Cadre gouvernemental de gestion

Sécurité de l'information

Québec

Cadre gouvernemental de gestion

Sécurité de l’information

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite par 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 978-2-551-25519-1 (en ligne)

Table des matières

Acronymes

Organismes publics

BAnQ	Bibliothèque et Archives nationales du Québec
CERT/AQ	Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise
CF	Contrôleur des finances
CSPQ	Centre de services partagés du Québec
MCE-SIDPC	Ministère du Conseil exécutif - Secrétariat aux institutions démocratiques et à la participation citoyenne
MJQ	Ministère de la Justice du Québec
MSP	Ministère de la Sécurité publique
SQ	Sûreté du Québec

Instances gouvernementales de concertation

CCGSI	Comité de coordination gouvernementale de la sécurité de l'information
EIMSIG	Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale

Intervenants en sécurité de l'information

COGI	Coordonnateur organisationnel de gestion des incidents
COSI	Conseiller organisationnel en sécurité de l'information
DPI	Dirigeant principal de l'information
DRI	Dirigeant réseau de l'information
DSI	Dirigeant sectoriel de l'information
RAIPRP	Responsable de l'accès à l'information et de la protection des renseignements personnels

Intervenants en sécurité de l’information (suite)

RASI	Responsable de l’architecture de sécurité de l’information
RCS	Responsable de la continuité des services
RDASI	Responsable du développement ou de l’acquisition des systèmes d’information
RE	Responsable de l’éthique
RGD	Responsable de la gestion documentaire
RGTI	Responsable de la gestion des technologies de l’information
ROSI	Responsable organisationnel de la sécurité de l’information
RSP	Responsable de la sécurité physique
RVI	Responsable de la vérification interne

1. Sommaire

Le cadre gouvernemental de gestion de la sécurité de l'information a été adopté 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) pour, entre autres, appuyer la mise en œuvre des dispositions de la nouvelle Directive sur la sécurité de l'information gouvernementale. Il précise également l'organisation fonctionnelle de la sécurité de l'information ainsi que les rôles et responsabilités nécessaires à une gouvernance forte et intégrée à cet égard, tant sur le plan gouvernemental que sur le plan sectoriel.

Sur le plan gouvernemental, les rôles et responsabilités sont assignés au dirigeant principal de l'information (DPI), à certains organismes publics ayant des responsabilités horizontales et aux instances gouvernementales de coordination et de concertation en matière de sécurité de l'information.

Le DPI joue donc un rôle central en matière de gestion et de coordination de la sécurité de l'information gouvernementale. À ce titre, il conseille le Conseil du trésor, notamment en ce qui a trait aux stratégies, aux politiques et aux cadres de gestion, dont il assure également le suivi de la mise en œuvre, et fournit aux organismes publics les outils et l'assistance leur permettant de prendre en charge les exigences de sécurité de l'information gouvernementale.

Le DPI a également la responsabilité de la mise en place des entités gouvernementales de coordination et de concertation, ainsi que celle de l'établissement des règles de fonctionnement afférentes. De plus, il assure la coordination de la gestion des risques à portée gouvernementale et, en collaboration avec l'Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (CERT/AQ)[1], relevant du Centre de services partagés du Québec (CSPQ), la coordination de la gestion des incidents à portée gouvernementale.

De plus, le CSPQ, le ministère de la Justice du Québec (MJQ), le ministère de la Sécurité publique (MSP), la Sûreté du Québec (SQ), le Secrétariat aux institutions démocratiques et à la participation citoyenne (SIDPC) du ministère du Conseil exécutif (MCE), Bibliothèque et Archives nationales du Québec (BAnQ) et le Contrôleur des finances (CF) sont investis de responsabilités horizontales en sécurité de l'information. À cet égard, ils exercent un rôle de conseillers auprès du DPI et des organismes publics, en lien avec leurs domaines d'intervention respectifs.

Par ailleurs, le présent cadre de gestion définit le rôle des instances de coordination et de concertation appelées à soutenir le DPI dans l'exercice de sa fonction de gouverne de la sécurité de l'information. Il s'agit du Comité de crise gouvernemental, de la Table des responsables organisationnels de la sécurité de l'information, du Comité de coordination gouvernementale de la sécurité de l'information (CCGSI), du Réseau des conseillers organisationnels en sécurité de l'information, de l'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG) et du réseau d'alerte gouvernemental.

1. *Computer Emergency Response Team* de l'Administration québécoise

Sur le plan sectoriel, les rôles et responsabilités sont assignés à chaque dirigeant d'organisme public, au dirigeant réseau de l'information (DRI), au dirigeant sectoriel de l'information (DSI), au responsable organisationnel de la sécurité de l'information (ROSI), au conseiller organisationnel en sécurité de l'information (COSI), au coordonnateur organisationnel de gestion des incidents (COGI), aux responsables des domaines connexes à la sécurité de l'information et aux comités sectoriels en sécurité de l'information.

Ainsi, le dirigeant d'organisme public est le premier responsable de la sécurité de l'information relevant de son autorité. À ce titre, il doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques de sécurité de l'information.

Le DRI et le DSI, respectivement désignés en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), veillent à l'application, par les organismes publics qui leur sont rattachés, des règles de gouvernance et de gestion établies en matière de sécurité de l'information.

Le ROSI, quant à lui, joue le rôle de porte-parole du DPI auprès de son organisation, à laquelle il communique les orientations et les priorités d'intervention gouvernementales en sécurité de l'information. Il assure également la coordination et la cohérence des actions en matière de sécurité de l'information qui sont posées par d'autres intervenants au sein de son organisation. De plus, il coordonne la contribution de son organisation aux processus de gestion des risques et de gestion des incidents à portée gouvernementale.

Le COSI apporte son soutien au ROSI au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information.

Le COGI collabore étroitement avec le ROSI et le COSI en leur fournissant le soutien technique nécessaire à l'exercice de leurs responsabilités. Il participe activement au réseau d'alerte gouvernemental et contribue à la mise en place du processus de gestion des incidents au sein de son organisation et du processus de gestion des incidents à portée gouvernementale.

Par ailleurs, le présent cadre de gestion précise les rôles des responsables de domaines connexes à la sécurité de l'information au sein d'un organisme public. Citons, à titre d'exemple, les rôles attribués aux détenteurs de l'information, au responsable de l'architecture de sécurité de l'information, au responsable de la sécurité physique et au responsable de la vérification interne. Ce cadre précise également les rôles des comités internes, tels le Comité chargé de la sécurité de l'information, le Comité de crise ministériel et le Comité de continuité des services.

2. Introduction

2.1 Objet

Le présent document, adopté 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), a pour objectif de compléter les dispositions de la Directive sur la sécurité de l'information gouvernementale. Il décrit, à cet égard, les rôles et les responsabilités nécessaires à une gestion intégrée de la sécurité de l'information au sein de l'Administration gouvernementale. Il vise également à établir une vision commune de la sécurité de l'information gouvernementale et à assurer la cohérence et la coordination des interventions en la matière.

2.2 Définitions

Détenteur de l'information : un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, dont le rôle est, notamment, d'assurer la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

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, 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.

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 qui nécessite une intervention concertée sur le plan gouvernemental.

Services communs de sécurité de l'information : services, utilisés par plusieurs organismes publics, dont la gestion est centralisée.

2.3 Champ d'application

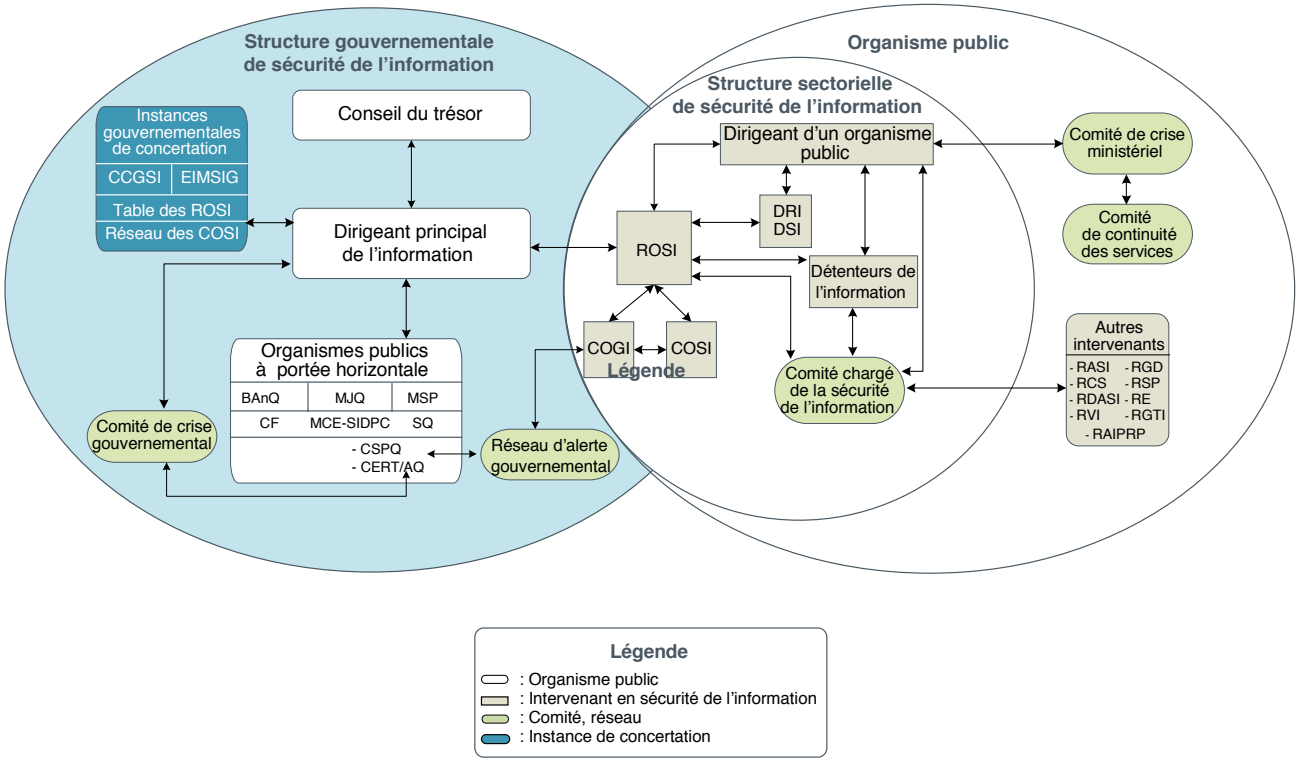
Le présent cadre de gestion s'applique aux organismes publics visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), ci-après appelée la Loi.

3. Organisation fonctionnelle de la sécurité de l'information

L'organisation de la sécurité de l'information au gouvernement du Québec s'articule autour des axes suivants :

1. **La structure horizontale**, constituée des instances gouvernementales ayant un rôle d'encadrement et de soutien pour les organismes publics ;

2. **La structure verticale**, constituée des organismes publics responsables de la prise en charge des exigences de la sécurité de l'information au sein de leur organisation.



4. Rôles et responsabilités sur le plan gouvernemental

4.1 Organisme central

Dirigeant principal de l'information

En vertu de ses obligations, énoncées dans la Loi et dans la Directive sur la sécurité de l'information gouvernementale, le DPI a notamment pour responsabilités :

- de proposer au Conseil du trésor des orientations, des politiques, des directives, des cadres de gestion, des standards et des services communs en matière de sécurité de l'information ;
- de mettre en œuvre les politiques et les directives adoptées en matière de sécurité de l'information gouvernementale, d'en surveiller l'application et d'en coordonner l'exécution ;
- de donner son avis au Conseil du trésor sur toute question relative à la sécurité de l'information gouvernementale ;
- d'assurer le suivi de la mise en œuvre des recommandations en matière de sécurité de l'information émises par le Conseil du trésor ;
- de coordonner la gestion des risques de sécurité de l'information à portée gouvernementale ;
- d'assurer, conjointement avec le CERT/AQ, la coordination et la gestion des incidents de sécurité de l'information à portée gouvernementale et, advenant de tels incidents, de formuler des recommandations en ce qui a trait aux actions à poser et d'assurer le suivi de la mise en œuvre de ces actions auprès des organismes publics ;
- de nommer les membres devant faire partie de la Table des responsables organisationnels de la sécurité de l'information et du Comité de coordination gouvernementale de la sécurité de l'information ;
- de mandater certains membres de la Table des responsables organisationnels de la sécurité de l'information, du Comité de coordination gouvernementale de la sécurité de l'information et du Réseau des conseillers organisationnels en sécurité de l'information pour exécuter des travaux en lien avec leurs domaines respectifs de compétence ;
- d'élaborer et de diffuser les pratiques et les outils nécessaires à la prise en charge des exigences de sécurité de l'information gouvernementale ;
- d'élaborer et de tenir à jour une base de connaissances sur les pratiques de sécurité de l'information d'intérêt pour les organismes publics ;
- d'examiner les plans d'action des organismes publics et de les conseiller sur les modifications à y apporter.

4.2 Organismes publics ayant des responsabilités horizontales

4.2.1 Centre de services partagés du Québec

Le CSPQ assure la gestion de la sécurité de l'information inhérente aux services communs qu'il fournit aux organismes publics. À cette fin, il :

- élabore et met en œuvre, de concert avec les organismes publics qui adhèrent à un service commun, un cadre de gestion de la sécurité de l'information propre à ce service, selon les bonnes pratiques à utiliser à cet égard ;
- met en place les mesures de sécurité de l'information, en tenant compte des paramètres convenus avec les organismes publics ;
- énonce, à l'endroit des organismes publics qui adhèrent à un service commun gouvernemental, les exigences en matière de sécurité de l'information auxquelles ils doivent se conformer.

Par l'entremise du CERT/AQ, le CSPQ assure, conjointement avec le DPI, la coordination de la gestion des incidents de sécurité de l'information à portée gouvernementale. À cette fin, il :

- assure la coordination du réseau d'alerte gouvernemental décrit à la section 4.3.6 ;
- effectue une veille globale des menaces et des vulnérabilités et, au besoin, en communique les résultats aux membres du réseau d'alerte gouvernemental ;
- soutient les équipes de réponse aux incidents des organismes publics en matière de gestion des incidents de sécurité de l'information ;
- fournit aux organismes publics les outils techniques et l'assistance qui leur permettront de gérer adéquatement la sécurité opérationnelle des systèmes et des réseaux ;
- organise et anime des ateliers techniques d'échanges d'expérience en matière de cybersécurité.

4.2.2 Ministère de la Justice du Québec

Le MJQ veille à la sécurité juridique de l'information gouvernementale. À cette fin, il contribue à l'application du cadre juridique des technologies de l'information, particulièrement dans le contexte des documents d'application et des règles de sécurité de l'information. Il exerce un rôle de conseiller en donnant des avis sur toute question de droit relative à la sécurité de l'information gouvernementale.

Par l'entremise de la Direction des registres et de la certification, et, plus particulièrement, de la Direction générale des services de justice et des registres, le MJQ contribue à accroître la confiance des parties visées par la prestation électronique des services gouvernementaux, en offrant des services de certification. Ses responsabilités à cet égard sont :

- de délivrer des clés et des certificats et d'en maintenir le niveau de confiance, conformément aux exigences prévues au cadre législatif en vigueur ;
- de fournir des services permettant de garantir :
  - l'identité des personnes ou l'identification des dispositifs agissant dans un environnement électronique ;
  - l'intégrité des documents et des échanges électroniques ;
  - la confidentialité des renseignements échangés ou conservés sur support informatique ;
  - l'établissement d'un lien clair entre une personne et un document technologique ou entre une personne et une action.
- d'assurer la planification, l'implantation, l'exploitation, l'entretien et l'évolution de l'infrastructure opérationnelle requise pour offrir le service ;
- d'assurer la cohérence opérationnelle entre les différents intervenants avec lesquels il collabore, soit le DPI (gestionnaire des encadrements administratif et technique), les organismes publics (gestionnaires de l'utilisation) et les agents de vérification de l'identité.

4.2.3 Ministère de la Sécurité publique

Le MSP assure une veille, sur le plan stratégique, des enjeux de sécurité ainsi que des menaces susceptibles de porter atteinte à la sécurité de l'information gouvernementale.

4.2.4 Sûreté du Québec

La SQ assure, auprès du DPI et des organismes publics, un service de soutien et une aide technique en matière d'évaluation des menaces et des risques stratégiques susceptibles d'affecter la sécurité de l'information gouvernementale. À ce titre, elle :

- contribue au processus de gestion des incidents de sécurité de l'information à portée gouvernementale ;
- conseille les responsables gouvernementaux en matière de sécurité des personnes, des renseignements et des biens ;

- coordonne les services d'enquêtes portant sur les infractions ainsi que les activités et les services relatifs à son mandat de sécurité et de protection auprès des organismes publics, en lien avec les objectifs de l'article 4 de la Directive sur la sécurité de l'information gouvernementale ;
- offre aux organismes publics la possibilité de recourir au Programme civil de filtrage de sécurité, afin de réaliser les enquêtes de bonnes mœurs des candidats devant occuper des postes évalués comme sensibles au sein de l'appareil gouvernemental québécois.

4.2.5 Ministère du Conseil exécutif

Le MCE, par l'entremise du SIDPC, assure, auprès du DPI et auprès des organismes publics, une fonction de conseiller en matière d'accès aux documents et de protection des renseignements personnels, afin que les principes et les exigences légales en matière d'accès à l'information et de protection des renseignements personnels soient intégrés aux outils, aux guides, aux normes et aux standards, aux séances de sensibilisation ou à tout autre document relatif à la sécurité de l'information.

4.2.6 Bibliothèque et Archives nationales du Québec

BANQ, par l'entremise du Conservateur des archives nationales du Québec, contribue à l'établissement des normes et des exigences de sécurité de l'information en ce qui concerne la conservation et la gestion intégrée des documents. Il assure également un rôle de conseiller auprès des organismes publics à cet égard.

4.2.7 Contrôleur des finances

Le CF est responsable de la comptabilité gouvernementale et de l'intégrité du système comptable du gouvernement. À ce titre, il s'assure de la fiabilité des données qui y sont enregistrées. Il peut formuler des recommandations concernant les mesures de sécurité et de contrôle à mettre en place dans les systèmes d'information à caractère financier des organismes publics, qu'ils soient en exploitation ou en développement ou lors d'une modification importante.

4.3 Instances de concertation

4.3.1 Comité de crise gouvernemental

Le Comité de crise gouvernemental est le centre de coordination de la réaction et de la décision lorsqu'un incident de sécurité de l'information à portée gouvernementale n'est pas maîtrisé en dépit des stratégies palliatives mises en œuvre. Présidé par le DPI ou son représentant, ce comité est composé de représentants des entités suivantes :

- le DPI, en tant que coordonnateur de la sécurité de l'information gouvernementale ;
- la Direction des communications du Secrétariat du Conseil du trésor, unique interlocuteur avec les médias ;
- le SIDPC du MCE, dans le cadre de l'exercice de sa fonction de conseiller auprès du DPI et auprès des organismes publics en matière d'accès aux documents et de protection des renseignements personnels ;
- le CSPQ, en tant qu'acteur majeur en matière de coordination des incidents à portée gouvernementale et de prestation de services communs ;
- le MSP, pour son expertise, sur le plan stratégique, à l'égard des enjeux de sécurité et des menaces susceptibles de porter atteinte à la sécurité de l'information gouvernementale ;
- la SQ, pour son expertise, ses conseils et son soutien en matière d'enquêtes et de renseignements de sécurité de l'État ainsi que sa capacité d'évaluation des menaces et des risques en la matière ;
- le MJQ, pour toute question de droit relative à la sécurité de l'information gouvernementale.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision.

4.3.2 Table des responsables organisationnels de la sécurité de l'information

De nature stratégique et tactique, la Table des responsables organisationnels de la sécurité de l'information exerce un rôle de conseiller, auprès du DPI, pour ce qui est de la définition, de la mise en œuvre et du suivi de l'application des politiques, des directives et des orientations gouvernementales de sécurité de l'information. À ce titre, elle contribue notamment :

- à l'élaboration des orientations, des politiques, des directives, des cadres de gestion, des standards, des plans d'action et des bilans gouvernementaux ;
- à l'établissement de la cohérence des plans d'action des organismes publics par rapport à l'approche stratégique gouvernementale de sécurité de l'information ;

- à l'identification des problématiques de sécurité de l'information survenant au sein de l'Administration gouvernementale et des pistes de solutions associées ;
- au déploiement des services communs de sécurité de l'information déterminés par le Conseil du trésor ;
- à la définition, à la mise en œuvre et au suivi des projets gouvernementaux de sécurité de l'information.

Cette table est présidée par le dirigeant principal de l'information ou son représentant. Ses membres se réunissent deux fois par année et ne peuvent déléguer leur présence. La table peut s'adjoindre d'autres spécialistes en mesure de lui assurer un soutien efficace dans l'exécution de ses travaux.

4.3.3 Comité de coordination gouvernementale de la sécurité de l'information

Le CCGSI est constitué de représentants des organismes publics ayant les responsabilités horizontales décrites à la section 4.2 et des représentants des réseaux de la santé et des services sociaux, de l'éducation et de l'enseignement supérieur, de la recherche, de la science et de la technologie. Il voit à la coordination des actions découlant de ces responsabilités horizontales et qui seraient d'intérêt pour les organismes publics.

Présidé par le DPI ou par son représentant, ce comité se réunit trois fois par année. Il peut s'adjoindre d'autres spécialistes en mesure de lui assurer un soutien efficace dans l'exécution de ses travaux.

4.3.4 Réseau des conseillers organisationnels en sécurité de l'information

Le Réseau des conseillers organisationnels en sécurité de l'information constitue une plateforme d'échanges et de partage des connaissances en matière de sécurité de l'information. Il permet notamment :

- au DPI de présenter les orientations, les priorités d'intervention et les réalisations gouvernementales ;
- aux membres d'exposer les travaux, réalisés au sein de leur organisation, qui seraient d'intérêt pour les autres organismes publics, ainsi que les problématiques d'ensemble et les pistes de solutions correspondantes.

Ce réseau est animé par le DPI ou son représentant. Il réunit ses membres trois fois par année.

4.3.5 Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale

L'EIMSIG est un partenariat regroupant les représentants du CERT/AQ, du MSP et de la SQ. Son mandat consiste à améliorer la connaissance des menaces et des incidents de sécurité de l'information gouvernementale au Québec. À ce titre, l'EIMSIG a pour objectif :

- d'accroître, sur une base régulière, le partage d'expertise et d'information entre ses membres et de partager les efforts de veille stratégique en rapport avec la sécurité de l'information ;
- de communiquer, s'il y a lieu, aux autorités gouvernementales et aux partenaires gouvernementaux, de l'information sur les menaces à la sécurité de l'information gouvernementale ;
- de produire, à l'intention du DPI, un rapport annuel sur les incidents déclarés de sécurité de l'information à portée gouvernementale.

Coordonnée par le CERT/AQ, l'EIMSIG tient, en moyenne, une dizaine de rencontres annuelles et maintient un lien privilégié avec le MJQ en ce qui a trait aux incidents pouvant requérir son attention.

4.3.6 Réseau d'alerte gouvernemental

Le réseau d'alerte gouvernemental est animé par le CERT/AQ. Il constitue une plateforme de partage d'information entre les coordonnateurs organisationnels de gestion des incidents désignés en vertu de la Directive sur la sécurité de l'information gouvernementale. Il permet à ses membres :

- de participer à la coordination des actions en cas d'incident à portée gouvernementale ;
- d'accéder à une information pertinente sur les menaces et les vulnérabilités en matière de sécurité de l'information ;
- d'échanger sur les solutions de sécurité de l'information ;
- de développer l'expertise en matière de sécurité de l'information et d'accroître la capacité de réaction en cas d'incidents.

5. Rôles et responsabilités sur le plan sectoriel

La présente section décrit les rôles et responsabilités en matière de sécurité de l'information attribués au dirigeant d'un organisme public et à d'autres fonctions. Ces rôles et responsabilités peuvent être assumés par une seule et même personne ; ils s'ajoutent alors aux fonctions qu'elle occupe au sein de l'organisation. La présente section décrit également les rôles des comités de coordination et de concertation dont l'exercice peut être cumulé par un seul et même comité.

5.1 Principaux intervenants

5.1.1 Dirigeant d'un organisme public

En tant que premier responsable de la sécurité de l'information relevant de son autorité, le dirigeant d'un organisme public doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Conseil du trésor. À ce titre, il :

- s'assure de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable par l'organisation ;
- s'assure de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus ;
- désigne les détenteurs de l'information, qui sont des employés de niveau cadre, qui ont pour responsabilité de s'assurer de la sécurité de l'information, et des ressources qui la sous-tendent, relevant de l'autorité de leur unité administrative.

5.1.2 Dirigeant réseau de l'information et dirigeant sectoriel de l'information

Le DRI et le DSI, désignés en vertu de la Loi, veillent à l'application, par les organismes publics qui leur sont rattachés, des règles de gouvernance et de gestion établies en matière de sécurité de l'information. À cet effet, ils :

- assurent le suivi de la mise en œuvre des recommandations émises par le Conseil du trésor ou par le DPI ;
- examinent les plans d'action des organismes publics et conseillent ces derniers sur les modifications à y apporter ;
- contribuent, conjointement avec le DPI et le CERT/AQ, à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

5.1.3 Responsable organisationnel de la sécurité de l'information

Le ROSI joue le rôle de porte-parole du DPI auprès de son organisation, à laquelle il communique les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information. Il assiste le dirigeant de l'organisme public pour ce qui est de la détermination des orientations stratégiques et des priorités d'intervention. De plus, il le représente en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale. Il a, en outre, comme responsabilité :

- de soumettre à la consultation du comité chargé de la sécurité de l'information de son organisation, les orientations, les politiques, les directives, les cadres de gestion, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information ;
- d'assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein de son organisation par d'autres intervenants dont les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique ;
- de s'assurer de la contribution de son organisation au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale ;
- de définir et de mettre en œuvre les processus officiels de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents ayant mis ou qui auraient pu mettre en péril la sécurité de l'information gouvernementale ;
- de s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information ;
- de coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information.

5.1.4 Conseiller organisationnel en sécurité de l'information

Le COSI apporte son soutien au ROSI au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information. Au-delà de son rôle de soutien auprès du ROSI, le COSI est notamment chargé :

- de mettre en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard ;
- de produire les bilans et les plans d'action de sécurité de l'information ;
- de participer aux négociations des ententes de service et des contrats et de formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information ;
- de tenir à jour le registre d'autorité de la sécurité de l'information ;
- d'assister les détenteurs de l'information pour ce qui est de la catégorisation de l'information relevant de leur responsabilité et de la réalisation des analyses de risques de sécurité de l'information ;
- de contribuer à la mise en œuvre des processus officiels de sécurité de l'information de son organisation.

5.1.5 Coordonnateur organisationnel de gestion des incidents

Outre sa participation active au réseau d'alerte gouvernemental, le COGI a notamment comme responsabilité :

- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information de son organisation ;
- d'assurer la coordination des membres CERT/AQ qui lui sont rattachés et de mettre en œuvre les stratégies de réaction appropriées ;
- de contribuer aux analyses de risques de sécurité de l'information, d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées ;
- de contribuer à la mise en œuvre du processus gouvernemental de gestion des incidents de sécurité de l'information ;
- d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications ;
- de collaborer étroitement avec le ROSI et de lui fournir le soutien technique nécessaire à l'exercice de ses responsabilités.

5.2 Autres intervenants

5.2.1 Détenteurs de l'information

Les détenteurs de l'information désignés par le dirigeant d'un organisme public sont notamment chargés :

- de participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans ;
- de catégoriser l'information relevant de leur responsabilité selon sa valeur au niveau de la disponibilité, de l'intégrité et de la confidentialité ;
- de veiller à ce que les mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, soient mises en place et appliquées ;
- de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus ;
- d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels.

5.2.2 Responsable de l'architecture de sécurité de l'information

Le responsable de l'architecture de sécurité de l'information :

- conçoit et met en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information ;
- arrime les solutions retenues aux processus organisationnels de sécurité de l'information ;
- participe à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires développées ou acquises par son organisation.

5.2.3 Responsable de la continuité des services

Le responsable de la continuité des services assure la gestion et la coordination du plan de continuité des services de son organisation. Plus particulièrement, il :

- coordonne l'élaboration du plan de continuité des services, veille à sa mise en œuvre et en assure la mise à jour ;
- assure la planification et la coordination des tests initiaux et récurrents.

5.2.4 Responsable de la sécurité physique

Le responsable de la sécurité physique met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle. Plus particulièrement, le responsable de la sécurité physique :

- conçoit et met en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de son organisation ;
- s'assure de la mise au rebut sécuritaire des supports de l'information ;
- élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

5.2.5 Responsable de la gestion des technologies de l'information

Le responsable de la gestion des technologies de l'information :

- contribue à l'élaboration et à la mise en œuvre de directives contribuant à assurer la sécurité de l'information numérique ;
- met en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par son organisation, dont les plans de reprise informatique en cas de sinistre ;
- met en place un cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

5.2.6 Responsable de la vérification interne

Le responsable de la vérification interne joue un rôle clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement au regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, il évalue, examine ou vérifie, notamment :

- l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre ;
- l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

5.2.7 Responsable de la gestion documentaire

Le responsable de la gestion documentaire :

- collabore à la conception des systèmes informatiques, administratifs ou autres et s'assure qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires pour permettre une saine gestion des connaissances et du patrimoine informationnel, la préservation des preuves et le respect des lois ;
- collabore étroitement avec les détenteurs de l'information ainsi qu'avec le responsable ou le conseiller organisationnel en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

5.2.8 Responsable de l'accès à l'information et de la protection des renseignements personnels

Le responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). À ce titre, il :

- communique au responsable organisationnel de la sécurité de l'information les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles ;
- contribue à assurer la cohérence et l'harmonisation des interventions avec la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale.

5.2.9 Responsable du développement ou de l'acquisition de systèmes d'information

Le responsable du développement ou de l'acquisition de systèmes d'information conçoit, réalise et documente les fonctionnalités de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, à intégrer aux systèmes d'information. Il s'assure également de leur bon fonctionnement.

5.2.10 Responsable de l'éthique

Le responsable de l'éthique veille à l'intégration de l'éthique aux processus de gestion de la sécurité de l'information, afin d'assurer la régularisation des conduites et la responsabilisation individuelle.

5.3 Comités

5.3.1 Comité chargé de la sécurité de l'information

Le Comité chargé de la sécurité de l'information d'un organisme public est la principale instance de concertation en matière de sécurité de l'information. Plus particulièrement, il :

- examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'organisation, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information ;
- analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisation.

Ce comité est présidé par le dirigeant de l'organisme public ou son représentant. Il comprend, notamment, le responsable et le conseiller organisationnel en sécurité de l'information, les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de la vérification interne, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique.

5.3.2 Comité de crise ministériel

En cas d'incident critique de sécurité de l'information, le Comité de crise ministériel d'un organisme public est le groupe décisionnel appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. À ce titre, il a pour rôle :

- d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information ;
- d'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants ;
- de décider du déploiement ou non des plans de continuité des services ;
- de proposer des orientations à suivre ou des actions à poser en cas de sinistre ;
- de formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation ;
- de communiquer avec les médias.

Le noyau permanent de ce comité est composé de représentants de la haute direction, du responsable organisationnel de la sécurité de l'information, du

responsable de la protection des renseignements personnels, du responsable de la sécurité physique et du responsable de la continuité des services. Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision. Citons, à titre d'exemple, les détenteurs de l'information ou les conseillers pour les volets juridique, technologique et de communication avec les médias et les ressources humaines.

Le Comité de crise ministériel est présidé par le dirigeant de l'organisme public ou son représentant.

5.3.3 Comité de continuité des services

Le Comité de continuité des services d'un organisme public est principalement composé du responsable de la continuité des services, des détenteurs de l'information, du responsable organisationnel de la sécurité de l'information, du conseiller organisationnel en sécurité de l'information et du coordonnateur organisationnel de gestion des incidents. Il a pour rôle, notamment :

- de procéder à l'évaluation des dommages ;
- de recommander au Comité de crise ministériel l'adoption d'une déclaration de sinistre ;
- d'assurer la mise en œuvre du plan de mobilisation ;
- d'assurer la coordination avec les intervenants de l'extérieur de l'organisme public.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision. Il est présidé par le responsable de la continuité des services ou son représentant.

Juin 2014

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique