

POLITIQUE 2500-031

TITRE :	Politique de gestion intégrée des risques		
ADOPTION :	Conseil d'administration	Résolution :	CA-2013-05-27-11
ENTRÉE EN VIGUEUR :	27 mai 2013		
MODIFICATION :	Conseil d'administration	Résolution :	CA-2022-10-31-08

TABLE DES MATIÈRES

1. PRÉAMBULE.....	2
2. OBJECTIFS	2
3. DÉFINITIONS	2
4. CHAMPS D'APPLICATION	3
5. PRINCIPES DIRECTEURS	3
6. RÔLES ET RESPONSABILITÉS.....	4
7. PROCESSUS DE GESTION DES RISQUES	5
8. RESPONSABILITÉ DE LA DIFFUSION ET DE LA MISE À JOUR DE LA POLITIQUE	6
9. ENTRÉE EN VIGUEUR	6
ANNEXE.....	7

1. PRÉAMBULE

L'Université de Sherbrooke reconnaît qu'il y a lieu, au-delà des exigences formelles et des pratiques habituelles, de se doter d'une politique sur la gestion intégrée des risques qui permette leur prise en compte de manière rigoureuse et systématique dans le processus de surveillance de la gestion par les instances de l'Université et dans le processus décisionnel de la direction et des unités.

2. OBJECTIFS

La présente politique a pour but d'établir les modalités de gestion intégrée des risques et de faciliter leur application et suivi par le conseil d'administration, les comités du conseil, le comité de direction de l'Université de Sherbrooke, les facultés, centres universitaires et services.

La démarche de gestion intégrée des risques est basée sur un processus rigoureux et systématique mis en œuvre par le comité de direction de l'Université. Il est destiné à fournir une assurance raisonnable quant aux risques majeurs auxquels est exposée l'Université et aux mesures d'atténuation mises en place pour les mitiger.

Cette politique vise également à définir les mécanismes de contrôle, les responsabilités des acteurs concernés et à développer une culture institutionnelle de gestion intégrée des risques.

3. DÉFINITIONS

3.1. Comité de direction de l'Université

Le comité de direction de l'Université est composé du recteur ou de la rectrice, du recteur adjoint ou de la rectrice adjointe, du secrétaire général ou de la secrétaire générale et des vice-recteurs et vice-rectrices.

3.2. Gestion intégrée des risques

Démarche rigoureuse, systématique, continue et intégrée visant à recenser, évaluer, atténuer et surveiller les risques majeurs auxquels est exposée l'Université. La gestion intégrée des risques fait partie intégrante des mécanismes d'une saine gestion, elle favorise la prise de décisions stratégiques et contribue à l'atteinte des objectifs de l'organisation.

3.3. Risque

Le risque représente l'incertitude quant à l'évolution d'un événement ou d'un résultat futur. Dans le cadre de cette politique, les risques évalués sont ceux pouvant affecter :

- la communauté étudiante;
- les ressources humaines;
- l'exécution de la mission et l'atteinte des objectifs stratégiques de l'Université;
- la situation financière de l'Université;
- la conformité aux lois et aux règlements;
- la continuité des opérations;
- la réputation de l'Université;
- les actifs, infrastructures matérielles et numériques.

Le niveau d'un risque est estimé en fonction de l'impact de sa matérialisation (gravité) et de la probabilité d'occurrence perçue de cette matérialisation (vraisemblance), selon une échelle établie (références en annexe).

3.4. Impact

Conséquence découlant de la matérialisation d'un risque.

3.5. Probabilité d'occurrence

Possibilité qu'un événement se produise ou non.

3.6. Propriétaire de risque

Le propriétaire de risque est la personne désignée par le comité de direction de l'Université pour gérer un des risques qu'il a identifiés. Il doit élaborer les mesures d'atténuation et rendre compte de l'efficacité des mesures mises en œuvre pour mitiger le risque.

3.7. Risque inhérent

Risque lié aux activités, sans tenir compte des mesures d'atténuation ou de contrôle existantes.

3.8. Risque résiduel

Risque qui perdure malgré les mesures d'atténuation ou de contrôle mises en place. Il résulte de l'évaluation de l'effet de ces mesures.

3.9. Seuil de tolérance au risque

Niveau maximal de risque que l'organisation est prête à accepter. Ce niveau est déterminé par le comité de direction de l'Université et le conseil d'administration en référence aux objectifs stratégiques et au risque résiduel.

4. CHAMPS D'APPLICATION

La *Politique de gestion intégrée des risques* incombe prioritairement au comité de direction de l'Université et également, sans limitation, à l'ensemble des gestionnaires du Rectorat, des facultés, instituts et services en plus des responsables des projets.

Elle s'applique à toutes les catégories de risques : stratégiques, opérationnels, financiers, ressources humaines ou liés à la divulgation de l'information et des renseignements personnels sensibles, réputationnels et à la conformité réglementaire.

5. PRINCIPES DIRECTEURS

La démarche de gestion intégrée des risques doit :

- s'arrimer aux objectifs stratégiques et opérationnels de l'Université;
- être flexible et permettre la mise à jour des risques significatifs de manière continue;
- soutenir la prise de décision à tous les niveaux de l'organisation et l'affectation des ressources;
- entraîner la mise en place de mesures de mitigation par les propriétaires et responsables afin de réduire le risque à un niveau acceptable par la haute direction de l'Université;
- être révisée périodiquement par les instances.

6. RÔLES ET RESPONSABILITÉS

La gestion des risques incombe prioritairement à la direction et aux gestionnaires propriétaires de risque ou responsables de mesure d'atténuation ou de contrôle. Elle implique plusieurs intervenants de tous les secteurs de l'organisation, attendu qu'il s'agit d'une responsabilité partagée. Chaque intervenant a un rôle spécifique et assume les responsabilités qui lui sont propres. Ces rôles et responsabilités étant interdépendants, ils doivent s'exercer en concertation afin d'assurer la saine gestion des risques auxquels l'Université est exposée.

6.1. Conseil d'administration

Le conseil d'administration veille à l'identification des principaux risques et à la mise en place d'une gestion des risques. Il s'assure que des systèmes appropriés sont en place afin d'identifier, d'examiner et de maîtriser les risques qui pourraient entraver la bonne conduite de l'Université.

6.2. Comité des finances et d'audit

Le comité des finances et d'audit examine les principaux dossiers comportant des risques auxquels l'Université doit faire face ainsi que les mesures de mitigation prises pour prévenir, contrôler et maîtriser ces risques, et recommande au conseil d'administration les actions appropriées. Il s'assure que l'Université soit dotée d'un processus robuste, efficace et permanent d'identification et de gestion intégrée des risques. Par son mandat, il s'assure également de l'intégrité et de la conformité des systèmes de contrôle interne et d'information de gestion de l'Université.

6.3. Comité de gouvernance des ressources informationnelles

Le comité de gouvernance des ressources informationnelles examine les risques relatifs aux ressources informationnelles auxquels l'Université doit faire face ainsi que les mesures prises pour prévenir, contrôler et maîtriser ces risques, et fait état au conseil d'administration des actions retenues par la direction de l'Université.

6.4. Recteur ou rectrice

Le recteur ou la rectrice, ou la personne à qui il délègue cette responsabilité, soutient le processus de gestion intégrée des risques et s'assure que les principaux risques reliés aux activités de l'Université soient identifiés et que des plans d'action et de mitigation visant à gérer ces risques soient mis en place.

Le recteur ou la rectrice informe le conseil d'administration sur une base régulière de l'évolution des tendances et des risques significatifs émergents. Le conseil universitaire est également informé des risques significatifs relevant de sa compétence.

6.5. Responsable de la démarche de gestion intégrée des risques

La rectrice ou le recteur attribue à un membre du comité de direction de l'Université la responsabilité de la mise en place de la démarche et de l'application de la *Politique de gestion intégrée des risques*.

La personne responsable :

- assure la mise en place et la mise à jour de la politique et des processus qui en découlent;
- coordonne les mesures à mettre en place et s'assure d'un soutien auprès des propriétaires des risques dans l'exercice d'analyse et d'évaluation des risques et des mesures de mitigation dans leurs secteurs d'activités;
- coordonne la production des plans d'action et s'assure de l'intégration et de la prise en compte de l'ensemble des risques relevés dans l'élaboration des plans;
- voit au suivi de ces plans, notamment en ce qui a trait au processus d'implantation, et de réévaluation des contrôles;
- coordonne la reddition de comptes relative à ce processus aux diverses instances.

6.6. Vice-rectrice ou vice-recteur / secrétaire générale ou secrétaire général

Chaque vice-rectrice et chaque vice-recteur et la secrétaire générale ou le secrétaire général, lorsqu'il est propriétaire d'un risque, est responsable de développer et mettre en place des stratégies et des mesures de mitigation ou de contrôle visant à réduire les risques à un niveau acceptable selon le seuil de tolérance établi.

6.7. Responsable désigné d'une mesure de mitigation ou de contrôle

De concert avec le propriétaire de risque, veiller à la conception, à la mise en place et au fonctionnement adéquat de la mesure d'atténuation ou de contrôle dont il est responsable. Il doit accompagner les gestionnaires impliqués dans l'application de la mesure et apporter les correctifs nécessaires lorsque la contribution de la mesure à l'atténuation du risque est insuffisante. Il doit également évaluer l'efficacité de la mesure, en fonction des besoins du propriétaire de risque et faire rapport à ce dernier.

6.8. Bureau de l'audit interne

Le Bureau de l'audit interne assiste le comité des finances et d'audit et le comité de direction de l'Université en jouant un rôle de surveillance, d'examen, d'évaluation et de recommandation en vue d'une amélioration continue des contrôles et des processus sous-jacents à la gestion intégrée des risques. Il peut être interpellé au besoin afin de valider la robustesse d'un contrôle ou d'une mesure de mitigation en lien avec un risque jugé critique.

6.9. Autres participants au processus de gestion intégrée des risques

Le conseil universitaire, les doyennes et doyens, les directrices et directeurs des services, d'instituts et de certains centres universitaires de formation, le chef de la sécurité de l'information organisationnelle, ainsi les responsables de fonction de nature indépendante participent à l'identification des principaux risques lors de l'étape d'identification dans le cadre du processus de gestion intégrée des risques.

6.10. Gestionnaires et autres membres du personnel de l'Université

Les gestionnaires et les autres membres du personnel communiquent sans délai à leur supérieur immédiat tout nouveau risque qui peut entraver l'atteinte des objectifs stratégiques de l'Université et ceux de leur unité.

7. PROCESSUS DE GESTION DES RISQUES

Les principales étapes du processus de gestion intégrée des risques sont les suivantes :

- Identification des risques;
- Évaluation du risque (probabilité d'occurrence et impact) ;
- Priorisation selon l'évaluation du niveau des risques identifiés ;
- Élaboration et mise en place de plans d'action afin de mitiger les risques retenus;
- Suivi des plans d'action et de l'efficacité des mesures de mitigation mises en place pour l'évaluation du niveau de risque résiduel;
- Intégration en continue des risques émergents.

Une présentation auprès des instances appropriées (comité des finances et d'audit, comité de gouvernance des ressources informationnelles et conseil d'administration) du rapport de suivi des plans d'action des risques institutionnels est réalisée deux fois par année.

Une révision intégrale et complète du processus de gestion des risques doit être réalisée au moment jugé opportun, et ce au plus tard 3 ans après la dernière révision. Cette révision peut être arrimée au processus d'élaboration du plan stratégique de l'Université de Sherbrooke.

8. RESPONSABILITÉ DE LA DIFFUSION ET DE LA MISE À JOUR DE LA POLITIQUE

Le membre du comité de direction de l'Université responsable de la gestion intégrée des risques assure la diffusion et la mise à jour de la présente politique, au plus tard à tous les 5 ans.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration.

ANNEXE
Outil d'évaluation des risques – guide

Probabilité de matérialisation du risque

Guide aux fins d'évaluation				
Cote	Description		Fréquence des événements liés au risque	Pourcentage de probabilité
4	Très élevée	En train de se matérialiser, ou se matérialisera plus d'une fois dans la prochaine année	Très fréquent	75-100 %
3	Élevée	Se matérialisera probablement à court terme (d'ici un ou deux ans)	Assez fréquent	50-75 %
2	Modérée	Probabilité modérée de matérialisation estimée à une fois par deux ans	Fréquent	25-50 %
1	Faible	Probabilité limitée de matérialisation estimée à une fois par cinq ans	Peu fréquent	0-25 %

Impact du risque

Cote	Description	Financier	Gestion des ressources humaines*	Image / réputation	Continuité de service	Lois/règlements et conformité	Objectifs stratégiques
4	Très élevée	Variation défavorable de plus de 5 M \$ de dollars du budget d'opérations	Impact important sur l'ensemble du personnel	Couverture médiatique négative et répétitive	Arrêt prolongé, pour une période de 4 semaines et plus (48 heures et plus pour l'informatique)	Plusieurs lois / règlements internes ou externes ne sont pas respectés et les activités de l'université ne peuvent être maintenues	Affecte l'atteinte de l'ensemble des objectifs du plan stratégique
3	Élevée	Variation défavorable de 3 à 5 M \$ de dollars du budget d'opérations	Impact modéré sur l'ensemble du personnel ou important sur une grande partie du personnel	Couverture médiatique négative non récurrente	Arrêt prolongé, pour une période de 3 à 4 semaines (24 à 48 heures) pour l'informatique)	Certaines lois / règlements internes ou externes ne sont pas respectés et les activités de l'université sont touchées de manière importante	Affecte l'atteinte de plusieurs objectifs stratégiques
2	Modérée	Variation défavorable de moins de 1 M \$ de dollars du budget d'opérations	Impact sur une grande partie du personnel ou important sur un petit groupe de personnel	Critiques importantes de partenaires / clients, mais non médiatisées	Arrêt prolongé, pour une période de 2 à 3 semaines (12 à 24 heures) pour l'informatique)	Quelques lois / règlements internes ou externes ne sont pas respectés et les activités de l'université sont touchées de manière modérée	Affecte l'atteinte d'un objectif stratégique
1	Faible	Variation défavorable de 0,3 à 1 M \$ de dollars du budget d'opérations	Impact modéré sur un petit groupe de personnel	Critiques importantes isolées à un ou un nombre limité de partenaires / clients	Arrêt prolongé, pour une période de 1 à 2 semaines (4 à 12 heures) pour l'informatique) ou moins	Une loi ou un règlement interne ou externe n'est pas respecté qui n'affecte pas les activités de l'université	Affecte l'atteinte de sous objectifs

*Gestion des ressources humaines inclus principalement la pénurie de main-d'œuvre, la santé organisationnelle et l'engagement.

Niveaux de risque

			GRAVITÉ (Impact du risque)			
			Faible	Modéré	Élevé	Très élevé
			1	2	3	4
VRAISEMBLANCE (Probabilité de matérialisation du risque)	Très élevé	4	4	8	12	16
	Élevé	3	3	6	9	12
	Modéré	2	2	4	6	8
	Faible	1	1	2	3	4

Actions recommandées :

Vert	< ou = 3,99	Risque acceptable
Jaune	Entre 4 et 8,99	Plan d'action requis au cours des 12 prochains mois
Orange	Entre 9 et 12,99	Plan d'action requis au cours des 6 prochains mois
Rouge	> ou 13	Agir dans les plus brefs délais Plan d'action requis au cours des 3 prochains mois