Pratique recommandée en sécurité de l'information

PR-075

Guide d'élaboration d'un cadre de gestion de la sécurité de l'information

ENSEMBLE on fait avancer le Québec

Québec

Guide d’élaboration d’un cadre de gestion de la 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
2e étage, secteur 800
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 – juillet 2016
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71119-3 (en ligne)

Table des matières

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

Makram Mourad Laribi, chargé de projet
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Dany Michaud
Commission de protection du territoire agricole du Québec

Daniel Guimont
Commission des lésions professionnelles

Claude Côté
Commission des transports du Québec

Jacques Blouin
Régie de l'assurance maladie du Québec

Javier Betancur
Contrôleur des finances

Marthe- Anaïs Kambou
Ministère de la Santé et des Services sociaux

Mario Trudel
Société de l'assurance automobile du Québec

Pierre Bonhomme
Ministère de l'Éducation, du Loisir et du Sport

Notes à l'intention du lecteur

Note 1 :	Le terme « organisme public » 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 2 :	Le qualificatif « sectoriel » est utilisé pour désigner ce qui se rapporte à un organisme public.
Note 3 :	Le qualificatif « gouvernemental » est utilisé pour désigner ce qui se rapporte à l'ensemble des organismes publics.
Note 4 :	Certains termes ou acronymes sont définis dès leur première apparition dans le texte. Ces définitions sont également présentées à l'annexe I – Définitions.
Note 5 :	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 6 :	Le présent guide a été élaboré en prenant appui sur les normes1 internationales de sécurité de l'information, particulièrement la norme ISO/IEC 27001 (Techniques de sécurité - Systèmes de gestion de la sécurité de l'information) et la norme ISO/IEC 27002 (Recueil de bonnes pratiques en sécurité de l'information).

1. Norme : Accord entériné par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.

1. Introduction

Le présent guide vise à soutenir les organismes publics dans l'élaboration et la mise en œuvre d'un cadre sectoriel de gestion de la sécurité de l'information.

Le cadre sectoriel de gestion de la sécurité de l'information est élaboré par le responsable organisationnel de la sécurité de l'information (ROSI), en soutien à la mise en œuvre de la politique de sécurité de l'information de l'organisation. Il répond à deux objectifs : adopter une organisation fonctionnelle de la sécurité de l'information et attribuer les rôles et responsabilités des intervenants à tous les niveaux de l'organisation.

1.1 Mise en 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 gouvernementale. Celle-ci est appuyée par :

- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement;
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ quatre documents définissant le cadre de gouvernance de la sécurité de l'information dans l'administration québécoise[2];
- ✓ la politique de sécurité de l'information de l'organisme public concerné.

De plus, le présent guide répond à l'obligation du DPI d'accompagner les organismes publics et de leur apporter le soutien nécessaire dans la prise en charge des exigences de sécurité de l'information gouvernementale, notamment par l'élaboration et la diffusion de guides, pratiques et outils en la matière.

1.2 Portée et champ d'application

Le présent guide s'applique à l'information gouvernementale consignée dans un document,[3] tel que ce terme est décrit à 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 présent document 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 (voir l'annexe II).

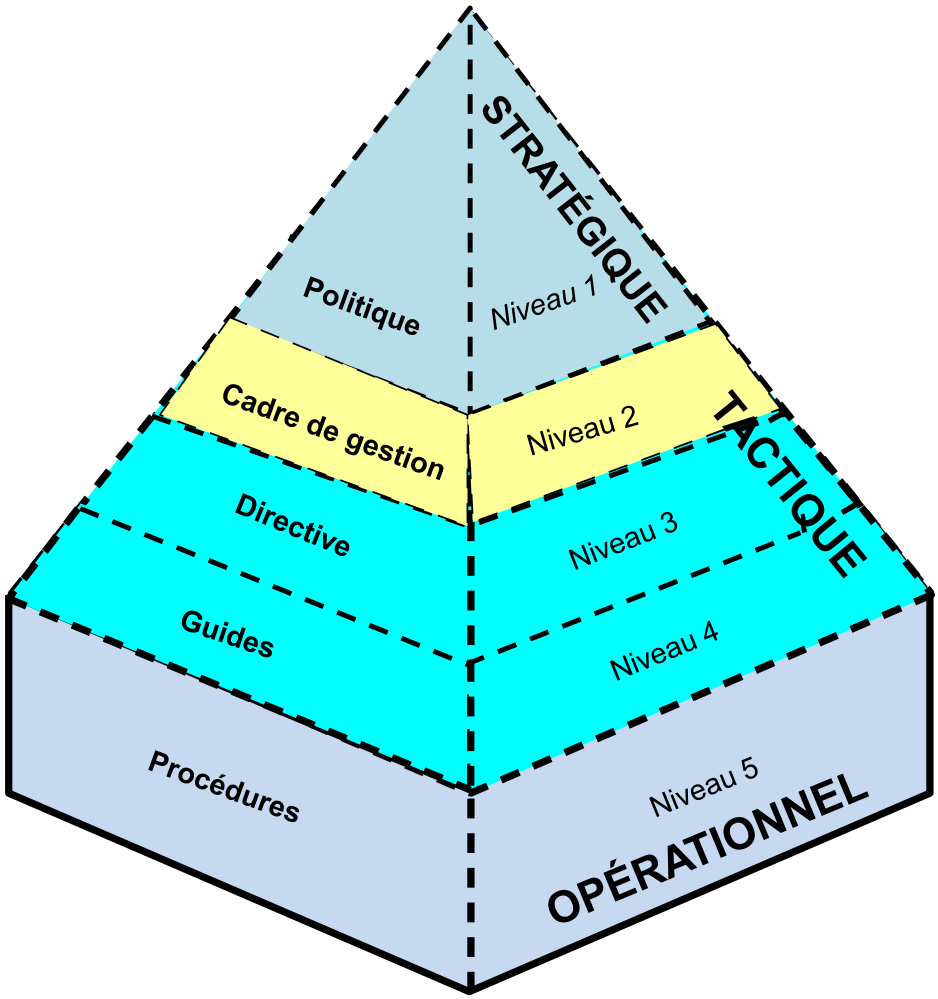
2. Les quatre documents dont il est question ici sont la Directive sur la sécurité de l'information gouvernementale, le Cadre gouvernemental de gestion de la sécurité de l'information, le Cadre de gestion des risques et des incidents à portée gouvernementale et l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information.
3. Document : Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrits sous l'une de ces formes ou en un autre système de symboles.
   [...] est assimilée 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.
   [Source : la Loi concernant le cadre juridique des technologies de l'information – article 3]

2. Rappel du cadre normatif sectoriel de sécurité de l'information

Le schéma présenté ci-dessous illustre la hiérarchie des principales composantes du cadre normatif sectoriel de sécurité de l'information. Ces composantes se traduisent notamment :

- ✓ au niveau stratégique, par la politique de sécurité de l'information;
- ✓ au niveau tactique, par le cadre de gestion, les directives et les guides;
- ✓ au niveau opérationnel, par des procédures décrivant les étapes d'un processus d'implantation ou de mise en œuvre d'une mesure de sécurité[4].

Figure 1 : Structure du cadre normatif sectoriel



4. Mesure de sécurité de l'information : Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.
[Source : OQLF – Grand dictionnaire terminologique]

2.1 Niveau 1 : Politique de sécurité de l'information

La politique de sécurité de l'information témoigne de l'importance accordée par l'organisation à la protection de l'information gouvernementale. Elle énonce des principes généraux et fixe des responsabilités à l'endroit de certains intervenants clés, notamment, à l'égard des utilisateurs [5], du sous-ministre ou dirigeant d'organisme, du responsable organisationnel de la sécurité de l'information (ROSI), des gestionnaires et des détenteurs.

2.2 Niveau 2 : Cadre de gestion de la sécurité de l'information

Le cadre de gestion de la sécurité de l'information, objet du présent guide, vise à compléter les dispositions de la politique. À cet effet, il précise l'organisation fonctionnelle en matière de sécurité de l'information et décrit les responsabilités de divers intervenants ainsi que les rôles des comités sectoriels.

2.3 Niveau 3 : Directives

D'application obligatoire, une directive vise à préciser, pour un domaine d'application particulier de sécurité de l'information (sécurité des locaux et des équipements, échanges sécuritaires de l'information, etc.), les dispositions à respecter aux fins d'assurer la sécurité de l'information. Mentionnons, à titre d'exemple, les directives portant sur la gestion des accès à l'information, les règles à adopter par les utilisateurs des assistants numériques personnels ou la protection des supports amovibles (mémoires Flash, disques durs, etc.).

2.4 Niveau 4 : Guides

Les guides visent à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir le caractère contraignant[6].

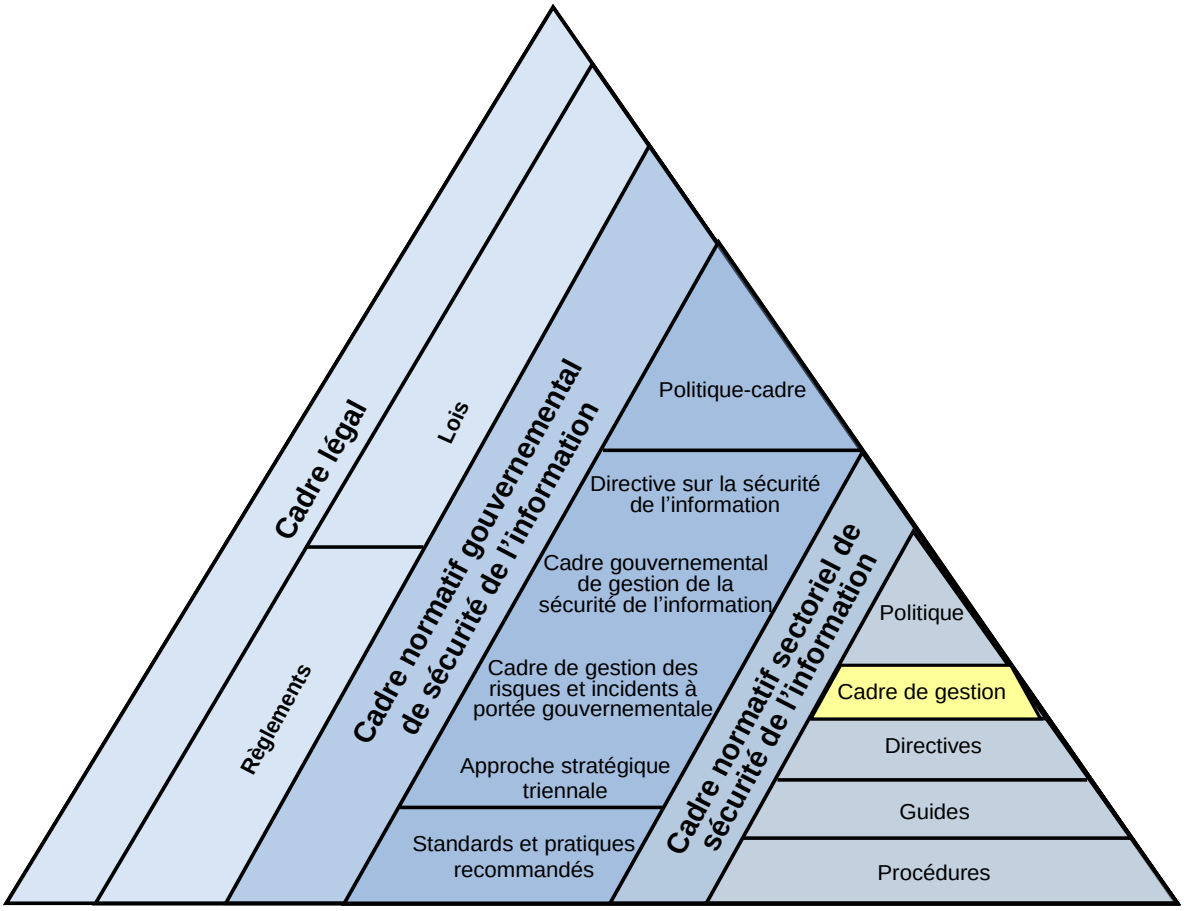
2.5 Niveau 5 : Procédures

Une procédure est un ensemble d'étapes à franchir, de moyens à prendre et de méthodes à suivre dans l'exécution d'une tâche. Elle décrit en détail les étapes d'un processus humain ou technologique d'implantation ou d'application d'une mesure de sécurité, qu'elle soit administrative ou technologique. Citons, à titre d'exemple, les procédures se rapportant à la délivrance ou la révocation des cartes d'accès, à la destruction sécuritaire des documents administratifs ou à l'attribution des mots de passe.

5. Utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'organisation ou y a accès.
6. Source : OQLF – Grand dictionnaire terminologique.

3. Positionnement du cadre de gestion

Figure 2 : Positionnement de la politique par rapport au cadre légal et normatif



Comme l'illustre la figure 2 présentée ci-dessus, le cadre de gestion de la sécurité de l'information complète les dispositions de la politique et renforce le cadre normatif sectoriel, tout en s'appuyant sur le cadre légal et le cadre normatif gouvernemental. Ce dernier est constitué :

- ✓ de la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ de la Directive sur la sécurité de l'information gouvernementale, du cadre gouvernemental de gestion de la sécurité de l'information, du cadre de gestion des risques et des incidents à portée gouvernementale et de l'approche stratégique triennale;
- ✓ de standards, à l'instar de ceux portant sur l'interopérabilité ou l'utilisation intégrale du français dans les technologies de l'information et des communications;
- ✓ des pratiques gouvernementales comme celles portant sur la catégorisation de l'information, l'utilisation sécuritaire des assistants numériques personnels ou la gestion des incidents.

Quant au cadre légal, il est constitué de lois, générales ou propres à un organisme public, et de règlements dont les dispositions touchent spécialement la sécurité de l'information et la protection des renseignements personnels.

4. Composantes du cadre de gestion

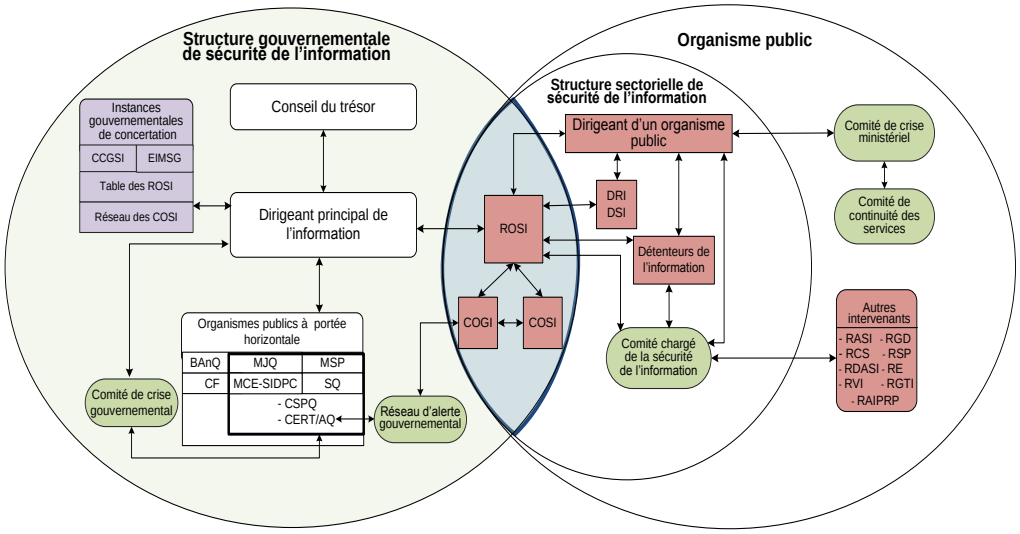
Le cadre sectoriel de gestion de la sécurité de l'information s'articule autour de trois composantes : la structure fonctionnelle de la sécurité de l'information, le partage des responsabilités entre les intervenants et les rôles attribués aux comités de coordination et de concertation.

4.1 Structure fonctionnelle de la sécurité de l'information

La sécurité de l'information qu'un organisme public détient dans l'exercice de sa mission passe par la mise en place d'une structure organisationnelle, conforme au cadre gouvernemental de gestion de la sécurité de l'information. Une telle structure doit répondre au besoin de mettre en place une gouvernance sectorielle, forte et intégrée, favorisant la concertation entre les organismes publics et permettant de tirer avantage de la complémentarité de leurs ressources et de l'efficacité de leurs actions.

La structure de gouvernance illustrée dans la figure 3, présentée ci-dessous, répond à cette préoccupation, en favorisant la communication avec le DPI, la participation aux instances gouvernementales de concertation, au réseau d'alerte gouvernemental et au comité de crise gouvernemental.

Figure 3 : Structure fonctionnelle de la sécurité de l'information



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
- DRI : Dirigeant réseau de l'information
- DSI : Dirigeant sectoriel de l'information
- RASI : Responsable de l'architecture de sécurité de l'information
- RCS : Responsable de 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
- RAIPRP : Responsable de l'accès à l'information et de la protection des renseignements personnels
- RSP : Responsable de la sécurité physique
- RVI : Responsable de la vérification interne

L'organisation sectorielle de la sécurité de l'information s'articule autour de trois composantes :

1. Les principaux responsables de la sécurité de l'information

   Il s'agit de personnes désignées pour assurer les fonctions de sécurité de l'information sur les plans stratégique (dirigeant d'organisme, ROSI, DRI et DSI), tactique (ROSI, DRI, DSI, COSI) et opérationnel (COGI).

2. Les autres intervenants en matière de sécurité de l'information

   Il s'agit de personnes désignées pour assurer des fonctions dans des domaines connexes à la sécurité de l'information et qui ont à jouer un rôle-clé, particulièrement au regard des mesures de sécurité de l'information se rapportant à leurs domaines d'intervention respectifs. Citons, à cet égard, les détenteurs de l'information, les vérificateurs internes, les responsables en gestion documentaire, les responsables en gestion des technologies de l'information, etc.

3. Les instances sectorielles de coordination et de concertation

   La coordination et la concertation en matière de sécurité de l'information au sein d'un organisme public repose sur trois comités. Il s'agit :

   - ✓ du comité chargé de la sécurité de l'information, principale instance de concertation en matière de sécurité de l'information;
   - ✓ du comité responsable de la mise en œuvre de stratégies de continuité des services en cas de sinistre;
   - ✓ du comité de crise sectoriel, centre de coordination de la réaction et de la décision lorsqu'un incident de sécurité de l'information n'est pas maîtrisé en dépit des stratégies palliatives mises en œuvre.

4.2 Responsabilités des intervenants et rôles des comités

Les responsabilités des intervenants et les rôles des comités de coordination et de concertation sont décrits dans le cadre gouvernemental de gestion de la sécurité de l'information. Les responsabilités doivent être assumées par :

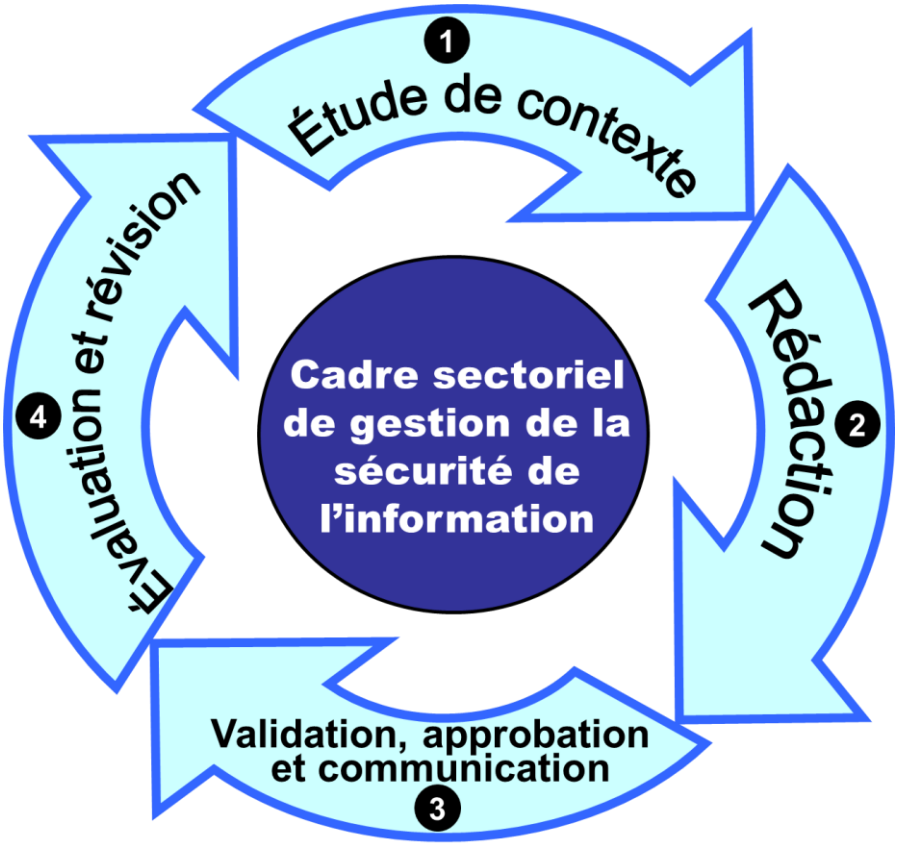
- ✓ les principaux intervenants en sécurité de l'information, comme le dirigeant d'organisme public, le ROSI, le DRI, le DSI, le COSI et le COGI;
- ✓ les autres intervenants exerçant dans des domaines connexes à la sécurité de l'information, comme les détenteurs de l'information, les vérificateurs internes, les responsables en gestion des technologies de l'information, etc.

Quant aux rôles, ils reviennent au comité chargé de la sécurité de l'information, au comité de continuité des services et au comité de crise sectoriel.

5. Démarche de réalisation et de mise en œuvre

Pour la réalisation et la mise en œuvre d'un cadre sectoriel de gestion de la sécurité de l'information, les étapes illustrées et décrites ci-dessous sont requises.

Figure 3 : Étapes de réalisation d'un cadre de gestion



5.1 Étude de contexte

La détermination des composantes d'un cadre de gestion de la sécurité de l'information, vue à la section 4, prend appui sur :

- ✓ le cadre légal et le cadre réglementaire, gouvernemental et sectoriel, décrits à la section 3;
- ✓ les normes et standards de l'industrie;
- ✓ la mission de l'organisation et les risques auxquels elle est exposée;
- ✓ la politique de sécurité de l'information de l'organisme public;
- ✓ les priorités d'actions gouvernementales;
- ✓ tout autre document pertinent (p. ex. orientations gouvernementales, recommandations du vérificateur général, recommandations du vérificateur interne, etc.).

5.2 Rédaction

Pour l'élaboration du cadre sectoriel de gestion de la sécurité de l'information, les organismes pourront s'appuyer sur les composantes décrites à la section 4 et sur le modèle « cadre sectoriel de gestion de la sécurité de l'information - modèle générique », joint à l'annexe III.

Les principaux éléments à considérer dans le cadre de cette étape sont les suivants :

- ✓ la raison d'être du cadre de gestion;
- ✓ la terminologie et les acronymes utilisés;
- ✓ les lois, les règlements, les directives ainsi que les normes et les standards;
- ✓ la structure fonctionnelle retenue par l'organisation, en conformité avec le cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ les responsabilités des intervenants en sécurité de l'information à tous les niveaux de l'organisation ainsi que les rôles des comités de coordination et de concertation en la matière;
- ✓ les dispositions finales, notamment l'approbation du cadre de gestion par le dirigeant de l'organisme public, sa date d'entrée en vigueur et ses modalités de révision.

5.3 Validation, approbation et communication

La validation du cadre de gestion nécessite la contribution des entités administratives de l'organisation et du comité chargé de la sécurité de l'information. Le cadre de gestion est approuvé par le sous-ministre ou le dirigeant d'organisme.

Une fois approuvé, le cadre de gestion est diffusé, auprès de l'ensemble du personnel de l'organisation, en utilisant les moyens appropriés, notamment :

- ✓ les sites Web (intranet ou extranet);
- ✓ les trousses de sensibilisation à la sécurité de l'information;
- ✓ les bannières publicitaires sur le site intranet ou extranet;
- ✓ les articles dans les journaux internes;
- ✓ etc.

Il convient également d'organiser, à l'intention de l'ensemble du personnel, des séances de formation et de sensibilisation, afin de s'assurer d'une bonne compréhension des énoncés du cadre de gestion et de leur application par ce dernier.

5.4 Évaluation et révision

Le cadre de gestion est régulièrement évalué, notamment en ce qui a trait à la pertinence de ses énoncés à l'égard des nouveaux enjeux de sécurité de l'information.

Une fois l'étape d'évaluation terminée, le cadre de gestion pourra faire l'objet d'une révision qui assurera l'adéquation de ses énoncés aux besoins de l'organisation en matière de sécurité de l'information.

ANNEXE I Définitions

Actif informationnel : Une information, quels que soient son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Continuité des services : Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Document : Ensemble constitué d'information portée par un support. L'information y est délimitée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.
[...] est assimilée 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.
[Source : Loi concernant le cadre juridique des technologies de l'information - article 3]

Guide : Document administratif à caractère pédagogique qui vise à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir le caractère contraignant.
[Source : OQLF - Grand dictionnaire terminologique]

Intégrité : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Mesure de sécurité de l'information : Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.
[Source : OQLF – Grand dictionnaire terminologique]

Norme : Accord entériné par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.
[Source : Lexique gouvernemental]

Pratique : Savoir ou manière de faire qui, dans une organisation, conduisent au résultat souhaité et qui sont portés en exemple auprès des pairs afin de leur faire partager l'expérience qui leur permettra une amélioration collective.
[Source : Inspirée de l'OQLF – Grand dictionnaire terminologique]

Procédure : Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.
[Source : OQLF – Grand dictionnaire terminologique]

Processus : Suite cohérente d'activités et d'opérations d'une organisation traduisant les besoins de la clientèle et des employés dans une logique de création de valeur.

Renseignement personnel : Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité.
[Source : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels]

Ressources informationnelles : Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Standard : Norme qui n'a été ni définie ni entérinée par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium.

Utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'organisation ou y a accès.

ANNEXE II Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement - article 2

LRQ, chapitre G-1.03

LOI SUR LA GOUVERNANCE ET LA GESTION DES RESSOURCES INFORMATIONNELLES DES ORGANISMES PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT

CHAPITRE I
Article 2. Pour l'application de la présente loi, sont des organismes publics :

1° les ministères du gouvernement;

2° les organismes budgétaires énumérés à l'annexe 1 de la Loi sur l'administration financière (chapitre A-6.001), à l'exception de ceux mentionnés au paragraphe 5°, et la Sûreté du Québec;

3° les organismes autres que budgétaires énumérés à l'annexe 2 de cette loi, à l'exception de ceux mentionnés au paragraphe 5° et de l'Agence du revenu du Québec, de même que la Commission administrative des régimes de retraite et d'assurances, la Commission de la santé et de la sécurité du travail, le Conseil de gestion de l'assurance parentale dans l'exercice de ses fonctions fiduciaires, la Régie des rentes du Québec et la Société de l'assurance automobile du Québec dans l'exercice de ses fonctions fiduciaires;

4° les commissions scolaires, le Comité de gestion de la taxe scolaire de l'île de Montréal, les collèges d'enseignement général et professionnel et les établissements universitaires mentionnés aux paragraphes 1° à 11° de l'article 1 de la Loi sur les établissements d'enseignement de niveau universitaire (chapitre E-14.1);

5° les agences de la santé et des services sociaux et les établissements publics visés par la Loi sur les services de santé et les services sociaux (chapitre S-4.2), les personnes morales et les groupes d'approvisionnement en commun visés à l'article 383 de cette loi, le Conseil cri de la santé et des services sociaux de la Baie James institué en vertu de la Loi sur les services de santé et les services sociaux pour les autochtones cris (chapitre S-5), les centres de communication santé visés par la Loi sur les services préhospitaliers d'urgence (chapitre S-6.2), le Commissaire à la santé et au bien-être, la Corporation d'urgences-santé, Héma-Québec, l'Institut national d'excellence en santé et en services sociaux, l'Institut national de santé publique du Québec et l'Office des personnes handicapées du Québec;

6° les autres organismes désignés par le gouvernement.

Sont considérées comme des organismes budgétaires ou autres que budgétaires les personnes désignées ou nommées par le gouvernement ou par un ministre, avec le personnel qu'elles dirigent, dans le cadre des fonctions qui leur sont attribuées par la loi, le gouvernement ou le ministre et qui sont respectivement énumérées aux annexes 1 et 2 de la Loi sur l'administration financière.

2011, c. 19, a. 2.

ANNEXE III Cadre sectoriel de gestion de la sécurité de l'information - modèle générique

N. B. Le présent modèle a été rédigé pour s'appliquer à un ministère. Il peut être adapté pour s'appliquer à tout organisme public.

Table des matières

1. Introduction

Le présent cadre vient en complément de la politique de sécurité de l'information. Il vise à renforcer la gouvernance de la sécurité de l'information du ministère, par la mise en place d'une structure organisationnelle de la sécurité de l'information et la définition des rôles et responsabilités à tous les niveaux de l'organisation.

1.1 Contexte

Le présent cadre est adopté en application du paragraphe (a) du premier alinéa de l'article 7 de la Directive sur la sécurité de l'information gouvernementale. Celle-ci fait obligation aux organismes publics d'adopter et de mettre en œuvre un cadre de gestion de la sécurité de l'information, de le maintenir à jour et d'en assurer l'application.

1.2 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, et dont le rôle est, notamment, de s'assurer de 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.

Utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'organisation ou y a accès.

Système d'information : Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation. (*OQLF – Grand dictionnaire terminologique*).

1.3 Cadre légal et administratif

Le cadre de gestion s'inscrit principalement dans un contexte régi par :

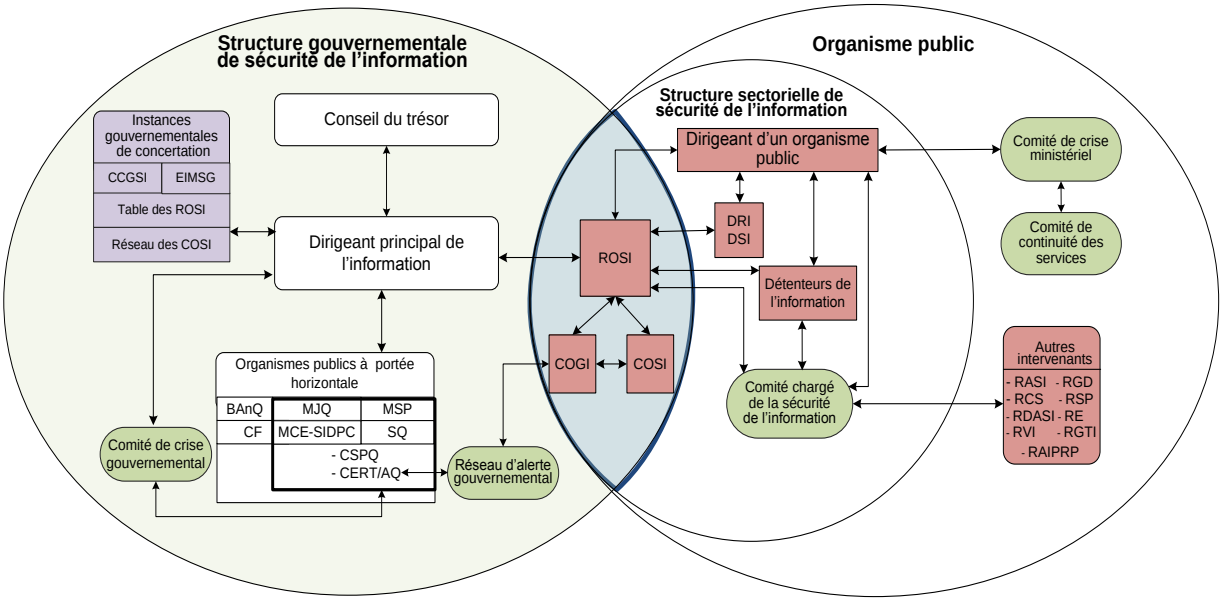
- ✓ la Loi sur le ministère;
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- ✓ la Loi concernant le cadre juridique des technologies et 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);
- ✓ le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 02);
- ✓ la Directive sur la sécurité de l'information gouvernementale;

- ✓ le Cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ le Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information gouvernementale;
- ✓ la Politique de sécurité de l'information.

2. Aucune entrée de table des matières n'a été trouvée.

3. Aucune entrée de table des matières n'a été trouvée.Organisation fonctionnelle de la sécurité de l'information[7]

7. Pour obtenir plus de détails sur la structure gouvernementale de sécurité de l'information, veuillez consulter le « cadre gouvernemental de gestion de la sécurité de l'information ».



Légende

- : Organisme public
- : Intervenant en sécurité de l'information
- : Comité, réseau
- : Instance de concertation

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
- DRI : Dirigeant réseau de l'information
- DSI : Dirigeant sectoriel de l'information
- RASI : Responsable de l'architecture de sécurité de l'information
- RCS : Responsable de 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
- RAIPRP : Responsable de l'accès à l'information et de la protection des renseignements personnels
- RSP : Responsable de la sécurité physique
- RVI : Responsable de la vérification interne

L'organisation de la sécurité de l'information s'articule autour de :

- la structure horizontale constituée des instances gouvernementales ayant un rôle d'encadrement et de soutien pour les organismes publics;
- la structure sectorielle d'un organisme public.

Pour obtenir plus de détails, le lecteur pourra consulter le « cadre gouvernemental de gestion de la sécurité de l'information ».

4. **Aucune entrée de table des matières n'a été trouvée.**Rôles et responsabilités

Les responsabilités en matière de sécurité de l'information sont attribuées aux intervenants suivants :

4.1 **Aucune entrée de table des matières n'a été trouvée.**Les principaux intervenants

4.1.1 Dirigeant d'organisme public

Le dirigeant d'organisme public est le premier responsable de la sécurité de l'information. À ce titre, il veille au respect du cadre gouvernemental de sécurité de l'information et s'acquitte de ses obligations, telles qu'elles sont édictées dans la Directive sur la sécurité de l'information gouvernementale. À cet effet, il :

- ✓ adopte les orientations stratégiques de la sécurité de l'information du ministère, la politique, le cadre de gestion, les directives et les plans d'actions en la matière et en assure la mise en œuvre;
- ✓ approuve les bilans de sécurité de l'information;
- ✓ désigne le responsable organisationnel de la sécurité de l'information, le conseiller organisationnel de la sécurité de l'information, le coordonnateur organisationnel de gestion des incidents ainsi que les détenteurs, et leur attribue les responsabilités définies par le présent cadre de gestion;
- ✓ s'assure de la mise en œuvre des processus officiels de sécurité de l'information permettant, notamment, de veiller à la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- ✓ s'assure de la réalisation périodique d'audits de sécurité de l'information et de tests d'intrusion et de vulnérabilités, conformément aux énoncés de la Directive sur la sécurité de l'information gouvernementale, et en dégage les priorités d'actions ainsi que les échéanciers afférents;
- ✓ favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor;
- ✓ s'assure que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comprennent des clauses garantissant le respect des exigences de sécurité de l'information;
- ✓ s'assure de la mise en place d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
- ✓ approuve et présente aux instances gouvernementales concernées les plans d'action et les bilans requis, conformément aux énoncés de la Directive sur la sécurité de l'information gouvernementale.

4.1.2 Dirigeant sectoriel de l'information (DSI)[8]

Le DSI veille à l'application, par les organismes publics qui lui sont rattachés, des règles de gouvernance et de gestion établies en matière de sécurité de l'information. À cet effet, il :

- ✓ assure le suivi de la mise en œuvre des recommandations émises par le Conseil du trésor ou par le dirigeant principal de l'information;
- ✓ examine les plans d'action des organismes publics et leur donne des conseils quant aux modifications à y apporter;
- ✓ contribue, conjointement avec le dirigeant principal de l'information et le CERT/AQ, à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

4.1.3 Responsable organisationnel de la sécurité de l'information (ROSI)

Le responsable organisationnel de la sécurité de l'information représente le sous-ministre auprès du ministère et auprès du dirigeant principal de l'information, en matière de sécurité de l'information. À cet égard, il :

- ✓ joue le rôle de porte-parole du dirigeant principal de l'information en matière de sécurité de l'information et lui fait part de ses réalisations;
- ✓ transmet à son ministère les orientations et les priorités d'intervention gouvernementales et s'assure de leur mise en œuvre;
- ✓ soumet, aux fins de consultation, au comité chargé de la sécurité de l'information, 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;
- ✓ assure la coordination et la cohérence des actions de sécurité de l'information menées au sein du ministère par d'autres intervenants dont, notamment, 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;
- ✓ s'assure de la contribution du ministère au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
- ✓ déclare au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale;
- ✓ déclare au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale;
- ✓ définit et met en œuvre les processus officiels de sécurité de l'information tels que la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- ✓ coordonne l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;
- ✓ participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information;
- ✓ participe à des comités interministériels et représente le ministère en matière de sécurité de l'information.

8. Il peut s'agir également du dirigeant réseau de l'information (DRI). Le modèle proposé cite le DSI, puisqu'il a été élaboré pour s'appliquer à un ministère.

4.1.4 Le conseiller organisationnel en sécurité de l'information (COSI)

Le conseiller organisationnel en sécurité de l'information apporte, au niveau tactique, son soutien au ROSI, notamment en ce qui concerne la mise en œuvre des mesures de sécurité et la mise en place des processus officiels de sécurité de l'information. À cet égard, il :

- ✓ met en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;
- ✓ produit les bilans et les plans d'actions de sécurité de l'information du ministère;
- ✓ s'assure de l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans le cadre des ententes de service et des contrats;
- ✓ assiste les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information;
- ✓ élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
- ✓ tient à jour le registre d'autorité de la sécurité de l'information;
- ✓ participe au réseau des conseillers organisationnel en sécurité de l'information;
- ✓ propose au ROSI des orientations, des plans d'action et des bilans;
- ✓ assure la coordination et la réalisation de projets de sécurité de l'information.

4.1.5 Le coordonnateur organisationnel de gestion des incidents (COGI)

Le coordonnateur organisationnel de gestion des incidents participe activement au réseau d'alerte gouvernemental et collabore étroitement avec le ROSI et le COSI. Il a notamment pour responsabilités :

- ✓ de contribuer à la mise en place du processus sectoriel de gestion des incidents de sécurité de l'information et du processus gouvernemental de gestion des incidents;
- ✓ de tenir à jour le registre des incidents ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informés le ROSI et le comité chargé de la sécurité de l'information;
- ✓ de contribuer à l'analyse des risques de sécurité de l'information, de déterminer les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- ✓ d'assurer la coordination de l'équipe de réponse aux incidents de sécurité de l'information des organismes publics qui lui sont rattachés et de mettre en œuvre les stratégies de réaction appropriées;
- ✓ d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunication.

4.2 **Aucune entrée de table des matières n'a été trouvée.** Les autres intervenants

4.2.1 Détenteurs de l'information

Les détenteurs de l'information désignés par le ministère sont notamment chargés :

- ✓ de catégoriser l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité;
- ✓ d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels;
- ✓ 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 veiller à la mise en place et à l'application des mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels;
- ✓ de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus.

4.2.2 Le gestionnaire

Le gestionnaire est responsable de la mise en œuvre, auprès du personnel relevant de son autorité, des dispositions de la politique de sécurité de l'information. Il doit principalement :

- ✓ informer son personnel des dispositions de la politique sur la sécurité de l'information et de toute directive, de tout standard et de toute procédure en vigueur en matière de sécurité de l'information, ainsi que des modalités liées à leur mise en œuvre, et le sensibiliser à la nécessité de s'y conformer;
- ✓ s'assurer que les actifs informationnels mis à la disposition de son personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
- ✓ s'assurer que la sécurité de l'information est prise en compte dans tout contrat de service attribué par son unité administrative et voir à ce que tout consultant, partenaire ou fournisseur s'engagent à respecter et respectent les règles de sécurité de l'information du ministère.

4.2.3 Responsable de l'architecture de sécurité de l'information

Le responsable de l'architecture de sécurité de l'information doit, notamment :

- ✓ concevoir et mettre en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;
- ✓ arrimer les solutions retenues aux processus organisationnels de sécurité de l'information;
- ✓ participer à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires, élaborées ou acquises par le ministère.

4.2.4 Responsable de la gestion des technologies de l'information

Le responsable de la gestion des technologies de l'information doit, notamment :

- ✓ mettre 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;

- ✓ mettre 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.

4.2.5 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 ROSI les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible;
- ✓ contribue à assurer la cohérence et l'harmonisation des interventions entre 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.

4.2.6 Responsable de la gestion documentaire

Le responsable de la gestion documentaire doit, notamment :

- ✓ collaborer à la conception des systèmes informatiques, administratifs ou autres et s'assurer qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois;
- ✓ collaborer étroitement avec les détenteurs de l'information, 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.

4.2.7 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 et s'assure de leur bon fonctionnement.

4.2.8 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 du ministère. 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.

4.2.9 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 du ministère;
- ✓ 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.

4.2.10 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 la détermination, 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.

4.2.11 Responsable de l'éthique

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

4.3 **Aucune entrée de table des matières n'a été trouvée.**Les comités

4.3.1 Comité chargé de la sécurité de l'information

Le comité chargé de la sécurité de l'information est la principale instance ministérielle 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 du ministère, 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 du ministère.

Ce comité est présidé par le sous-ministre ou son représentant. Il nécessite, notamment, la participation du ROSI, des détenteurs de l'information ainsi que des 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.

4.3.2 Comité de continuité des services

Le comité de continuité des services est principalement composé du responsable de la continuité des services, des détenteurs de l'information, du ROSI, du COSI et du COGI. 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 externes.

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

4.3.3 Comité de crise ministériel

En cas d'incident critique de sécurité de l'information, le comité de crise ministériel 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, principalement :

- ✓ 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 prendre 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 ROSI, 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 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 sous-ministre ou son représentant.

5. Dispositions finales

5.1 Date d'entrée en vigueur

Le présent cadre de gestion de la sécurité de l'information est complémentaire à la politique sur la sécurité de l'information du ministère. Il entre en vigueur à la date de son approbation et demeure en application tant et aussi longtemps qu'il n'est pas abrogé, modifié ou remplacé par un autre cadre de gestion.

5.2 Approbation

Le présent cadre de gestion de la sécurité de l'information est approuvé par :

_____ _____

Sous-ministre Date

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique