POLITIQUE DE LA GESTION INTÉGRÉE DES RISQUES

16 novembre 2023
Version officielle

Rédigée par le comité d'audit,
Caroline Soulas et Jo-Ann Hajdamacha

CFA Montréal

TABLE DES MATIÈRES

Note : L'usage du masculin dans ce document a pour unique but d'alléger le texte.

PRÉAMBULE

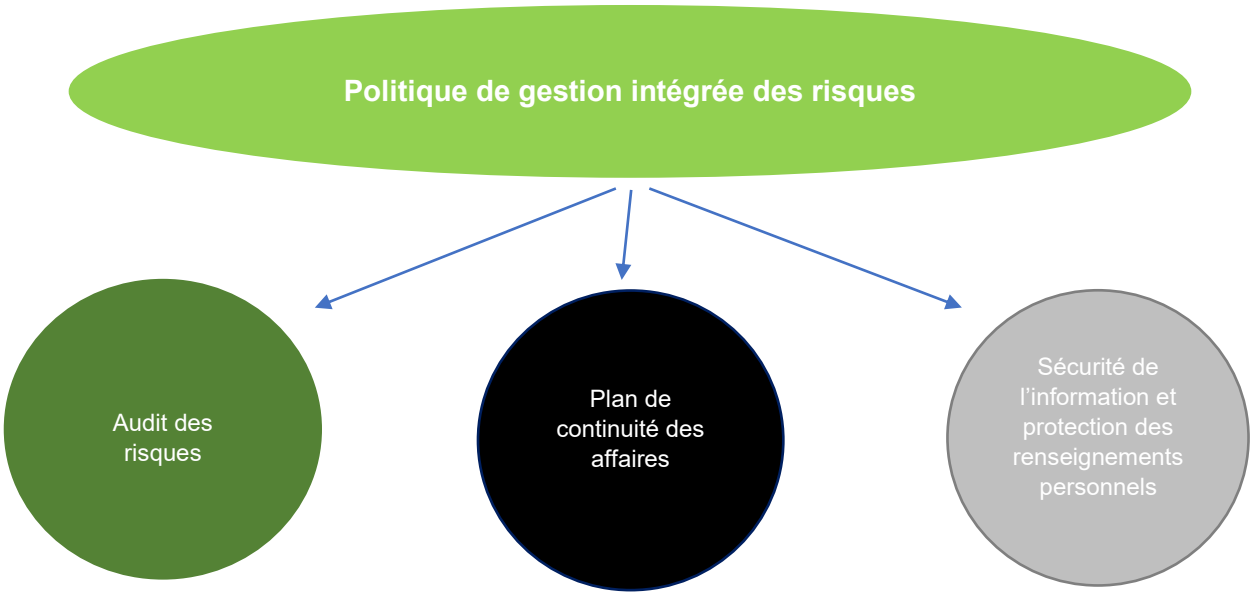
La capacité de CFA Montréal (ci-après « l'Association ») à gérer efficacement ses risques est une des dimensions de sa performance globale. La gestion intégrée des risques, la sécurité de l'information, la protection des renseignements personnels et les stratégies mises en place afin de les gérer et d'assurer la continuité des affaires permet à l'Association d'opérer dans les limites de la tolérance aux risques formulée par le C.A., et de lui fournir une marge de manœuvre raisonnable concernant l'atteinte de ses objectifs.

Considérant la taille de sa structure, son statut d'organisme sans but lucratif, la nature de ses activités et sa mission, l'Association est exposée à moins de risques qu'une grande entreprise.

Dans le processus de gestion de risques, il est toutefois important de tenir compte du lien commercial et des obligations que l'Association détient envers le CFA Institute qui encadre les opérations des sociétés à l'aide d'ententes et de licences dont, entre autres :

- Member Society Licencing agreement (*«MSLA»*)
- Member Society Software Sharing Agreement (*«MSSSA»)*

Ce lien d'affaires comporte des bénéfices tangibles, car L'Association peut compter sur des ressources financières, juridiques, humaines et technologiques supplémentaires. Toutefois, l'Association demeure une entité légale à part entière qui doit offrir des services de qualité à ses membres tout en assurant sa bonne santé financière et en étant conforme aux lois et règlements qui la régissent. Des processus efficaces et rigoureux de gestion sont essentiels à la viabilité de l'Association afin de prévenir des incidents opérationnels majeurs et/ou fournir une préparation optimale afin d'y faire face. Cette politique et les guides opérationnels qui en découlent seront révisés selon un cycle de deux (2) années afin de permettre une réflexion périodique ayant pour but l'amélioration des processus.



La présente politique édicte les principes qui encadrent la gestion intégrée des risques alors que les guides opérationnels qui la complètent déterminent les procédures et contrôles mis en place afin de mitiger les risques liés aux éléments suivants :

1. **Audit des risques** : facilite la compréhension et l'analyse des enjeux et permet une priorisation des risques en amont ou une mitigation des risques, le cas échéant;

2. **Plan de continuité des affaires** : documente les stratégies mises de l'avant afin de répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une situation d'urgence et/ou d'une perturbation;

3. **Sécurité de l'information et protection des renseignements personnels** : établit les principes directeurs et les lignes de conduite à suivre en matière d'accès à l'information, de protection des renseignements personnels et de sécurité de l'information, dans le respect de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé*, aussi appelée Loi 25 (*ci-après appelée « la Loi »)* en septembre 2021.

CONTEXTE

La présente politique de la gestion intégrée des risques *(ci-après appelée « la politique »)* s'inscrit dans un processus d'amélioration continue de la gouvernance et de la gestion de L'Association. Plus particulièrement, la politique s'inscrit dans sa volonté de déployer les meilleures pratiques dans la gestion des risques auxquels l'Association est exposée dans le cadre de ses activités, afin de favoriser la prise d'actions et de décisions éclairées dans le respect de ses objectifs, de sa vision et de sa mission.

Cette démarche vise également à implanter une culture de la gestion des risques au sein de l'Association.

Outre cette politique et les guides opérationnels la supportant, l'Association dispose de plusieurs outils de gouvernance qui soutiennent la gestion intégrée des risques et qui peuvent être consultés en tout temps :

- Règlements généraux
- Politique de gouvernance
- Diagnostic de gouvernance
- Manuel des employés incluant la politique de prévention du harcèlement au travail
- Code de conduite des administrateurs
- Code de conduite des employés
- Code de conduite des bénévoles
- Politique de gestion des conflits d'intérêt
- Politique de placements
- Politique sur la diversité, l'équité et l'inclusion (DEI)
- Politique de gestion financière et contrôles internes *(en cours de rédaction)*

CONCEPTS CLÉS ET DÉFINITIONS

LEXIQUE

Culture de risque
La culture de risque se rapporte aux attitudes et aux comportements associés à la gestion du risque au sein de l'Association, notamment si la gestion du risque est considérée comme une partie intégrante du processus de prise de décision, ou s'il s'agit seulement d'une obligation de rendre des comptes, si l'Association est réfractaire au risque ou si les risques portent aussi des possibilités, si la gestion du risque est intégrée à tous les niveaux de l'Association ou s'il s'agit uniquement d'un processus descendant.

Gestion intégrée des risques
La gestion intégrée des risques favorise une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'Association d'une manière cohérente et structurée. Elle favorise la prise de décisions stratégiques qui contribuent à l'atteinte des objectifs globaux de l'Association. Elle exige une évaluation continue des risques auxquels une organisation peut faire face à tous les niveaux, le regroupement des résultats à l'échelle de l'Association et une communication, une surveillance et un examen adéquats. Elle fait partie intégrante des mécanismes d'une saine gestion. Il ne s'agit pas d'éviter le risque mais plutôt de prendre des décisions éclairées quant aux mécanismes de contrôle à mettre en œuvre pour réduire le risque à un niveau acceptable tout en tirant profit des possibilités que l'incertitude présente pour les objectifs d'une organisation.

Guides opérationnels
Établis par la direction générale au niveau tactique, ceux-ci permettent d'appuyer, de développer et de préciser la politique en déterminant les mécanismes concrets et la façon de procéder afin de gérer de façon intégrée les risques de l'Association.

Matrice des risques
Outil d'identification, d'analyse et de classement de l'ensemble des risques identifiés comme une menace à l'atteinte des objectifs.

Partie prenante
Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité de l'Association.

Politique de la gestion de risques
Elle établit les grands principes de la gestion du risque et clarifie les rôles et les responsabilités de chacun. C'est l'ensemble des éléments établissant les fondements et dispositions stratégiques et organisationnelles qui chapeautent la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue de la gestion des risques au sein de l'Association.

Profil de risque
Décrit les principaux risques auxquels l'Association est confrontée, y compris les menaces et les opportunités

Propriétaire du risque
Personne ou entité ayant la responsabilité du risque et l'autorité pour le gérer.

Risque : inhérent, résiduel et anticipé
La définition généralement acceptée du risque est « l'effet de l'incertitude sur les objectifs ». D'un point de vue technique, le risque exprime la probabilité et les répercussions d'un événement susceptible de nuire à l'atteinte des objectifs de l'Association. Les termes « la probabilité et les répercussions d'un événement » laissent entendre qu'il faut faire, à tout le moins, une analyse quantitative et qualitative pour évaluer les risques. Pour chaque risque considéré, il faut évaluer deux choses : la probabilité ou l'éventualité que l'événement survienne et l'ampleur de ses répercussions ou de ses conséquences s'il survient. Il faut rappeler qu'étant donné que le risque se rapporte à l'effet de l'incertitude, et donc à une perspective d'avenir, les risques se distinguent des enjeux, des problèmes ou des conditions existants. Le niveau de risque observé avant de prendre en compte les mécanismes existants constitue le niveau de risque « inhérent ». Le risque qui subsiste lorsque sont appliqués les mécanismes de contrôle constitue le niveau de risque « résiduel ». Le risque qui subsiste lorsque sont appliqués les mécanismes de contrôle existants et ceux dont la mise en œuvre est planifiée constitue le niveau de risque « anticipé ».

Tolérance au risque
Niveau maximal de risque que l'Association est prête à accepter aux fins d'atteinte des objectifs fixés. Ce seuil de tolérance est défini par le C.A. en référence aux objectifs stratégiques.

CATÉGORIES DE RISQUES

Risques financiers
Risques qui concernent l'ensemble des événements entraînant des pertes de bénéfices découlant d'une variation des facteurs économiques.

Risques opérationnels
Risques de pertes dus à des défaillances ou inadéquations attribuables à des personnes, des processus, des systèmes ou résultats d'évènements externes.

Risques réputationnels
Le risque de réputation, ou risque d'image de marque, correspond à l'impact que peut avoir une erreur de gestion sur l'image d'une organisation entrainant une opinion publique défavorable.

Risques stratégiques
Risques qui affectent la stratégie de gestion ou la mission. Découlent de l'incapacité de l'Association à mettre en œuvre des plans d'action, des stratégies, des processus décisionnels adaptés aux changements touchant l'évolution de son environnement d'affaires.

PRINCIPES DIRECTEURS

Gestion des risques : une responsabilité partagée
C'est une responsabilité organisationnelle qui concerne chaque employé, administrateur, bénévole et fournisseur qui doivent contribuer à la gestion intégrée des risques selon les dispositions prévues par la présente politique et celles qui y sont connexes.

Conformité
L'Association s'assure également que l'application de ses politiques soit conforme aux lois et aux réglementations lui étant applicables. Le CFA Institute est propriétaire de la marque CFA® et des données relatives aux membres et aux candidats. Les activités de gestion intégrée des risques doivent tenir compte des engagements de L'Association stipulés dans les différentes ententes avec le CFA Institute en terme, notamment, de la protection de la marque et des données confidentielles.

Transparence et imputabilité
Il est important de disposer de la meilleure information disponible afin d'avoir une compréhension adéquate des risques qui se doivent d'être documentés. Toute décision doit s'appuyer sur des données validées et sur une évaluation appropriée des risques effectuée selon les principes de la présente politique. Les décisions doivent également être communiquées aux parties prenantes à l'interne et à l'externe.

Amélioration continue
La politique ainsi que les processus qui en découlent doivent être revus afin de s'assurer qu'ils sont toujours adaptés en cas de changements significatifs au niveau du contexte interne, externe ou organisationnel de l'Association.

ÉNONCÉ DE TOLÉRANCE AUX RISQUES

Afin de préserver une saine gestion de ses finances et de ses ressources, CFA Montréal adopte une posture « modérée » face à l'ensemble des types de risques en conservant toutefois une tolérance plus « faible » à l'égard des risques réputationnels. Guidée par ses valeurs et sa mission, l'Association accepte d'encourir des risques mesurés et circonscrits et des pertes financières raisonnables afin de soutenir sa volonté d'innover et de créer des services à valeur ajoutée pour ses membres.

PORTÉE

01. La politique relative à la gestion intégrée des risques de l'Association s'applique aux employés, aux administrateurs et à l'ensemble des personnes qui participent à la gouvernance de l'Association tels que les bénévoles.

OBJECTIFS

02. Appuyer la prise de décision et le respect des priorités à l'échelle de l'Association, ainsi que la réalisation des objectifs organisationnels et l'obtention des résultats prévus, et ce, tout en maintenant la confiance des membres.
03. Assurer la conformité de l'Association quant aux lois et aux règlements qui encadrent son fonctionnement;
04. Soutenir la direction, guider les employés, les administrateurs et les bénévoles et clarifier les rôles de chacun;
05. Cerner, évaluer, gérer et surveiller les risques pouvant affecter l'atteinte de la mission, de la vision ainsi que des objectifs stratégiques et opérationnels de l'Association;
06. Agir de manière proactive en mettant en œuvre des mécanismes de contrôle, lorsqu'approprié, afin d'éviter que les risques identifiés ne puissent entraver l'atteinte des objectifs organisationnels.
07. Assurer un équilibre entre le degré d'intervention en réponse aux risques et les contrôles établis et favoriser la souplesse et l'innovation pour améliorer le rendement et les résultats obtenus.

RÔLES ET RESPONSABILITÉS

Conseil d'administration

08. Approuve la politique de la gestion intégrée des risques soumise par le comité d'audit.
09. Établit et communique son niveau de tolérance aux risques dans un énoncé inclus à la présente politique.
10. Sur une base bisannuelle, reçoit du comité d'audit et valide le profil de risques de l'Association et la matrice qui en découle. Pour l'année intercalée, valide les recommandations du comité d'audit en matière de l'évolution des risques de l'Association et la pertinence des mesures correctives en place.
11. Veille à ce que la direction générale gère efficacement les risques identifiés en y attribuant les ressources matérielles, humaines et financières requises et joue son rôle de promoteur de la gestion intégrée des risques au sein de l'Association.
12. S'assure qu'une considération soit accordée aux risques importants lors de l'élaboration des orientations stratégiques.

Comité d'audit

13. Rédige et révise la politique de gestion intégrée des risques.
14. Valide les guides opérationnels rédigés par la direction générale qui en découlent.
15. Conduit l'audit bisannuel des risques de l'Association, en fait rapport au C.A. et formule des recommandations pour améliorer le fonctionnement du processus de gestion intégrée des risques. Pour l'année intercalée, procède à l'évaluation de l'évolution des risques ainsi qu'à la révision des mesures correctives en place si nécessaire et fait rapport de ses recommandations au C.A.

Direction générale

16. Est responsable de la gestion intégrée des risques.
17. Promeut une culture de la gestion intégrée des risques au sein de l'Association grâce, entre autres, à une bonne communication aux parties prenantes.
18. S'assure que les principes et les pratiques de gestion des risques sont compris et appliqués au sein de l'Association.
19. Participe à l'analyse et à la priorisation des risques en collaboration avec le comité d'audit.
20. Propose les stratégies afin de mitiger les risques qui ont été identifiés comme étant prioritaires dans un plan d'action qui est approuvé par le C.A.
21. Voit à la réalisation du plan d'action et à l'implantation des mesures avec l'appui de son équipe interne.
22. Est responsable de la rédaction et de la mise à jour des guides opérationnels qui découlent de la politique de gestion intégrée des risques.
23. Informe le C.A. de tout incident contrevenant à la saine gestion des risques.

Employés

24. Les employés doivent contribuer à la mise en place des mesures de mitigation des risques au niveau opérationnel.
25. Ils doivent communiquer à la direction générale, sans délai, tout risque pouvant nuire à l'atteinte des objectifs ou au fonctionnement de l'Association dont ils ont connaissance.

Autres comités

26. Les comités surveillent les risques en lien avec leur mandat. La direction générale effectue, auprès d'eux, un suivi régulier sur l'évolution des risques et l'efficacité des mesures de contrôle mises en place.

RÉVISION DE LA POLITIQUE

27. La politique de gestion intégrée des risques de L'Association est révisée tous les deux (2) ans ou lors de changements significatifs pouvant avoir un impact sur son application, afin qu'elle demeure actuelle et pertinente.

Conception	Octobre 2023
Dernière approbation	16 novembre 2023
Prise d'effet	16 novembre 2023
Fréquence de révision	À tous les trois ans
Prochaine révision	Novembre 2026