Pratique recommandée en sécurité de l'information

PR-062

Guide d'élaboration et de mise en œuvre d'un processus de gestion des risques de sécurité de l'information

Guide d’élaboration et de mise en œuvre d’un processus de gestion des risques de sécurité de l’information

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71123-0

Table des matières

Sigles et Acronymes ____ III
Remerciements ____ IV
Notes à l'intention du lecteur ____ IV
Préambule ____ 1
1. Introduction ____ 2
1.1 Contexte ____ 2
1.2 Portée ____ 3
1.3 Public cible ____ 3
1.4 Cadre légal et normatif ____ 3
2. Positionnement du processus de gestion des risques de sécurité de l'information (PGRSI) ____ 4
3. Définition des rôles et responsabilités ____ 6
4. Démarche d'élaboration et de mise en œuvre d'un PGRSI ____ 8
4.1 Étape 1 – Établissement du contexte ____ 8
4.1.1 Organisation de la gestion des risques ____ 8
4.1.2 Champ d'application et portée ____ 8
4.1.3 Facteurs d'évaluation des risques ____ 8
4.2 Étape 2 – Analyse des risques ____ 9
4.2.1 Identification des risques ____ 9
4.2.2 Estimation ou évaluation des risques ____ 12
4.2.3 Classement des risques (réordonnancement) ____ 13
4.2.4 Identification des risques à portée gouvernementale ____ 13
4.2.5 Procédure de communication des risques à portée gouvernementale ____ 15
4.3 Étape 3 – Plan de traitement des risques ____ 15
4.3.1 Traitements possibles ____ 15
4.3.2 Acceptation du plan de traitement des risques ____ 16
4.4 Étape 4 – Mise en place des mesures de sécurité ____ 17
4.5 Étape 5 – Communication des risques ____ 17
4.6 Étape 6 – Revue des risques ____ 17

4.7 ÉTAPE 7 – AMÉLIORATION DE LA GESTION DES RISQUES _____ 18
5. EXEMPLE CONCRET D'APPLICATION DU PGRSI _____ 19
ANNEXE I DÉFINITIONS _____ 25
ANNEXE II CADRE LÉGAL ET NORMATIF _____ 26
ANNEXE III LES INDICATEURS D'APPRÉCIATION DU PRGSI _____ 27

Sigles et Acronymes

OP :	Organisme public
PGRSI :	Processus de gestion des risques de la sécurité de l'information
SGSI :	Système de gestion de la sécurité de l'information

Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel pour leur participation et le travail accompli.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Lyonel Vallès, chargé de projet
Socheat Sonn, conseiller
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Daniel Landry
Sureté du Québec

Carmen St-Laurent
Bureau de décision et révision

Mohamed Nasr
Régie du logement

Diane Archambault
TéléQuébec

Hind Belqorchi
Curateur public du Québec

Alain R. Pagé
Régie de l'énergie

Notes à l'intention du lecteur

Note 1 :	Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document.
Note 2 :	Le terme « organisme public » ou « organisme » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].
Note 3 :	Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.
Note 4 :	Certains termes ou acronymes sont définis à leur première apparition dans le texte. Ces définitions sont également présentées à l'annexe A – Acronymes, sigles et définitions

Préambule

Le présent guide propose une démarche visant à soutenir les organismes publics dans l'élaboration et la mise en œuvre d'un processus de gestion des risques de sécurité de l'information (PGRSI).

Conforme à la norme ISO/IEC 27005 et prenant appui sur la norme ISO/IEC 31000, le PGRSI permet aux organismes publics (OP) de prendre en charge les risques de sécurité de l'information auxquels ils sont exposés. Le processus se décline en sept étapes et permet l'analyse des risques ainsi que l'établissement de leur plan de traitement.

Tenant compte du fait que certains risques peuvent dépasser les limites d'un organisme public, le PGRSI prend également en compte les risques ayant une portée gouvernementale; le processus décrit donc les procédures nécessaires à leur déclaration au dirigeant principal de l'information (DPI).

Le présent guide fournit des exemples concrets, une liste d'indicateurs d'appréciation d'un PGRSI pour s'assurer de l'efficacité de la mise en œuvre du processus et une étude de cas portant sur un OP fictif, suffisamment élaborée pour permettre une bonne compréhension de la démarche proposée.

1. Introduction

La protection de l'information, qu'elle soit numérique ou non, est au cœur des préoccupations de tout organisme public. Ces préoccupations revêtent une grande importance, car les technologies de l'information sont en constante évolution et le volume d'information produite, enregistrée et échangée à chaque année s'accroît de plus en plus. En effet, cette situation a fait apparaître de nouvelles menaces et de nouveaux risques pouvant altérer la disponibilité, l'intégrité et la confidentialité de l'information.

C'est en relation directe avec cette évolution que la gestion des risques[1] est devenue une pratique incontournable en matière de gouvernance de la sécurité de l'information. Celle-ci est à la base de toute action de sécurité de l'information. Elle ne doit pas être perçue comme une contrainte, mais comme un défi qu'il faut constamment relever.

La grande majorité des organismes sont conscients de l'importance d'une bonne gestion des risques de sécurité de l'information; toutefois, les résultats du bilan gouvernemental sur la sécurité de l'information pour l'exercice 2010-2012 indiquent que des efforts doivent encore être consentis avant qu'une telle pratique ne soit adoptée par l'ensemble des organismes publics.

1.1 Contexte

Le présent guide s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information. Celle-ci prend appui sur la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, sur la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics et sur quatre documents définissant le nouveau cadre de gouvernance de la sécurité de l'information dans l'Administration québécoise :

- ✓ La Directive sur la sécurité de l'information gouvernementale, qui énonce, à l'article 7, alinéa c), que les organismes publics doivent « s'assurer de la mise en œuvre des processus formels de sécurité de l'information permettant, notamment, d'assurer la gestion des risques [...] ».
- ✓ Le Cadre gouvernemental de gestion de la sécurité de l'information, qui complète les dispositions de la Directive sur la sécurité de l'information gouvernementale, en précisant l'organisation fonctionnelle de la sécurité de l'information ainsi que les rôles et responsabilités sur les plans gouvernemental et sectoriel.
- ✓ L'Approche stratégique gouvernementale en sécurité de l'information 2014-2017, qui fixe les cibles gouvernementales à atteindre en matière de sécurité de l'information pour les trois prochaines années et définit les indicateurs gouvernementaux de suivi du degré d'atteinte de celles-ci. D'ailleurs, la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information pour l'ensemble des organismes publics constitue l'un des objectifs stratégiques de cette approche.
- ✓ Le Cadre de gestion des risques et des incidents à portée gouvernementale, qui présente une approche novatrice de gestion des risques et des incidents susceptibles de porter atteinte à la sécurité de l'information gouvernementale et qui peuvent 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 fournie par d'autres organismes publics.

1. Risque **:** De manière générale, sans être nécessairement appliqué au domaine de la sécurité de l'information, un risque est une probabilité d'apparition d'une menace qui, devant l'exploitabilité d'une vulnérabilité, peut potentiellement entraîner un impact sur un actif informationnel (actif ou information).

1.2 Portée

Le présent guide couvre les étapes d'élaboration, de mise en œuvre et d'amélioration d'un processus de gestion des risques de sécurité de l'information.

Il s'applique à l'information gouvernementale consignée dans un document, au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). L'information visée est celle qu'un organisme public détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

Le processus décrit dans le présent guide n'est pas limité aux risques de type technologique; il est applicable à toute forme de risque de sécurité de l'information, quelles qu'en soient la source, la nature, la gravité ou la catégorie d'impact associée.

Il est à l'usage des organismes publics visés par l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

1.3 Public cible

Le présent guide est principalement à l'usage :

- ✓ du responsable organisationnel de la sécurité de l'information (ROSI);
- ✓ du conseiller organisationnel en sécurité de l'information (COSI);
- ✓ du coordonnateur organisationnel de gestion des incidents (COGI);
- ✓ des détenteurs de l'information ou de leurs mandataires désignés;
- ✓ d'intervenants dans des domaines connexes à la sécurité de l'information (vérificateur interne, responsable de gestion documentaire, responsable de la sécurité physique, etc.).

Les responsabilités de ces derniers en matière de sécurité de l'information sont décrites dans le cadre gouvernemental de gestion de la sécurité de l'information. Les responsabilités qui sont liées à la gestion des risques sont détaillées au chapitre 3**.** Définition des rôles et responsabilités.

1.4 Cadre légal et normatif

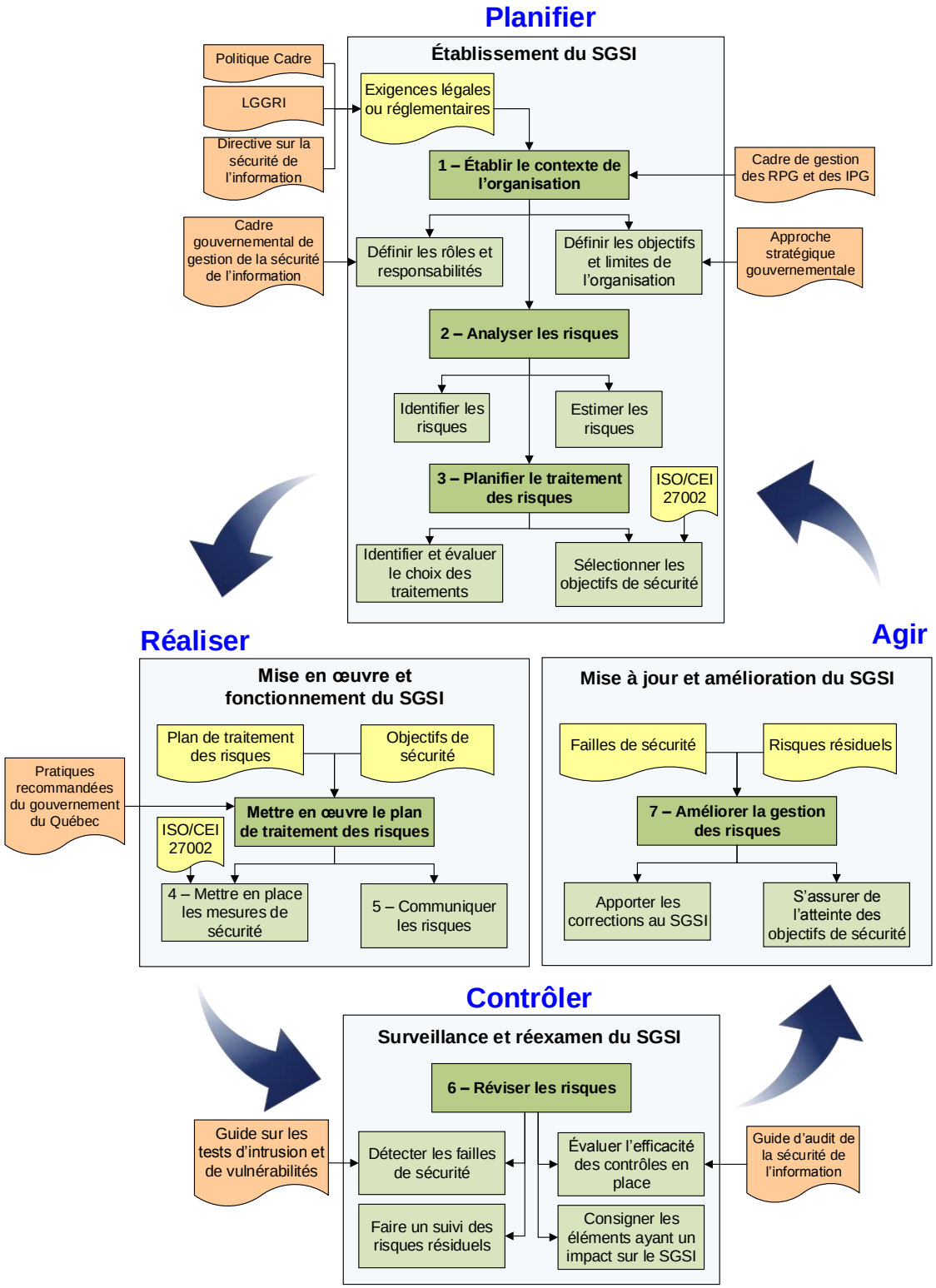
Le processus de gestion des risques de sécurité de l'information (PGRSI) s'inscrit dans un cadre légal et normatif comprenant des lois, des directives, des pratiques gouvernementales, des normes internationales et des standards de l'industrie. Les principaux éléments constitutifs de ce cadre sont présentés à l'Annexe III.

2. Positionnement du processus de gestion des risques de sécurité de l'information (PGRSI)

Dans le chapitre 2, nous proposons une illustration permettant de positionner le PGRSI par rapport au système de gestion de la sécurité de l'information (SGSI), comme le préconise la norme ISO/IEC 27001. Cette norme propose une démarche d'amélioration continue de la sécurité de l'information, axée sur les risques.

La figure 1 illustre la structure d'un SGSI de façon globale. Elle y intègre ses composantes, numérotées de 1 à 7, dans les 4 étapes du cycle d'amélioration continue de la sécurité de l'information (planifier, réaliser, contrôler et agir).

Figure 1 - Système de gestion de la sécurité de l'information



3. Définition des rôles et responsabilités

La mise en place d'un PGRSI par un organisme public nécessite la contribution de plusieurs intervenants. Le tableau présenté ci-dessous en décrit les rôles et responsabilités.

Acronyme ou sigle	Rôle	Responsabilité
Dirigeant OP	Dirigeant d'organisme public	S'assurer de la mise en place de mesures de réduction des risques de sécurité de l'information, valider les plans de traitement des risques provenant du PGRSI, orienter les décisions de gestion en fonction des risques identifiés et traités.
DRI	Dirigeant réseau de l'information	Suivre la mise en œuvre des PGRSI des établissements de son réseau et examiner leurs plans d'action.
DSI	Dirigeant sectoriel de l'information	Suivre la mise en œuvre des PGRSI des établissements qui lui sont rattachés et examiner leurs plans d'action.
ROSI	Responsable organisationnel de la sécurité de l'information	Assister le dirigeant de l'OP dans la détermination des orientations stratégiques et des priorités d'intervention, présenter les plans de traitement des risques au comité de sécurité de l'information et au dirigeant de l'OP, inviter les entités administratives visées à désigner leurs représentants aux différents ateliers de gestion des risques, ajuster les priorités de traitement des risques.
COSI	Conseiller organisationnel en sécurité de l'information	Contribuer à la conception et à la mise en œuvre de processus formels de sécurité de l'information, notamment celui de la gestion des risques. Le COSI anime les ateliers de gestion des risques, assiste les détenteurs dans la définition des plans de traitement des risques et vérifie le déploiement des contrôles de sécurité.
RGRSI	Responsable de la gestion des risques de sécurité de l'information	Certaines organisations peuvent attribuer la gestion des risques à un seul intervenant distinct (autre que le COSI ou le ROSI), soit le responsable de la gestion des risques de sécurité de l'information (RGRSI). Son rôle étant d'intervenir en matière de gestion des risques en sécurité de l'information, le RGRSI a les responsabilités combinées du COSI et du ROSI, précédemment décrites. Il travaille en étroite collaboration avec le ROSI pour assurer le suivi de la gestion des risques. Puisque le RGRSI s'occupe du volet gestion des risques en sécurité de l'information, le COSI n'aura pas à le faire.
COGI	Coordinateur organisationnel de la gestion des incidents	Contribuer à la mise à jour des risques en fonction des différents incidents survenus, vérifier l'aspect opérationnel des contrôles de sécurité.
Détenteurs	Détenteur d'actifs ou d'information	Orienter les priorités des plans de traitement des risques. Signaler au ROSI les effets possibles des changements organisationnels sur les contrôles existants.

Acronyme ou sigle	Rôle	Responsabilité
RASI	Responsable de l'architecture de sécurité de l'information	Intervenir dans les ateliers de gestion des risques pour le volet « Architecture de sécurité de l'information », arrimer les contrôles de sécurité à l'architecture de sécurité.
RGTI	Responsable de la gestion des technologies de l'information	Intervenir dans les ateliers de gestion des risques pour le volet « Technologies de l'information », arrimer les contrôles de sécurité aux technologies de l'information, informer les participants aux ateliers de gestion des risques des contrôles existants et opérationnels.
RCS	Responsable de la continuité des services	Intervenir dans les ateliers de gestion des risques pour le volet « Continuité des services », arrimer les contrôles de sécurité aux stratégies de continuité des services.
RSP	Responsable de la sécurité physique	Intervenir dans les ateliers de gestion des risques pour le volet « Contrôles physiques », arrimer les contrôles de sécurité aux contrôles physiques existants, informer les participants aux ateliers de gestion des risques des différents contrôles existants et opérationnels.
RDASI	Responsable du développement ou de l'acquisition de systèmes d'information	Contribuer aux ateliers de gestion des risques pour le volet « Intégration de la sécurité, des contrôles et de la PRP dans le développement ou l'acquisition de systèmes d'informations ».
RAIPRP	Responsable de l'accès à l'information et de la protection des renseignements personnels (PRP)	Contribuer aux ateliers de gestion des risques pour le volet « Protection des renseignements personnels ».

4. Démarche d'élaboration et de mise en œuvre d'un PGRSI

La démarche d'élaboration et de mise en œuvre d'un PGRSI s'appuie sur des ateliers de travail, organisés au sein d'un organisme public. Elle est réalisée en sept étapes.

4.1 Étape 1 – Établissement du contexte

Quel que soit le type d'actif informationnel[2] considéré, la gestion des risques requiert que soient précisés l'organisation à mettre en place, le champ d'application et la portée du processus ainsi que les facteurs d'évaluation des risques.

4.1.1 Organisation de la gestion des risques

La gestion des risques se fait dans le cadre d'ateliers de travail animés par le responsable organisationnel de la sécurité de l'information (ROSI) ou son représentant, éventuellement le conseiller organisationnel en sécurité de l'information (COSI). Plusieurs intervenants peuvent y participer, notamment les détenteurs des actifs étudiés et d'autres intervenants qui auront pour tâche de rendre disponible l'information relative à leur domaine d'activité respectif. Citons, à cet égard, le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP), le responsable de l'architecture de sécurité de l'information (RASI), le responsable de la gestion des technologies de l'information (RGTI), le responsable de la continuité des services (RCS), etc.

4.1.2 Champ d'application et portée

On procède à la définition du champ d'application et de la portée du PGRSI afin d'assurer que les actifs visés sont pris en compte dans l'appréciation du risque. Le champ d'application peut ainsi être restreint pour, à titre d'exemple, se limiter aux risques découlant d'actions involontaires ou de non-conformité à certaines dispositions légales.

4.1.3 Facteurs d'évaluation des risques

Les facteurs d'évaluation des risques doivent être définis pour déterminer les priorités du traitement des risques associés à un actif informationnel. Selon le domaine d'application et les objectifs de la gestion des risques, différents facteurs peuvent s'appliquer. À titre d'exemple, les facteurs suivants peuvent être considérés : facteurs DIC[3], risques associés à la PRP, etc.

Les critères d'impact des risques

- ✓ Les critères d'impact (ou de conséquence) des risques sont définis en fonction du degré de dommages ou des coûts engendrés par une concrétisation d'un risque lié à la sécurité de l'information. Ces critères d'impact sont à surveiller et à contrôler par l'organisation et permettent d'évaluer le niveau de gravité des risques. À titre d'exemple, les critères suivants peuvent être considérés :
- ✓ l'atteinte à la disponibilité, à la confidentialité et à l'intégrité de l'information;

2. Actif informationnel : Tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1). Cette même loi assimile au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.
3. DIC : Disponibilité, intégrité, confidentialité.

- ✓ la perte d'activités, de services ou de valeur financière;
- ✓ l'atteinte à l'image de marque de l'organisation;
- ✓ le non-respect des exigences légales et réglementaires;

Les seuils de tolérance aux risques

- ✓ Il convient que l'organisme définisse les seuils de tolérance aux risques, afin de prendre une décision éclairée en ce qui a trait à l'acceptation d'un risque. Ces seuils de tolérance sont multiples et dépendent souvent des politiques, des objectifs et des intérêts des parties prenantes de l'organisation. À titre d'exemple, les seuils suivants peuvent être utilisés :
- ✓ le rapport entre les bénéfices estimés et le risque estimé;
- ✓ le rapport entre les coûts et les bénéfices lorsqu'un risque est accepté;
- ✓ le délai de mise en place des mesures de sécurité pour atténuer un risque;
- ✓ le respect des exigences légales et réglementaires ainsi que des normes et standards;

4.2 Étape 2 – Analyse des risques

L'analyse des risques permet d'identifier et de classer les risques selon la priorité de traitement qui leur sera accordée. Cette étape regroupe :

1. l'identification du risque, qui consiste à déterminer une liste de risques (pour un actif informationnel donné en fonction des critères définis précédemment);
2. l'évaluation du risque, qui permet d'en mesurer l'importance et, par conséquent, de déterminer, pour chaque actif informationnel, une liste de risques triée par ordre d'importance;
3. le classement des risques, qui permet de les réordonner selon leur importance en matière de priorité de traitement, établie à l'aide de paramètres complémentaires comme des choix de gestion.

4.2.1 Identification des risques

À partir des critères de base prédéfinis, l'étape d'identification des risques permet de produire une liste de risques potentiels à évaluer pour chaque actif informationnel étudié, tout en se demandant comment, où et quand ces risques peuvent survenir.

L'identification des risques se fait selon cinq activités complémentaires :

1. l'identification des actifs informationnels;
2. l'identification des menaces;
3. l'identification des mesures de sécurité existantes;
4. l'identification des vulnérabilités;
5. l'identification des impacts.

Il est à noter que, selon la méthodologie choisie, ces activités peuvent être effectuées dans un ordre différent.

4.2.1.1 Identification des actifs informationnels

Un actif informationnel représente tout élément contenant de l'information ayant de la valeur pour l'organisation et qui, par conséquent, nécessite une protection. Il est important de fixer des limites quant au niveau de détail des actifs à identifier, tout en s'assurant d'avoir suffisamment d'information pour apprécier les risques associés. Ce niveau de détail ou de granularité peut être affiné au cours du processus ou lors des itérations ultérieures.

Les détenteurs des actifs informationnels doivent également être identifiés, car ils sont souvent les personnes les plus aptes à déterminer la valeur des actifs que l'organisation détient. Certains éléments d'information supplémentaires comme, entre autres, la localisation (physique et logique), les composantes liées à l'actif, les utilisateurs, peuvent être identifiés pour faciliter l'évaluation du risque.

4.2.1.2 Identification des menaces

Les actifs précédemment identifiés sont exposés à des menaces qui sont susceptibles de les endommager et qui peuvent, dans certains cas, rendre un service essentiel indisponible. Ces menaces peuvent survenir autant de l'intérieur que de l'extérieur de l'organisation. Il est donc important de les identifier afin de prévoir ou de mettre en place les mesures adéquates.

Selon le contexte organisationnel étudié, il existe plusieurs types de menaces[4] que l'on peut considérer. Citons, par exemple, les menaces de type :

- ✓ dommage physique (p. ex. incendie, dégât d'eau, etc.);
- ✓ catastrophe naturelle (p. ex. inondation, séisme, etc.);
- ✓ défaillance technique (p. ex. dysfonctionnement d'un logiciel, saturation du système, etc.);
- ✓ compromission d'information (p. ex. vol de matériel ou d'information, espionnage à distance, etc.);

L'information permettant d'identifier les menaces peut souvent être obtenue auprès du détenteur, des utilisateurs et d'autres intervenants dans des domaines connexes à la sécurité de l'information. La connaissance des incidents antérieurs, les registres de menaces antérieures (s'ils existent), de même que l'expérience obtenue dans le passé en matière d'appréciation des menaces sont également des sources d'information non négligeables pour aider à l'identification des menaces actuelles et émergentes.

4.2.1.3 Identification des mesures de sécurité existantes

L'identification des mesures de sécurité existantes permet d'évaluer le niveau de protection de l'organisation face aux menaces. Une évaluation de ces mesures est également nécessaire afin de garantir que celles-ci fonctionnent correctement dans le contexte actuel. En effet, si une mesure de sécurité est dysfonctionnelle, des vulnérabilités peuvent être engendrées et exploitées. Dans un tel cas, il est important d'identifier les mesures complémentaires à mettre en place.

Plusieurs activités peuvent aider à l'identification des mesures de sécurité existantes, notamment :

- ✓ la consultation des documents internes relatifs aux mesures de sécurité (p. ex. le plan de mise en œuvre du traitement des risques, les rapports d'état de situation en sécurité, la description détaillée des processus de l'organisation, etc.);
- ✓ la consultation des utilisateurs ainsi que des responsables des opérations, de la sécurité de l'information, de la sécurité physique, des systèmes d'information, etc. Ces intervenants sont les mieux placés pour signaler quelles mesures de sécurité sont réellement mises en œuvre et si elles fonctionnent;

4. Si le lecteur désire avoir d'autres exemples de menaces, il peut consulter l'annexe C de la norme ISO/IEC 27005 – Gestion du risque en sécurité de l'information.

- ✓ l'analyse des résultats des audits de sécurité. Un audit de sécurité permet de déterminer, pour un ensemble de mesures de sécurité, si elles sont appropriées, suffisantes et efficaces.

4.2.1.4 Identification des vulnérabilités

L'absence de mesures de sécurité ou encore une mesure dysfonctionnelle, inefficace, mal implantée ou utilisée de manière incorrecte peuvent constituer des vulnérabilités. Ces vulnérabilités sont alors susceptibles d'être exploitées par des menaces visant à endommager les actifs informationnels et, conséquemment, à nuire à l'organisme.

Il existe plusieurs types de vulnérabilités[5] qui peuvent être exploitées. Citons, notamment, celles de type :

- ✓ matériel (mauvaise installation du matériel, absence de programme de remplacement, etc.);
- ✓ logiciel (attribution erronée des droits d'accès, réglage incorrect des paramètres, etc.);
- ✓ réseau (voies de communication non protégées, connexion au réseau public non protégé, etc.);
- ✓ personnel (formation et sensibilisation insuffisantes, absence de personnel, etc.);
- ✓ site (réseau électrique instable, accès physique peu sécurisé, etc.);
- ✓ organisme (absence de politique relative à l'utilisation des courriels, accord de service absent ou insuffisant, etc.).

Plusieurs activités proactives telles que les tests d'intrusions, les revues de code et l'utilisation d'outils d'analyse de failles de sécurité peuvent aider à identifier les vulnérabilités. Il est à noter que les résultats de ces activités sont parfois erronés, en raison du contexte dans lequel les tests ont été réalisés ou du moment précis de leur réalisation. D'autres méthodes complémentaires telles que les entretiens avec les utilisateurs, les inspections et l'analyse des documents liés aux incidents survenus peuvent alors être utilisées.

4.2.1.5 Identification des impacts

L'identification des impacts permet de déterminer les dommages ou les pertes, sur le plan de la disponibilité, de l'intégrité et de la confidentialité, quant aux actifs identifiés. Un impact survient lorsqu'une menace exploite une vulnérabilité ou un ensemble de vulnérabilités découlant de mesures de sécurité inadéquates. Identifier un impact revient à identifier le risque ou scénario de risque qui est la combinaison de tous ces éléments.

Les types d'impacts peuvent se résumer de la manière suivante :

- ✓ le temps nécessaire à une réparation;
- ✓ le temps de travail perdu ou la perte d'une opportunité;
- ✓ les problématiques concernant la santé et la protection des biens et des personnes;
- ✓ les coûts et les connaissances nécessaires à une réparation éventuelle;
- ✓ l'atteinte à l'image de marque.
- ✓ À la fin de cette étape, les risques sont identifiés; ils devront être évalués lors d'une étape ultérieure.

5. Si le lecteur veut avoir d'autres exemples de vulnérabilités, il peut consulter l'annexe D de la norme ISO/IEC 27005 - Gestion du risque en sécurité de l'information.

Par ailleurs, l'identification des risques au niveau de l'organisme permet d'identifier certains risques à portée gouvernementale[6] (RPG). Pour obtenir plus de détails sur les RPG, le lecteur peut consulter le point 4.2.4. Identification des risques à portée gouvernementale.

4.2.2 Estimation ou évaluation des risques

L'estimation ou l'évaluation des risques consiste à attribuer une valeur à chaque scénario de risque identifié au point 4.2.1. Cette évaluation peut être quantitative ou qualitative.

L'évaluation quantitative nécessite de disposer de statistiques et de chiffres concrets pour effectuer un calcul de coûts ou de dommages. Prenons l'exemple d'un organisme qui manipule des produits chimiques potentiellement dangereux pour la santé. Une étude a conclu que le risque que ces produits contaminent la population environnante et causent la mort ou des blessures graves est inférieur à 0,01 sur 1 million d'habitants, ce qui est 100 fois plus sûr que les normes canadiennes. À la suite de cette évaluation quantitative, le niveau d'impact de ce risque est jugé très faible.

Lorsqu'on ne dispose pas de chiffres ou de statistiques, l'évaluation qualitative peut être employée. Celle-ci permet de déterminer un ordre d'importance du risque. La figure suivante en donne un exemple (tiré de la norme ISO/IEC 27005) :

Figure 2 - Grille de mesure des risques (ISO/IEC 27005)

Grille de mesure						
Probabilité (apparition de l'évènement)		Très basse	Basse	Moyenne	Élevée	Très élevée
Gravité de l'impact	Très basse	0	1	2	3	4
	Basse	1	2	3	4	5
	Moyenne	2	3 (Exemple 2)	4	5	6
	Élevée	3	4	5	6	7
	Très élevée	4	5	6 (Exemple 1)	7	8

Dans ce cas, l'importance de chaque risque est évaluée en fonction d'une estimation de la probabilité d'apparition des menaces (qui déclencheront le risque) et en fonction de la gravité de l'impact si le risque se concrétise.

Exemple 1 : Une organisation pourrait évaluer à 6 sur 8 l'impact d'un risque d'intrusion de l'extérieur (au moyen d'Internet) qui utiliserait une vulnérabilité non identifiée et qui aurait un impact destructif sur une base de données. La probabilité d'apparition de cette menace pourrait être moyenne et la gravité de l'impact peut être très élevée. La mesure de ce risque est 6.

Exemple 2 : La divulgation volontaire d'information sensible peut être évaluée à 3 si la probabilité de survenance d'un tel événement est basse et que la gravité de l'impact est moyenne.

6. Risque 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 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.

4.2.3 Classement des risques (réordonnancement)

Le classement des risques permet d'obtenir, pour un actif informationnel donné, une liste de risques évalués, puis classés par ordre d'importance. Il s'agit donc de mettre en parallèle l'évaluation des risques et les besoins d'affaires ou les priorités d'un autre ordre (un règlement par exemple).

Exemple 1 : Un organisme a pour priorité de s'assurer que les processus de vérification d'identité des utilisateurs qui utilisent des services sont fonctionnels, disponibles et sans failles.

Exemple 2 : Un organisme accorde la priorité à la qualité des services, donc à la disponibilité de ses systèmes.

4.2.4 Identification des risques à portée gouvernementale

Le but d'un PGRSI est non seulement de permettre à un organisme public de mettre en place un processus formel de gestion des risques de portée sectorielle (limité au périmètre de l'organisation), mais aussi de communiquer au DPI un ensemble de risques qui pourraient transcender ce périmètre et, ainsi, avoir des conséquences graves sur le plan gouvernemental (risques à portée gouvernementale ou RPG).

Selon le cadre de gestion des risques et des incidents à portée gouvernementale, un risque de sécurité de l'information à portée gouvernementale (RPG) se définit comme suit :

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 fournie par d'autres organismes publics.

Le tableau suivant, détaillant la portée des risques, peut aider à mieux comprendre ce qu'est un RPG.

		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[7] à la population La conséquence sur la santé ou le bien-être est circonscrite et maîtrisée	Affecte des services indispensables à la population Met 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

Pendant le processus de gestion des risques de sécurité de l'information dans un organisme public, l'identification et l'évaluation des risques pour certains actifs informationnels peuvent révéler certains risques de portée gouvernementale. 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, ce 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 de l'information devant être révélée lors du dépôt du budget est connue des médias une journée à l'avance.

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

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

4.2.5 Procédure de communication des risques à portée gouvernementale

Conformément à l'alinéa d) de l'article 7 de la Directive sur la sécurité de l'information gouvernementale, les organismes publics ont pour obligation de déclarer au DPI les risques de sécurité de l'information à portée gouvernementale. La procédure à utiliser à cet égard est décrite dans le Guide de mise en œuvre du cadre de gestion des risques à portée gouvernementale.

4.3 Étape 3 – Plan de traitement des risques

Sur la base des résultats de l'analyse des risques, il convient d'élaborer un plan de traitement. Ce plan comporte, notamment :

- ✓ la définition des rôles et responsabilités de tous les intervenants appelés à mettre en œuvre le plan de traitement des risques;
- ✓ une brève description du processus de gestion des risques de sécurité de l'information;
- ✓ une liste des risques identifiés, avec les résultats de leur évaluation;
- ✓ une liste de travaux ou de décisions de traitement pour chacun des risques identifiés, par ordre d'importance;
- ✓ les échéanciers prévus pour les travaux de mise en œuvre du plan de traitement des risques classés par ordre de priorité;
- ✓ un suivi périodique des risques en cas d'ajout ou de retrait d'un risque, ou encore de modification des niveaux de gravité des risques.

4.3.1 Traitements possibles

Les traitements possibles sont de quatre types : l'acceptation, l'évitement, le transfert et l'atténuation. Un risque peut éventuellement faire l'objet d'un ou de plusieurs traitements.

4.3.1.1 L'acceptation ou le maintien du risque

L'acceptation du risque consiste à prendre le risque, sans mettre de mesures particulières en place soit parce que le niveau de risque est acceptable, soit parce que les conséquences ne sont pas critiques.

Par exemple, le fait de remplacer une gestion papier par l'utilisation d'une base de données engendre globalement un risque acceptable; il faut néanmoins vérifier ce que contient cette base de données pour s'assurer de ne pas prendre d'autres risques en effectuant ce remplacement.

4.3.1.2 L'évitement du risque

L'évitement du risque consiste à refuser de prendre le risque. Il sera alors nécessaire soit d'éviter les conditions d'apparition du risque, soit d'éviter une activité qui pourrait faire apparaître le risque.

Par exemple, s'il existe un risque de divulgation d'information numérique lorsqu'un équipement donné est connecté à un réseau, un organisme peut refuser de prendre ce risque en évitant de connecter cet équipement à son réseau.

4.3.1.3 Le transfert du risque

Le transfert du risque consiste à faire prendre le risque éventuel par une tierce partie jugée plus apte à en assurer le traitement, notamment par le biais d'un contrat. Pour ne pas aggraver la situation ou engendrer davantage de risques, une analyse approfondie du sous-traitant (niveau de compétence, services offerts, etc.) et du contexte général du transfert de risque est nécessaire. Dans cette situation, des clauses précises doivent être clairement définies au contrat.

Il est à noter que, lors du transfert d'un risque à une tierce partie, seule la responsabilité de gestion du risque est transférée, car il est généralement impossible de transférer la responsabilité légale d'un impact si le risque se concrétise.

Ainsi, un organisme qui décide de transférer le risque lié à la protection des renseignements personnels de ses clients ne serait pas à l'abri d'un éventuel impact sur son image de marque si ces renseignements étaient divulgués, puisque l'organisme est toujours le premier responsable de la sécurité de l'information qu'il détient. Les clients attribueront toujours la responsabilité des impacts indésirables à l'organisme.

4.3.1.4 L'atténuation du risque

L'atténuation du risque consiste à diminuer un risque, par la sélection et la mise en place de mesures de sécurité ou de contrôles de sécurité (termes équivalents). En général, les mesures de sécurité peuvent fournir plusieurs types de protection, telles la surveillance, la détection, la prévention, la sensibilisation, la dissuasion, l'atténuation des impacts, la correction et la récupération.

La sélection de ces mesures de sécurité doit tenir compte de plusieurs facteurs, notamment :

- ✓ des seuils de tolérance aux risques, définis lors de l'établissement du contexte;
- ✓ des exigences légales, réglementaires et contractuelles;
- ✓ des coûts liés à l'acquisition, l'exploitation et la maintenance des mesures par rapport à la valeur des actifs protégés.

Par exemple, une mesure pourrait être de vérifier l'identité d'une personne qui souhaite accéder à un local et un contrôle consisterait en l'utilisation d'un laissez-passer pour y accéder.

4.3.2 Acceptation du plan de traitement des risques

Le but de cette activité est de s'assurer de la cohérence du plan de traitement des risques, avant sa mise en œuvre. La validation permet une acceptation officielle des mesures proposées, conformément aux critères de base définis au point 4.1.2 - Champ d'application et portée.

Les mesures proposées seront notamment acceptées si les risques résiduels qui en découlent ne dépassent pas les seuils de tolérance fixés par l'organisation. Dans le cas contraire, l'organisation peut néanmoins décider d'accepter une mesure comportant des risques résiduels qui dépassent le seuil de tolérance, si les bénéfices associés sont très avantageux. Une révision des seuils de tolérance est parfois nécessaire s'ils sont inadaptés. Les décisions de traitement non conformes doivent être commentées et justifiées.

À l'issue de cette étape, le plan est soumis à l'approbation de la haute direction.

4.4 Étape 4 – Mise en place des mesures de sécurité

La mise en place des mesures de sécurité doit se faire de façon à éviter l'apparition de nouveaux risques. Elle nécessite, notamment, l'instauration de nouveaux contrôles et de nouvelles procédures à suivre, si l'on veut exploiter les mesures de façon optimale. Des procédures en cas d'incidents de sécurité liés aux mesures mises en place doivent également être définies.

Il convient, au besoin, de mettre en œuvre des programmes de formation et de sensibilisation pour s'assurer d'une bonne compréhension des nouvelles procédures de la part du personnel concerné.

Par exemple, pour réduire le risque résiduel lié à l'indisponibilité des serveurs d'une organisation en raison d'une coupure de courant, il a été décidé d'installer un système auxiliaire d'alimentation électrique. Des contrôles doivent être mis en place pour éviter que ce système d'appoint ne soit indisponible à son tour.

4.5 Étape 5 – Communication des risques

Le but de cette activité est de tirer profit, de manière officielle, de l'expérience acquise dans la gestion des risques de sécurité de l'information.

La communication des risques consiste à échanger l'information sur les risques, notamment à propos de leur existence, leur probabilité d'apparition, leur gravité, etc.

Elle doit se faire à l'interne et, dans certains cas, entre plusieurs organismes. L'information communiquée peut être considérée comme étant confidentielle et doit donc être traitée avec les précautions nécessaires.

Par exemple, le fait de communiquer, au sein de l'organisme, les risques liés à l'emploi de messageries externes (p. ex. Yahoo, Google, etc.) lors de l'envoi de courriels permet de sensibiliser les employés aux dangers et aux conséquences liés à cette utilisation non recommandée en milieu de travail (p. ex. risque de fuite d'information, interception illicite des messages, etc.).

Voici un autre exemple : le fait de communiquer, entre organismes, les traitements associés aux risques à portée gouvernementale permet d'échanger l'information sur les méthodes de réduction de ces risques et, donc, d'augmenter le niveau de maturité des organismes publics en matière de gestion des risques.

4.6 Étape 6 – Revue des risques

Les risques ne sont pas statiques. Ils évoluent, tout comme les menaces, les vulnérabilités, la probabilité de leur apparition et leurs impacts. Une revue des risques sur une base régulière est donc nécessaire afin d'inclure, s'il y a lieu, les nouveaux risques, de s'assurer qu'aucun risque n'est négligé ou sous-estimé et que le contexte, les résultats de l'analyse des risques de même que les traitements des risques restent adaptés aux circonstances actuelles.

La revue des risques s'effectue au niveau des facteurs de risques (valeurs des actifs, menaces, vulnérabilités, impacts et probabilité d'apparition) et de la gestion des risques (contexte, analyse des risques, traitement des risques et mise en place des mesures de sécurité).

L'objectif de cette revue est le suivant :

Pour les facteurs de risques :

- ✓ identifier les changements qui surviennent dans l'organisation (par exemple, une réorganisation peut changer l'efficacité d'un contrôle précédemment mis en place);
- ✓ identifier les risques considérés comme étant faibles, mais qui pourraient évoluer vers un niveau élevé (par exemple, autrefois, une fuite d'information pouvait provenir presque exclusivement du personnel, mais aujourd'hui, elle peut provenir de l'extérieur);

- ✓ identifier les nouvelles menaces (par exemple, l'utilisation de nouvelles technologies peut permettre des actions qui n'étaient pas possibles auparavant et qui sont donc non contrôlées).

Pour la gestion des risques :

- ✓ évaluer la pertinence des risques et leur adéquation avec les traitements (par exemple : A-t-on toujours besoin d'un pare-feu ou les nouvelles mesures mises en place par de tierces parties ont-elles une influence sur notre sécurité?);
- ✓ évaluer la disponibilité de l'information nécessaire à la gestion des risques (par exemple : Cette information est-elle stockée en lieu sûr? Est-elle colligée? Est-elle à jour?);
- ✓ identifier de nouveaux risques ou la prédominance d'anciens risques résiduels.

4.7 Étape 7 – Amélioration de la gestion des risques

Dans un contexte d'amélioration continue, la gestion des risques se réalise en plusieurs itérations. Celles-ci dépendent du nombre d'actifs informationnels visés, de la finesse des analyses précédentes et des besoins en matière de sécurité de l'information. Ainsi, il est possible qu'une nouvelle itération fasse ressortir de nouveaux risques, notamment ceux qui ont été identifiés, mais qui n'ont pas été traités, ou ceux découlant de la revue des risques et du suivi des risques résiduels.

Élaboration et suivi des indicateurs d'appréciation du PGRSI

Afin de s'assurer de l'efficacité de la mise en œuvre d'un PGRSI, il convient pour les OP d'en élaborer les indicateurs d'appréciation et d'en assurer le suivi. À cet effet, le Guide d'élaboration d'un tableau de bord de sécurité de l'information[8] précise, à l'annexe B, dans la fiche descriptive numéro 6 (« Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information »), les six indicateurs suivants :

- ✓ Le PGRSI est-il clairement défini et connu des intervenants concernés?
- ✓ L'établissement et l'analyse du contexte organisationnel sont-ils réalisés?
- ✓ L'identification des risques est-elle effectuée?
- ✓ L'analyse et l'évaluation des risques sont-elles effectuées?
- ✓ Les traitements des risques sont-ils planifiés?
- ✓ Le suivi et la revue des risques sont-ils prévus et mis en œuvre?

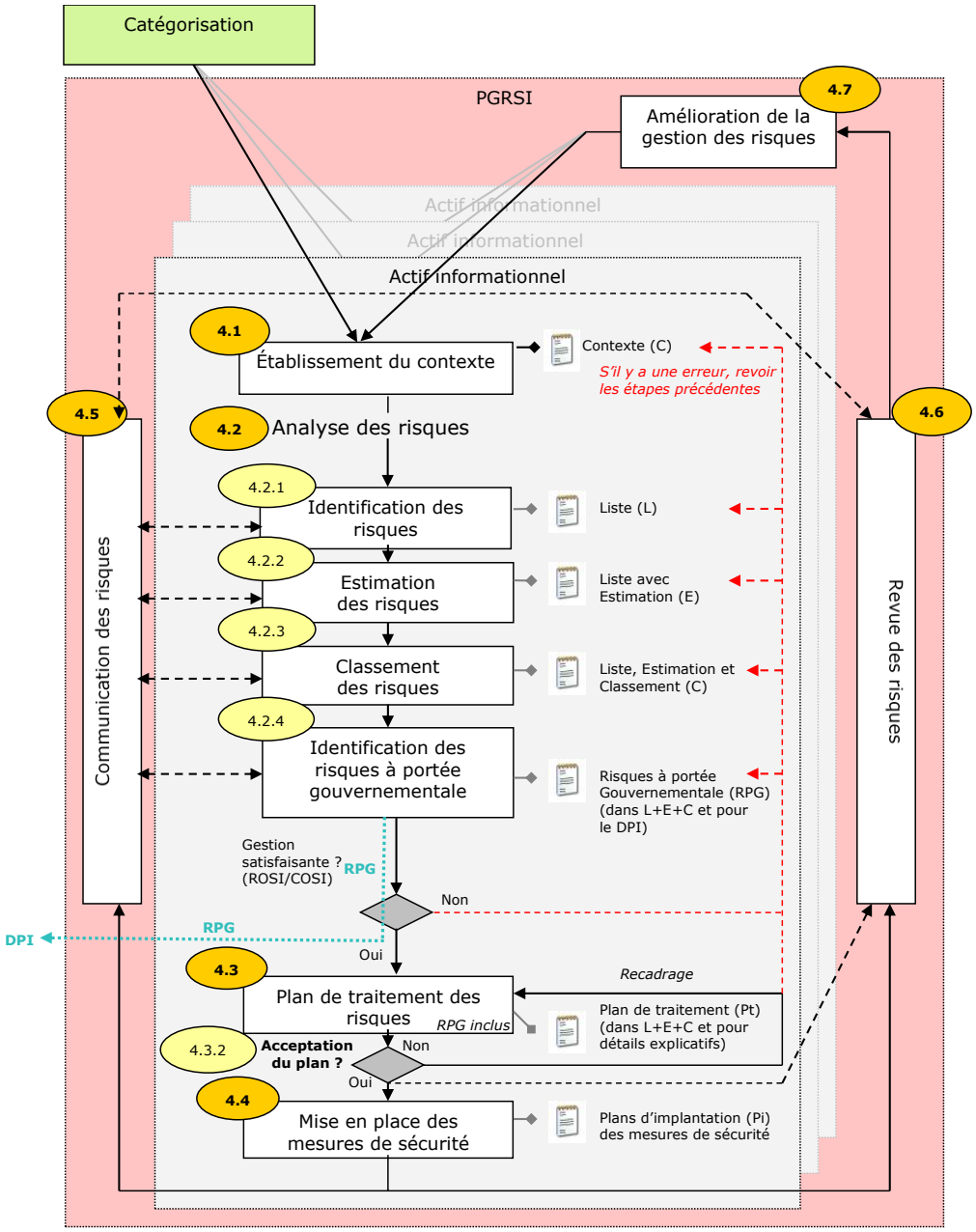
Plusieurs indicateurs dont décrits de manière plus détaillée à l'Annexe III du présent guide.

8. Guide d'élaboration d'un tableau de bord de sécurité de l'information.

5. Exemple concret d'application du PGRSI

Le chapitre 5 présente un exemple de mise en place d'un PGRSI dans un organisme public fictif. La figure 3 illustre la démarche d'élaboration et de mise en œuvre d'un PGRSI. Les numéros indiqués dans la figure renvoient aux sous-sections du chapitre 4 du présent guide.

Figure 3 - Fonctionnement du PGRSI



Mise en situation

L'exemple suivant illustre la mise en place d'un PGRSI par un organisme public fictif.

La haute direction accorde une importance particulière à la disponibilité des services qu'elle fournit à la population et à la sécurité de l'information colligée auprès de cette dernière, ce qui lui permet de remplir sa mission (contexte de travail).

En vue de mettre en œuvre le PGRSI, le ROSI et le COSI de l'organisme public ont organisé des ateliers de travail, animés par le COSI. Les responsabilités des intervenants participant aux ateliers sont décrites au chapitre 3**.** Définition des rôles et responsabilités du présent guide.

L'exercice antérieur de catégorisation[9] des actifs informationnels a permis au ROSI et au COSI de déterminer les premiers actifs devant faire l'objet d'une gestion des risques. Il s'agit de la base de données (BD) de l'organisme et des applications de prestation électronique de services (PES) aux citoyens.

Par souci de simplification, le présent exemple se limitera à ces deux actifs et aux risques associés. La mise en place du PGRSI se déroule selon les sept étapes décrites dans le présent guide.

Étape 1 - Établissement du contexte

L'établissement du contexte a permis de limiter la portée de la gestion des risques aux actifs critiques de l'organisation, notamment ceux liés à la disponibilité des services offerts à la population et à la confidentialité de l'information colligée.

Le COSI consigne l'information nécessaire à la gestion des risques, comme l'indique le tableau présenté ci-dessous. Il est à noter que la structure du tableau et le niveau de détail afférent sont laissés au choix de l'organisme.

Objectifs de la gestion des risques	Documenter le niveau d'exposition aux risques de l'organisation pour des prises de décisions futures et en prendre conscience. Déterminer comment réagir face aux événements qui peuvent perturber la prestation électronique de services aux citoyens, et ce, en vue de préserver la crédibilité de l'organisation.
Limites	Se limiter aux risques liés à la prestation électronique de services aux citoyens.
Approche	La gestion des risques se fait dans le cadre d'ateliers de travail animés par le conseiller organisationnel en sécurité de l'information (COSI). Les orientations et les priorités d'intervention sont données par le ROSI.
Responsables	ROSI, COSI, RAIPRP, RASI, RGTI, responsable de la BD, responsable de la salle des serveurs, responsable de la PES.
Facteurs d'évaluation des risques	Accorder une priorité à l'évaluation des actifs critiques et se concentrer sur les critères de disponibilité et de confidentialité.
Critères d'impact des risques	Les critères d'impact suivants doivent être contrôlés et atténués : ✓ la non-conformité légale en matière de PRP; ✓ la perte de disponibilité des PES; ✓ l'atteinte à la réputation de l'organisation.

9. Catégorisation : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles déterminent le degré de sensibilité de cette information et, conséquemment, la protection qu'il faut lui accorder.

Seuils de tolérance des risques	Les risques sont acceptables si : ✓ les normes, standards et règlements de sécurité de l'information sont respectés; ✓ le temps de récupération à la suite d'un impact ne dépasse pas un jour pour les risques liés à la PES.

Étape 2 - Analyse des risques

- ✓ Identification des actifs informationnels

  L'identification des actifs informationnels a déjà été réalisée au cours du processus de catégorisation, exécuté antérieurement.

- ✓ Identification des menaces

  Par exemple : Quels sont les menaces qui pèsent sur les actifs identifiés? Y a-t-il séparation entre les tâches incompatibles? Y a-t-il des accès distants à la base de données? Les applications de PES fonctionnent-elles correctement?

  Pour aider à l'identification des menaces, l'organisation pourra notamment consulter les types de menaces présentés à l'annexe C de la norme ISO/IEC 27005.

- ✓ Identification des mesures de sécurité existantes

  Certaines questions d'ordre général peuvent être posées, notamment : « Un audit de sécurité a-t-il été réalisé? Quels en sont les résultats? Les mesures fonctionnent-elles en situation réelle? Les employés sont-ils formés à l'égard des mesures de sécurité en place? ».

  Plus particulièrement, l'organisme pourrait, entre autres, se poser les questions suivantes : « Est-ce que les droits d'accès sont bien gérés? Quel est le degré de robustesse du système d'authentification en place? Les éléments de la base de données sont-ils chiffrés? Comment l'accès physique à la salle des serveurs est-il sécurisé? ».

- ✓ Identification des vulnérabilités

  À partir des menaces répertoriées et des mesures de sécurité existantes, on doit s'interroger sur les vulnérabilités. Dans le cas qui nous intéresse, il faut se demander, entre autres, si le système d'exploitation sur lequel fonctionnent les applications et les applicatifs de gestion de BD sont à jour et si des tests d'intrusion ont été effectués au niveau physique et logique. Le cas échéant, on doit chercher à en connaître les résultats.

- ✓ Identification des impacts possibles

  À partir des actifs, des menaces, des mesures de sécurité existantes et des vulnérabilités identifiés, on doit mettre en évidence les conséquences négatives qu'une perte au niveau de la disponibilité, de l'intégrité ou de la confidentialité peut avoir sur les actifs. On peut se demander, entre autres, quelles seraient les conséquences sur les services aux citoyens en cas d'indisponibilité de la base de données et quels seraient les impacts sur l'image de l'organisme ou du gouvernement si de l'information confidentielle sur des citoyens était divulguée.

À l'issue de l'atelier de travail, des risques sont identifiés, auxquels il pourrait être nécessaire d'associer un commentaire.

Tableau 1 - Liste des risques identifiés

#	Risques	Commentaires
1	Indisponibilité de l'information de la BD en raison d'une mauvaise gestion des sauvegardes	Insuffisance des mesures de protection des moyens de sauvegarde
2	Accès non autorisé à la salle des serveurs	Problèmes dans la mise à jour des contrôles d'accès physique
3	Modification non autorisée des données en raison de la non-séparation des tâches incompatibles	Les administrateurs systèmes ont accès aux données en production
4	Fuite d'information en raison d'un manque de contrôle des requêtes de la PES vers la BD	Tests d'intrusions et de vulnérabilités non réalisés sur les systèmes

Note à l'intention du lecteur : L'exemple se limite à quatre risques. Dans une situation réelle, ceux-ci pourraient être plus nombreux et plus détaillés; de plus, ils pourraient varier selon la complexité de l'organisation.

L'évaluation de la gravité des risques s'effectue selon la grille proposée au point 4.2.2 Estimation ou évaluation des risques du présent guide.

Tableau 2 - Liste des risques évalués

#	Risques	Gravité	Commentaires
1	Indisponibilité de l'information de la BD en raison d'une mauvaise gestion des sauvegardes	2	Insuffisance des mesures de protection des moyens de sauvegarde
2	Accès non autorisé à la salle des serveurs	1	Problèmes dans la mise à jour des contrôles d'accès physique
3	Modification non autorisée des données en raison de la non-séparation des tâches incompatibles	4	Les administrateurs systèmes ont accès aux données en production
4	Fuite d'information en raison d'un manque de contrôle des requêtes de la PES vers la BD	6	Tests d'intrusions et de vulnérabilités non réalisés sur les systèmes

En fonction des résultats de l'évaluation des risques précédemment effectuée, les risques sont classés par ordre décroissant sur le plan de la gravité (6 = élevée; 1 = basse). Ce classement permettra d'établir des priorités quant aux mesures correctives à mettre en place.

Tableau 3 - Liste des risques classés

#	Risques	Gravité	Commentaires
4	Fuite d'information en raison d'un manque de contrôle des requêtes de la PES vers la BD	6	Tests d'intrusions et de vulnérabilités non réalisés sur les systèmes
3	Modification non autorisée des données en raison de la non-séparation des tâches incompatibles	4	Les administrateurs systèmes ont accès aux données en production
1	Indisponibilité de l'information de la BD en raison d'une mauvaise gestion des sauvegardes	2	Insuffisance des mesures de protection des moyens de sauvegarde
2	Accès non autorisé à la salle des serveurs	1	Problèmes dans la mise à jour des contrôles d'accès physique

Étape 3 - Plan de traitement des risques

Le plan de traitement des risques devra tenir compte des objectifs de l'organisme (la disponibilité des services à la population et la sécurité de l'information colligée pour fournir les services).

Tableau 4 - Traitement des risques

#	Risques	Gravité	Commentaires	Traitements
4	Fuite d'information en raison d'un manque de contrôle des requêtes de la PES vers la BD	6	Tests d'intrusions et de vulnérabilités non réalisés sur les systèmes Risque très important pouvant devenir un risque à portée gouvernementale (RPG)	Réduction ✓ Réaliser des tests d'intrusions et de vulnérabilités ✓ Chiffrer le contenu de la base de données ✓ Prévoir la revue de code ou négocier les relations de soutien avec le fournisseur
3	Modification non autorisée des données en raison de la non-séparation des tâches incompatibles	4	Les administrateurs systèmes ont accès aux données en production	Réduction ✓ Revue des systèmes utilisés, durcissement des systèmes et séparation des comptes utilisateurs ✓ Trace des connexions et renforcement des procédures de contrôle des traces
1	Indisponibilité de l'information de la BD en raison d'une mauvaise gestion des sauvegardes	2	Insuffisance des mesures de protection des moyens de sauvegarde	Transfert Utilisation d'un partenaire extérieur pour la gestion des sauvegardes Risque résiduel à confiner au plus vite : vérification des procédures du partenaire.

2	Accès non autorisé à la salle des serveurs	1	Problèmes dans la mise à jour des contrôles d'accès physique	Réduction Renforcement des politiques et des procédures d'accès aux locaux

Pour chacune des mesures de réduction du risque, on doit déterminer des mesures de sécurité et en établir les coûts. Une validation de ces mesures est faite pour assurer que les risques résiduels sont acceptables par rapport aux seuils de tolérance. Le plan de traitement des risques en découlant est ensuite soumis à l'approbation de la haute direction.

Étape 4 – Mise en place des mesures de sécurité

Pour chaque mesure de sécurité retenue, un plan d'implantation est établi (détails de la mesure, procédures à suivre, etc.). La mise en place des mesures se fait en commençant par le risque ayant le niveau de gravité le plus élevé.

Étape 5 – Communication des risques

Les RPG éventuellement identifiés sont communiqués au DPI (selon la procédure décrite dans le Guide de mise en œuvre du cadre de gestion des risques à portée gouvernementale).

Étape 6 – Revue des risques

La revue des risques effectuée de façon périodique permet d'identifier les changements survenus dans l'organisation, l'évolution éventuelle des risques et l'apparition de nouveaux risques ou la prédominance d'anciens risques résiduels. Cette revue permet également de vérifier l'adéquation et l'efficacité du plan de traitement, dans le but d'en améliorer l'efficacité.

Étape 7 – Amélioration de la gestion des risques

Puisque le PGRSI est un processus itératif et en constante amélioration, d'autres itérations seront à prévoir, selon les besoins de l'organisation.

ANNEXE I Définitions

Définitions

Actif informationnel : Tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1). Cette même loi assimile au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Catégorisation : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles déterminent le degré de sensibilité de cette information et, conséquemment, la protection qu'il faut lui accorder.
(Source : Guide relatif à la catégorisation des documents technologiques en matière de sécurité, V1.2, octobre 2003)

Risque : De manière générale, sans être nécessairement appliqué au domaine de la sécurité de l'information, un risque est une probabilité d'apparition d'une menace qui, face à l'exploitabilité d'une vulnérabilité, peut potentiellement entraîner un impact sur un actif informationnel (actif ou information). (Source : Norme ISO/IEC 27005)

Risque 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 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. (Source : Cadre de gestion des risques et des incidents à portée gouvernementale)

ANNEXE II Cadre légal et normatif

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales.

Fondements légaux

- ✓ la Directive sur la sécurité de l'information gouvernementale;
- ✓ la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ les lois sectorielles régissant la mission de chaque organisme.

Fondements normatifs

- ✓ le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ le cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ les normes internationales, notamment : normes ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 et ISO/IEC 31000;
- ✓ les politiques et directives de sécurité de l'information propres à chaque organisme;
- ✓ les pratiques gouvernementales en matière de sécurité de l'information.

ANNEXE III Les indicateurs d'appréciation du PRGSI

Pour s'assurer de la mise en place d'un PGRSI au sein d'un organisme public, l'OP prendra appui sur une liste d'indicateurs d'appréciation, répartis en trois catégories :

- ✓ la mise en place du PGRSI;
- ✓ l'opérabilité du PGRSI;
- ✓ la qualité de fonctionnement du PGRSI.

À chacune de ces catégories est associé un type d'indicateur soit de type binaire

(Vrai = V ou Faux = F), soit de type numérique (échelle de 1 à 4).

En ce qui concerne la mise en place du PGRSI, le principal aspect à considérer est celui de la structure déployée. Le but des indicateurs de cet aspect est de vérifier si tous les éléments sont présents pour le fonctionnement d'un PGRSI. En cas de migration de l'architecture existante vers une autre structure cible, une réévaluation de ces indicateurs est nécessaire afin de s'assurer que la nouvelle structure répond aux exigences du PGRSI.

Concernant l'opérabilité du PGRSI, les indicateurs consistent à mesurer l'efficacité de la structure en place. Ces indicateurs peuvent être différents d'un organisme public à un autre. Ils ont néanmoins un tronc commun.

En ce qui a trait à la qualité de fonctionnement du PGRSI, deux aspects différents sont à prendre en compte, soit l'aspect interne de l'organisme public et l'aspect flux gouvernemental.

À titre indicatif, le tableau suivant présente un regroupement d'indicateurs; ils ne sont pas exhaustifs pour tous les organismes publics, mais constituent un minimum requis.

#	Nature et aspect	Indicateur	Type
01	Mise en place du PGRSI (structure)	Tous les intervenants sont-ils désignés?	V/F
02	Mise en place du PGRSI (structure)	Tous les intervenants sont-ils informés de leurs rôles et responsabilités respectifs?	V/F
03	Mise en place du PGRSI (structure)	Tous les intervenants ont-ils lu le guide de mise en place d'un PGRSI?	V/F
04	Mise en place du PGRSI (structure)	La structure adoptée prend-elle en compte les particularités de l'organisme public (réseau, sectoriel, horizontal, taille ou autre)?	V/F
05	Mise en place du PGRSI (structure)	La structure adoptée est-elle consignée dans un document?	V/F
06	Mise en place du PGRSI (structure)	La structure adoptée est-elle consignée dans un document à jour?	V/F
07	Mise en place du PGRSI (structure)	Le processus de gestion des risques a-t-il été adopté par l'ensemble des intervenants (sur la base de la structure à jour)?	V/F
08	Mise en place du PGRSI (structure)	Les documents définissant les rôles et responsabilités des intervenants permettant l'opérabilité du PGRSI sont-ils disponibles?	V/F

09	Mise en place du PGRSI (structure)	Les documents définissant les rôles et responsabilités des intervenants permettant l'opérabilité du PGRSI sont-ils à jour?	V/F
10	Opérabilité du PGRSI (tronc commun)	La liste des risques potentiels étudiés vient-elle de scénarios prédéterminés?	V/F
11	Opérabilité du PGRSI (tronc commun)	La liste des risques potentiels étudiés est-elle figée?	V/F
12	Opérabilité du PGRSI (tronc commun)	La constitution des scénarios de risques prend-elle en compte les particularités de l'organisme public?	V/F
13	Opérabilité du PGRSI (tronc commun)	La constitution des scénarios de risques peut-elle facilement s'adapter à tous les actifs et à toute l'information gérée par l'organisme public?	1-4
14	Opérabilité du PGRSI (tronc commun)	La liste des risques potentiels étudiés est-elle adaptée à l'organisme public?	1-4
15	Opérabilité du PGRSI (tronc commun)	La liste des risques potentiels étudiés prend-elle en considération l'ensemble des obligations légales de l'organisme?	V/F
16	Opérabilité du PGRSI (tronc commun)	La constitution des scénarios de risques peut-elle répondre à un niveau de granularité suffisant pour certains cas particuliers?	1-4
17	Opérabilité du PGRSI (tronc commun)	La constitution des scénarios de risques peut-elle être adaptée à un niveau de granularité suffisant pour certains cas particuliers?	V/F
18	Opérabilité du PGRSI (tronc commun)	La constitution des scénarios de risques peut-elle dégager des scénarios dont l'impact aurait une portée gouvernementale?	V/F
19	Opérabilité du PGRSI (tronc commun)	Les scénarios de risques étudiés sont-ils référencés de manière à pouvoir être consultés facilement au sein d'un organisme public?	V/F
20	Opérabilité du PGRSI (tronc commun)	Les scénarios de risques étudiés sont-ils référencés de manière à pouvoir être colligés facilement au niveau gouvernemental s'ils sont de nature « risques à portée gouvernementale »?	V/F
21	Opérabilité du PGRSI (tronc commun)	Les grilles de mesure des scénarios de risques sont-elles définies?	V/F
22	Opérabilité du PGRSI (tronc commun)	Les grilles de mesure des scénarios de risques sont-elles approuvées?	V/F
23	Opérabilité du PGRSI (tronc commun)	Les grilles de mesure des scénarios de risques peuvent-elles être adaptées aux critères d'évaluation des risques?	1-4
24	Opérabilité du PGRSI (tronc commun)	La mesure des scénarios de risques peut-elle être quantitative?	V/F
25	Opérabilité du PGRSI (tronc commun)	La mesure des scénarios de risques peut-elle être qualitative?	V/F

26	Opérabilité du PGRSI (tronc commun)	Une liste de scénarios types de base a-t-elle été constituée (applicable à tous les ateliers)?	V/F
27	Opérabilité du PGRSI (tronc commun)	Les documents permettant le fonctionnement du PGRSI sont-ils disponibles?	V/F
28	Opérabilité du PGRSI (tronc commun)	Les documents permettant le fonctionnement du PGRSI sont-ils à jour?	V/F
29	Opérabilité du PGRSI (tronc commun)	Les plans de traitement des risques prennent-ils en compte les quatre traitements possibles?	V/F
30	Qualité de fonctionnement (interne)	Les processus de fonctionnement du PGRSI sont-ils documentés?	V/F
31	Qualité de fonctionnement (interne)	Les processus de fonctionnement du PGRSI sont-ils à jour?	1-4
32	Qualité de fonctionnement (interne)	Les processus de fonctionnement du PGRSI sont-ils en fonction?	V/F
33	Qualité de fonctionnement (interne)	Les processus de fonctionnement du PGRSI peuvent-ils être optimisés?	1-4
34	Qualité de fonctionnement (interne)	Le processus de validation des plans de traitement des risques est-il centralisé au même endroit pour tous les plans?	V/F
35	Qualité de fonctionnement (interne)	Le processus de validation des plans de traitement des risques, s'il est distribué, est-il synchrone au sein de l'organisme public?	1-4
36	Qualité de fonctionnement (interne)	La gestion des incidents de l'organisme public alimente-t-elle le ROSI pour la prise en compte future de risques non détectés lors d'une itération?	1-4
37	Qualité de fonctionnement (interne)	La gestion des incidents de l'organisme public alimente-t-elle le COSI pour la prise en compte future de risques non détectés lors d'une itération?	1-4
38	Qualité de fonctionnement (flux gouvernemental)	Les risques à portée gouvernementale sont-ils transmis au DPI?	V/F
39	Qualité de fonctionnement (flux gouvernemental)	Le responsable de la gestion des incidents de l'organisme public déclare-t-il au CERT/AQ les incidents dont la portée pourrait être d'ordre gouvernemental?	V/F

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique