portefeuille et règlement des sinistres) au maximum.

Au nombre des tâches purement opérationnelles de la gestion du risque dont l'externalisation est autorisée (Cm 13), on compte dans le secteur bancaire par exemple la surveillance du risque de crédit, l'analyse des crédits ou la surveillance des limites de crédit et de négoce.

Bien que la fonction de *compliance* ne puisse pas être externalisée dans son intégralité, des tâches purement opérationnelles peuvent l'être, notamment celles portant sur l'identification, l'analyse, l'évaluation, le pilotage et la surveillance des risques de *compliance* propres à l'entreprise. Toutefois, aucune délégation des fonctions de conduite centrales ne doit en résulter ; la direction et l'organe de haute direction doivent au moins se réserver le dernier mot en matière d'évaluation et de pilotage du risque.

[5] Cf. Circ.-FINMA 2017/1 « Gouvernance d'entreprise – banques » et Circ.-FINMA 2017/2 « Gouvernance d'entreprise – assureurs ».

Dans le cadre d'une fonction de *compliance*, les tâches stratégiques mais aussi celles liées à la conception de l'organisation, comme la définition des stratégies et des lignes directrices, la mise à disposition des ressources et les décisions de principe sur la nature et l'étendue de l'instauration d'une fonction de *compliance* durable, ne font pas partie des activités opérationnelles.

Pour les entreprises des catégories de surveillance 4 et 5, des externalisations complètes sont possibles dans les limites précitées. Concernant le transfert des fonctions de risque et de *compliance*, il convient de se référer aux circulaires FINMA 17/1 et 17/2 relatives à la gouvernance d'entreprise.

4.3.2 Banques (Cm 15 et 16)

Comme auparavant, les *outsourcings* des banques et des négociants en valeurs mobilières restent par principe permis sans autorisation explicite de la FINMA.

Les banques d'importance systémique doivent se conformer à des prescriptions spécifiques concernant la continuité des prestations de services critiques en cas d'insolvabilité (imminente) (cf. Cm 15 et 16 ainsi que 44 et 45). Le but de ces exigences est d'éviter que la défaillance ou l'interruption soudaine de fonctions d'importance systémique n'ait de répercussions sur la stabilité du marché financier. Pour assurer la continuité des fonctions d'importance systémique, il est nécessaire que les prestations de services requises à cet effet (prestations de services critiques) puissent être maintenues en cas d'insolvabilité (imminente). Les externalisations ne doivent pas non plus compliquer la restructuration et une liquidation ordonnée en cas d'insolvabilité.

L'externalisation de prestations de services critiques auprès de banques appartenant au même groupe augmente la complexité de l'apport de la prestation de service ainsi que l'interaction opérationnelle et rend plus difficile la restructuration en cas de crise. Elle renforce en outre le risque de contagion au cas où la banque qui apporte la prestation de services devient à son tour insolvable. C'est pourquoi les banques d'importance systémique ont désormais l'interdiction d'externaliser des prestations de services critiques auprès d'autres banques appartenant au même groupe. Toute banque d'importance systémique doit garantir ce point dans le cadre de son plan d'urgence (art. 9 al. 2 let. d LB en relation avec l'art. 60 ss OB).

Lorsque les prestations de services sont fournies par la banque elle-même (prestations de services *inhouse*), les exigences requises pour assurer la continuité en cas d'insolvabilité sont réglées dans le cadre de la Circ.-FINMA 08/21 « Risques opérationnels – banques » (Cm 136.1). Les exigences encadrant le recours à un tiers ou à une société de prestations de services interne au groupe pour l'apport de prestations de services critiques font partie intégrante de la présente circulaire.

Les nouvelles prescriptions applicables aux banques d'importance systémique ont été développées en référence aux évolutions du droit international dans ce domaine, notamment aux lignes directrices du CSF. Elles concrétisent les prescriptions légales portant sur le plan d'urgence en lien avec les externalisations.

4.3.3 Entreprises d'assurance (Cm 17 à 20)

Par principe, il est possible d'externaliser toute fonction aussi bien au sein du groupe qu'à l'extérieur de celui-ci tant que les exigences liées au plan d'exploitation conformément à l'art. 4 al. 2 let. j LSA et les autres prescriptions légales sont remplis et que les intérêts des assurés sont sauvegardés (cf. art. 6 al. 1 LSA). L'externalisation de la gestion du risque et de la *compliance* est possible sous réserve des restrictions visées au chiffre 4.3.1.

Une modification essentielle d'un *outsourcing* déjà approuvé est soumise à approbation au sens de l'art. 5 al. 2 LSA. Il convient fondamentalement de juger et de décider au cas par cas s'il s'agit d'une modification soumise à déclaration ou à approbation. En l'occurrence, les exigences déterminantes sont celles définies dans la présente circulaire.

Les Cm 18 à 20 décrivent les assouplissements qui sont octroyés aux captives d'assurance directe ou de réassurance dans le domaine des externalisations. Dans ce contexte, un *outsourcing* est possible dans un cadre plus large qui tient compte des intérêts et de la structure spécifiques aux captives d'assurance directe et de réassurance. Cette réglementation correspond à la pratique actuelle de la FINMA.

4.4 Exigences pour les entreprises externalisatrices

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

L'établissement d'un inventaire des prestations de services externalisées est, d'une part, nécessaire à la surveillance des risques opérationnels. D'autre part, l'inventaire permet de faire la lumière sur le portefeuille des prestations de services externalisées en cas d'assainissement. Pour les entreprises d'assurance, l'inventaire est en fait une part du formulaire de saisie J du plan d'exploitation, ce qui correspond à la pratique actuelle.

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

L'entreprise qui opte pour un *outsourcing* risque dans certaines circonstances de se retrouver dans une relation de dépendance au prestataire. Avec les prestataires externes notamment, l'effet *lock-in* ou effet de captivité peut réduire la marge de manœuvre future d'un établissement, par exemple du fait de coûts de transition ou de changement élevés en cas de changement voire de défaillance du prestataire. Les réflexions correspondantes doivent être menées dès le début du processus de décision relative à l'externalisation et du choix du prestataire. Pour ce faire, il faut tenir compte de l'importance stratégique de la tâche d'entreprise externalisée et de la complexité du projet d'*outsourcing*.

4.4.3 Responsabilité (Cm 29)

La responsabilité en matière d'externalisation reste au sein de l'entreprise externalisatrice resp. des personnes devant en garantir une activité irréprochable.

4.4.4 Sécurité (Cm 30 et 31)

Les dispositions de la Circ.-FINMA 08/07 relatives au dispositif de sécurité et aux exigences contractuelles en matière de sécurité ont été abrégées, leur contenu reste toutefois inchangé.

Les prescriptions visées aux Cm 31 à 33 de la Circ.-FINMA 08/7 concernant la sécurité, l'intégrité et la véracité des données des clients sont supprimées. Les obligations correspondantes découlent du droit de la protection des données (cf. le chiffre 4.4.5 ci-après).

4.4.5 Secret des affaires et secret professionnel, protection des données

En Suisse, le traitement des données personnelles est globalement régi par la loi sur la protection des données (LPD ; RS 235.1), par l'ordonnance sur la protection des données (OLPD ; RS 235.11) ainsi que d'autres sources de droit, ce qui a permis d'établir une pratique abondante. Les banques doivent par ailleurs se conformer à l'art. 47 LB portant sur le secret bancaire. Le traitement des données électroniques des clients par les banques est, quant à lui, réglé dans l'annexe 3 de la Circ.-FINMA 08/21.

Afin d'éviter des doublons et d'éventuelles divergences dans les développements du droit de la protection des données, et de garantir, parallèlement, une délimitation claire entre les exigences prudentielles de la surveillance des marchés financiers et les obligations ancrées dans le droit privé conformément à la loi sur la protection des données, les dispositions figurant jusqu'à présent dans la Circ.-FINMA 08/07 en lien avec la protection des données sont radiées (cf. les anciens Cm 31 à 33, Cm 36 et Cm 37 à 39). Pour les mêmes raisons, l'ancien principe 6 (information des clients) sur lequel la Circ.-FINMA 08/7 allait au-delà des exigences relevant du droit de la protection des données, notamment sur les obligations d'information complètes et sur le droit de résiliation extraordinaire selon le Cm 39 de la Circ.-FINMA 08/07, est supprimé.

4.4.6 Audit et surveillance (Cm 32 à 35)

Excepté des adaptations terminologiques, les dispositions correspondantes restent inchangées.

Dans le domaine de la surveillance des assurances, les externalisations étaient jusqu'à présent contrôlées dans le cadre de la surveillance directe par la FINMA. Dans le sillage de la révision de la circulaire, la surveillance des assurances va introduire la surveillance indirecte pour les transferts à l'étranger, en complément de la surveillance directe, dans la mesure où, sinon, ces transactions pourraient être soustraites à la surveillance directe sur fond de libéralisation des transferts à l'étranger. C'est la raison pour laquelle la FINMA étudie entre autres s'il faut créer de nouveaux champs d'audit sur ce thème dans le cadre de la Circ.-FINMA 13/3.

En lien avec les externalisations par *cloud*, le besoin a parfois été exprimé d'adapter plus fortement les exigences de la circulaire portant sur les droits de contrôle aux besoins des prestataires de *cloud* (notamment en ce qui concerne l'exigence visée au Cm 32 d'un droit de regard et de contrôle intégral, permanent et sans entraves). La FINMA observe avec attention les développements dans le domaine de l'*outsourcing* par *cloud*. Le projet de révision renonce toutefois à de nouvelles adaptations spécifiques

au *cloud*, d'autant plus que la FINMA peut, dans des cas particuliers, reconnaître des exceptions à certaines dispositions de la circulaire (Cm 46). Par ailleurs, il a été délibérément conféré à la circulaire une forme neutre à l'égard de la technologie.

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

Lorsqu'une banque planifie de transférer à l'étranger le traitement de grandes quantités de CID, elle doit désormais en informer la FINMA au préalable. Le traitement de grandes quantités de CID par les banques est par ailleurs soumis au respect des dispositions de la Circ.-FINMA 08/21. Dans le cas des entreprises d'assurance, l'information intervient déjà dans le cadre de l'obligation d'autorisation pour les modifications du plan d'exploitation prévue par la loi (art. 5 al. 2 LSA en relation avec l'art. 5 OS).

Le second élargissement concerne la disponibilité et l'accès aux données dont le traitement a été transféré à l'étranger et qui sont indispensables en cas de liquidation ou d'assainissement de la banque ou de l'entreprise d'assurance concernées.

Au niveau des entreprises d'assurance, les données relatives aux polices et aux sinistres ainsi que celles concernant la fortune liée qui doivent être immédiatement disponibles dans le cas d'un assainissement ou d'une liquidation revêtent une importance particulière dans ce contexte. Sont également importantes les données nécessaires pour réaliser le bouclement statuaire et constater tout surendettement.

Par « accès », on entend la possibilité de lire les données et de pouvoir les traiter en Suisse. Les banques et les entreprises d'assurance doivent en outre organiser la conservation des données afin de garantir à tout moment les droits de regard des clients.

4.4.8 Contrat (Cm 39 à 45)

L'introduction d'une teneur minimale pour les contrats d'*outsourcing* concerne des mentions qui doivent également être portées à l'inventaire (Cm 21). Par ailleurs, les contrats d'*outsourcing* doivent être élaborés de manière à garantir le respect des exigences de la circulaire (cf. notamment les renvois figurant au Cm 41). C'est dans cette optique que s'inscrit le fait de n'autoriser le prestataire à faire appel à des personnes auxiliaires que si le respect de la circulaire reste garanti sur une base contractuelle.

Dans le cadre de la mise en œuvre des lignes directrices du CSF, des prescriptions minimales additionnelles relatives à la structure des contrats ont par ailleurs été formulées pour les banques d'importance systémique, avec un rôle important pour la continuité des prestations de services critiques en cas de liquidation, d'assainissement ou de restructuration. Il s'agit d'une part de s'assurer que les relations concernant les prestations de services critiques puissent être transférées à une banque de transition en cas d'assainissement afin de garantir leur bon fonctionnement. Il faut par ailleurs garantir par contrat que le fournisseur de prestations de services critiques ne puisse pas les suspendre à un moment inopportun, oblitérant ainsi le bon fonctionnement de la banque d'importance systémique.

5 Conséquences

Le fait que les exigences de la présente circulaire soient désormais généralement applicables aux externalisations internes au groupe représente une certaine charge liée à la mise en œuvre de ces dernières (que l'on pense à l'établissement du dispositif de sécurité, Cm 31) ainsi qu'à une charge d'audit accrue. Toutefois, rapportées à la réduction des risques, qu'il ne faut pas négliger même en cas d'externalisations au sein d'un groupe, elles semblent appropriées.

Aucun durcissement ou assouplissement matériel ne découle de la radiation des mesures relatives à la protection des données. La radiation du principe « Information des clients » représente un assouplissement pour les banques. En l'occurrence, il s'agit notamment de l'abandon du droit de résiliation extraordinaire, ordonnée conformément au droit de la surveillance, ainsi que de l'obligation d'informer, pour autant qu'elle ne découle pas d'autres sources de droit.

L'exigence qui impose que les données requises pour l'assainissement soient accessibles en Suisse peut nécessiter certaines adaptations notamment dans le domaine informatique. Toutefois, au vu des proportions accrues des externalisations, cette exigence apparaît comme centrale pour garantir l'efficacité de la surveillance ainsi que la capacité d'assainissement voire de liquidation des entreprises externalisatrices. Cette exigence est également proportionnelle. C'est celle qui est la moins contraignante parmi les différentes approches réglementaires (par ex. approbation préalable, restriction quantitative des externalisations, etc.) et elle est en outre fondée sur des principes, ce qui permet aux assujettis de décider eux-mêmes de la manière dont ils veulent la mettre en œuvre.

Les nouvelles prescriptions pour les banques d'importance systémique constituent en premier lieu une concrétisation des prescriptions légales fixées pour le plan d'urgence et devraient représenter une charge supplémentaire pour les banques concernées. La disposition qui interdit d'externaliser des prestations de services critiques auprès des banques du même groupe financier est une restriction pour les banques d'importance systémique qui apparaît toutefois proportionnée puisqu'elle contribue à garantir la stabilité des marchés financiers. Dans leur ensemble, les nouvelles prescriptions qui s'appliquent aux banques d'importance systémique sont le gage d'une plus grande sécurité en matière de continuité des fonctions d'importance systémique en cas de crise et visent à empêcher que les externalisations nuisent à la protection des créanciers, des investisseurs et du marché financier.

Concernant les entreprises d'assurance, la libéralisation permettant d'externaliser toutes les fonctions essentielles apporte des assouplissements. En contrepartie, une attention accrue est apportée à la disponibilité, à la lisibilité et à la sauvegarde des données vitales (Cm 38).