CUPSA | ASPC

COMMUNIQUÉ

17-COM-001 18 juillet 2017

Publication d'un guide pour l'impartition de services de technologies de l'information

L'Association des superviseurs prudentiels des caisses (ASPC) vient de publier un guide pour l'impartition de services de technologies de l'information (TI) regroupant les principes et pratiques de base pour la surveillance des ententes d'impartition dans les coopératives de crédit et les caisses populaires canadiennes.

Ces directives sont conformes aux normes internationales et peuvent être adaptées en fonction de la taille relative, de l'envergure, de la complexité et du profil de risque de l'institution.

L'ASPC encourage les coopératives de crédit et les caisses populaires canadiennes à envisager l'inclusion de ces principes, de ces pratiques et des rôles et des responsabilités décrits dans son guide aux structures de gestion des risques informatiques en vigueur chez eux.

Chaque organisme membre de l'ASPC peut choisir d'appliquer ce guide tel quel ou dans une version modifiée, à sa discrétion. L'ASPC continuera de se tenir informée sur les plus récentes études, la recherche et les directives internationales liées à la gestion du risque en TI.

À propos de l'ASPC

L'Association des superviseurs prudentiels des caisses (ASPC) est un regroupement interprovincial composé d'organismes d'assurance-dépôts et de superviseurs prudentiels répartis dans l'ensemble du Canada. L'ASPC œuvre à maintenir le caractère sain et durable du secteur des caisses canadiennes, au moyen d'actions concertées. Pour plus de renseignements, consultez le site Web de l'ASPC, www.ASPC-aspc.ca.

Guide pour l'impartition de services de technologies de l'information

Présentation

L'impartition a lieu lorsqu'une procédure ou une fonction qui pourrait être effectuée par une coopérative de crédit ou une caisse populaire est confiée à un fournisseur de services. Cette pratique rend la coopérative de crédit ou la caisse populaire plus dépendante de tiers, ce qui peut entraîner une augmentation des risques. Toutefois, l'impartition ne soustrait pas la coopérative de crédit ou la caisse populaire de sa responsabilité en dernier ressort envers les fonctions informatiques.

Ce document a été créé pour accroître la sensibilisation aux concepts liés à l'impartition dans le contexte des technologies de l'information et pour aider les gestionnaires de haut niveau à envisager le recours à des ressources externes au sein de leur institution. Les directives qu'il contient s'appliquent aux ententes d'impartition d'importance dans le secteur des TI.

Ce guide peut être adapté en fonction de la taille relative, de l'envergure, de la complexité et du profil de risque de chaque institution. En plus du présent document, l'ASPC encourage les coopératives de crédit et les caisses populaires à consulter les documents de même nature préparés par d'autres organismes de réglementation.

Principes et pratiques de l'impartition dans le secteur des TI

Le conseil d'administration et la haute direction des coopératives de crédit et des caisses populaires sont ultimement responsables de toutes les fonctions et services informatiques confiés à des tiers. La haute direction de l'institution doit aussi veiller à ce que toutes les ententes d'impartition respectent les exigences légales et réglementaires.

Politique d'impartition

Les coopératives de crédit et les caisses populaires devraient élaborer une politique en matière d'impartition, dans laquelle les points suivants pourraient être abordés :

- critères pour le choix des fournisseurs en entreprises partenaires (diligence appropriée);
- confidentialité, sécurité et protection des renseignements;
- accès aux bureaux et aux ressources informatiques;
- précision du travail accompli et respect des échéanciers;
- surveillance du rendement et vérifications prévues pour les contrats importants;

- résolution des différends.

Une politique d'impartition devrait aussi préciser les critères visant à établir si une responsabilité confiée à un tiers est suffisamment importante pour faire l'objet de vérifications supplémentaires comme un contrat écrit officiel et un droit de vérification.

Une bonne politique en matière d'impartition aidera la direction à préciser, mesurer, atténuer et contrôler les risques associés à l'impartition. Elle devrait, plus précisément, assurer la continuité de toute activité d'exploitation confiée à un tiers.

Importance relative

La gestion de tout risque associé à l'impartition dépend de l'importance relative de l'entente qui la régit. L'importance relative peut être établie en fonction d'un certain nombre de facteurs, notamment :

- l'effet de l'entente sur la situation financière, la réputation et les activités de la coopérative de crédit ou la caisse populaire si le fournisseur de services manque à ses obligations durant une certaine période de temps;
- la capacité de la coopérative de crédit ou de la caisse populaire à maintenir ses contrôles internes et à respecter les exigences réglementaires si le fournisseur de services manque à ses obligations;
- le coût des services impartis et le coût de remplacement éventuel du fournisseur de services;
- la difficulté et le délai nécessaire pour trouver un autre fournisseur de services ou pour ramener à l'interne les tâches à accomplir;
- le risque de concentration entraîné par le recours à un seul fournisseur de services à qui sont confiées de multiples fonctions.

Des directives supplémentaires visant à évaluer l'importance d'un contrat sont jointes à l'**annexe 1** du présent document.

Diligence appropriée

Les ententes d'impartition importantes doivent faire l'objet de diligence raisonnable. Les coopératives de crédit et les caisses populaires devraient évaluer si un fournisseur de services possède la capacité, l'expertise et l'expérience nécessaires pour mener à bien le mandat qui lui a été imparti. Cet examen devrait tenir compte de critères qualitatifs (sur le plan opérationnel, par exemple) et quantitatifs (sur le plan financier, entre autres). Cet

examen devrait être réalisé à nouveau lors de la renégociation ou du renouvellement de toute entente d'impartition.

Le processus de diligence raisonnable variera en fonction de l'importance relative des responsabilités imparties. Des contrôles très stricts doivent être exercés lorsqu'un fournisseur de services exécute, par exemple, des fonctions bancaires essentielles.

Les coopératives de crédit et les caisses populaires doivent exercer un contrôle sur les ententes d'impartition afin de s'assurer que les fournisseurs de services respectent leurs obligations contractuelles et offrent le niveau de services attendu.

Les facteurs dont il faut tenir compte dans le cadre du processus de diligence raisonnable pourraient inclure, entre autres :

- L'expérience et les compétences techniques du fournisseur de services; ces critères peuvent inclure la réputation du fournisseur (plaintes, litiges en suspens), la précision, la sécurité, la protection de la vie privée et la confidentialité.
- La viabilité du fournisseur de services qui peut inclure, notamment :
    - sa stabilité financière (p. ex. états financiers vérifiés les plus récents);
    - ses mécanismes de contrôle interne et de surveillance;
    - les mesures mises en place pour la reprise des activités et en cas d'urgence; les conséquences d'une non-exécution devraient aussi être prises en compte.
- La philosophie d'entreprise et la culture du fournisseur de services, ainsi que la façon dont celles-ci s'harmonisent à celles de la coopérative de crédit ou de la caisse populaire (p. ex. partagent-ils un engagement similaire en matière de gestion des risques?).

Ententes contractuelles

L'une des principales méthodes de gestion des risques associés à l'impartition consiste à disposer d'un contrat écrit clair avec le fournisseur de services. Toutes les activités d'importance imparties doivent, au minimum, faire l'objet d'un contrat écrit officiel[1].

Les contrats avec les fournisseurs de services peuvent inclure les éléments suivants :

- la nature et l'étendue du service imparti;
- les questions de sous-traitance;

[1]On trouvera des renseignements supplémentaires à ce sujet dans le document *Key Attributes of Effective Resolution Regimes for Financial Institutions* du Financial Stability Board daté du 15 octobre 2014.

- les mesures de rendement et les exigences relatives aux déclarations;
- le mécanisme de résolution des différends, y compris en ce qui concerne la non-exécution et la résiliation;
- les questions de propriété et d'accès aux actifs;
- la vérification et les droits d'accès;
- les questions de confidentialité, de protection de la vie privée et de sécurité;
- le prix et la question des assurances.

Lorsqu'une fonction informatique est impartie, surtout lorsqu'il s'agit d'une fonction bancaire, une coopérative de crédit ou une caisse populaire devrait se concentrer sur les questions contractuelles afin d'assurer la sécurité et la continuité du service :

Confidentialité, protection de la vie privée, sécurité

Le contrat devrait préciser quelle partie est responsable de la sécurité et de la confidentialité des données de la coopérative de crédit ou de la caisse populaire et de celles de leurs membres. On devrait y préciser notamment :

- l'étendue et la définition de l'information à protéger;
- les obligations respectives des parties, y compris les procédures;
- la responsabilité pour les pertes entraînées par une infraction à la sécurité;
- les processus de notification en cas d'infraction.

Pour assurer la confidentialité et la sécurité des données, le contrat doit livrer les détails des mesures pour isoler les données et les fonctions de la coopérative de crédit ou de la caisse populaire de celles du fournisseur de services.

Plan opérationnel d'urgence

Le contrat devrait inclure les détails des mesures et des ressources du fournisseur de services pour assurer la continuité des fonctions imparties. La coopérative de crédit ou la caisse populaire pourrait exiger du fournisseur de services de procéder régulièrement à des essais de son plan de reprise après sinistre. La coopérative de crédit ou la caisse populaire qui impartit des fonctions de son système bancaire devrait accorder une attention particulière à la planification de ses mesures d'urgence. Pour plus de renseignements, veuillez consulter le *Guide de planification de la reprise après sinistre* de l'ASPC.

Propriété, accès et droits de vérification

Le contrat devrait établir qui détient les droits de propriété des actifs pertinents tels que les codes sources, les applications et les rapports (y compris les actifs issus des données de la coopérative de crédit ou de la caisse populaire).

Le contrat devrait également préciser les droits d'utilisation du fournisseur de services des actifs de la coopérative de crédit ou de la caisse populaire, y compris les données des membres et les droits d'accès de la coopérative de crédit ou de la caisse populaire à ses propres actifs. Les droits des parties de se vérifier l'une l'autre devraient aussi être précisés. Pour les fonctions critiques telles que celles qui touchent les systèmes bancaires, le contrat doit inclure le droit de la coopérative de crédit ou de la caisse populaire de vérifier ou d'obtenir les résultats d'audit de l'environnement de contrôle interne du fournisseur de services.

Sous-traitance

Le contrat doit préciser les règles et les limites régissant les responsabilités confiées à la sous-traitance. Si la sous-traitance est permise, le contrat doit préciser que toutes les obligations relatives au respect de la vie privée, à la sécurité, à l'accès et aux obligations de vérification s'appliquent au sous-traitant.

Rôles et responsabilités dans le cadre de l'impartition de services de TI

Une compréhension rigoureuse des rôles et responsabilités appropriés est essentielle à une impartition efficace des fonctions administratives. L'ASPC a établi les principaux rôles et responsabilités[2] comme suit :

Conseil d'administration/comité de vérification

- Approuve et revoit régulièrement les politiques qui s'appliquent à l'impartition;
- Maintient la sensibilisation aux contrats d'envergure qui sont impartis.
- Veille à ce que la direction donne suite aux grandes conclusions issues de rapports pertinents traitant des ententes d'impartition.
- Prend connaissance des rapports des gestionnaires concernant les ententes d'impartition, notamment les conclusions de rapports de vérification interne et des rapports sur l'efficacité du contexte de contrôle chez les fournisseurs indépendants.

[2]Les rôles et responsabilités décrits dans le présent document devraient être adaptés en fonction de la taille, de l'envergure et de la complexité propres à chaque coopérative de crédit ou caisse populaire.

Haute direction

- Établir le moyen le plus efficace d'exécuter les fonctions administratives essentielles (recourir à l'interne ou décider d'aller vers l'impartition).
- Comprendre la relation entre les fournisseurs indépendants de services bancaires (p. ex. les entreprises avec qui la coopérative de crédit ou la caisse populaire a une relation contractuelle directe) et d'autres grands fournisseurs de services bancaires offrant du soutien et des solutions intégrées ou qui sont reliées (p. ex. les entreprises avec qui la coopérative de crédit ou la caisse populaire n'a pas de relation contractuelle directe).
- Élaborer des politiques d'impartition qu'approuvera le conseil d'administration et mettre en œuvre des politiques et des procédures pour l'impartition et les contrats.
- Fournir au conseil des rapports réguliers sur les risques informatiques les plus importants.

Vérification interne

- Puisque la vérification interne doit pouvoir se pencher sur tous les principaux processus et activités administratifs d'importance, toutes les fonctions imparties devraient faire l'objet des vérifications appropriées.

Tiers fournisseurs de services

- Offrir l'assurance et, au besoin, des rapports de vérification sur les produits et les services qu'ils offrent aux coopératives de crédit et aux caisses populaires.

Organismes de réglementation

- Offrir l'encadrement et assurer la surveillance des pratiques exemplaires relatives aux ententes d'impartition.

CUPSA | ASPC

Annexe 1 – Exemples d'ententes d'impartition importantes

*Inspirés des lignes directrices B-10 du Bureau du surintendant des institutions financières.

Les ententes d'impartition de grande importance peuvent porter, par exemple, sur les éléments suivants :

- gestion et entretien des systèmes d'information (p. ex. saisie et traitement de données, centre de données, gestion des locaux, soutien des utilisateurs, centres de dépannage);
- traitement de documents (p. ex. chèques, reçus de cartes de crédit, paiement de factures, relevés de compte bancaire, autres paiements d'entreprise);
- traitement de demandes (p. ex. polices d'assurance, prêts, cartes de crédit);
- administration des prêts (p. ex. négociation et traitement des prêts, gestion des garanties, recouvrement);
- gestion de placements (p. ex. gestion de portefeuilles, gestion de liquidités);
- gestion administrative (p. ex. virements électroniques de fonds, traitement de la paye, opérations d'intendance, contrôle de la qualité, achats);
- ressources humaines (p. ex. administration des avantages sociaux, recrutement).

Les lignes directrices pour la gestion des risques associés à l'impartition ne s'appliquent pas, de façon générale, aux éléments suivants :

- les ententes de compensation et de règlement entre les membres ou les participants à des systèmes de compensation et de règlement reconnus;
- les services de messagerie, d'impression, de poste régulière, les services publics et la téléphonie;
- les services de formation spécialisés;
- les services consultatifs tels que les opinions juridiques, certains services-conseils en placements qui n'entraînent pas directement de décisions d'investissements tels que les avis juridiques, certains services-conseils de placement, les évaluations indépendantes ou les syndics de faillite;
- l'achat de biens, de matériel, de logiciels, de logiciels commerciaux et d'autres produits;
- les services d'enquête sur les antécédents de crédit et les antécédents, et les services d'information;
- la réparation et l'entretien d'immobilisations;
- l'entretien et le soutien liés aux logiciels sous licence;
- l'aide temporaire et le personnel contractuel;
- le recrutement spécialisé.