CUPSA | ASPC

COMMUNIQUÉ

14-COM-002 14 juillet 2014

Lignes directrices relatives à la gouvernance des technologies de l'information (TI)

L'Association des superviseurs prudentiels des caisses (ASPC) a créé un groupe de travail sur les risques liés aux technologies de l'information (TI), qui se concentre sur les pratiques de gouvernance et de gestion des risques des TI au sein des caisses du Canada.

Ce comité a reçu le mandat de définir des moyens d'accroître la sensibilisation à l'importance des pratiques de gestion des risques en matière de TI dans les caisses, ainsi que d'accroître la priorité que les organismes de réglementation des caisses provinciales accordent à la gouvernance et à la surveillance des technologies de l'information.

Les membres de l'ASPC reconnaissent que la gouvernance et la gestion des risques en matière de TI constituent une activité opérationnelle essentielle qui contribue au succès des caisses. Les membres ont décidé d'accorder une plus grande importance et une priorité plus élevée aux pratiques de gouvernance et de gestion des risques des TI au sein des institutions financières coopératives canadiennes.

Dans sa première étape, l'ASPC publie une ligne directrice relative à la gouvernance des technologies de l'information, ayant pour objectif de présenter les principes de base de la gouvernance des TI, et de définir les rôles et les responsabilités des principaux intervenants. Ces orientations sont destinées aux conseils d'administration et sont adaptables à la taille, à la nature, la complexité et au profil de risque des caisses sur une base individuelle.

Au fur et à mesure des avancées du groupe de travail, l'ASPC pourrait présenter des lignes directrices sur d'autres sujets, notamment sur l'audit des TI, l'impartition, la gestion et la sécurité des réseaux informatiques, de même que la planification de la continuité des activités (PCA) et le plan de reprise après catastrophe (PRC).

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 de 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 à www.cupsa-aspc.ca.

Principes directeurs, rôles et responsabilités
Gouvernance des technologies de l'information

La gouvernance des technologies de l'information (TI) est un sous-ensemble de la gouvernance d'entreprise axé sur les TI et leur harmonisation avec les objectifs de l'entreprise et les pratiques efficaces de gestion du risque. La mission de la gouvernance des TI est : d'harmoniser les investissements en TI et leurs priorités avec les objectifs et la stratégie de l'organisation, de hiérarchiser et de gérer les demandes de services de TI qui optimisent le rendement de l'organisation, de gérer les principaux risques et menaces de façon proactive, d'assurer une utilisation responsable des ressources et des actifs et d'améliorer le rendement organisationnel des TI.

L'Association des superviseurs prudentiels des caisses (ASPC) présente cette ligne directrice afin de permettre aux institutions de mieux comprendre les principes de la surveillance efficace de la gouvernance des TI et l'attribution appropriée des rôles et des responsabilités. Les pratiques et les principes décrits dans ces orientations sont conçus de façon à s'adapter à la taille, à la nature, à la complexité et au profil de risque d'une institution, et ils sont conformes aux principes de gouvernance des TI définis par l'*IT Governance Institute* (*ITGI*).

Principe directeur n^{o} 1 – Alignement stratégique

L'alignement stratégique permet que les initiatives et les normes relatives aux TI soutiennent la stratégie et les objectifs de l'institution. Cela implique donc :

- Obtenir l'appui de la haute direction en ce qui concerne les TI.
- Comprendre les besoins de l'entreprise.
- Élaborer une stratégie et des objectifs pour les TI.

Les pratiques courantes pourraient comprendre :

- L'assurance que les TI font partie du processus de planification stratégique.
- L'alignement de la stratégie en matière de TI avec les objectifs organisationnels.
- L'existence d'un comité directeur des TI.

Principe directeur n^{o} 2 – Création de valeur

Grâce à la création de valeur, l'investissement dans les TI apporte de la valeur en sélectionnant judicieusement les investissements et en les gérant sur tout leur cycle de vie. La création de valeur efficace assure que les projets TI sont terminés à temps, respectent les budgets et répondent aux attentes. Cela implique donc :

- Définir les éléments déclencheurs et les objectifs du projet.
- Définir les éléments déclencheurs et les objectifs de la prestation de services.

- Surveiller la gestion du projet et les objectifs de prestation.
- Favoriser les communications à propos de la valeur des TI.

Les pratiques courantes pourraient comprendre :

- L'identification efficace des besoins;
- des plans de communication pour les nouveaux projets;
- le suivi et la divulgation des projets TI;
- l'atteinte des objectifs établis des projets TI;
- la phase de réalisation des avantages comprise dans les procédures de fermeture des projets.

Principe directeur n^{o} 3 – Gestion du risque

La gestion du risque favorise la protection des biens TI, la reprise après catastrophe et la continuité des activités, notamment la sécurité et l'intégrité des informations. Cela implique :

- Déterminer la tolérance pour le risque de l'institution, en ce qui concerne les TI.
- Définir les stratégies en matière de sécurité de l'information et de gestion des risques des TI.
- Surveiller la mise en œuvre des stratégies de gestion des risques des TI.
- Comprendre les mandats de conformité et de réglementation.
- S'assurer que les informations sont gérées selon des pratiques efficaces de contrôle de la qualité.
- Collaborer avec les fonctions d'audit informatique et les superviseurs.

Les pratiques courantes pourraient comprendre :

- l'établissement de procédures de contrôle des changements;
- la détermination de l'appétit pour le risque en matière de TI et l'élaboration de stratégies d'atténuation faisant parties du cadre de gestion intégrée du risque de l'institution;
- des processus de conformité à la règlementation;
- l'existence d'un cadre de gouvernance des données;
- des politiques de classification de l'information (types de données et niveaux d'accès);
- documentation sur l'analyse des répercussions sur les activités;
- des processus de gestion de la sécurité de l'information (confidentialité, classification, etc.);
- des procédures établies pour la planification de la continuité des activités et de reprise après catastrophe, et pour la gestion des incidents et le recours à la hiérarchie.

Principe directeur n^{o} 4 – Gestion des ressources

La gestion des ressources examine l'optimisation de l'utilisation et de l'allocation des ressources TI, et la façon dont l'institution gère et distribue les ressources TI essentielles. Cela implique :

- Surveiller l'attribution des ressources et la gestion du portefeuille.
- Gérer les actifs informationnels (« *hardware* et *software* »).
- Veiller sur les tiers fournisseurs de services et les ententes d'impartition.
- Mettre en œuvre les normes d'architecture standardisée.

Les pratiques courantes pourraient comprendre :

- un personnel adéquat pour la gestion de TI, tant à l'interne qu'à partir d'ententes d'impartition;
- des processus de prestation de services;
- la planification et l'attribution des ressources;
- des budgets opérationnels et d'investissements des TI;
- des protocoles de gestion des actifs TI;
- des ententes sur les niveaux de service (ENS) avec tous les fournisseurs indépendants;
- des rapports de confirmation présentés par tous les tiers fournisseurs de services.

Principe directeur n^{o} 5 – Gestion du rendement

La gestion du rendement vise à examiner les procédures suivies par le personnel de TI en ce qui concerne : la surveillance de leur stratégie de mise en œuvre des TI, l'évaluation de la réussite des projets, et la vérification du niveau de prestation de services de qualité observé. Cela implique :

- Assurer la satisfaction des clients.
- Maintenir les niveaux de service prévus.
- Évaluer la valeur commerciale de la prestation de services.
- Encourager les initiatives d'amélioration des processus TI.

Les pratiques courantes pourraient comprendre :

- des mesures de la gestion du rendement des TI;
- des rapports sur le rendement des TI;
- une liste recensant des processus identifiés avec les améliorations proposées;
- l'inclusion de l'efficacité de la gestion du rendement dans l'étendue de l'audit.

CUPSA | ASPC

Rôles et responsabilités dans la gouvernance des TI

Une bonne compréhension de l'adéquation des rôles et des responsabilités est indispensable à un cadre de gouvernance efficace des TI. Voici les principaux rôles et responsabilités établis par l'ASPC :

Conseil d'administration :

- Examiner et approuver une stratégie de gouvernance et des politiques des TI, visant leur utilisation efficace.
- Examiner les rapports sur les progrès des initiatives stratégiques.
- Évaluer et surveiller l'alignement entre les objectifs organisationnels et les priorités des TI ainsi que le processus de prise de décision.
- S'assurer que la gouvernance des TI est incluse dans le cadre de contrôle interne.

Haute direction

- Planifier, prioriser et organiser des projets de TI, puis attribuer des budgets adéquats à ces projets au sein de l'institution.
- Dédier des ressources à la réalisation des initiatives de TI.
- Présenter au conseil d'administration des rapports sur le rendement, l'efficacité et la sécurité de l'infrastructure des TI.
- Présenter au conseil d'administration des rapports sur le progrès des principales initiatives stratégiques relatifs aux TI (p.ex., migrations entre les systèmes bancaires, nouveaux produits, etc.).

Audits interne et externe

- Évaluer la structure et l'efficacité du contrôle interne du système.
- Confirmer que l'infrastructure des TI protège les actifs, conserve l'intégrité des données et fonctionne efficacement, dans le but d'atteindre les objectifs organisationnels.

Tiers fournisseurs de services

- Présenter aux institutions des rapports qui confirment que les produits hébergés ou externalisés ont fait l'objet d'une vérification et d'une évaluation adéquates.

Autorités de réglementation

- Fournir des normes de saines pratiques d'affaires pour la gouvernance et la gestion du risque des TI.
- Évaluer le respect des normes sur les saines pratiques d'affaires en matière de gouvernance et de gestion du risque des TI.

- Prendre des mesures de supervision appropriées et collaborer avec les institutions afin d’assurer leur mise en œuvre de saines pratiques d’affaires pour la gouvernance et la gestion du risque des TI.