Bureau du surintendant des institutions financières Canada
Office of the Superintendent of Financial Institutions Canada

Rapport de vérification interne de la gestion du risque d'entreprise

Bureau du surintendant des institutions financières

Novembre 2011

BSIF
OSFI

Canada

Table des matières

1. Contexte

Introduction

Les travaux d'assurance de la Vérification interne visent à déterminer si les processus de gestion du risque, les dispositifs de contrôle et la structure décisionnelle du Bureau du surintendant des institutions financières (**BSIF**), tels que conçus et présentés par la direction, sont adéquats et fonctionnent de manière à pouvoir cerner et gérer adéquatement les facteurs de risque.

Le Comité de vérification et la surintendante ont consenti à ce qu'une vérification de la gestion du risque d'entreprise (**GRE**) soit inscrite au Plan de vérification interne du BSIF pour 2010-2011. Le présent rapport rend compte des résultats de cette vérification. Il s'appuie sur les travaux achevés à la fin d'avril 2011. Les recommandations aideront l'équipe responsable de la GRE à sans cesse améliorer le cadre de contrôle de la gestion des risques.

Le présent rapport a été soumis au Comité de vérification et il a été approuvé par la surintendante en novembre 2011. La surintendante et les surintendants auxiliaires, qui ont préparé la réponse de la direction qu'on trouvera dans présent rapport, en ont également pris connaissance.

Raison pour laquelle la gestion des risques est importante

La gestion des risques aide le BSIF à mettre au point un cadre général pour gérer ses risques et lui permet de formuler des stratégies visant à atténuer les risques et à harmoniser ressources et priorités pour s'assurer de toujours respecter ses plans et priorités.

Conformément à la *Politique sur la vérification interne* et à la *Directive sur les comités ministériels de vérification* du SCT, le comité :

> *« doit exercer d'une manière intégrée, axée sur le risque et méthodique une surveillance des principaux secteurs de gestion, de contrôle et de reddition de comptes, y compris l'établissement de rapports, au sein du ministère »* et
>
> « *est chargé d'examiner le profil de risque du ministère et de donner tout conseil pertinent à ce sujet à l'administrateur général »*

Objectifs opérationnels

La gestion du risque d'entreprise du BSIF se définit tout simplement ainsi.

> *« La gestion du risque consiste à gérer le risque à l'intérieur de limites de tolérance établies. »*[1]

Le risque est défini comme suit.

> « *Le risque s'entend de tout obstacle à la réalisation des objectifs de l'organisation.* »

La tolérance au risque s'entend :

> *« … du niveau de risque résiduel que l'on est prêt à assumer compte tenu de l'ampleur des contrôles…* ».

Suite à la page suivante

[1]Cadre de gestion du risque global au BSIF (Novembre 2008). À la recommandation du Secrétariat du Conseil du Trésor, la notion de risque global est maintenant rendue par le terme « risque d'entreprise ».

1. Contexte, suite

Contexte

Le contexte dans lequel le BSIF évolue comporte des éléments des risques susceptibles de nuire à la réalisation de son mandat et de ses objectifs. Même si bon nombre de ces risques sont omniprésents, la mesure dans laquelle ils menacent la réalisation des objectifs du BSIF varie selon la conjoncture économique et financière et d'après le contexte du secteur des services financiers. L'exécution du mandat et la réalisation des objectifs du BSIF dépend de la capacité de ce dernier de recenser, d'évaluer, de prioriser et de développer, en temps utile et de manière efficace, des initiatives axées sur les aspects où son exposition au risque est la plus élevée.

La GRE permet au BSIF de cerner et de gérer ses risques de manière proactive au moyen d'un processus d'évaluation continue des risques. L'approche de communication en amont et en aval de la GRE permet de faire en sorte que ceux dont la connaissance de l'organisation est la plus étendue peuvent contribuer en temps opportun à la détermination et l'évaluation des principaux risques et que des stratégies d'atténuation soient intégrées à la planification stratégique et des activités. Cette approche favorise l'adoption et le soutien des cadres, des gestionnaires et des employés pour garantir la qualité et l'uniformité de l'application de la GRE ainsi que sa capacité d'évaluer l'importance relative des risques dans l'ensemble du BSIF.

L'*Annexe 1 : GRE – Structures et interactions* énonce les cinq composantes de la structure de la GRE du BSIF, son intégration et ses interactions ainsi que la provenance de l'information sur la gestion des risques.

Gestion des risques – GRE

Dans son *Cadre de gestion du risque d'entreprise au BSIF*, le BSIF classe les *risques* en deux catégories : *externes* et *internes*. La *catégorie des risques externes* comprend la conjoncture économique et financière, le contexte du secteur des services financiers, le cadre juridique du BSIF et les catastrophes. Ils s'entendent d'événements dont le BSIF ne peut changer le cours, mais qu'il doit être en mesure de surveiller afin d'en atténuer les répercussions.

La catégorie des *risques internes* comprend les risques généralement liés aux ressources humaines, aux processus (processus *décisionnel*, processus *internes* et processus de *gestion des relations*), aux *systèmes à l'appui* et à la *culture* (valeurs fondamentales et gestion du changement).

Le coordonnateur de la GRE du BSIF supervise le processus de GRE à l'échelle de l'organisation et présente à la direction un survol trimestriel des risques. Les coordonnateurs sectoriels des risques sont chargés de coordonner le processus sectoriel d'identification, d'analyse et de signalement des risques au sein de chaque secteur, conformément à la *Politique sur la gestion du risque d'entreprise au BSIF* (la *Politique sur la GRE*) et au *Cadre de gestion du risque d'entreprise au BSIF* (le *Cadre de GRE*).

La GRE du BSIF est une façon systématique de développer et d'améliorer la capacité de gérer les risques à l'échelle de l'organisation grâce à la compréhension, à l'identification, à la priorisation, à l'évaluation, au règlement et à la communication des enjeux liés aux risques au moyen d'une approche dynamique d'évaluation des risques.

Suite à la page suivante

1. Contexte, suite

Contexte (suite)

Gestion des risques des secteurs

Les coordonnateurs sectoriels des risques facilitent la vaste participation des gestionnaires et des employés à la gestion des risques et aux communications permanentes grâce à des séances d'information périodiques au cours desquelles les responsables des secteurs font le point sur les principaux risques et sur les stratégies d'atténuation du secteur dont ils sont chargés. Les risques sont évalués sur une base trimestrielle, les registres des risques sont mis à jour, de nouveaux risques y sont ajoutés ou des risques existants en sont retirés, selon le cas, et un résumé des risques est remis à la haute direction. Une fois l'an, les risques sont évalués de façon plus officielle et les secteurs mettent à jour leur registre des risques; ces registres servent à préparer le sommaire de la GRE qui est pris en compte dans le processus annuel de planification du BSIF.

Comité d'examen des risques nouveaux

Le Comité d'examen des risques nouveaux (CERN) du BSIF se réunit périodiquement afin de cerner les principaux risques externes qui influent sur le secteur des services financiers, de même que les plans de travail et les priorités connexes associés à ces risques. Le Comité rend compte à la haute direction et aux gestionnaires sur une base permanente et les résultats de ses évaluations des risques sont intégrés au sommaire de la GRE à des fins de planification intégrée.

Planification intégrée annuelle

La *Politique sur la GRE* définit les attributions et les responsabilités de ceux qui participent à la gestion des risques et qui ont besoin des évaluations des risques des secteurs détaillées et formelles, à des fins de validation avant le début du processus annuel de planification intégrée du BSIF qui servira au processus de planification de l'organisation. Les coordonnateurs des risques de la GRE consolident les risques de leur secteur dans un résumé des risques du secteur qui sert de composante clé du modèle de planification et du cycle de planification intégrée du BSIF.

Rapports sur la gestion des risques

Outre les rapports sur la gestion des risques dans le cadre du processus annuel de planification du BSIF, il y a des moyens formels et informels de rendre compte de la gestion des risques, y compris les évaluations de certains risques et les stratégies d'atténuation de ces risques mises en place. L'information concernant les principaux risques et les principales stratégies appliquées figurent dans des communications diffusées à l'échelle du BSIF, par exemple, L'Info-capsule; il en est question dans les séances de discussion ouverte et elle fait périodiquement l'objet de séances d'information sur la gestion des risques du BSIF à l'intention du Comité de vérification.

Les responsables des secteurs et de la GRE mettent la haute direction et leurs gestionnaires et employés respectifs des résultats de leur évaluation des risques (profil). Le Comité d'examen des risques nouveaux rend également périodiquement compte à la haute direction et aux gestionnaires *des risques externes influant sur le secteur des services financiers et de leurs éventuelles répercussions sur les activités du BSIF*. En outre, l'équipe de la GRE donne au Comité de vérification une séance d'information trimestrielle sur la gestion des risques au BSIF.

On rend officiellement compte de la gestion des risques au BSIF et des enjeux connexes dans le document Plan et priorités du BSIF, le Rapport annuel et le Rapport ministériel sur le rendement. Ces rapports tiennent compte des risques influant sur la capacité du BSIF de réaliser sa Priorité à long terme.

2. Objectif, portée et méthode de la vérification

Objectif de la vérification

La vérification a pour objet de fournir une assurance raisonnable :

- du fait que le cadre de contrôle[2] de la GRE permet de cerner, de prioriser, d'évaluer, de régler et de communiquer les risques externes et internes et les pratiques de contrôle / d'atténuation connexes (conception);
- de la mesure dans laquelle :
  - la politique, les directives et les procédures sur la GRE et les instruments / outils connexes sont compris et en place et qu'ils fonctionnent tel que prévu (opérations);
  - la GRE est intégrée à la planification (stratégique et des activités) de l'organisation et aux opérations des secteurs;
  - les rapports et les communications sur la GRE sont intégrés aux rapports et communications du BSIF.

Portée de la vérification

La vérification porte sur le cadre de contrôle de la GRE au *1er décembre 2010* et sur les améliorations en cours / prévues.

La vérification est axée sur la *Politique sur la GRE* et les procédures et les instruments / outils connexes utilisés pendant la période du *1er avril 2010 à avril 2011*.

Questions hors de la portée de la vérification

- Un examen du *Cadre de planification intégrée*, sauf pour ce qui est de l'intégration de la GRE au processus de planification stratégique et de planification des activités des secteurs.
- Un examen des *rapports sur le rendement* du BSIF, sauf pour ce qui est de l'intégration des rapports sur la gestion des risques, s'il y a lieu.

Méthode de la vérification

La vérification a été effectuée selon les Normes internationales pour la pratique professionnelle de la vérification interne de l'Institut des vérificateurs internes, conformément à la politique du Conseil du Trésor sur la vérification interne.

Dans le cadre de la vérification, trois examens ont été effectués.

- Un examen *de la politique, des procédures et des instruments / outils* utilisés pour évaluer le cadre de contrôle de la GRE et son intégration à la planification stratégique et des activités et aux opérations des secteurs / divisions ainsi que sa conformité à la politique, aux directives et aux consignes du gouvernement.
- Un examen de l'*application du cadre de contrôle de la GRE et des renseignements / documents* à l'appui utilisés pour cerner, prioriser et évaluer les enjeux liés aux risques, prendre des décisions à cet égard et soumettre les questions aux échelons supérieurs ainsi que des communiqués / rapports sur les risques externes et internes et les pratiques d'atténuation connexes, y compris :

Suite à la page suivante

[2] Se reporter à l'annexe A sur les critères de contrôle de la GRE, un tableau des éléments de la structure décisionnelle, de gestion des risques et de contrôle applicables à la fonction de la GRE du BSIF.

2. Objectif, portée et méthode de la vérification, suite

Méthode de la vérification (suite)

- les *activités, processus et instruments / outils de gestion des risques* aux fins de la planification de la GRE au sein des secteurs et de l'organisation;
- *la supervision de la gestion des risques et les rapports et communications sur la gestion des risques* à l'échelle de l'organisation et des secteurs / divisions;
- les attributions en matière de gestion des risques et les pratiques connexes du Comité de vérification, de la haute direction et des responsables de la gestion des opérations.

- des entrevues :
  - *avec le coordonnateur de la GRE et les coordonnateurs sectoriels des risques ainsi qu'avec le directeur général, Finances et planification intégrée;*
  - avec les *gestionnaires et les employés du secteur des Opérations qui participent à la gestion des risques et à la planification intégrée*;
  - *avec les gestionnaires qui appuient les divisions (GI / TI, Ressources humaines, Finances, Sécurité et Communications)* pour ce qui est de l'intégration de la gestion de leurs risques à la planification intégrée et du secteur des Opérations;
  - *avec les surintendants auxiliaires des secteurs, le président du Comité de vérification et le surintendant.*

Les résultats de ces examens et entrevues sont consolidés pour garantir que la GRE du BSIF est uniforme et équilibrée à l'échelle de l'organisation.

Critères de contrôle interne

Les *Critères de contrôle de la GRE, Annexe A*, serviront de point de départ à l'évaluation du cadre de contrôle de la GRE.

Ces critères s'appuient sur les politiques, directives et consignes du gouvernement que voici.

- *Politique sur la gestion des risques*
- *Guide de mise en œuvre de la gestion intégrée du risque*
- *Politique sur le contrôle interne*
- *Politique sur la vérification interne*
- *Directive sur les comités ministériels de vérification*
- *Cadre de responsabilisation de gestion*
- *Cadre de contrôle de la gestion* et *Vérification interne horizontale des profils de risque des organisations dans les grands ministères et organisme*, du Secteur de la vérification interne du SCT (avril, 2010), et cadre de contrôle reconnu à l'échelle internationale du COSO[3] tel qu'adapté au contexte des activités et des risques du BSIF
- Recommandations de l'évaluation indépendante de 2009 du programme de GRE du BSIF

Suite à la page suivante

[3] COSO : Committee of Sponsoring Organizations of the Treadway Commission

3. Conclusion

Conclusion

Même si le BSIF a instauré et applique toutes les composantes d'un cadre de gestion des risques complet au moyen de sa *Politique sur la GRE*, du *Cadre de GRE* et de son *Cadre de planification intégrée* et des consignes connexes, des améliorations s'imposent pour en accroître l'efficacité ainsi qu'expliqué dans le présent rapport.

Un effort ciblé doit être déployé pour[4] :

- adopter un cadre de contrôle interne structuré et exhaustif afin de garantir l'uniformité dans l'évaluation des contrôles et des contrôles des documents provisoires pour les principaux risques;
- améliorer la qualité et la cohérence des registres des risques, un outil indispensable aux fins de la GRE, afin que les risques soient compris et regroupés de la même façon à l'échelle du BSIF;
- faire en sorte que l'exposition aux risques soit plus transparente en la séparant de la tolérance au risque, afin de faciliter la prise de décisions à l'égard des risques.

Voici les pratiques de gestion et de contrôle qui ont été observées à l'égard de la gestion des risques du BSIF.

- Au moyen de son analyse des forces, faiblesses, possibilités et menaces (FFPM) au chapitre de la planification intégrée, de ses séances de planification sans frontières et de la surveillance continue des risques externes, nouveaux et internes, le BSIF démontre un engagement rigoureux à l'égard de la gestion des risques.
- Avec sa *Priorité à long terme* et l'*Info-capsule*, le BSIF tient les employés au courant des risques qui importent.
- Le Comité d'examen des risques nouveaux et la Division de la recherche cernent et évaluent les risques externes et nouveaux éventuelles sur le plan des répercussions qu'ils pourraient avoir sur les institutions financières et les travaux et ressources de réglementation et de surveillance du BSIF.
- Les membres de la haute direction et du Comité de vérification sont mis au courant des enjeux et des préoccupations liés aux risques par l'entremise du sommaire de la GRE, qui se fonde sur les *registres des risques*, et de discussions individuelles.
- Les risques sont consignés dans des registres trimestriels, par secteurs administratifs et d'activités; ces registres font l'objet d'un examen et d'une mise à jour plus approfondis une fois l'an en prévision de la planification et de l'établissement des priorités.

Nous tenons à souligner la collaboration et l'échange de points de vue dont nous avons bénéficié tout au long de la vérification, spécialement les améliorations à la GRE qui ont été proposées. Sans le soutien obtenu, il aurait été impossible de procéder à un examen de cette ampleur et de mettre l'accent sur ce qui importe.

_____ _____

Dirigeant principal de la vérification, Date
Vérification interne

Suite à la page suivante

[4] Se reporter à l'*Annexe 2 : Processus d'évaluation des risques*

4. Réponse de la direction

Aperçu

Nous remercions l'équipe de vérification pour leur démarche empreinte de collaboration dans la conduite de cette vérification. Des représentants des fonctions de la GRE et de la planification intégrée ont pris connaissance des constatations, observations et recommandations y figurant.

La direction accepte les trois principaux thèmes du rapport (soit méthodologie, reddition de comptes et production de rapports) et est généralement d'accord avec les observations qui les appuient. Compte tenu des liens qui existent entre certaines des recommandations, la direction souhaite formuler les commentaires que voici.

Réponse

Politique sur la GRE et Cadre de GRE *– Nous reconnaissons les révisions recommandées à la Politique sur la GRE et au Cadre de GRE pour ce qui est de présenter le processus de gestion des risques du BSIF comme un outil de gestion intégrée et de faire renvoi aux robustes pratiques de communication des risques déjà instaurées à l'échelle de l'organisation, et nous y souscrivons. Ces documents seront révisés en conséquence et une exigence stipulant que la Politique et le Cadre doivent être périodiquement examinés et mis à jour sera ajoutée.*

Cadre de contrôle interne et documentation sur les contrôles – *Le Comité de direction a approuvé une initiative visant à planifier et délimiter une approche pour élaborer un cadre de contrôle interne à l'échelle de l'organisation. Les travaux à cet égard, notamment l'intégration à la GRE, ont été amorcés. Des représentants de la GRE et de la planification intégrée participent aux travaux du groupe de travail interne. Les recommandations du groupe seront présentées au Comité de direction au début de 2012.*

Risque résiduel et tolérance au risque *– Au départ, la direction séparera le risque résiduel et la tolérance au risque pour chaque risque dans le cadre de la méthode de préparation des registres des risques perfectionnée. Au cours des derniers mois, le Comité de direction a demandé au surintendant auxiliaire des Services intégrés de diriger une initiative visant à passer en revue le* Cadre de tolérance au risque *du BSIF et à élaborer une politique sur la propension à prendre des risques. On envisagera la possibilité de définir une tolérance au risque d'entreprise pour les secteurs / sous-secteurs d'activité, une fois la tolérance au risque de l'ensemble de l'organisation définie.*

Suite à la page suivante

4. Réponse de la direction suite

Réponse (suite)

Qualité des registres des risques

- Mise à jour trimestrielle des registres des risques – Compte tenu du fait que la préparation des registres des risques sur une base trimestrielle semble prendre du temps (générant peu de nouveaux résultats, voire aucun) et du chevauchement avec d'autres activités opérationnelles, la direction étudiera la possibilité de diminuer la fréquence de la présentation des rapports et de la ramener à une fois l'an au niveau sectoriel selon un calendrier conforme au processus de planification global. Par souci d'uniformité dans les rapports, les grilles des registres des registres et les instructions pour les remplir seront examinés et mis à jour. Les coordonnateurs sectoriels collaboreront pour s'assurer que la qualité des registres soit uniforme d'un secteur à l'autre. Les pratiques améliorées de préparation des registres des risques et l'établissement de liens avec le processus de planification intégrée permettront de rehausser la qualité et la cohérence du processus de GRE.

- Énoncés des répercussions et tolérances – Nous reconnaissons que le fait de préparer des énoncés des répercussions aux niveaux des secteurs et des secteurs / sous-secteurs d'activité facilite l'évaluation des répercussions d'un risque sur les opérations et sur le secteur en question. On envisagera la possibilité de définir la tolérance au risque aux niveaux des secteurs / sous-secteurs d'activité et des secteurs, une fois déterminée la tolérance au risque à l'échelle de l'organisation, comme nous l'avons vu plus tôt.

- Gestion des mesures d'atténuation – Nous nous pencherons sur des options pour surveiller et suivre les mesures d'atténuation et en rendre compte.

Processus de contrôle

- Supervision de la direction – Nous nous pencherons sur des options concernant la préparation des rapports en vue de renforcer ou de compléter le sommaire de la GRE, à l'intention des cadres, afin de rehausser la transparence du profil de risque du BSIF à l'intention de la haute direction. Nous envisagerons la possibilité de modifier la méthodologie pour améliorer les rapports sur les risques nouveaux et les risques élevés à l'intention des gestionnaires.

- Gestion de l'information sur les risques – À notre avis, un système de GRE automatisé et intégré pour renforcer notre processus de gestion des risques n'est pas nécessaire à court terme et nous ne souhaitons donc pas amorcer des travaux à cette fin pour le moment.

- Capacité et compétences des responsables de la gestion des risques – Nous sommes d'accord avec l'idée d'affecter au départ des ressources supplémentaires à la mise en œuvre des améliorations au processus de GRE et nous pensons que cela peut se faire à même l'effectif déjà en place. À plus long terme, nous étudierons les besoins en ressources (compétences et capacité) aux fins de la coordination soutenue de la fonction de la gestion des risques au BSIF. Il faudra considérer les ressources requises en fonction des liens au Cadre de contrôle interne appliqué à l'échelle de l'organisation.

Suite à la page suivante

5. Observations et recommandations

5.1
Politique sur la gestion du risque d'entreprise* et *Cadre de gestion du risque d'entreprise

Observation : La *Politique sur la GRE* et le *Cadre de GRE* du BSIF n'ont pas été examinés et mis à jour depuis 2005 et 2008, respectivement. Les pratiques courantes n'y sont donc pas entièrement prises en compte.

La *Politique sur la GRE* et le *Cadre de GRE* du BSIF n'ont pas été examinés et mis à jour depuis 2005 et 2008, respectivement. Ainsi, ces documents ne prennent pas en compte toutes les pratiques ayant cours à l'heure actuelle. Par conséquent :

- **Le *Cadre de GRE* ne fait pas état des solides pratiques en matière de communication à l'échelle du BSIF.** À notre avis, cette communication est l'ingrédient principal de l'intégration de la gestion des risques au travail quotidien et à la planification intégrée du BSIF.

  La fonction décisionnelle de la GRE du BSIF rend des comptes au surintendant et à la haute direction. Les risques font l'objet de rapports informels et formels à la haute direction et le Comité de vérification a droit à des séances d'information trimestrielles sur les enjeux liés aux risques influant sur les opérations du BSIF. Le *coordonnateur de la GRE* rencontre les gestionnaires des secteurs pour passer en revue l'évaluation de leurs risques (registres des risques) et recenser les sources de préoccupation / de risque afin de les soulever dans le cadre des séances d'information trimestrielles.

  Le BSIF tient les employés au courant des principaux facteurs de risque au moyen de sa *Priorité à long terme* et de l'*Info-capsule* de la surintendante.

  Le *Comité d'examen des risques nouveaux* et la *Division de la recherche* cernent et étudient les facteurs de risque externes et les nouveaux facteurs de risque quant à leurs éventuelles répercussions sur les institutions financières et à la nécessité de réviser les plans de travail et les ressources des opérations. L'information sert à renseigner la haute direction et les gestionnaires des secteurs au sujet des éventuelles répercussions sur les institutions financières et les opérations du BSIF et à renseigner aussi le personnel affecté aux opérations.

  L'Annexe 2, Processus d'évaluation des risques, signale les principaux points de communication dans le cadre de l'actuel processus d'évaluation des risques. D'après la nature de l'information sur les risques, recueillie tant à l'extérieur qu'à l'interne, et l'importance de faire preuve de jugement pour évaluer l'incidence des risques dans l'atteinte des objectifs opérationnels, une communication robuste est essentielle.

  Après en avoir discuté avec les personnes chargées d'évaluer les risques et d'en rendre compte et avoir examiné les *registres des risques* et le *Sommaire de la GRE,* nous estimons que la haute direction et les gestionnaires participent beaucoup à la communication des risques à l'échelle du BSIF.

Suite à la page suivante

5. Observations et recommandations, suite

5.1
***Politique sur la gestion du risque d'entreprise* au BSIF et *Cadre de gestion du risque d'entreprise* au BSIF** (suite)

- **Les liens et responsabilités des responsables de la planification intégrée et les évaluations des risques et les activités permanentes des secteurs ne sont pas intégrés au *Cadre de gestion du risque d'entreprise* au BSIF.**

  Les principales composantes d'une gestion exhaustive des risques au BSIF, *Annexe 1, Structures et interactions de la GRE*, sont définies dans la *Politique sur la GRE*, le *Cadre de GRE* et le *Cadre de planification intégrée*.

  Le *Cadre de GRE* préconise l'examen annuel approfondi des risques des secteurs et, s'il y a lieu, des sous-secteurs d'activité à des fins de planification et l'examen et la mise à jour trimestriels des *registres des risques*. Pour que la gestion des risques soit considérée et appliquée comme un outil de gestion intégrée, il faudrait intégrer à la *Politique sur la GRE* et au *Cadre de GRE* les liens entre la planification intégrée et les évaluations des risques des secteurs.

  Au moyen de son analyse des *forces, faiblesses, possibilités et menaces (FFPM)* au chapitre de la planification intégrée, de ses *séances de planification sans frontières* et de la surveillance continue des risques externes, nouveaux et internes, le BSIF démontre un engagement rigoureux à l'égard de la gestion.

Recommandation : Toutes les composantes des pratiques de gestion des risques du BSIF devraient être intégrées à la *Politique sur la GRE* et au *Cadre de GRE* et ces documents devraient être périodiquement examinés et mis à jour pour garantir qu'ils demeurent pertinents.

5.2
Cadre de contrôle interne et documentation sur les contrôles

Observation : Il n'y a pas de cadre de contrôle interne structuré et exhaustif. La façon d'évaluer les contrôles est informelle et incohérente et elle n'est pas toujours transparente.

Le *Cadre de GRE* énonce la nécessité de considérer des contrôles internes pour évaluer les risques et déterminer les stratégies d'atténuation / les contrôles nécessaires. On s'attend à ce que les gestionnaires examinent et évaluent sans cesse leurs risques et contrôles. Cet exercice informel est utile, mais il n'est pas assez robuste pour garantir que les contrôles internes en place sont suffisants afin d'équilibrer le risque et la tolérance au risque et que les contrôles sont appliqués comme prévu.

Étant donné qu'il n'y a pas un cadre de contrôle interne de base, il est difficile de déterminer si toutes les composantes du contrôle interne – contrôles de la structure décisionnelle, de la gestion des risques et des processus – ont été prises en compte dans l'évaluation du contrôle interne et si les contrôles sont déterminés et évalués de manière uniforme. Les risques sont-ils sur-contrôlés ou sous-contrôlés?

Un cadre de contrôle interne structuré et exhaustif permettrait au BSIF d'assurer l'uniformité ainsi que l'utilisation et la compréhension communes des contrôles internes, de concilier efficacité des contrôles et effort requis, d'éviter des activités de contrôle excessif / insuffisant et de faciliter la reddition de comptes sur les risques et les contrôles. Nous avons constaté, à bien des reprises, que des activités qui n'étaient pas des mécanismes de contrôle figuraient dans les registres des risques à titre de contrôles et que les contrôles en vigueur n'étaient pas indiqués dans les registres des risques.

Recommandation : Il faudrait mettre au point un cadre et des consignes de contrôle interne officiels et les intégrer à la GRE. Entre temps, il faudrait documenter et évaluer les contrôles dans les registres des risques.

Suite à la page suivante

5. Observations et recommandations, suite

5.3 Risque résiduel et tolérance au risque

Observation : Le risque résiduel n'est pas évident puisqu'il est combiné à la tolérance au risque ; il est donc difficile de le comprendre et cela ne facilite pas la prise de décisions concernant les risques.

À l'heure actuelle, aux fins d'évaluer les risques, on combine *le risque, les contrôles et la propension à prendre des risques* afin de déterminer la cote de *tolérance au risque* des secteurs / sous-secteurs d'activité. Le risque est-il potentiellement sous-contrôlé, à surveiller, acceptable ou potentiellement sur-contrôlé?

Le processus ne permet donc pas d'évaluer l'*exposition au risqu*e (risque moins contrôles) ou le *risque résiduel*. Il est donc difficile de savoir à quoi correspond l'*exposition au risque* et si elle est acceptable ou non.

Il importe de séparer le *risque résiduel* de la *tolérance au risque*, afin que le processus d'évaluation fournisse un point de *décision sur le risque* (se reporter à l'*Annexe 2 : Processus d'évaluation des risques*). Dans l'évaluation des risques, un point de décision sur le risque est essentiel pour intégrer la gestion des risques aux opérations quotidiennes. Devrions-nous accepter le risque (l'*exposition au risque* est en équilibre avec la propension à prendre des risques) ou faudrait-il prendre des mesures d'atténuation? Le secteur / sous-secteur d'activité est-il potentiellement sous-contrôlé ou sur-contrôlé? Faudrait-il réviser les plans et ressources des opérations pour que le risque continue de cadrer avec la tolérance au risque ?

Nous avons remarqué que près de la moitié des risques déclarés dans les registres des risques des secteurs et des secteurs d'activité sont cotés à surveiller, c'est-à-dire qu'il faudrait peut-être renforcer les contrôles actuellement en place en fonction du niveau actuel de l'exposition au risque; toutefois, étant donné que le risque résiduel n'est pas transparent, il est difficile de déterminer l'exposition et la tolérance générales que le BSIF accepte. La manière dont les risques cotés potentiellement sous-contrôlés à l'échelle des divisions ont été regroupés en une cote s'appliquant à l'ensemble du BSIF n'était pas toujours évidente.

Recommandation : Dans le processus d'évaluation des risques, il faudrait séparer le risque résiduel et la tolérance au risque et intégrer un point de décision sur le risque.

5.4 Qualité des registres des risques

Observation : Il faut rehausser la qualité et la cohérence des registres des risques, un outil clé de la GRE, pour garantir que la pertinence de la gestion des risques et l'harmonisation avec la tolérance au risque du BSIF sont bien comprises. Dans l'ensemble, les registres des risques et la mise à jour trimestrielle ne sont pas considérés comme un outil de gestion, mais plutôt comme un exercice de conformité.

Les secteurs du BSIF, épaulés par les *coordonnateurs de la GRE* tiennent à jour sur une base trimestrielle les *registres des risques* à l'échelle des secteurs d'activité des secteurs et, parfois, des divisions et des sous-secteurs d'activité. Les registres visent à gérer les activités d'atténuation et liées aux risques; ils apportent de l'information clé aux fins du processus annuel de planification des activités et d'établissement des priorités des secteurs et des divisions. Les coordonnateurs de la GRE présentent aux gestionnaires de leur secteur respectif les principales préoccupations / principaux enjeux liés aux risques et les mesures d'atténuation proposées.

D'après les discussions avec les personnes chargées de mettre à jour et d'examiner les *registres* et d'en rendre compte et de notre étude des *registres*, nous avons constaté que la préparation des registres prenait beaucoup de temps et était souvent considérée comme un exercice de conformité ou un double emploi d'autres activités opérationnelles quotidiennes.

Suite à la page suivante

5. Observations et recommandations, suite

5.4 Qualité des registres des risques (suite)

Nous avons relevé des incohérences dans l'interprétation du Cadre et dans ce qu'il faut inscrire dans les registres, d'où de la difficulté à regrouper et comprendre les résultats à l'échelle du BSIF. Il était parfois ardu de comprendre les enjeux sous-jacents liés aux risques, les contrôles existants et les conséquences du risque dans l'atteinte des objectifs des activités et du BSIF.

Nous avons remarqué que le *Cadre de GRE* n'était pas appliqué de manière uniforme aux fins de la préparation des registres des risques. En particulier,

- les évaluations des risques inhérents du même risque variaient d'un secteur à l'autre,
- les critères aux fins de l'évaluation de la tolérance au risque n'étaient pas toujours les mêmes,
- des éléments se retrouvaient dans certains registres des risques et dans d'autres, pas, par exemple
  - contrôles,
  - calendrier des mesures,
  - risques atténués et dans d'autres, seulement des risques devant être atténués,
  - activités d'atténuation des risques acceptables.

Des activités d'atténuation des risques acceptables laissent entendre que le risque est potentiellement sur-contrôlé.

Les registres des risques ne démontrent pas clairement les répercussions d'un risque sur les objectifs opérationnels et le mandat du BSIF.

En examinant des registres des risques représentatifs, nous avons observé que le lien entre les *répercussions du risque* et la *tolérance au risque* et l'objectif (les objectifs) des *secteurs / sous-secteurs d'activité* n'est pas toujours clairement établi. Même si les *répercussions* d'un risque sont cotées, il est difficile d'évaluer la gravité du risque, ses répercussions sur les opérations et le niveau de contrôle nécessaire ainsi que l'incidence du risque sur la capacité du BSIF de s'acquitter de son mandat et de réaliser ses priorités à long terme.

Compte tenu que les évaluations des contrôles laissent à désirer, il est difficile de déterminer si les risques sont gérés de manière adéquate. Le risque et le contrôle sont-ils en équilibre (le risque résiduel est inférieur ou égal à la tolérance au risque du secteur / sous-secteur d'activité) ou le risque est-il sur-contrôlé ou sous-contrôlé?

D'après l'examen des *registres* de notre fonction de VI, nous avons constaté que le lien entre le risque pour les objectifs du BSIF et la cote de *tolérance au risque* attribuée était parfois évident et dans d'autres cas, il ne l'était pas.

Les mesures d'atténuation sont gérées de manière informelle et ne sont pas bien documentées dans les registres des risques.

Il n'y a pas de processus officiel pour surveiller et suivre la mise en œuvre des mesures visant à atténuer les risques et en rendre compte. Dans notre examen des registres des risques, nous avons observé ce qui suit.

- Les contrôles existants ne sont pas toujours pris en compte.
- Les mesures achevées ne sont pas toujours ajoutées comme contrôle.
- Les mesures d'atténuation ne sont pas liées aux plans d'action des activités et des opérations.
- Des mesures classées mesures d'atténuation sont des mesures usuelles.
- L'état d'avancement et le calendrier des mesures d'atténuation ne sont pas toujours indiqués dans les registres des risques.

Suite à la page suivante

5. Observations et recommandations, suite

5.4 Qualité des registres des risques (suite)

Recommandation : 1) Le *Cadre de GRE* devrait être appliqué de manière uniforme aux fins de la préparation des registres des risques afin que les risques soient compris et regroupés de la même façon dans tout le BSIF. Il faudrait préciser les instructions relatives aux registres des risques des secteurs et améliorer la grille pour favoriser une approche commune. 2) Il faudrait officiellement intégrer les registres des risques aux rapports sur les opérations de gestion. 3) Le coordonnateur de la GRE devrait superviser la qualité des registres des risques.

5.5

Supervision de la direction

Observation : La direction ne reçoit pas suffisamment d'information sur les risques pour exercer une surveillance adéquet.

Le principal outil de gestion des risques, ce sont les *registres des risques* des secteurs / sous-secteurs d'activité dans lesquels les principaux risques et les évaluations des risques sont documentés et énoncent l'information sur les risques : les répercussions du risque, le risque inhérent sous-jacent, les contrôles internes existants, l'orientation du risque et la tolérance au risque. S'il y a lieu, les mesures d'atténuation pertinentes sont énoncées aux fins d'examen et d'approbation par la direction sur une base trimestrielle. Ces registres sont utilisés pour préparer un sommaire de la GRE à l'intention de la haute direction et du Comité de vérification.

En fonction des discussions avec les *coordonnateurs sectoriels des risques*, les registres sont examinés par les dirigeants des secteurs et mis à jour sur une base trimestrielle; ils font l'objet d'un examen approfondi informel aux fins de l'exercice annuel de planification. Les registres sectoriels sont pris en compte dans la préparation du sommaire narratif de la GRE à l'intention de la haute direction.

L'information sur les évaluations des risques n'est toutefois pas synthétisée dans les profils de risque de l'organisation selon les principaux risques et les secteurs / sous-secteurs d'activité, à l'échelle des secteurs et du BSIF, pour donner un aperçu des risques dans l'ensemble du BSIF à l'intention des gestionnaires.

Il faut regrouper l'information sur les risques et les évaluations des risques des secteurs / sous-secteurs d'activité, des secteurs et de l'organisation pour fournir une vision globale ou un *tableau de bord* des risques. Quels sont les risques urgents? Dans quels secteurs / sous-secteurs d'activité les risques urgents se retrouvent-ils? Ces visions des risques sont-elles conformes à la vision descendante de la direction? Y a –t-il une concentration de risques dans un sous-secteur d'activité en particulier? Y a-t-il des *risques communs* qui devraient être gérés en collaboration?

Un *aperçu à l'intention de la direction* comporterait de l'information sur les risques, par exemple, le risque inhérent, les contrôles, l'exposition au risque et la propension à prendre des risques, l'orientation du risque et la décision prise à l'égard du risque (accepter le risque ou prendre une mesure d'atténuation). Un *tableau de bord* des risques indiquerait les risques élevés et toute concentration des risques et l'endroit où ils le sont. Dans la même veine que le tableau de bord des risques nouveaux, les tableaux de bord des risques donneraient de l'information sur les répercussions du risque sur le BSIF et l'état d'avancement des mesures d'atténuation prises. Il serait ainsi possible de présenter un tableau de haut niveau de la condition du risque et des mesures d'atténuation prises dans les secteurs / sous-secteurs d'activité et les secteurs, d'où un profil des risques du BSIF davantage transparent.

Recommandation : Il faudrait améliorer les rapports sur les risques pour y intégrer progressivement un rapport global sur les évaluations des risques élevés et la concentration des risques aux échelles des secteurs / sous-secteurs d'activité, des secteurs et de l'organisation.

Suite à la page suivante

5. Observations et recommandations, suite

5.6 Gérer l'information sur les risques

Observation : Il est difficile et fastidieux de gérer l'information et les rapports sur les risques

On estime qu'à l'heure actuelle, quelque 200 éléments de risque et près de 500 mesures d'atténuation sont gérés et déclarés dans les *registres des risques*. Ces volumes avec une surveillance et des rapports améliorés et avec l'adoption d'une structure de contrôle interne laissent entendre qu'il faut mettre au point un système de GRE automatisé et intégré permettant de mieux enregistrer l'information sur les risques, de mieux la surveiller et de mieux en rendre compte aux échelles des secteurs / sous-secteurs d'activité, des secteurs et de l'organisation.

Il est tout aussi important d'avoir un système de GRE intégré permettant de saisir l'information sur les contrôles internes et les risques et les évaluations des risques et d'y avoir accès, de suivre les mesures d'atténuation et de rendre compte de la gestion des risques dans l'ensemble de l'organisation. Les efforts ne seront plus déployés pour accomplir des tâches administratives et de maintenance, mais bien pour gérer les risques, prendre des décisions à l'égard des risques et rendre compte aux échelles des opérations et de la direction.

Le système de GRE s'appuierait sur les inventaires adaptés des risques et des contrôles internes du BSIF; il permettrait de mettre en application la méthodologie et le processus de GRE du BSIF, de tenir à jour des évaluations des risques approfondies à plusieurs niveaux (organisation, secteur et sous-secteur d'activité) et d'offrir diverses capacités de produire des rapports sur la gestion des risques.

Nous encourageons le BSIF à étudier les avantages que représente l'acquisition d'un système de GRE intégré. Pour faire un peu partie de la Stratégie sur la GI / TI, on pourrait acquérir un système Web offrant l'avantage d'un système de GRE spécialisés avec soutien technique et au plan de la gestion des risques qui pourrait être interne à une date ultérieure.

Recommandation : Le BSIF devrait tenir compte des avantages que représente l'acquisition d'un système de GRE intégré pour appuyer la gestion des risques dans l'ensemble de l'organisation.

5.7 Capacité de gestion des risques et compétences en gestion des risques

Observation : Raffermir la capacité de gestion des risques et renforcer les compétences en gestion des risques à l'échelle du BSIF

Pour raffermir la méthodologie, les processus et les outils de gestion des risques, il faudra offrir une formation spécifique en gestion des risques aux personnes responsables des évaluations des risques et à celles qui y participent ainsi qu'aux *coordonnateurs des risques*.

Compte tenu des améliorations apportées à la gestion des risques, il importe que le BSIF définisse les compétences et capacités nécessaires pour mettre en œuvre et tenir à jour la gestion des risques et les calendriers connexes dans l'ensemble de l'organisation.

Compte tenu des efforts qui devraient être déployés pour apporter les améliorations à la gestion des risques et offrir la formation connexe, il faudra, à notre avis, affecter des ressources pour diriger la gestion des risques et mettre en œuvre les améliorations à la GRE.

Recommandation : Il faudrait définir les compétences et capacités nécessaires pour mettre en œuvre une fonction de gestion des risques à l'échelle du BSIF et la tenir à jour.

Suite à la page suivante

Annexe A – Critères de contrôle de la GRE

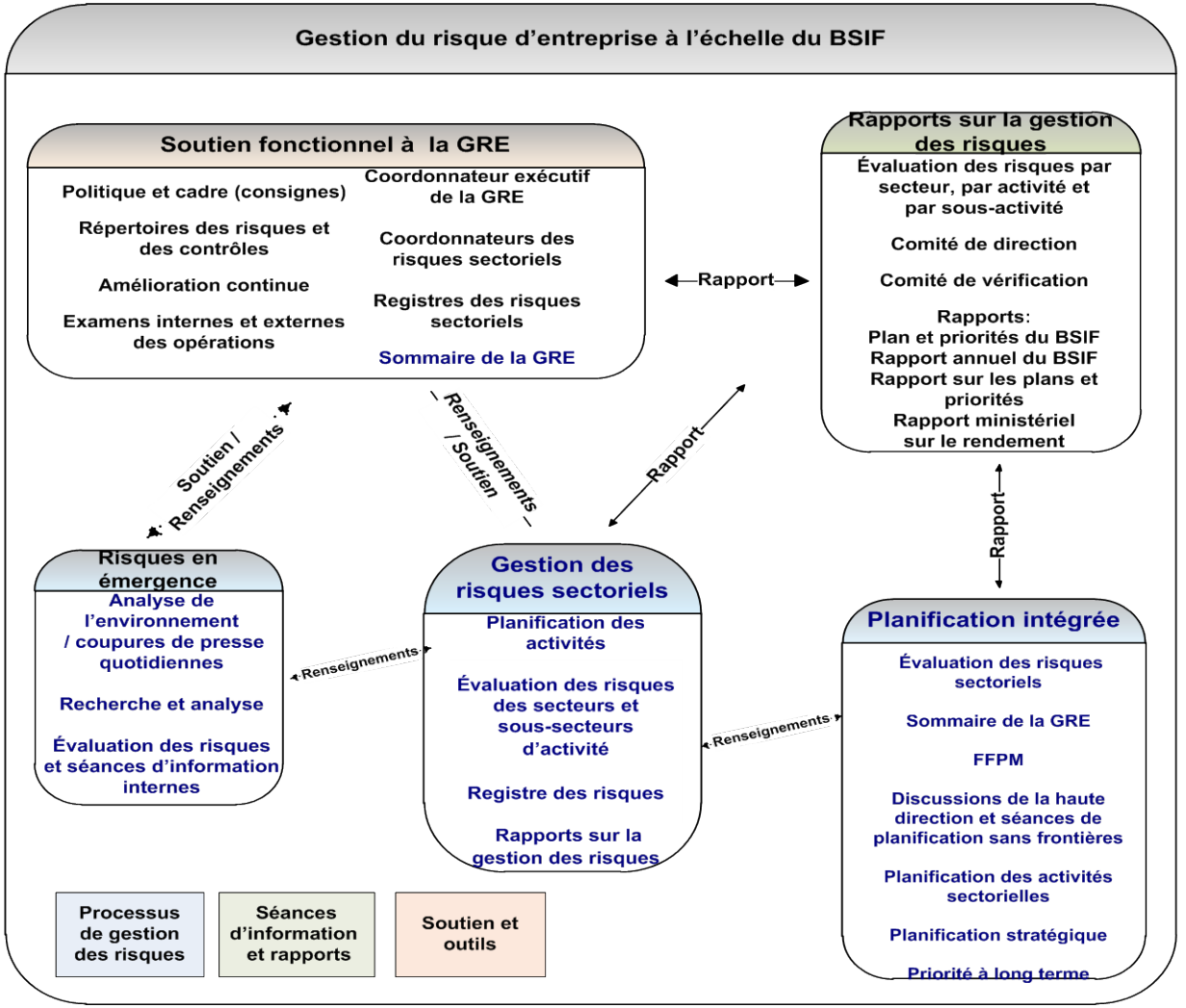
Élément	Composantes
Gestion des risques	▪ Les *risques externes et internes* liés à la fonction de GRE du BSIF sont cernés et évalués et des mesures / contrôles d'atténuation sont mis en place, conformément à la *Politique sur la GRE* ▪ Il y a une *structure* permettant de gérer et de suivre les risques / enjeux en ce qui a trait à l'intégralité, la rigueur et la nature courante de la fonction de GRE ▪ La haute direction a *communiqué son opinion et ses décisions* relativement aux risques, aux contrôles internes et à la tolérance au risque
Structure décisionnelle	
Contexte opérationnel	▪ La GRE tient compte des *valeurs du BSIF et de sa détermination à intégrer la gestion des risques* à la planification et aux opérations des activités et de l'organisation ▪ Les *obligations redditionnelles, les responsabilités, le processus décisionnel et les rapports* au sujet de la gestion des risques aux échelles du Comité de vérification, de la haute direction, de l'organisation et des activités, les mesures de suivi, le signalement des problèmes liés aux risques aux échelons supérieurs et les décisions et les rapports sur les risques sont définis et communiqués aux dirigeants et aux employés ▪ Les *ressources aux fins de la* GRE et des secteurs sont prévues, conformément au profil de risque du BSIF et à ses plan et priorités ▪ *Les compétences notamment techniques*, y compris la formation officielle et officieuse nécessaire pour maintenir les niveaux des connaissances et l'expertise requise sont énoncées

Définition des objectifs	▪ *La politique, les objectifs, les plans, les cadres des risques et des contrôles et la méthodologie relative aux risques (descendante, ascendante) en matière de GRE :*
	  ▪ sont définis et communiqués aux dirigeants et aux employés;
	  ▪ sont conformes aux objectifs (et au plan et aux priorités) du BSIF et les appuient;
	  ▪ cadrent avec les rapports sur le rendement du BSIF;
	  ▪ respectent les politiques, directives, normes et consignes du gouvernement
	▪ Des *pratiques en matière de gestion des risques et de tolérance (qualitative et quantitative) au risque* ont été établies aux échelles des secteurs / sous-secteurs d'activités, des secteurs et de l'organisation

Information et communication	▪ Les *exigences en matière d'information sur les risques et les contrôles internes*, y compris les structures des risques et des contrôles internes, le risque inhérent (impact et probabilité), le risque résiduel et la tolérance au risque sont définies et intégrées aux pratiques et rapports en matière de gestion des risques ▪ Les *rapports sur la gestion des risques* sont établis et communiqués aux dirigeants et aux employés, s'il y a lieu, notamment l'analyse FFPM, les évaluations des risques (registres) des secteurs et des secteurs / sous-secteurs d'activités, les risques nouveaux, le sommaire sur les risques (tableau de bord) et son intégration à des documents clés comme la Priorité à long terme, les Plans et priorités et le Rapport annuel

Élément	Composantes
	▪ Il y a des *voies de communication ouvertes et en temps opportun* entre les gestionnaires et les employés. ▪ Pour voir à ce que les exigences relatives aux risques et aux contrôles soient communiquées. ▪ Pour garantir que les communications sur la gestion des risques et les décisions prises à l'égard des risques sont à jour et cohérentes ▪ Une *mémoire d'entreprise* est intégrée aux processus de GRE et elle est tenue à jour grâce à l'information portant sur les évaluations des risques et les décisions prises à l'égard des risques
Surveillance et rapports de gestion	▪ Il y a un *processus d'amélioration continue de la GRE* pour surveiller ce qui suit et en rendre compte. ▪ Réalisation des objectifs en matière de GRE. ▪ Respect de la politique, des processus et des pratiques en matière de gestion des risques. ▪ Suffisance des ressources de GRE pour appuyer la gestion des risques. ▪ Des *pratiques et outils en matière de rapports de gestion sont instaurés*, par exemple, analyse des risques (impact, probabilité et distribution des risques) et rapports sur les risques portant notamment sur les objectifs opérationnels à risque, les considérations relatives à la compensation et au processus décisionnel concernant les risques et mesures de contrôle / d'atténuation avec échéanciers cibles
Processus de contrôle	
Processus et activités de contrôle	▪ Il y a un processus de *supervision de la gestion* de la fonction de GRE. ▪ Il y a des *processus* qui définissent ce qui suit. ▪ Les exigences relatives aux procédures et aux activités pour : ▪ Cerner les risques nouveaux et en analyser la pertinence pour le BSIF et la gestion des risques ▪ Aider les secteurs à effectuer sans cesse des évaluations des risques et des contrôles ▪ Cerner, évaluer et mesurer la probabilité et l'impact, prioriser, prendre des décisions à l'égard des risques, surveiller et rendre compte des risques et des pratiques de contrôle / d'atténuation connexes ▪ La concordance entre le risque résiduel et la tolérance au risque respective (goût du risque). ▪ Le processus d'intégration de l'information sur les risques nouveaux et la planification et des activités permettant de cerner les risques nouveaux des secteurs et de l'organisation à la gestion des risques globale du BSIF ▪ Les échéanciers (calendrier) et les produits livrables ▪ Des *plans de sauvegarde et de continuité de l'information sur la GRE,* des instruments / outils à l'appui et le personnel nécessaire sont en place

Annexe 1 : Structures et interactions de la GRE



Annexe 2 : Processus d'évaluation des risques