CADRE DE GESTION DES RISQUES ET DES INCIDENTS À PORTÉE GOUVERNEMENTALE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Octobre 2013

UN QUÉBEC POUR TOUS

Québec

Table des matières

Sommaire exécutif

Le Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information, pris en vertu de l'article 21 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), présente une approche novatrice visant à renforcer la façon de gérer certains événements reliés au cycle de vie de l'information gouvernementale. Ce cadre est applicable aux ministères, ainsi qu'à la plupart des organismes publics, y compris ceux du réseau de l'Éducation, du réseau de l'Enseignement supérieur, de la Recherche, de la Science et de la Technologie et du réseau de la Santé et des Services sociaux.

Le risque à portée gouvernementale (RPG) est un risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services d'autres entités gouvernementales. L'incident de sécurité de l'information à portée gouvernementale (IPG) est, quant à lui, la conséquence observable de la concrétisation d'un risque, produisant un effet négatif sur le gouvernement, qui nécessite une intervention.

Une saine gestion des risques et des incidents doit faire partie de tout processus intégré de gestion de la sécurité de l'information au sein des organisations. Le cadre présenté s'appuie sur les processus ministériels et apporte un niveau additionnel de gouvernance, garantissant ainsi une identification continue des situations de risques potentiels et, dans certains cas, une réponse appropriée lorsqu'un risque se transforme en un incident à portée gouvernementale.

De plus, le document démontre l'avantage de couvrir les risques et les incidents qui pourraient être en lien avec la réalisation de l'une ou de l'autre des missions attribuées en matière de sécurité civile. En cas de sinistre majeur, réel ou imminent, certains organismes publics pourraient, en effet, être appelés à réaliser des actions, qui vont au-delà des activités qu'ils réalisent habituellement, dans le but d'assurer la sécurité de la population.

Le Québec doit être prêt à répondre adéquatement à tous les types de sinistres. La coordination en matière de sécurité civile a d'ailleurs été mise à l'épreuve lors de la crise du verglas en 1998, lors des inondations au Saguenay en 1996 et, plus récemment, lors de la préparation à la pandémie de grippe A (H1N1) en 2009.

Il existe actuellement une opportunité d'attribuer une responsabilité en matière de sécurité civile au dirigeant principal de l'information (DPI), qui est en lien avec la gestion des risques et des incidents à portée gouvernementale. Le DPI pourrait, à travers les processus à mettre en place pour gérer les RPG et les IPG, apporter son soutien et son expertise afin de garantir la disponibilité de l'information, lorsqu'elle est nécessaire au bon fonctionnement des différentes missions prévues dans le Plan national de sécurité civile *(*PNSC).

La démarche présentée pour la gestion des RPG sera d'abord mise de l'avant avec la collaboration d'un sous-ensemble d'organismes publics. Un certain nombre d'itérations permettra d'augmenter progressivement la quantité d'organismes publics interpelés dans le cadre de l'exercice. Une fonction de revue et de suivi permettra de suivre la progression de la

couverture des organismes publics, et produira l'information de gestion pertinente aux autorités, notamment les indicateurs sur le niveau d'exposition aux risques.

L'établissement d'une relation d'affaires entre le DPI et les organismes publics, visant la gestion de certains risques et de certains incidents aux conséquences graves pour le gouvernement, contribuera de manière significative à la maturation du processus gouvernemental de gestion de la sécurité. Cette stratégie permettra au DPI d'agir efficacement face aux menaces de sécurité de l'information, en bénéficiant d'une connaissance approfondie des scénarios aux conséquences inacceptables pour le gouvernement, et en lui définissant un rôle formel dans la gestion des incidents à portée gouvernementale.

1 INTRODUCTION

Le présent document, pris en vertu de l'article 21 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), propose une approche novatrice en matière de gestion des risques et des incidents en sécurité de l'information pour le gouvernement du Québec. Cette approche permet l'identification de certains risques, susceptibles de produire des conséquences graves pour le gouvernement, par l'application d'un processus réalisé avec la collaboration des organismes publics de l'administration gouvernementale. De plus, les éléments présentés abordent aussi la gestion des incidents qui se produisent lorsque la menace associée à un risque se réalise.

Les risques et les incidents visés sont ceux qui sont relatifs à la sécurité de l'information gouvernementale, et dont l'ampleur de leurs conséquences déborderait des limites d'une seule organisation. Ils sont considérés à portée gouvernementale, car la collaboration de plusieurs organismes publics est nécessaire pour en assurer une gestion optimale et, le cas échéant, pour coordonner le retour à une situation normale.

Dans un premier temps, les notions de RPG et d'IPG seront expliquées et des définitions seront élaborées. En s'appuyant sur les tendances au plan national et international, les RPG en sécurité de l'information sont définis comme étant susceptibles de produire des conséquences graves sur la livraison de services indispensables à la population, sur la vie, la santé ou le bien-être des personnes, sur l'atteinte aux droits des citoyens à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement et la confiance des citoyens envers l'État, ou sur la prestation de services d'autres entités gouvernementales.

Après avoir décrit ce qu'est un RPG, le document présentera les activités nécessaires à son identification et à son traitement, ainsi que le lien avec le processus de gestion des risques déjà en place dans les organismes publics. Les éléments présentés s'inspirent d'un cadre plus général de gestion du risque établi par l'Organisation internationale de normalisation, ainsi que de pratiques reconnues en vérification de la sécurité des systèmes d'information.

Enfin, les dernières sections seront consacrées à la gestion des incidents à portée gouvernementale. Bien que l'objectif poursuivi soit d'éviter qu'un risque ne se réalise et produise un incident, il est nécessaire de prévoir la manière de gérer de pareilles situations.

Le DPI est l'autorité gouvernementale la mieux placée pour coordonner la gestion des RPG et des IPG. Ce dernier bénéficie d'une table de concertation des responsables organisationnels de la sécurité de l'information, d'un réseau des conseillers organisationnels en sécurité de l'information et d'un réseau des coordonnateurs organisationnels de gestion des incidents, sur lequel le DPI pourrait s'appuyer pour étendre le processus à tous les organismes publics.

2 POSITIONNEMENT SUR LA PORTÉE DES RISQUES ET DES INCIDENTS EN SÉCURITÉ DE L'INFORMATION

La présente section expose les principaux constats relatifs à la gestion des risques et des incidents et décrit les principales tendances à l'échelle nationale et internationale.

2.1 Contexte de la gestion des risques et des incidents

L'information est au cœur des services livrés par le gouvernement à la population. La valeur de cette information est considérable, compte tenu du rôle qu'elle joue dans les différents processus des organismes publics, dont certains sont extrêmement importants pour la sécurité ou le bien-être des citoyens.

Les éléments qui menacent l'information gouvernementale sont complexes, variés et en constante évolution. De nombreux aléas, comme les défaillances technologiques, peuvent affecter de manière importante la disponibilité de cette information. D'autres menaces, comme la falsification de renseignements, la consultation non autorisée de données confidentielles ou les cyberattaques, peuvent également produire un impact de grande importance sur l'information détenue ou communiquée dans le cadre des activités courantes de chaque organisme.

Des mesures de sécurité sont en place pour minimiser la probabilité que survienne un événement portant atteinte à l'information détenue ou communiquée par les organismes publics. Une saine gestion des risques contribue à faire en sorte que ces mesures soient toujours présentes et efficaces au niveau requis.

Par ailleurs, les meilleures pratiques en sécurité de l'information nous apprennent que la gestion des risques, à elle seule, n'est pas suffisante pour garantir la sécurité de l'information dans une organisation. Une saine gestion des risques devient plus efficace si elle est combinée à un processus de gestion des incidents, car inévitablement certains risques deviendront des incidents.

Certaines menaces ne peuvent pas être éliminées par la gestion des risques. Par exemple, le risque associé à un vol de renseignements confidentiels par un employé légitimement autorisé ne peut pas être complètement éliminé par la mise en place de mesures préventives ou dissuasives. À partir du moment où une organisation accepte que, pour fonctionner, elle a besoin de certaines informations, automatiquement elle accepte de composer avec des risques inhérents à son actif informationnel.

La gestion des risques en sécurité de l'information, actuellement appliquée au gouvernement, est caractérisée par une approche purement sectorielle, voire en silo, où chaque organisme décide de l'ensemble des paramètres pour les risques auxquels il est exposé (niveau de tolérance aux risques, sélection des stratégies de traitement, critères d'acceptation des risques résiduels, etc.). Un mécanisme formel de coordination au niveau gouvernemental soutenu par un processus de cueillette d'informations auprès des organismes publics sera mis en place pour renforcer la capacité de l'Administration à prendre en charge les RPG et assurer le suivi de leur traitement.

Pour sa part, la gestion des incidents en sécurité de l'information n'est pas entièrement réalisée en silo, car elle peut tirer profit de certaines fonctions communes (services communs offerts

par le CERT/AQ[1], réseau d'alerte gouvernemental, etc.). Par contre, la gestion des incidents au niveau gouvernemental reste trop souvent cantonnée dans les incidents de nature technologique, alors que la majorité des incidents, qui ne sont pas de nature technologique, sont encore gérés à l'intérieur des organismes publics sans coordination gouvernementale.

2.2 Analyse de la situation actuelle

Plusieurs gouvernements, ainsi que des organisations internationales de normalisation, ont contribué à l'établissement de bases nécessaires à la mise en œuvre de processus de haut niveau d'appréciation et de gestion des risques et des incidents applicables à une multitude de domaines, notamment celui de la sécurité de l'information.

2.2.1 Éléments normatifs et méthodologiques

Au milieu des années 90, l'Australie et la Nouvelle-Zélande ont innové en publiant une norme générale sur la gestion des risques. Modifiée en 1999 et en 2004, la norme AS/NZS 4360 est devenue un manuel générique de gestion des risques susceptibles d'affecter les organisations privées ou publiques dans le cas de catastrophes majeures ou de situations d'urgence.

Plus récemment, l'Organisation internationale de normalisation (ISO) a proposé une approche générique de la gestion des risques à travers la norme ISO 31000. L'approche de l'ISO ne préconise pas de moyens pour mettre en œuvre la gestion des risques, mais amène un formalisme pouvant être adapté à un très vaste éventail de besoins et d'organisations.

De plus, l'ISO a publié, en 2008, la première norme de gestion des risques de sécurité des systèmes d'information. La norme ISO 27005 décrit le processus de gestion, mais ne fournit aucune orientation destinée à identifier ou à traiter les différents risques. Il appartient donc à chaque organisation de définir son approche en fonction du contexte de gestion des risques ou des caractéristiques du secteur d'activité concerné.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) développe des outils d'analyse des risques, notamment à travers la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité), qui permettent d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information. L'approche française facilite également la communication au sein de l'organisme et avec ses partenaires afin de contribuer au processus de gestion des risques de sécurité. La méthode EBIOS permet de mettre en œuvre les principes des normes ISO 27005 et ISO 31000.

En matière de gestion des incidents, l'ISO consacre un chapitre de la norme 27002 aux mécanismes pour la mise en place de procédures visant leur détection et leur traitement. D'autres référentiels de pratiques recommandées en sécurité de l'information, comme l'*Information Technology Infrastructure Library* (ITIL) et le *Control Objectives for Information and related Technology* (CobiT), mettent également l'emphase sur l'importance de développer des mécanismes efficaces de prise en charge des incidents.

2.2.2 Vigie internationale et nationale

En Australie, le gouvernement de l'État de Victoria a élaboré un cadre de gestion des risques, dans lequel il a clairement identifié que les conséquences de certains risques peuvent

[1] Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise

outrepasser le domaine d'un organisme, et a abordé la problématique de l'interdépendance entre ceux-ci. Cette notion est identifiée sous le terme « Risques interagences gouvernementales et risques horizontaux[2] ». Le cadre préconise que chaque agence produise un rapport annuel, dans lequel elle certifie qu'elle dispose d'un processus de gestion des risques effectif et à un niveau satisfaisant. Une entité centrale supervise les activités du processus en apportant un soutien et en tenant un registre sur les risques horizontaux.

Aux États-Unis, plus d'une organisation a élaboré des lignes directrices en matière d'autoévaluation ou de gestion des risques. Le département de la Sécurité intérieure des États-Unis (United States Department of Homeland Security) a élaboré, en 2009, des orientations en matière de risques, mettant l'emphase sur les fonctions essentielles du secteur des technologies de l'information. De son côté, l'Institut national des standards et de la technologie (National Institute of Standards and Technology) a élaboré un cadre de référence pour l'identification des risques dans les systèmes d'information de l'Administration.

Le gouvernement du Canada, quant à lui, a produit, en 2001, un premier cadre stratégique de gestion des risques, qui a ensuite été mis à jour en 2010. Selon le gouvernement fédéral, la gestion des risques peut être extrêmement rentable lorsque les ministères évaluent leurs risques convenablement et déterminent la façon la plus économique de les minimiser ou de les supprimer complètement.

Au niveau provincial, le gouvernement de la Colombie-Britannique a créé, dans sa structure administrative, une entité dédiée à l'encadrement de la gestion des risques au niveau gouvernemental, le *Risk Management Branch and Government Security Office*. Cette entité a produit des lignes directrices adressées aux ministères et aux organismes qui englobent tous les risques, et pas seulement ceux reliés à la sécurité de l'information. Le cadre prend appui sur la norme australo-néo-zélandaise AS/NSZ 4360.

En juillet 2013, l'Organisation de coopération et de développement économiques (OCDE) amendait la *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* du 23 septembre 1980. L'OCDE reconnaît notamment l'importance de l'évaluation des risques dans l'élaboration de politiques et de mesures pour protéger la vie privée. Elle reconnaît également le défi que représente la sécurisation des données de caractère personnel dans un environnement ouvert interconnecté, dans lequel les données de caractère personnel sont de plus en plus une ressource qui a de la valeur.

En ce qui a trait à la gestion des incidents en sécurité de l'information, autant les administrations que les grandes entreprises sont alignées sur la méthodologie des *Computer Emergency Response Team* (CERT), dont les bases furent établies par l'Université Carnegie Mellon à Pittsburgh en 1988. Les tâches prioritaires qui sont assumées par l'unité permanente qui constitue le CERT sont les suivantes :

- Centralisation des demandes d'assistance à la suite d'incidents de sécurité (attaques) sur les réseaux et les systèmes d'information : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents;

[1] «Interagency and statewide risks»

- Traitement des alertes et réaction aux attaques informatiques : analyses techniques, échanges d'information avec d'autres CERT, contribution à des études techniques spécifiques;
- Établissement et maintenance d'une base de données des vulnérabilités;
- Prévention par diffusion d'information sur les précautions à prendre pour minimiser les risques d'incidents ou, au pire, leurs conséquences;
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CERT nationaux et internationaux.

Par ailleurs, plusieurs États ont adopté des dispositions pour encadrer la déclaration des incidents de sécurité de l'information. C'est ainsi qu'en Alberta des mesures législatives, applicables au secteur public et privé, reliées aux failles de sécurité des renseignements personnels ont été adoptées[3].

Au plan européen, le parlement, par voie de directive[4], a rendu obligatoire, pour les entreprises fournissant des services de télécommunications publics, la déclaration à l'autorité nationale compétente de toute atteinte à la sécurité ayant eu un impact significatif sur le fonctionnement des réseaux et des services.

Aux États-Unis, obligation[5] est faite aux agences fédérales de déclarer à l'autorité nationale compétente (FISIC)[6] dans les 24 heures, sans excéder les 48 heures, les incidents de sécurité de l'information répondant à des critères déterminés.

2.2.3 Contexte gouvernemental québécois

Au plan gouvernemental québécois, depuis 2003, le Bureau du dirigeant principal de l'information met à la disposition des organismes publics, un outil méthodologique ainsi qu'un guide d'utilisation pour aider ces derniers à réaliser leurs analyses de risques en sécurité de l'information. Le ministère des Services gouvernementaux de l'époque, dans sa stratégie gouvernementale en sécurité de l'information 2005-2009, avait d'ailleurs fixé, comme date butoir, le 31 mars 2008, pour la réalisation, par les ministères et les organismes, des analyses de risques de sécurité des systèmes essentiels et stratégiques.

En juin 2011, la Commission d'accès à l'information du Québec (CAI) recommandait dans son rapport quinquennal[7] que la Loi sur l'accès et la Loi sur la protection dans le secteur privé soient modifiées par l'ajout d'une obligation de lui déclarer les failles de sécurité qui surviennent dans les organismes publics et les entreprises et qui impliquent des renseignements personnels.

Au plan sectoriel et en vertu des dispositions de la Directive sur la sécurité de l'information gouvernementale, les ministères et les organismes doivent, notamment, instaurer un mécanisme d'identification et d'évaluation périodique des risques afin de s'assurer de l'adéquation des mesures de sécurité en vigueur par rapport aux risques encourus.

---

[3] http://www.oipc.ab.ca/Content_Files/Files/Publications/Key_Steps_in_Responding_to_a_Privacy_Breach.pdf
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:fr:PDF, article 13 bis
[5] http://www.govtrack.us/congress/bills/113/hr1163/text/ih#
[6] FISIC : Federal information security incident center
[7] http://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf

Au dernier bilan de l'exercice 2009-2010, un peu plus de la moitié seulement des ministères et des organismes visés ont déclaré avoir réalisé au moins une analyse de risques, et environ le tiers de ces analyses dataient de plus de trois ans. Il y a donc encore des efforts à fournir pour que les risques de sécurité de l'information au plan sectoriel soient identifiés et pris en charge de manière adéquate.

Parmi les ministères et les organismes ayant réalisé une analyse de risques, huit d'entre eux ont identifié des risques susceptibles de produire des conséquences directes sur le fonctionnement d'autres ministères et organismes. Sept ministères et organismes ont quant à eux rapporté des risques susceptibles de mettre en danger la vie, la santé ou le bien-être des personnes, et trois ont identifié des risques susceptibles de nuire gravement à l'économie du Québec.

Le constat que nous pouvons tirer de l'analyse du contexte gouvernemental québécois est que certains types de risques pourraient causer des impacts au-delà du domaine d'une seule organisation et engendrer ainsi de graves conséquences pour l'Administration gouvernementale ou pour la population. L'expérience du DPI ainsi que les échanges avec les experts du domaine tendent à appuyer ce constat.

Les réponses au Rapport sur l'état de situation gouvernemental en matière de sécurité de l'information 2009-2010 tendent donc à confirmer le besoin de développer un mécanisme pour identifier, évaluer et faire un suivi de certains risques qui pourraient produire des conséquences graves. En effet, ce ne sont pas tous les ministères et organismes qui ont développé une connaissance approfondie de leurs risques, et un mécanisme de coordination, qui assurerait le suivi de la mise en œuvre des traitements, n'est actuellement pas intégré dans le processus gouvernemental de gestion de la sécurité.

En matière de gestion des incidents en sécurité de l'information, le gouvernement du Québec a mis sur pied une Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise (CERT/AQ). Ce dernier a pour mission d'aider les organismes publics dans la prévention et la gestion des incidents cybernétiques. Cette aide se traduit par des gestes concrets de prévention en sécurité informatique et de support lors d'incidents. Le CERT/AQ a également un mandat d'amélioration de la sécurité au gouvernement du Québec.

2.3 Positionnement sur les risques et les incidents à portée gouvernementale

La présente sous-section propose une façon de distinguer les risques et les incidents qui sont à portée gouvernementale de ceux dont la portée se limite à un seul organisme public, afin de permettre l'élaboration de processus de gestion appropriés.

2.3.1 Identification des risques à portée gouvernementale

Les RPG sont avant tout des risques dont les impacts débordent des limites d'un seul organisme public. Dans ce cas, l'organisme public qui est concerné n'est plus seul à devoir se prononcer sur l'application d'un traitement ou d'une mesure correctrice, car il n'est pas le seul à subir les conséquences liées à la réalisation de la menace anticipée. C'est le cas des menaces aux conséquences potentiellement graves pour la population ou pour l'image du gouvernement, ainsi que celles susceptibles de perturber les services offerts par d'autres organismes publics.

L'objectif premier des organismes publics est de fournir des services à la population. Certains de ces services sont indispensables, alors que d'autres ne le sont pas. Les services

indispensables sont ceux qui répondent aux besoins primaires des individus, également appelés besoins élémentaires ou physiologiques, comme se nourrir ou assurer la sécurité de leur personne physique. Le risque nuisant à l'accomplissement des services indispensables à la population revêt donc une importance particulière d'un point de vue gouvernemental et doit être considéré à portée gouvernementale.

Parallèlement, certains risques peuvent produire une conséquence qui ne peut être prise en charge seulement par l'organisme public qui y est exposé de façon directe. C'est notamment le cas de tous les risques reliés aux interdépendances en matière d'information ou de traitement de l'information entre organisations qui, généralement, créent des conséquences à plus d'un endroit lorsqu'ils se manifestent. Eux aussi devraient être considérés à portée gouvernementale.

La conséquence d'un risque peut, quant à elle, être mesurée selon l'importance de son impact, potentiel ou confirmé, sur la population. Il est d'usage de mesurer la gravité d'un impact sur la population selon l'empêchement de satisfaire les besoins fondamentaux, élémentaires ou physiologiques des individus, ou selon toute autre échelle distinguant les besoins élémentaires par rapport aux autres besoins non essentiels.

Par ailleurs, Il est établi par la Charte québécoise des droits et libertés de la personne et le chapitre 3 du Code civil que le droit à la réputation et au respect de la vie privée est un droit fondamental. Le risque dont la conséquence empêche la population de satisfaire à ses besoins et droits fondamentaux devrait lui aussi être considéré à portée gouvernementale. Un bris de confidentialité de renseignements personnels détenus par un organisme public peut donc affecter les droits fondamentaux des citoyens à la protection des renseignements personnels qui les concernent et peut également porter atteinte au droit au respect de leur vie privée.

Un autre critère selon lequel un risque donné peut être qualifié à portée gouvernementale est son importance sur l'image du gouvernement. Dans certains cas, l'image d'un seul organisme serait entachée par la mauvaise gestion d'un risque. Dans d'autres cas, c'est l'image du gouvernement dans son ensemble qui serait touchée, créant ainsi une situation nettement plus grave. Par exemple, un bris de confidentialité à l'égard d'information de nature sensible ou stratégique peut avoir un impact sur l'image de l'ensemble du gouvernement et susciter une perte de confiance des citoyens envers l'État.

En somme, un risque en matière de sécurité de l'information, placé dans le contexte d'un organisme public, peut donc être classifié selon l'importance ou la gravité des cinq catégories suivantes :

- L'entrave à la fourniture de services indispensables à la population;
- L'existence de conséquences directes ou indirectes sur d'autres organismes publics fournissant des services indispensables à la population;
- L'impact réel ou potentiel sur la sécurité et le bien-être de la population;
- L'impact réel ou potentiel sur le respect des droits des citoyens à la protection des renseignements personnels qui les concernent et au respect de leur vie privée;
- L'effet sur l'image du gouvernement et la perte de confiance des citoyens envers l'État.

2.3.2 Synthèse et définition du risque à portée gouvernementale

Le tableau ci-dessous résume les principaux éléments qui caractérisent un RPG et qui le distinguent d'un risque dont la portée se limite à une seule organisation, c'est-à-dire un risque à portée sectorielle (ou simplement « risque sectoriel »).

Un risque peut être considéré à portée gouvernementale s'il possède au moins une caractéristique de la colonne de droite.

Tableau 1 - Portée des risques

		Portée du risque	
		Sectorielle	**Gouvernementale**
Conséquence	**Pour l'Administration**	Limitée à un seul organisme public	Touche plus d'un organisme public
	Pour la population	Affecte des services qui **ne sont pas** indispensables[8] à la population La conséquence sur la santé ou le bien-être est circonscrite et maîtrisée	Affecte les services indispensables à la population Mets en danger la santé ou le bien-être d'un groupe d'individus Affecte la confidentialité de l'information sensible et porte atteinte au droit à la protection des renseignements personnels et au respect de la vie privée des personnes concernées
Image du gouvernement et confiance des citoyens		Affecte l'image d'un seul organisme, mais pas du gouvernement dans son ensemble N'est pas citée sur des tribunes importantes, dans des médias écrits à grand tirage, à la radio ou à la télévision	Affecte l'image du gouvernement et la confiance des citoyens

Pour un risque donné, ce ne sont pas toutes les caractéristiques de la colonne de droite qui doivent être rencontrées, mais une seule uniquement. Par exemple, il se peut que la concrétisation d'un risque n'ait aucune conséquence tangible pour la population. Dans un tel cas, aucune réponse ne peut être associée à cette ligne du tableau.

Une définition de cette nouvelle notion qu'est le risque à portée gouvernementale pourrait donc être formulée en reprenant l'essence des éléments présentés au tableau 1. Il va sans dire qu'un risque à portée gouvernementale est avant tout un risque, et que ce risque est relatif à la sécurité de l'information. À son tour, la sécurité de l'information se définit essentiellement à travers trois dimensions, soit la disponibilité, l'intégrité et la confidentialité.

La combinaison des quatre catégories de risques mentionnés à la section 2.4.1 permet d'énoncer la définition suivante :

Risque de sécurité de l'information à portée gouvernementale : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le

[8] Par « services indispensables » on entend « les services sans lesquels la santé ou le bien-être d'un groupe d'individus sont affectés ».

bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

2.3.3 Définition de l'incident à portée gouvernementale

Un incident en matière de sécurité de l'information peut être vu comme un événement qui se produit lorsqu'un risque se réalise. De façon similaire, un incident à portée gouvernementale pourrait être défini comme la conséquence de la réalisation d'un RPG.

L'utilisation des éléments présentés dans le tableau 1 pour définir l'incident à portée gouvernementale, qui rend la définition de l'IPG indépendante de celle du RPG, permet de produire la définition suivante :

Incident de sécurité de l'information à portée gouvernementale : Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale et qui nécessite une intervention concertée au plan gouvernemental.

2.3.4 Exemples de risques et d'incidents à portée gouvernementale

Selon le raisonnement de la section précédente, un risque de sécurité de l'information peut être considéré à portée gouvernementale s'il possède une ou plusieurs des caractéristiques précédemment énoncées, c'est-à-dire qu'il perturbe directement ou indirectement la livraison de services indispensables à la population, qu'il produise des conséquences sur la vie, la santé ou le bien-être des personnes et le respect de leurs droits fondamentaux, ou qu'il affecte l'image du gouvernement dans son ensemble, et suscite une perte de confiance des citoyens envers l'État.

Les mises en situation suivantes donnent des exemples de risques et d'incidents à portée gouvernementale :

Situation 1 : Un virus informatique affecte certains appareils du réseau de la santé et des services sociaux et force l'interruption de certains services de télécommunications, perturbant plusieurs activités au sein d'établissements voués au maintien de la santé et au bien-être des personnes.

Cette situation décrit un incident à portée gouvernementale, car elle met en danger la santé ou le bien-être d'un groupe d'individus.

Situation 2 : Un organisme analyse le risque et les conséquences potentielles d'un vol de renseignements personnels à son site de relève. Ces renseignements permettent l'identification des abonnés à ses services électroniques. La conclusion de l'analyse fait ressortir que les renseignements en question pourraient être utilisés pour demander frauduleusement la délivrance d'un permis auprès d'un autre organisme public. Cela peut également mener à un vol d'identité qui pourrait avoir de graves conséquences pour les personnes concernées.

La situation décrit un risque à portée gouvernementale, car la conséquence pour l'Administration ne se limite pas exclusivement à un seul organisme, mais pourrait en affecter un autre indirectement.

Situation 3 : Des mesures de sécurité du personnel inadéquates font en sorte que des informations devant être révélées lors du dépôt du budget sont connues des médias une journée à l'avance.

La situation décrit un incident à portée gouvernementale, car elle affecte l'image du gouvernement dans son ensemble.

3 GESTION DES RISQUES À PORTÉE GOUVERNEMENTALE

La présente section décrit l'approche en matière de gestion des RPG. Elle ne tient pas pour acquise la présence d'un processus de gestion des risques à portée sectorielle au sein des organismes publics, comme présenté à la section suivante, mais peut bénéficier de la présence d'un tel processus lorsque celui-ci est déjà instauré.

3.1prApproche évolutive et itérative

Il est nécessaire que l'approche adoptée par le DPI permette ultimement de recenser tous les risques à portée gouvernementale. De plus, la façon de mettre en œuvre l'identification des RPG ainsi que le choix des organismes publics à interpeler dans l'exercice doivent être adaptés aux échéanciers que le DPI souhaite appliquer au processus de gestion des RPG.

La liste suivante décrit les différentes étapes d'un processus simple permettant d'identifier les RPG. Ce processus inclut des itérations mettant en relation le DPI et les organismes publics afin de recenser les RPG et mettre en place des mécanismes de suivi appropriés.

1. Sélectionner un ensemble d'organismes publics à inclure dans un premier exercice d'identification des RPG;
2. Réaliser l'analyse des RPG avec les organismes publics sélectionnés;
3. Élaborer des recommandations en matière de traitement et d'intervention;
4. Documenter les interrelations et les dépendances en matière d'information gouvernementale avec les autres organismes publics;
5. Produire un rapport au Conseil du trésor;
6. Ajouter, pour la prochaine itération du processus, les organismes publics qui répondent aux deux critères suivants :
    - Ils n'ont pas déjà été étudiés par le DPI dans le cadre de l'identification des RPG;
    - Ils ont des interrelations ou des dépendances en matière d'information gouvernementale avec un ou plusieurs organisme(s) déjà étudié(s).

3.2 Présentation du modèle

La figure 1 ci-après présente une vue d'ensemble du processus proposé pour la gestion des RPG. Le DPI est l'entité gouvernementale qui coordonnera toutes les activités présentées. Les organismes publics qui prennent part à l'exercice sont consultés à deux étapes du processus. Ce modèle est valide qu'il y ait ou non un processus formel de gestion des risques dans les organismes publics qui prennent part à l'exercice.

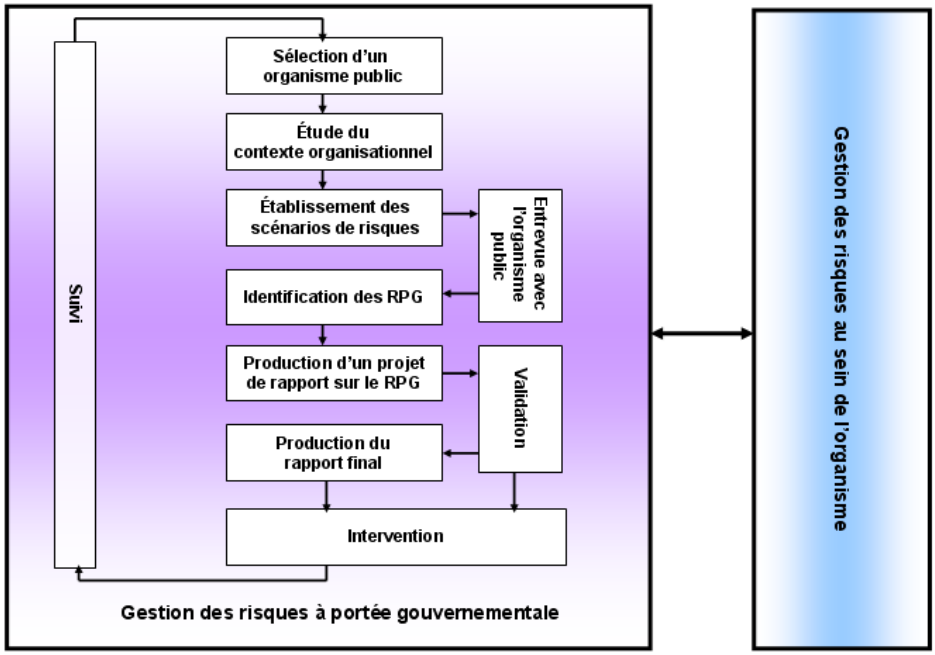

Figure 1 – Gestion des RPG

3.3 Détail des activités de gestion des risques à portée gouvernementale

Les différentes activités du modèle de gestion des RPG présentées à la figure 1 sont développées dans les sous-sections qui suivent.

3.3.1 Sélection d'un organisme public

La première étape du processus consiste en la sélection, par le DPI, d'organismes publics pour participer à l'identification des RPG.

À cette étape, le DPI informera chaque organisme sélectionné au moyen d'une communication officielle, permettant à l'organisme de désigner les ressources spécialisées en gestion des risques qui seront contactées par les représentants du DPI.

3.3.2 Étude du contexte organisationnel

Chaque fois qu'un organisme public est sélectionné, le DPI procède à l'analyse du contexte de l'organisme afin d'établir les bases à la formulation des scénarios de risques. L'étude du contexte organisationnel comprend le recensement des lois et des règlements qui définissent les responsabilités de l'organisme public, ainsi que la compréhension du cadre dans lequel il évolue.

Toute forme de documentation peut être utilisée pour étudier et documenter le contexte organisationnel, notamment les rapports de vérification, publiquement accessibles, produits par le Vérificateur général, ou toute source d'information fiable, rapports de gestion ou autres, qui énoncent des constats ou des recommandations.

Il est également nécessaire que l'étude du contexte brosse un premier portrait de toute forme d'interdépendance avec les autres organismes publics ou avec des tiers externes à

l'administration publique, afin de cerner les possibles effets en cascade ou cumulatifs qui pourraient être associés ultérieurement à un RPG.

3.3.3 Établissement des scénarios de risques

Une fois le contexte organisationnel établi, le DPI procédera à la constitution de scénarios de RPG susceptibles de toucher directement ou indirectement les activités de l'organisme qui est analysé.

Toute forme de documentation peut être utilisée pour établir les scénarios de risques, notamment l'évolution des menaces, les revues de presse, les orientations gouvernementales ou les rapports antérieurs sur les RPG. Ces scénarios devront prendre en considération l'état actuel des menaces et l'incidence de la concrétisation d'une menace sur la population, sur l'image du gouvernement ou sur les activités des autres organismes publics. Ils devront également couvrir de manière exhaustive les actifs informationnels les plus importants de l'organisme ainsi que les principaux services que l'organisme public livre à la population. Ce sont ces scénarios qui serviront de base à l'entrevue réalisée avec l'organisme.

3.3.4 Entrevue avec l'organisme public

Une fois les scénarios de risques établis, le DPI prendra rendez-vous avec l'organisme visé par l'exercice afin d'évaluer son exposition aux RPG. Au cours de l'entrevue, l'organisme validera les scénarios de risques élaborés par le DPI, et informera ce dernier sur les mesures de sécurité en place ainsi que sur son appréciation quant à leur efficacité.

L'organisme qui a une connaissance de ses risques, obtenue par un processus interne de gestion des risques en matière de sécurité de l'information, pourra alimenter le DPI sur l'importance du risque résiduel qui subsiste après l'application des mesures de sécurité. Dans le cas contraire, le DPI basera son analyse sur la description des mesures de sécurité en place et sur l'appréciation de leur efficacité pour déterminer quels risques sont des RPG.

3.3.5 Production d'un projet de rapport sur les risques à portée gouvernementale

Après l'entrevue avec l'organisme public, le DPI procédera à l'analyse des informations colligées lors de la rencontre, et corrigera au besoin tout élément de son étude du contexte organisationnel qui aurait été précisé lors des échanges. C'est lors de cette analyse que les RPG sont identifiés.

Cette étape peut nécessiter la mise en relation d'éléments qui sont externes à l'organisme qui prend part à l'exercice, comme c'est le cas lorsqu'il y a une forte dépendance en matière de ressources informationnelles avec des tiers. Le DPI constituera une cartographie des interdépendances pour soutenir son analyse des RPG, et la mettra continuellement à jour en y intégrant toute information nouvellement recueillie auprès des organismes publics.

3.3.6 Validation

L'organisme public sera informé des éléments du projet de rapport le concernant, et pourra commenter les constats du DPI en matière de RPG. Il pourra faire part de ses commentaires relatifs au projet de rapport et amener toute précision additionnelle relative aux RPG identifiés, ainsi qu'aux mesures de sécurité en place ou prévues pour les gérer.

3.3.7 Production du rapport final

Une fois le contenu du projet de rapport validé par les organismes publics et selon le cas, commenté ou précisé, le DPI produira la version définitive du rapport destiné au Conseil du trésor. Le DPI inclura dans ce rapport :

- La présentation des RPG recensés auprès des organismes publics qui auront été contactés au cours de l'exercice;
- Ses recommandations en matière de traitement des RPG identifiés;
- L'information sur le suivi et la prise en charge des RPG identifiés au cours des années antérieures, jusqu'à ce que le risque résiduel soit à un niveau qu'il juge acceptable.

3.3.8 Intervention

L'étape d'intervention est l'équivalent, dans le modèle de gestion du RPG, de l'étape de traitement du risque qui fait partie du processus de gestion au sein de l'organisme. Cette étape vise à s'assurer d'une prise en charge adéquate des RPG, en confirmant la présence d'un traitement proportionnel au RPG identifié.

Les principales étapes de l'intervention doivent permettre au DPI de :

- Recueillir l'information sur une stratégie de traitement d'un RPG, incluant l'échéancier de mise en œuvre par l'organisme responsable;
- Mettre à jour la cartographie des interdépendances en matière de RPG;
- Apprécier le niveau de risque résiduel qui subsiste après application d'une stratégie de traitement et juger de son acceptabilité au niveau gouvernemental;
- Formuler des recommandations de prise en charge du RPG, si nécessaire, à l'organisme public concerné.

Il est à noter que cette étape d'intervention n'est pas forcément séquentielle à l'étape « Production du rapport final », car si la situation le requiert, le DPI pourrait intervenir, auprès de l'organisme public concerné, immédiatement après l'étape de validation.

3.3.9 Suivi du risque

Comme c'est le cas pour les processus de gestion de risques au sein des organismes publics, le processus de gestion des RPG doit prévoir une activité de suivi qui est en relation avec les autres activités du modèle. Dans le cas du processus de gestion des RPG, le suivi doit au moins permettre :

- De s'assurer que les organismes publics disposent de toute l'information nécessaire pour alimenter le DPI en matière de RPG;

- D'analyser les événements dont les répercussions se font sentir à l'échelle gouvernementale afin d'assurer l'arrimage avec les critères d'identification des RPG;
- De contrôler le temps d'exécution des différentes étapes du processus et d'assurer un flux d'informations adéquat pour la production de rapports au Conseil du trésor, selon la fréquence désirée;
- D'identifier les risques émergents.

3.4 Relation avec la gestion des risques au sein des organismes publics

La gestion des risques à portée gouvernementale et la gestion des risques au sein des organismes publics sont deux grandes activités pouvant bénéficier, de manière réciproque, l'une de l'autre.

La gestion des RPG peut bénéficier du résultat de tout processus ministériel de gestion des risques, lequel pourrait identifier certains RPG, sans avoir suivi la démarche du DPI en cette matière. Cette situation s'explique par le fait qu'une analyse des risques, menée par un organisme, doit couvrir de manière exhaustive ses actifs informationnels, ainsi que les menaces auxquelles ces derniers sont exposés.

Réciproquement, un processus interne de gestion des risques en sécurité de l'information pourra bénéficier des extrants du processus de gestion des RPG. Par exemple, les constats du DPI, communiqués à l'organisme public, pourront être utilisés pour créer ou pour valider leur propre connaissance des risques, et des conséquences s'y rattachant, pour lui-même ou pour d'autres organismes, liées à une mauvaise gestion de ces derniers.

4 GESTION DES RISQUES AU SEIN DES ORGANISMES PUBLICS

Cette section présente le modèle de gestion des risques, comme il doit être appliqué au sein des organismes publics, afin d'atteindre les objectifs visés par le processus. Ce modèle fait également référence à l'interrelation possible avec le processus de gestion des RPG présenté à la section précédente.

4.1 Présentation du modèle

La figure 2 présente une vue d'ensemble sur les activités composant le modèle de gestion des risques inspiré de la norme ISO 31000.

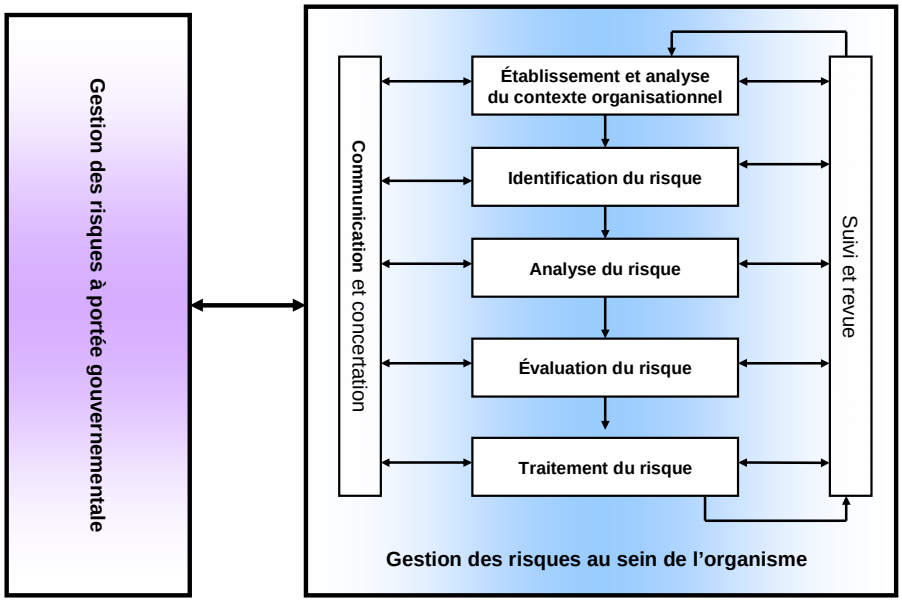

Figure 2 - Gestion des risques au sein d'un organisme public

4.2 Description des activités de gestion des risques au sein d'un organisme public

Une explication détaillée des différentes activités d'un processus interne de gestion des risques, lorsqu'un tel processus existe au sein d'un organisme public, est présentée dans les sous-sections qui suivent.

4.2.1 Établissement et analyse du contexte organisationnel

Le contexte organisationnel comprend les caractéristiques de l'environnement, dans lequel l'organisme public évolue en termes d'obligations légales et réglementaires, d'engagements contractuels ainsi que tout autre élément propre au domaine d'affaires de l'organisation et qui influence sa tolérance aux risques.

Il est très important d'appuyer les processus de gestion des risques au sein d'un organisme public par une compréhension commune de ce contexte organisationnel, car ce dernier aura une grande influence sur la suite du processus.

4.2.2 Identification du risque

Après avoir établi et documenté son contexte organisationnel, l'organisme public identifie les sources de risques, les différents impacts, les événements, ainsi que leurs causes et leurs conséquences potentielles. Cette étape a pour objectif de dresser une liste exhaustive des risques basée sur les événements susceptibles d'empêcher, de gêner ou de retarder l'atteinte des objectifs visés par les activités de l'organisme public.

Cette identification doit couvrir les risques dont la source est sous le contrôle de l'organisme public ou non, et ce, même si la source ou la cause du risque peut ne pas être évidente. De plus, il convient que l'identification du risque comporte l'examen des réactions en chaîne des conséquences particulières, y compris les effets en cascade et cumulatifs.

4.2.3 Analyse du risque

À cette étape du processus, l'organisme développe une compréhension approfondie du risque auquel il fait face. L'analyse fournit les données qui permettront aux autorités de décider de traiter les risques ou non. Elle permet de proposer des stratégies et des méthodes de traitement appropriées, surtout lorsque les différentes options impliquent des avantages et des inconvénients à prendre en considération.

L'analyse du risque implique la prise en compte des causes et des sources des différents risques, de leurs conséquences ainsi que de la vraisemblance que ces conséquences surviennent. Il convient de prendre en compte également les moyens de maîtrise des risques existants, leur efficacité et leur performance.

L'analyse du risque peut être menée à différents niveaux de détail en fonction du risque, de la finalité de l'analyse, des données et des ressources disponibles. Elle peut être qualitative ou quantitative selon les circonstances.

4.2.4 Évaluation du risque

Sur la base des résultats de l'analyse du risque, le but de l'évaluation du risque est de déterminer les risques nécessitant un traitement ainsi que la priorité dans la mise en œuvre des moyens de mitigation.

L'évaluation du risque consiste à mettre en relation le niveau de risques, déterminé au cours de l'étape d'analyse, avec les différents éléments issus de l'analyse du contexte organisationnel. Sur la base de cette comparaison, il est possible d'identifier quels sont les risques qui feront l'objet d'un traitement et d'anticiper sur la nature du mode de mitigation le plus approprié.

4.2.5 Traitement du risque

Le traitement du risque implique le choix et la mise en œuvre d'une ou de plusieurs mesures pour atténuer le risque. Il implique un processus itératif, touchant un ou plusieurs organisme(s) public(s) mettant en œuvre le traitement et évaluant son efficacité. Les principales étapes de ce processus sont :

- Évaluer un traitement du risque;
- Décider si le niveau de risques résiduel est tolérable;
- Générer un nouveau traitement du risque si le niveau n'est pas tolérable;

- Apprécier l'efficacité de ce traitement.

Les options de traitement du risque ne s'excluent pas nécessairement les unes des autres. Elles peuvent inclure :

- Un refus du risque marqué par la décision de ne pas commencer ou de poursuivre l'activité porteuse du risque;
- L'élimination de la source de risques;
- Une modification de la vraisemblance ou des conséquences du risque;
- Un partage du risque avec une ou plusieurs autres organisations (organismes publics ou organisations externes);
- Un maintien du risque fondé sur un choix argumenté.

4.2.6 Suivi et revue du risque

Tout processus de gestion de risques doit prévoir une activité de suivi qui est en relation avec les autres activités du modèle. Ce suivi peut être périodique ou ponctuel et devrait permettre à l'organisme public :

- De s'assurer que les moyens de maîtrise sont efficaces et performants, aussi bien dans leur conception que dans leur utilisation;
- D'obtenir des informations supplémentaires pour améliorer l'appréciation du risque;
- D'analyser et de tirer les leçons des événements (y compris des incidents en matière de sécurité de l'information), des changements, des tendances, des succès et des échecs;
- De détecter les changements dans le contexte organisationnel pouvant influencer la façon dont l'organisme gère ses risques ou ses priorités;
- D'identifier les risques émergents.

4.2.7 Communication et concertation

La communication et la concertation avec les différents intervenants dans la gestion du risque doivent être maintenues à toutes les étapes d'un processus de gestion des risques. Elles doivent faciliter des échanges d'information pertinents et précis.

Par conséquent, des stratégies de communication et de concertation doivent être élaborées relativement tôt. La communication et la concertation nous assureront que les intervenants, notamment les personnes responsables de la mise en œuvre des différentes activités, ont compris les principes de prise de décision et les raisons pour lesquelles certaines actions sont nécessaires.

5 POSITIONNEMENT EN MATIÈRE D'INCIDENTS À PORTÉE GOUVERNEMENTALE

La présente section expose les principaux constats relatifs à la gestion des incidents en matière de sécurité de l'information. L'information présentée tient compte des pratiques recommandées en matière de gestion des incidents qui devraient être mises en place dans les organismes publics.

5.1 Contexte de la gestion des incidents

Par rapport à la gestion des risques, où aucun mécanisme gouvernemental de coordination n'est actuellement en place, la gestion des incidents est appuyée par des processus centraux. En effet, le CSPQ, par l'entremise du CERT/AQ, offre aux organismes publics un ensemble de services liés à la prise en charge des incidents en sécurité de l'information, tels ceux relatifs aux réseaux de télécommunications, aux virus et autres codes malicieux, etc.

5.2 Positionnement sur les incidents à portée gouvernementale

L'offre gouvernementale en matière de gestion des incidents du CSPQ présente, par l'entremise du CERT/AQ, certaines forces, mais ne suffit pas à assurer la prise en charge de toutes les situations découlant d'un risque à portée gouvernementale. Les éléments suivants en décrivent certaines limitations :

- Les incidents sont déclarés sur une base volontaire par les organismes publics;
- Les incidents déclarés ne couvrent pas nécessairement tous les incidents, notamment ceux qui impliquent l'information sur des supports autres que numériques;
- L'absence d'un processus gouvernemental de gestion des incidents en sécurité de l'information facilite les communications entre les organismes publics et définit les stratégies de réaction appropriées, incluant la gestion de crise.

6 GESTION DES INCIDENTS À PORTÉE GOUVERNEMENTALE

La présente section décrit le processus de gestion des incidents à portée gouvernementale qui devrait compléter à la fois les processus de gestion des incidents mis en œuvre par les organismes publics et le processus de gestion des risques à portée gouvernementale.

6.1 Structure gouvernementale d'intervention

Le graphique qui suit présente la structure gouvernementale d'intervention proposée jusqu'à maintenant aux organismes publics en matière de gestion des incidents. Cette structure distingue la coordination gouvernementale, laquelle est constituée du Sous-secrétariat aux ressources informationnelles et bureau du dirigeant principal de l'information, du CERT/AQ et de la Sûreté du Québec, de la coordination ministérielle qui doit être mise en place après un incident de sécurité de l'information.

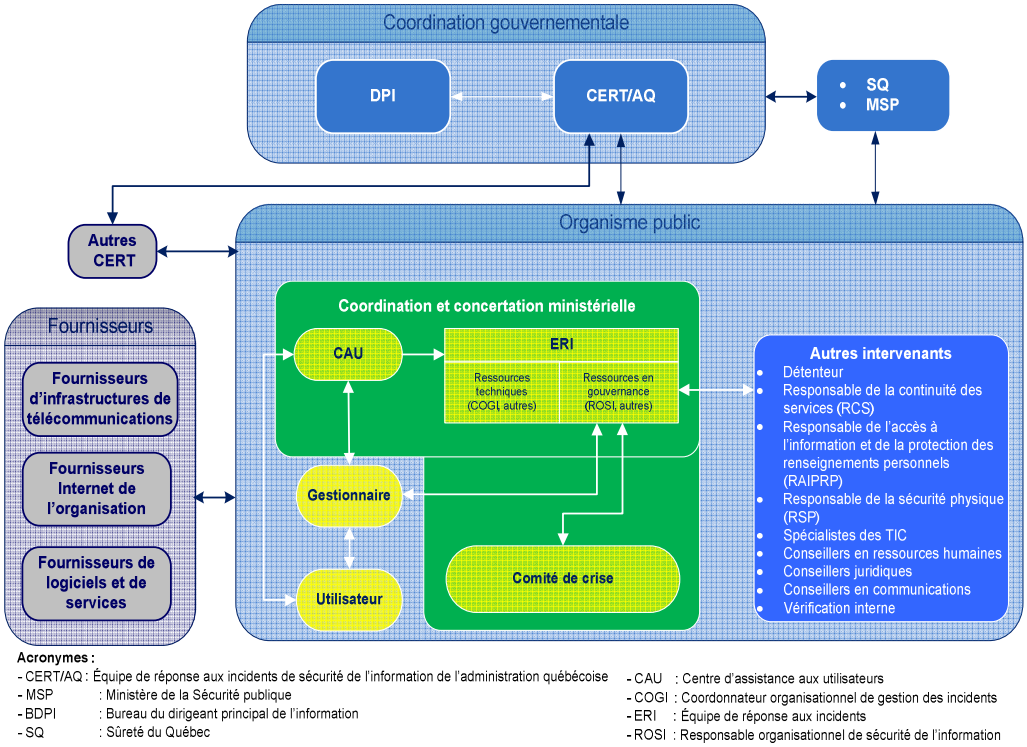

Figure 3 - Structure gouvernementale d'intervention

Selon le modèle de la figure 3, un premier niveau de coordination et de concertation, à la suite d'un incident de sécurité de l'information, est présent dans l'organisme public concerné. Cette coordination interpelle tous les spécialistes et les intervenants qui sont les plus susceptibles de détenir les connaissances fines permettant de cerner l'incident et de freiner sa propagation.

L'équipe de coordination au sein de l'organisme public est en relation avec les fournisseurs externes de l'organisme public, avec les autres équipes de réponse aux incidents en sécurité de l'information ainsi qu'avec le niveau gouvernemental de coordination. Ce second niveau de coordination constitue le comité de crise, commun à tous les organismes publics, qui assure la coordination horizontale à la suite d'un incident.

Le modèle de la figure 3 doit évoluer afin de mettre en évidence le rôle du comité de crise gouvernemental, lequel constitue le centre de coordination de la réaction à un IPG qui n'est pas déjà maîtrisé par les différentes mesures palliatives.

De plus, certains éléments compléteront le modèle de la figure 3 afin de faciliter la mise en œuvre de la structure gouvernementale d'intervention. Un processus gouvernemental, connu et révisé périodiquement, doit ainsi être développé afin de clarifier les rôles et les responsabilités, d'identifier nommément les personnes à alerter en cas d'IPG, etc.

6.2 Rôles et responsabilités des intervenants

6.2.1 Coordination gouvernementale

La coordination gouvernementale en cas d'incident repose en premier lieu sur la communication entre les différentes instances dotées de responsabilités particulières (CERT/AQ, SQ, MSP), le DPI, les responsables et les conseillers organisationnels en sécurité de l'information et les coordonnateurs organisationnels de gestion des incidents. Une communication régulière, soutenue par des mécanismes appropriés à une situation de crise, permettra aux différents intervenants de jouer leur rôle de manière efficace, en partageant une information à jour sur l'état de la situation.

Ainsi, l'instauration d'un processus gouvernemental de gestion des incidents permet de renforcer la capacité des organismes publics à détecter de tels incidents et à réagir de façon diligente, coordonnée et concertée. Il permet également, advenant un incident à portée gouvernementale, de s'assurer que les actions appropriées seront posées.

De plus, ce processus établit le seuil à partir duquel un protocole gouvernemental d'intervention doit être enclenché de même que les différentes étapes d'intervention, incluant la gestion de crise.

6.2.2 Organismes publics

La gestion des incidents à portée gouvernementale doit être encadrée par des règles précises quant à l'obligation des organismes publics de déclarer, auprès du CERT/AQ, les incidents à portée gouvernementale. Celui-ci leur apportera le soutien et l'assistance leur permettant d'en assurer adéquatement la gestion.

Également, les organismes publics devront mettre en œuvre un processus sectoriel de gestion des incidents et prévoir ses interactions avec le processus gouvernemental. Pour ce faire, ils prendront appui sur la pratique gouvernementale intitulée « Guide de gestion des incidents à portée sectorielle et gouvernementale ».

6.2.3 Fournisseurs

À toutes les étapes du processus de gestion d'un incident de sécurité de l'information, les instances de coordination doivent être en mesure d'impliquer, directement ou indirectement, les fournisseurs de services qui sont en relation avec les organismes publics. Qu'il s'agisse de la gestion d'un incident de nature technologique ou non, chaque fournisseur qui exploite, héberge ou conserve une partie des ressources informationnelles d'un organisme public peut avoir un rôle à jouer dans la gestion d'un incident.

7 GESTION DES INCIDENTS AU SEIN DES ORGANISMES PUBLICS

La présente section décrit les différentes activités qui devraient être en place dans les organismes publics en matière de gestion des incidents. Le processus de gestion des incidents à portée gouvernementale pourra prendre appui sur ces activités, et les mettre en relation au moment opportun avec des instances gouvernementales de coordination.

Les activités en question sont représentées à la figure 4. Elles débutent par la prévention face aux incidents en sécurité de l'information, et se terminent lorsqu'un organisme qui a été confronté à un incident s'en est rétabli totalement.

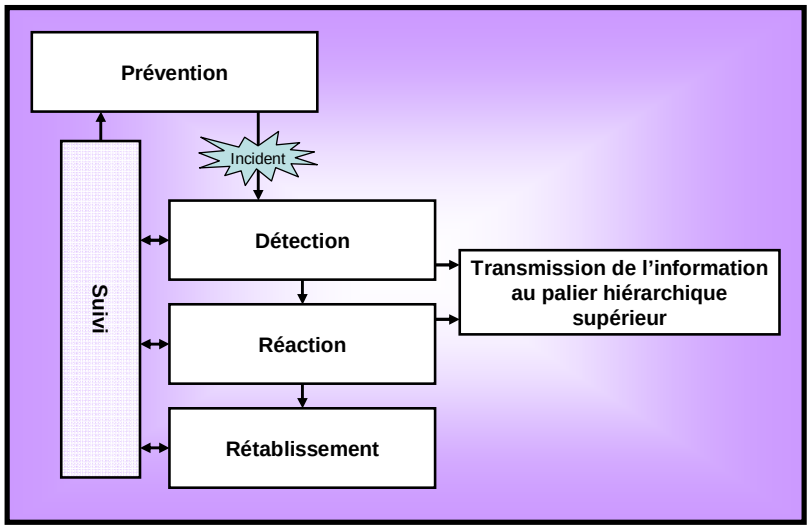

Figure 4 - Gestion des incidents au sein des organismes publics

7.1 Prévention

La prévention est la première activité qui devrait être présente, continuellement, dans toute organisation. Elle se traduit notamment par l'évaluation périodique des risques en matière de sécurité de l'information, par la mise en place d'une stratégie de vigie, par l'analyse des situations de vulnérabilité ainsi que par la formation et la sensibilisation continues des utilisateurs.

7.2 Détection

La détection est l'étape de gestion d'un incident qui permet de limiter ses effets sur l'organisation, en déployant les mesures permettant sa surveillance ou sa détection. Ces mesures, d'ordre organisationnel, juridique, technique ou humain, peuvent varier d'une organisation à l'autre et dépendent de plusieurs facteurs, notamment, l'architecture d'entreprise et l'architecture de sécurité de l'organisation, l'exposition aux menaces et la sensibilité de l'information traitée.

7.3 Réaction

La réaction permet à l'organisation de se mettre dans un mode réactif advenant un incident. Ce mode implique les actions d'analyse et d'évaluation des conséquences, de confinement des dommages occasionnés par l'incident, d'éradication de la cause de l'incident ou de recours à du personnel spécialisé ou à un palier hiérarchique supérieur.

La réaction à un incident comprend habituellement l'analyse et l'évaluation des conséquences, le confinement des dommages et l'éradication.

7.3.1 Transmission de l'information au palier hiérarchique supérieur

Dès la confirmation d'un incident potentiel ou réel, un processus de transmission de l'information au palier hiérarchique supérieur doit être amorcé. Ce processus s'inscrit dans un cadre gouvernemental visant la coordination des actions exécutées par divers intervenants.

La transmission de l'information au palier hiérarchique supérieur, parfois appelé « escalade », est un processus qui se définit comme un ensemble de procédures préétablies permettant, selon le niveau de gravité d'un incident, de recourir à des spécialistes ou à un palier de décision supérieur. Un tel processus doit être approuvé par la haute direction et être communiqué aux intervenants concernés. Une liste de personnes impliquées dans le processus doit être préalablement dressée et tenue à jour.

7.4 Rétablissement

Une fois l'incident traité et sa cause éliminée, il convient de recourir à une procédure de rétablissement afin de ramener l'organisation à une situation jugée acceptable. Dans le cas du traitement d'un incident de nature technologique, le rétablissement peut nécessiter la reconstruction des systèmes impactés.

7.5 Suivi

Cette étape, qui agit de manière transversale à travers les différentes étapes de la gestion des incidents, a pour objectif la constitution de toute documentation se rapportant aux événements relatifs à l'incident, ainsi que la mise à jour des directives et des procédures.

8 CONCLUSION

La vigie effectuée au niveau national et international, de même que l'expérience acquise en matière d'encadrement de la sécurité de l'information gouvernementale, tendent à démontrer la possibilité d'améliorer les processus existants de gestion des risques et de gestion des incidents en matière de sécurité de l'information. Le besoin provient essentiellement de l'absence d'un mécanisme formel de gestion pour les risques et les incidents à portée gouvernementale.

Les façons modernes d'organiser et de livrer les services à la population et aux entreprises poussent à sa limite le modèle actuel de gestion des risques et des incidents, lequel est fortement teinté d'une approche *en silo*. Certains gouvernements ont d'ailleurs déjà identifié le besoin que certains risques soient gérés d'une manière gouvernementale, plutôt qu'à un niveau ministériel ou sectoriel.

Le DPI du gouvernement du Québec est l'autorité la mieux placée pour coordonner les processus de gestion des risques et des incidents à portée gouvernementale, car ce dernier pourrait tirer profit des autres activités qu'il réalise en matière de gouvernance des ressources informationnelles. La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement donne d'ailleurs, au DPI, toute la légitimité en cette matière au sein d'un ensemble important d'organismes publics.

Ces derniers doivent prendre conscience que certaines actions en matière de sécurité doivent être cordonnées au niveau gouvernemental, plutôt que gérées à l'intérieur de chaque organisme. Le développement d'une culture gouvernementale pour gérer certains risques et

certains incidents devrait d'ailleurs s'appuyer sur l'expertise de chaque organisme public. Chaque organisme public est susceptible de trouver des avantages à collaborer avec le DPI en cette matière.

Le processus de gestion des RPG à mettre en place aurait enfin avantage à couvrir les activités pouvant être réalisées dans chacune des quatre dimensions de la sécurité civile, notamment dans l'optique d'assurer un équilibre avec la gouvernance des ressources informationnelles qui supporte les activités courantes des organismes publics. Les différentes activités liées aux missions du PNSC seraient donc couvertes par un processus horizontal de gestion des risques, en plus des processus sectoriels qui devraient être présents chez les différents porteurs de mission.

9 RÉFÉRENCES

ISO 27005 : Information technology – Security Techniques – Information security risk management, International Organization for Standardization – ISO (2008).

ISO 31000 : Management du risque – Principes et lignes directrices de mise en œuvre, International Organization for Standardization – ISO (2008).

Gouvernement du Canada, Cadre de gestion intégrée du risque, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12254.

Gouvernement de Colombie-Britannique, Risk Management Branch & Government Security Office Enterprise Risk Management, http://www.fin.gov.bc.ca/pt/rmb/erm.shtml.

Department of Homeland Security, Information Technology Sector Baseline Risk Assessment, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

NIST Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective, http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf.

Agence nationale de la sécurité des systèmes d'information, EBIOS 2010 - Expression des besoins et identification des objectifs de sécurité, http://www.ssi.gouv.fr/.

Gouvernement du Québec - Guide sur la gestion des incidents de sécurité de l'information gouvernementale(2010).

Québec

UN
QUÉBEC
POUR TOUS