Pratique recommandée en sécurité de l'information

PR-076

Guide établissant les critères de désignation des principaux intervenants en sécurité de l'information

Guide établissant les critères de désignation des principaux intervenants en sécurité de l’information

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

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

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

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

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

Dépôt légal – 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71118-6

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

Christian Marcotte
Ministère de l'Éducation, du Loisir et du Sport

Daniel Carpentier
Contrôleur des finances

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

Daniel Landry
Sûreté 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.
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 normes[1] 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. 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. Cette démarche s'appuie sur quatre documents structurants[2] qui permettent :

- ✓ d'instaurer une gouvernance de la sécurité de l'information, intégrée et concertée, fondée sur la préoccupation d'assurer des services de qualité aux citoyens et aux entreprises;
- ✓ d'optimiser les façons de faire en matière de sécurité de l'information, en privilégiant le partage et la mise en commun du savoir-faire, de l'information, des infrastructures et des ressources;
- ✓ d'encadrer, d'accompagner et de soutenir les organismes publics dans leur évolution vers une gestion rigoureuse et transparente, favorisant l'atteinte d'un niveau de maturité approprié[3] en matière de sécurité de l'information.

Cette démarche est également appuyée par la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics et par la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

Par ailleurs, le dirigeant principal de l'information (DPI) apporte aux organismes publics le soutien nécessaire dans la prise en charge des exigences de sécurité de l'information relevant de leur autorité, notamment par l'élaboration et la diffusion de pratiques et outils en la matière.

C'est dans ce contexte que le présent guide a été élaboré. Il vise à soutenir les organismes publics dans la désignation des intervenants devant occuper les fonctions de responsable organisationnel de la sécurité de l'information (ROSI), de conseiller organisationnel en sécurité de l'information (COSI) ou de coordonnateur organisationnel de gestion des incidents (COGI), ci-après désignés « les principaux intervenants ».

2. Portée et champ d'application

Le présent guide s'applique à l'information gouvernementale consignée dans un document[4], 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 (à ce sujet, consulter l'annexe II).

---

2. Les documents structurants se déclinent comme suit :
   - Directive sur la sécurité de l'information gouvernementale;
   - Cadre gouvernemental de gestion de la sécurité de l'information;
   - Cadre de gestion des risques et des incidents à portée gouvernementale;
   - Approche stratégique gouvernementale en sécurité de l'information 2014-2017.
3. Pour obtenir plus de détails sur le niveau de maturité, consulter l'Approche stratégique gouvernementale en sécurité de l'information 2014-2017 (section 5.6).
4. Document : 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 : Loi concernant le cadre juridique des technologies de l'information – article 3].

3. Profil des principaux intervenants

Les principaux intervenants en sécurité de l'information exercent une fonction transversale, dans un environnement où les systèmes de mission sont de plus en plus ouverts sur l'extérieur et dépendent fortement d'une technologie en constante évolution. Une telle conjoncture nécessite des architectures et des infrastructures interconnectées, où les risques d'atteinte à la sécurité de l'information exigent que les responsabilités[5] des principaux intervenants soient clairement définies.

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

3.1.1 Raison d'être de la fonction

« Le ministre ou le dirigeant d'un organisme public doit désigner un responsable organisationnel de la sécurité de l'information pour le représenter en matière de sécurité de l'information auprès de son organisation et auprès du dirigeant principal de l'information. Ce responsable doit être un employé régulier de l'organisme public et appartenir à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur. »

[Source : Directive sur la sécurité de l'information gouvernementale, article 8, paragraphe a]

Le ROSI assure la coordination et la cohérence des actions, dont les principales portent sur l'adoption d'une politique et d'un cadre de gestion de la sécurité de l'information ainsi que sur la mise en œuvre de processus officiels de gestion des risques, de gestion de l'accès à l'information et de gestion des incidents de sécurité de l'information.

3.1.2 Positionnement

Dans le contexte actuel, marqué par une gestion intégrée de la sécurité de l'information, le ROSI est appelé à jouer un rôle transversal, pour l'ensemble des systèmes de mission de l'organisation. De ce fait, et sans qu'il soit mis dans une situation de conflit d'intérêts, le ROSI doit bénéficier d'une marge de manœuvre qui dépend essentiellement de son positionnement hiérarchique, d'où l'avantage de son rapprochement du pouvoir décisionnel, voire de la haute direction.

3.1.3 Attributions caractéristiques

Les attributions caractéristiques du ROSI sont axées sur les enjeux liés à la maîtrise du risque de sécurité de l'information. Elles lui permettent d'assumer pleinement son rôle de porteur de la vision de sécurité de l'information et de garant de sa mise en œuvre. Les principales attributions caractéristiques se déclinent comme suit :

- ✓ conseiller la haute direction en matière de sécurité de l'information;
- ✓ promouvoir les orientations et les objectifs stratégiques gouvernementaux de sécurité de l'information au sein de son organisation;
- ✓ assurer la coordination des actions de sécurité de l'information;
- ✓ représenter le dirigeant d'organisme en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale;

5. Les responsabilités attribuées au ROSI, au COSI et au COGI sont décrites dans la présente section. Elles résument celles énoncées dans le cadre gouvernemental de gestion de la sécurité de l'information.

- ✓ mettre en place et animer les comités internes de coordination et de concertation en sécurité de l'information;
- ✓ définir et mettre en œuvre les orientations internes de sécurité de l'information;
- ✓ définir et mettre en œuvre les processus officiels de sécurité de l'information;
- ✓ soutenir les unités administratives et les détenteurs de l'information dans la prise en charge des exigences de sécurité de l'information;
- ✓ présenter au comité chargé de la sécurité de l'information et à la haute direction le bilan des réalisations en matière de sécurité de l'information et les priorités d'action;
- ✓ s'assurer de l'intégration des dispositions de sécurité de l'information dans le cadre des ententes de service et des contrats;
- ✓ s'assurer de la prise en compte des exigences de sécurité de l'information lors de la réalisation de projets de développement ou d'acquisition de systèmes d'information;
- ✓ coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
- ✓ instaurer un processus de veille sur les menaces et les vulnérabilités et sur les bonnes pratiques de sécurité de l'information.

3.1.4 Compétences liées au savoir (connaissances)

a) Connaissances générales

- ✓ Normes et standards en sécurité de l'information (ISO 27000, COBIT, etc.);
- ✓ Notions de base sur la gouvernance et la gestion de la sécurité de l'information;
- ✓ Cadre légal et réglementaire régissant la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels;
- ✓ Politiques et règles de sécurité :
  - Directive sur la sécurité de l'information gouvernementale;
  - Cadre gouvernemental de gestion de la sécurité de l'information;
  - Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information.

b) Connaissances propres à l'organisation

- ✓ Systèmes de mission de l'organisation;
- ✓ Contexte légal et normatif régissant la gouvernance des ressources informationnelles, dont la sécurité de l'information;
- ✓ Planification stratégique, politiques et directives de l'organisation;
- ✓ Orientations gouvernementales et sectorielles en ressources informationnelles.

3.1.5 Habiletés personnelles et professionnelles

Le ROSI appartient à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur. De ce fait, les habiletés personnelles et professionnelles du ROSI sont régies par le Référentiel de compétences du gestionnaire-leader de la fonction publique québécoise[6]. Les organismes publics font notamment usage de ce référentiel pour élaborer les profils de compétences du ROSI. Il y est fait mention des prédispositions essentielles et des compétences clés et complémentaires.

3.2 Conseiller organisationnel en sécurité de l'information (COSI)

3.2.1 Raison d'être de la fonction

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

[Source : Cadre gouvernemental de gestion de la sécurité de l'information, section 5.1.4]

Le COSI collabore étroitement avec le ROSI. Il lui apporte le soutien nécessaire dans le déploiement et la mise en œuvre de stratégies de sécurité de l'information. Plus particulièrement, le COSI intervient au plan tactique de la sécurité de l'information, en mettant en œuvre les orientations internes et les priorités d'action, notamment celles portant sur l'instauration de processus officiels de sécurité de l'information et de suivis de leur mise en œuvre.

3.2.2 Attributions caractéristiques

Les attributions caractéristiques du COSI sont, notamment :

- ✓ contribuer à l'évaluation du niveau de maturité de la sécurité de l'information de l'organisation et proposer des pistes de solutions visant son rehaussement;
- ✓ contribuer à la mise en œuvre des orientations internes découlant des directives gouvernementales et sectorielles, des politiques internes, des normes et standards et des pratiques gouvernementales de sécurité de l'information;
- ✓ produire le bilan des réalisations en matière de sécurité de l'information;
- ✓ proposer des plans d'action et s'assurer de leur mise en œuvre;
- ✓ assister les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans l'analyse des risques de sécurité de l'information;
- ✓ contribuer à la conception et la mise en œuvre de processus officiels de sécurité de l'information;
- ✓ contribuer à l'auto-évaluation de la sécurité de l'information;
- ✓ tenir à jour le registre d'autorité de la sécurité de l'information;
- ✓ contribuer à l'intégration de dispositions de sécurité de l'information aux ententes et aux contrats;
- ✓ contribuer à l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation du personnel à la sécurité de l'information;
- ✓ participer au processus de veille sur les menaces et les vulnérabilités et sur les bonnes pratiques de sécurité de l'information.

6. http://www.tresor.gouv.qc.ca/fileadmin/PDF/publications/referentiel_competences.pdf

3.2.3 Compétences liées au savoir (connaissances)

a) Connaissances générales

- ✓ Normes et standards en sécurité de l'information (ISO 27000, COBIT, etc.);
- ✓ Processus de gestion de la sécurité de l'information (gestion des risques, gestion des incidents, etc.);
- ✓ Méthodologies d'analyse des risques (MEHARI, OCTAVE, etc.);
- ✓ Cadre légal et réglementaire régissant la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels;
- ✓ Principes de gestion de projet;
- ✓ Connaissance des principes, des approches et des méthodes dans les domaines suivants :
  - gouvernance de la sécurité;
  - catégorisation des actifs informationnels;
  - gestion des risques, gestion des droits d'accès logiques et physiques, gestion des incidents et gestion de la continuité des services, audit, intégration de la sécurité dans le développement ou l'acquisition des systèmes.

b) Connaissances propres à l'organisation

- ✓ Systèmes de mission de l'organisation et de son environnement technologique;
- ✓ Contexte légal et normatif régissant la gouvernance des ressources informationnelles, dont la sécurité de l'information;
- ✓ Planification stratégique, politiques et directives de l'organisation;
- ✓ Orientations gouvernementales et sectorielles en ressources informationnelles.

c) Certifications constituant un atout

- ✓ CISM *(Certified Information Security Manager)*
- ✓ CISSP *(Certified Information Systems Security Professional)*
- ✓ CRISC *(Certified in Risk and in Information Systems Control)*
- ✓ Système de gestion de la sécurité de l'information *(Lead Implementer ISO 27001)*
- ✓ Système de gestion de la sécurité de l'information (*Lead Auditor ISO 27001*)
- ✓ Gestion des risques *(Lead Implementer ISO 27005)*
- ✓ Gestion des risques (*Lead Auditor ISO 27005*)
- ✓ CISA *(Certified Information Systems Auditor)*

3.2.4 Habiletés personnelles et professionnelles

Cette section est développée dans un document intitulé « Profil de compétences : Conseiller en sécurité de l'information », réalisé par la Direction du développement des personnes et des organisations du Secrétariat du Conseil du trésor. Il y fait référence des compétences retenues pour le profil du COSI et des comportements clés. Le document en question s'inscrit dans le cadre de la mise en œuvre du plan d'action en gestion des ressources humaines 2012-2015, notamment pour répondre à l'objectif visant à « renforcer l'expertise et développer les compétences nécessaires pour répondre aux priorités et aux enjeux gouvernementaux ».

3.3 Coordonnateur organisationnel de gestion des incidents (COGI)

3.3.1 Raison d'être de la fonction

« Le ministre ou le dirigeant d'un organisme public doit désigner un coordonnateur organisationnel de gestion des incidents pour le représenter auprès du Réseau d'alerte gouvernementale et y participer activement. Ce coordonnateur doit être un employé régulier de l'organisme public et appartenir à la classe d'emploi de niveau professionnel ou à une classe d'emploi de niveau supérieur. »

[Source : Directive sur la sécurité de l'information gouvernementale, article 8, paragraphe b]

Le coordonnateur organisationnel de gestion des incidents (COGI) agit au niveau opérationnel. Il apporte au ROSI et au COSI le soutien technique nécessaire pour qu'ils puissent s'acquitter de leurs responsabilités. Il est l'interlocuteur officiel de son organisation auprès du CERT/AQ [7] et contribue au réseau d'alerte gouvernemental[8].

3.3.2 Attributions caractéristiques

Les principales attributions caractéristiques du COGI sont, notamment :

- ✓ fournir au ROSI et au COSI le soutien technique nécessaire pour qu'ils puissent s'acquitter de leurs responsabilités;
- ✓ contribuer au processus gouvernemental de gestion des incidents et au réseau d'alerte gouvernemental;
- ✓ coordonner la gestion des incidents de sécurité de l'information à portée sectorielle;
- ✓ assurer la coordination du CERT/AQ de son organisation et mettre en œuvre les stratégies de réactions appropriées;
- ✓ contribuer aux analyses de risques de sécurité de l'information, déterminer les menaces et les vulnérabilités et mettre en place les solutions appropriées;
- ✓ contribuer à l'auto-évaluation de la sécurité des systèmes informatiques et des réseaux informatiques, notamment par des exercices d'audits et des tests d'intrusion;
- ✓ maintenir une veille continue sur les risques, les menaces et les vulnérabilités.

7. Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise, relevant du Centre de services partagés du Québec (CSPQ).
8. Pour obtenir plus de détails sur le réseau d'alerte gouvernemental, consulter le Cadre gouvernemental de gestion de la sécurité de l'information (section 4.3.6).

3.3.3 Compétences liées au savoir (connaissances)

a) Connaissances générales

- ✓ Techniques de base sur le fonctionnement des réseaux informatiques;
- ✓ Fonctionnement du processus de gestion des incidents à portée gouvernementale;
- ✓ Normes et standards en gestion des incidents de sécurité de l'information (ISO 27035, ITIL, etc.);
- ✓ Processus de gestion de la sécurité de l'information (gestion des risques, gestion des incidents, gestion des accès, etc.);
- ✓ Cadre légal et réglementaire régissant la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels.

b) Connaissances propres à l'organisation

- ✓ Systèmes de mission de l'organisation et de son environnement technologique;
- ✓ Contexte légal et normatif régissant la gouvernance des ressources informationnelles, dont la sécurité de l'information;
- ✓ Planification stratégique, politiques et directives de l'organisation;
- ✓ Orientations gouvernementales et sectorielles en ressources informationnelles.

c) Certifications constituant un atout :

- ✓ CEH[9] *(Certified Ethical Hacker)*
- ✓ Certifications Cisco
- ✓ Certifications Microsoft
- ✓ Certifications Linux
- ✓ Certifications Novell Netware
- ✓ Toute autre certification pertinente dans le domaine technologique

3.3.4 Habiletés personnelles et professionnelles

Comme pour le COSI, les habiletés personnelles et professionnelles du COGI sont développées dans un document intitulé « Profil de compétences : Conseiller en sécurité de l'information », réalisé par la Direction du développement des personnes et des organisations du Secrétariat du Conseil du trésor. Il y fait référence des compétences retenues pour le profil du COGI et des comportements clés. Le document en question s'inscrit dans le cadre de la mise en œuvre du plan d'action en gestion des ressources humaines 2012-2015, notamment pour répondre à l'objectif visant à « renforcer l'expertise et développer les compétences nécessaires pour répondre aux priorités et aux enjeux gouvernementaux ».

9. La certification CEH est utile pour la coordination et la gestion des incidents de nature technologique.

ANNEXE I Cadre légal et normatif

Le présent document s'appuie sur des lois, des directives, des normes, des standards et des pratiques gouvernementales. Ceux-ci constituent le cadre légal et normatif gouvernemental.

Sur le plan légal, citons :

- ✓ 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 (chapitre G-1.03);
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
- ✓ la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);
- ✓ la Loi sur l'administration publique (chapitre A-6.01);
- ✓ la Loi sur les archives (chapitre A-21.1), en ce qui a trait aux exigences relatives à la protection et à la conservation des documents électroniques ayant une valeur patrimoniale ou archivistique;
- ✓ la Loi modifiant diverses dispositions législatives eu égard à la divulgation de renseignements confidentiels en vue d'assurer la protection des personnes (LQ, 2001, chapitre 78);
- ✓ la Loi sur le droit d'auteur (fédérale) (LRC, 1985, chapitre C-42);
- ✓ la Loi sur le patrimoine culturel (chapitre P-9.002);
- ✓ les lois sectorielles régissant la mission de chaque organisme;
- ✓ la Directive sur la sécurité de l'information gouvernementale.

Sur le plan normatif, citons :

- ✓ le Cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ le Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ les normes internationales.

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.

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique