Ontario

Deposit Insurance Corporation of Ontario

Société ontarienne d'assurance-dépôts

NORMES DE SAINES PRATIQUES COMMERCIALES ET FINANCIÈRES

Cadre de la GESTION DU RISQUE D'ENTREPRISE

Janvier 2018

This document is also available in English.

Avertissement

Le présent document constitue un outil de référence pour aider les caisses populaires et credit unions de l'Ontario à mettre au point un cadre approprié de gestion du risque d'entreprise. Il ne se substitue à aucune des dispositions de la *Loi sur les caisses populaires et les credit unions*, au Règlement pris en application de cette loi, ni à aucune autre disposition juridique touchant les caisses populaires et credit unions de l'Ontario. La SOAD s'est efforcée de bonne foi de rédiger ce document dans les limites de ses pouvoirs légaux, mais elle n'émet à cet égard aucune assertion, garantie ou condition explicite ou implicite.

Remerciements

Nous voulons remercier les personnes suivantes pour leur aide dans la préparation de ce document :

Richard Adam (Northern); Martin Blais (Fédération des caisses Desjardins du Québec); Gay Chong (Windsor Family); Leo Gautreau (Meridian); Ron Hodges (Italian Canadian); Gérald Morin (Alterna); Luc Racette (L'Alliance des caisses populaires de l'Ontario Limitée); Sandy Shaw (First Ontario); Julian Sellers (Kawartha) et Fay Booker (Booker and Associates).

TABLE DES MATIÈRES

Aperçu

Mise en application

Ce document vise à fournir les lignes directrices pour la mise en œuvre d'un programme efficace de gestion du risque d'entreprise (GRE) à l'intention de **toutes les** caisses. Ce cadre de GRE devrait être utilisé en conjonction avec le guide d'application de GRE. Les principes de base décrits dans ces documents et la méthodologie et le processus adoptés devront être modifiés et convenablement adaptés pour refléter la taille et la complexité d'une caisse. La gamme des produits et services offerts aux sociétaires, la structure du capital, la couverture géographique, les stratégies de fonctionnement et la technologie devront également être prises en considération.

Avec la croissance en taille et en complexité d'une caisse, le programme de GRE devrait évoluer pour s'assurer que tous les risques émergents et croissants soient convenablement pris en compte et traités dans le cadre d'un processus continu d'examen et d'évaluation. En instaurant un processus de gestion convenable et efficace du risque d'entreprise, les **caisses** devraient prendre en compte les principes directeurs décrits à l'Annexe A.

Définitions

Le risque est un événement ou une activité qui peut avoir une incidence sur la capacité de la caisse à mener efficacement ses stratégies et à atteindre ses objectifs ou qui peut la faire manquer une opportunité importante.

La gestion du risque est un processus continu, impliquant le conseil d'administration de la caisse, la direction et d'autres membres du personnel. La gestion du risque constitue une démarche systématique permettant d'établir de meilleurs plans d'action en déterminant et évaluant les questions liées au risque/événements susceptibles d'avoir une incidence sur l'atteinte des objectifs d'affaires d'une organisation, en acquérant des connaissances à leur sujet, en agissant par rapport à ces questions et en les communiquant.

La propension au risque est le degré de risque, sur une large échelle, qu'une caisse est disposée à accepter ou à prendre dans la poursuite de ses buts.

La tolérance au risque est le niveau de risque que la caisse est prête à accepter dans différents domaines de risque. Elle se mesure en termes à la fois quantitatifs et qualitatifs.

Le chef de la direction des risques, s'il y a lieu, est normalement la personne responsable de la coordination et de la supervision de la gestion du processus de GRE ainsi que de l'approbation des rapports au comité d'audit.

Introduction

La gestion du risque d'entreprise est définie[1] comme : (traduction)

". . . un processus, conclu par le conseil d'administration, la direction et d'autres membres du personnel d'une entité, appliqué dans la mise en œuvre d'une stratégie pour l'ensemble de l'entreprise, conçu pour identifier des événements potentiels qui peuvent affecter l'entité et pour gérer le risque afin de rester dans les limites de sa propension au risque, pour fournir une assurance raisonnable en termes d'atteinte de ses objectifs. »

En résumé, la GRE :

- est un processus exhaustif, systématique, discipliné et proactif, utilisé pour identifier, évaluer, gérer et faire des rapports sur les risques importants aux niveaux stratégiques, commerciaux et des processus en rapport avec l'atteinte des objectifs de la caisse qui sont inhérents à la stratégie et à l'exploitation commerciales à un moment quelconque;
- est un processus de prise de décision pour la mesure et le traitement de toute variation (positive ou négative) par rapport aux objectifs visés de la caisse;
- constitue une base pour les processus de prise de décision de la caisse depuis le développement de sa stratégie et de ses objectifs jusqu'aux activités quotidiennes, la routine de la création de rapports et la conformité;
- permet à la direction de faire une utilisation/répartition plus efficace du capital et des ressources au sein de l'organisation afin d'optimiser les niveaux de capitalisation;
- optimise la gestion du risque en équilibrant le coût du risque avec celui du contrôle de tous les aspects des domaines de risque potentiel de la caisse afin de s'assurer que les objectifs organisationnels sont atteints;
- est une partie intégrante d'une gestion commerciale et financière depuis le processus de planification stratégique jusqu'aux activités quotidiennes de la caisse contribuant à l'identification et à la gestion de tous les risques et occasions matérielles internes et externes qui peuvent avoir une incidence sur son rendement, sa réputation et sa viabilité;
- cherche à améliorer et à préserver la viabilité à long terme de la caisse;
- est une responsabilité fondamentale du conseil d'administration et de la haute direction.

La GRE implique, à l'échelle de l'entreprise, une vue proactive et holistique de tous les risques et de l'appétit et de la tolérance au risque qui leur sont associés, afin d'assurer qu'ils soient complètement alignés aux objectifs et stratégies de la caisse; elle reflète la qualité, les compétences et les capacités des gens, de la technologie et du capital. La GRE aide également à identifier l'interdépendance et l'interaction des risques à travers

[1] Committee of Sponsoring Organizations (COSO) ERM Integrated Framework Document 2004

l'organisation et procure les outils permettant de rationaliser les activités de gestion du risque.

Objectifs

Le but de la GRE est de créer, protéger et améliorer la valeur pour le sociétaire et la viabilité de la caisse en gérant les incertitudes qui pourraient influencer l'atteinte des objectifs. La mise en œuvre d'une GRE efficace permet la réalisation des objectifs clés suivants :

Supervision : Tous les risques critiques ont été définis et sont actuellement gérés et surveillés de manière holistique, conformément à l'énoncé sur la propension au risque approuvé par le conseil d'administration.

Propriété et responsabilité : L'appropriation du risque est dévolue à des membres de la direction qui sont responsables d'identifier, évaluer, atténuer et faire des rapports sur l'exposition au risque.

Assurance : Le conseil d'administration, la direction et les sociétaires ont l'assurance raisonnable que le risque est géré de manière convenable dans des limites définies afin d'apporter de la valeur à l'organisation**.**

Avantages

Une caisse qui réussit à mettre en œuvre la GRE devrait s'attendre aux avantages suivants :

- Une utilisation plus efficace du capital et des ressources
- Une réduction vraisemblable des pertes d'exploitation
- Une diminution des coûts de conformité/audit
- Une détection plus rapide des activités illégales
- Moins de surprises
- L'accent mis sur la prévention à faible coût plutôt que sur les stratégies onéreuses de résolution
- Des économies par l'utilisation de renseignements sur le risque afin de simplifier et améliorer les processus
- L'augmentation de la sensibilisation et une vision intégrée des risques (existants et émergents)
- Une approche systématique et reproductible pour atténuer les risques et cerner les possibilités.
- Des décisions plus simples et éclairées

En étant informés, le conseil d'administration et la haute direction peuvent se montrer proactifs lorsqu'il s'agit de faire face aux risques et opportunités importants auxquels est confrontée la caisse en tant qu'institution financière. La GRE aide le conseil d'administration à cerner les questions liées au risque à priorité élevée et stratégiquement importantes. Les caisses peuvent identifier à qui appartient le risque et la meilleure manière d'y faire face à travers un processus exhaustif d'identification et d'évaluation du risque. Ceci assure que le niveau le plus convenable et optimal des ressources est affecté à des domaines de plus grand risque. La gestion du risque d'entreprise permet d'identifier les opportunités et aussi les risques.

Pour être efficace et ne pas créer de coûts indirects supplémentaires, la GRE devrait être intégrée dans les processus existants au sein de la caisse qui soutiennent des activités telles que la planification stratégique, la planification des activités, la surveillance de la conformité, la mesure du rendement et la reconfiguration des processus. Ériger la GRE dans des processus existants augmente la sensibilisation et la sensibilité au risque et aide à créer une culture là où le risque est évalué et géré de manière proactive à tous les niveaux.

Rôles et responsabilités

Les rôles et responsabilités clés du conseil d'administration et de la direction sont résumés dans le Tableau A ci-dessous.

TABLEAU A: Rôles et responsabilités clés de la GRE

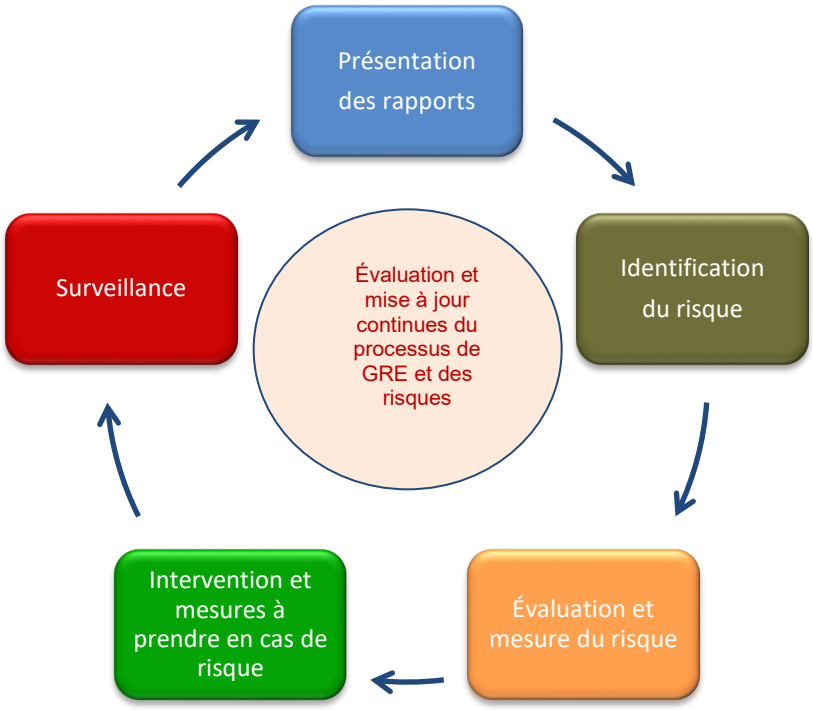
Le conseil d'administration assure la gouvernance du profil de risque de la caisse	La direction prend des mesures pour gérer les risques et les porter à un niveau acceptable
Superviser le cadre du risque d'entreprise – prendre de l'assurance sur son efficacité	Développer un processus de mise en œuvre de la gestion du risque d'entreprise à la caisse
Mettre en place, approuver, mettre annuellement à jour la politique qui régit le risque d'entreprise	Répartir les responsabilités pour l'appropriation du risque, la surveillance du risque, les rapports sur le risque
Faire clairement état de la propension/tolérance au risque dans la politique	Identifier le processus pour développer le profil de risque
Mieux comprendre le profil de risque global de la caisse aux niveaux inhérent et résiduel	Mettre en œuvre le processus pour développer le profil de risque et pour évaluer la gravité de chaque risque
Mieux comprendre les risques importants aux niveaux inhérent et résiduel	Mettre en œuvre le processus pour déterminer les réactions au risque et identifier si des mesures supplémentaires sont requises
Comprendre le niveau d'amortisseur de risque (capital) quant au risque résiduel total de la caisse	Déterminer le niveau d'amortisseur de risque (capital) en place et faire des recommandations là où il est insuffisant

Approuver l'acceptation des risques résiduels ou des mesures directes de réponse au risque supplémentaire là où le niveau résiduel est supérieur à la propension/tolérance établie au risque	Présenter au conseil d'administration le profil de risque de la caisse, notamment les risques notables au niveau inhérent et résiduel
Obtenir l'assurance que la direction a entrepris de mettre en œuvre les réponses au risque, tel qu'elles ont été présentées	Prendre des mesures et surveiller afin de vous assurer que les réponses au risque fonctionnent de manière efficace et continue
Surveiller les indicateurs de risque pour les risques connus notables sur une base trimestrielle et plus fréquemment lorsqu'il s'agit de risques spécifiques lorsque des problèmes surviennent	Présenter des rapports périodiques au conseil d'administration, qui montrent les indicateurs de risque et le niveau de risque par catégorie
Surveiller les risques émergents et discuter avec la direction de leurs implications	Présenter les renseignements sur les risques émergents au conseil d'administration

Le processus

La GRE est un processus continu et cyclique. Le conseil d'administration et la haute direction donnent le ton de la gestion du risque d'entreprise à la caisse. Ceci comprend la détermination de la propension au risque de la caisse et la façon d'identifier, mesurer et gérer les risques. Le processus de GRE comporte cinq étapes principales, tel qu'indiqué au Tableau B. Il est également important de s'assurer que le processus de GRE et les risques soient régulièrement réévalués et mis à jour afin de refléter les nouveaux renseignements et expériences pour que tous les risques notables soient convenablement identifiés et traités et qu'aucune opportunité matérielle ne soit omise.

TABLEAU B : Cycle de gestion du risque d'entreprise

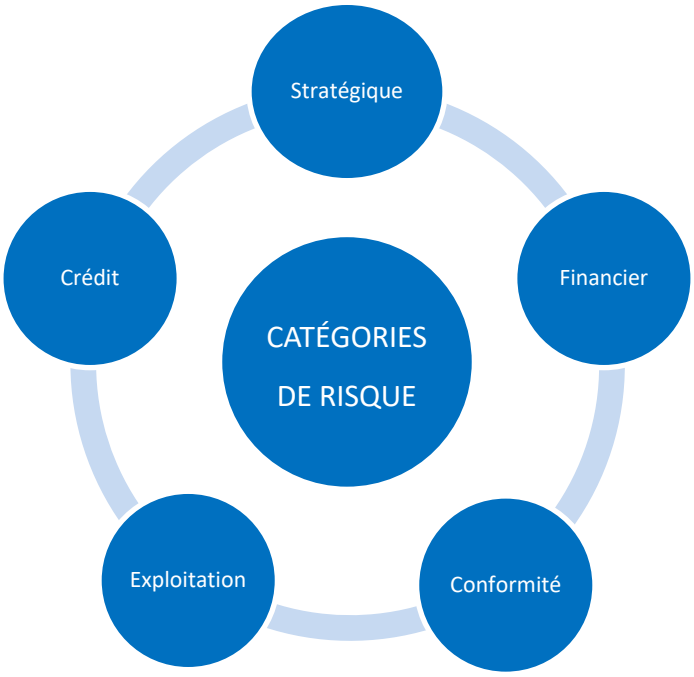


Le processus nécessite l'implication à tous les niveaux de la caisse; il exige la volonté de comprendre les risques auxquels fait face la caisse, d'aider à la création des réponses appropriées aux risques et de leur maintien dans des limites de propension et de tolérance au risque définies par le conseil d'administration et la haute direction.

Identification du risque

L'identification des risques devrait être faite sur une base continue pour les processus existants et de façon ponctuelle selon le besoin pour l'introduction de nouveaux produits, les projets ou les modifications des produits et processus existants. Il y a plusieurs techniques qui peuvent être utilisées pour aider à identifier les risques, notamment les questionnaires d'auto-évaluation, les sondages, les ateliers et les entretiens. Pour aider à l'identification du risque, les risques doivent être envisagés dans les catégories principales de risque, telles que les risques stratégiques, de crédit, financiers, d'exploitation et de conformité.

TABLEAU C: Échantillon de catégories principales de risque



Évaluation et mesure du risque

L'évaluation du risque comprend la prise en compte de la probabilité qu'un risque se produise et des conséquences de ce risque sur la réalisation des objectifs d'une caisse dans un délai donné. La probabilité de réalisation se base généralement sur la fréquence (nombre d'occurrences) d'apparition possible du risque sur un horizon temporel donné tel que le trimestre, la journée, le semestre, etc. Une probabilité ou fréquence plus élevée de réalisation de l'événement entraînera des pondérations de risque plus élevées. Un événement que l'on s'attend à voir apparaître d'un moment à l'autre se traduira aussi par une vraisemblance (probabilité) plus élevée.

L'incidence de la réalisation est généralement présentée sous forme d'un montant de perte en dollars ou un pourcentage d'incidence sur le bénéfice ou le capital; elle peut cependant être également définie en termes qualitatifs (p. ex. la réputation, la qualité du service, la conformité à la réglementation, etc.) quand on regarde sous l'angle des conséquences de la réalisation de l'événement à risque. L'ampleur ou la gravité d'un risque est basée sur le produit de sa vraisemblance (ou probabilité) et de son incidence.

Intervention et mesures à prendre en cas de risque

Pour chaque risque identifié, la caisse doit établir des choix de « réponse » adéquats afin d'optimiser la gestion du risque. Ils varient d' « accepter » à « éviter ».

Quatre choix possibles de réponse sont identifiés au Tableau D ci-dessous.

TABLEAU D : Échantillon de définitions de réponse au risque

Réponse	Définition
Accepter	La caisse décide d'accepter, gérer et surveiller le niveau de risque et de ne prendre aucune mesure pour réduire le risque.
Atténuer	La caisse est disposée à accepter un certain risque en mettant en œuvre des processus de contrôle pour gérer le risque dans des limites de tolérance définies
Transférer	La caisse choisit de transférer le risque à une tierce partie (p. ex., souscrire une assurance).
Éviter	La caisse pense que le risque est inacceptable et l'évitera spécifiquement (p. ex., arrêter de vendre un produit ou de prêter dans un marché particulier)

En général, si l'ampleur ou la gravité du risque analysé est élevée, la réponse au risque doit être forte (atténuer, transférer ou éviter). Chaque risque et la réponse associée doivent être soumis au gestionnaire responsable du domaine affecté par le risque. Dans le cadre du processus de réponse, la direction doit déterminer et documenter les mesures nécessaires à prendre (pour la prévention ou la détection) pour gérer le risque.

Surveillance

Les activités de risque et réponse au risque doivent être surveillées par le gestionnaire responsable afin d'assurer le maintien des risques notables dans les limites des niveaux acceptables, afin que les risques émergents et les lacunes soient identifiés et que la réponse au risque et les activités de contrôle soient conformes et appropriées. L'audit interne et le comité d'audit (ou autre comité mandaté par le conseil) contribuent de façon significative à confirmer que les dirigeants surveillent et gèrent le risque conformément aux niveaux établis.

Les indicateurs qui tombent en dehors des niveaux acceptables de risque doivent être traités de manière appropriée afin de ramener le risque dans des limites de niveaux acceptables. Ces risques qui demeurent supérieurs aux niveaux acceptables de risque doivent être examinés par le conseil d'administration dans une perspective d'approbation de toute stratégie nécessaire de résolution. Cette activité sera à la base des rapports au conseil d'administration et de la surveillance continue de la direction.

Il est également utile de « quantifier » l'exposition totale de risques notables (ou un sous-ensemble de risques) en termes d'incidence potentielle sur le capital. Bien que ce soit souvent subjectif et difficile à déterminer, cela aide à indiquer toute modification matérielle des niveaux de risque d'une période à une autre et pourrait identifier les risques potentiels qui autrement ne seraient pas relevés. Cela aide aussi à confirmer que le niveau d'exposition au risque total est dans les limites de la propension au risque de la caisse, tel que défini dans la politique.

Présentation des rapports

Le conseil d'administration, le comité de vérification et la haute direction, dans leur rôle de supervision, exigeront que les résultats du processus de GRE leur soient présentés sous forme de rapports afin d'obtenir l'assurance que les risques sont gérés dans les limites approuvées de niveaux de risque.

Les rapports de GRE au comité d'audit (ou autre comité créé à cet effet) ou au conseil d'administration doivent au minimum :

- résumer la nature et l'ampleur des risques notables;
- souligner tous les risques notables et ceux qui dépassent les niveaux acceptables de risque;
- identifier l'horizon temporel et l'état de toute activité de gestion de risque supplémentaire qui pourraient être nécessaires pour amener les risques dans des limites approuvées de niveaux de risque;
- identifier les tendances négatives des domaines de risque élevé et toute modification dans les activités de gestion du risque;
- souligner tout nouveau risque, notamment les activités d'évaluation, de réponse et de gestion :
- identifier tout risque matériel émergent;
- résumer toute exception aux politiques ou limites définies pour les risques clés

Le conseil d'administration devrait examiner périodiquement tous les domaines de risque (même ceux qui sont convenablement atténués dans des limites acceptables) pour avoir une compréhension complète de tous les risques notables auxquels est confrontée la caisse.

ANNEXES

A : PRINCIPES DIRECTEURS

Principes directeurs

En développant un processus de gestion convenable et efficace du risque d'entreprise, les caisses devraient prendre en compte les principes directeurs clés suivants :

- Les décisions devraient être prises en tenant compte de l'incidence sur l'organisation dans son ensemble, et pas seulement dans des secteurs particuliers;

- Le modèle de gouvernance devrait fournir un forum pour que les risques soient reconnus, discutés, débattus et pris en compte dans les décisions opérationnelles stratégiques;

- La gouvernance devrait mettre l'accent sur et permettre de rendre proactifs plutôt que réactifs les processus de gestion du risque;

- La structure de gouvernance du risque devrait prendre en compte et refléter les rôles et l'interaction avec les fonctions liées, notamment la conformité, l'audit interne, etc.;

- Il devrait y avoir une compréhension claire des exigences et des ressources appropriées pour fournir une assurance indépendante (p. ex., l'audit indépendant);

- Le modèle de gouvernance doit refléter la séparation des trois domaines principaux :

    - ✓ Les unités fonctionnelles qui prennent des risques et gèrent les risques qu'elles prennent;
    - ✓ La gestion du risque qui fournit la politique, les lignes directrices, les recommandations, les rapports et l'analyse des risques;
    - ✓ Les fonctions d'assurance indépendante telles que l'audit interne.

- Le modèle de gouvernance du risque devrait être modifié au fil du temps, à mesure que la caisse évolue.

B: MODÈLE DE POLITIQUE DE GRE

Objet

La caisse maintiendra un cadre de GRE solide pour s'assurer que :

- les risques et possibilités notables actuels et émergents sont identifiés et compris;
- les systèmes de gestion appropriée et prudente du risque pour gérer ces risques sont développés et effectivement mis en œuvre;
- des examens réguliers sont menés afin d'évaluer l'efficacité des mesures d'atténuation du risque;
- des rapports sont produits régulièrement sur l'adhésion à cette politique.

Objectifs

Les objectifs de cette politique sont :

- d'établir la propension au risque de la caisse;
- d'identifier les responsabilités clés du conseil d'administration, du comité d'audit et de la direction;
- de donner un aperçu de la fréquence, de la forme et du contenu des exigences de présentation des rapports.

Propension et tolérance au risque

La propension au risque de la caisse est MODESTE. *(La caisse doit définir cette notion du risque sur un plan tant « qualitatif » que « quantitatif »).* Les risques notables doivent suivre les politiques de gestion du risque et les stratégies de risque approuvées par le conseil d'administration.

La caisse devra établir les niveaux de tolérance au risque acceptables pour chacun des risques notables cernés, conformément à l'énoncé sur la propension au risque approuvé par le conseil d'administration et la haute direction (*Indiquez quels sont les niveaux de tolérance et la façon dont ils seront documentés.)*

Attributions

Le conseil d'administration est responsable :

- d'établir les niveaux de tolérance aux risques;
- de superviser les activités de GRE de la caisse;

- de comprendre la nature et l'ampleur des risques notables auxquels la caisse est exposée;
- d'examiner les rapports sur l'évaluation des niveaux de risque par rapport aux cibles stratégiques de risque définies;
- de réviser annuellement les politiques et stratégies de gestion du risque, y compris la propension au risque, pour s'assurer que les expositions au risque restent convenables et prudentes.

Le *(comité d'audit ou autre comité créé à cet effet)* est responsable :

- d'examiner l'identification par la direction des risques notables de la caisse conformément à la politique de GRE;
- de veiller à la mise en place de processus de gestion des risques pour mesurer, surveiller, gérer et atténuer ces risques, notamment en appliquant des politiques, des procédures et des contrôles pertinents;
- de superviser l'application des pratiques de GRE et l'identification continue des risques;
- de faire le rapport au conseil d'administration sur les risques d'exposition au risque.

La *direction (ou le Chef de la direction des risques)* est responsable :

- de recommander au conseil d'administration les niveaux de tolérance aux risques;
- d'identifier, de mesurer et d'évaluer les expositions notables au risque stratégiques, commerciaux et de processus;
- d'assurer qu'un niveau convenable de ressources soit alloué conformément aux cibles de propension au risque pour l'évaluation et la gestion du risque;
- d'atténuer l'exposition au risque au moyen de réponses adéquates au risque;
- de la surveillance de l'application des stratégies de réponses et d'atténuation;
- de l'élaboration des rapports sur les processus et résultats de GRE, notamment le niveau et la direction des expositions au risque et l'ampleur des activités de gestion de risque.

Présentation de rapports

La direction soumettra un rapport au *(comité d'audit ou autre comité créé à cet effet)* au moins une fois par trimestre. Le rapport devrait fournir des renseignements adéquats sur ce qui suit :

- la nature et l'ampleur des risques et possibilités notables;
- les risques notables et ceux qui dépassent leurs niveaux établis de risque;

- l'horizon temporel et l'état de toutes activités de gestion de risque supplémentaires qui pourraient être nécessaires pour amener les risques dans des limites approuvées de niveaux de risque;
- toute tendance négative des domaines de risque élevé et toute modification dans les activités de gestion du risque;
- tout nouveau risque notable, notamment les activités d'évaluation, de réponse et de gestion du risque;
- tout risque émergent;
- toute exception aux politiques ou limites établies par la caisse pour les risques clés.

Le *(comité d'audit ou autre comité créé à cet effet)* fera rapport au conseil d'administration dans son examen des activités de gestion du risque, notamment l'état de toutes exposition et tendance notables actuelles ou émergentes.

Examen de la GRE

L'efficacité du cadre de GRE devrait être évaluée de temps en temps; un examen de tous les risques notables et de l'environnement du risque de la caisse devrait être fait. De plus, toute modification du cadre de GRE devrait être présentée au conseil d'administration sous forme de recommandation.