AUTORITÉ DES MARCHÉS FINANCIERS

Politique-cadre de gouvernance des actifs informationnels

5 octobre 2022

Version administrative : 16 avril 2024

Table des matières

POLITIQUE-CADRE DE GOUVERNANCE DES ACTIFS INFORMATIONNELS DE L'AUTORITÉ

1. PRÉAMBULE

L'Autorité des marchés financiers (l'« Autorité ») est l'organisme de réglementation, de surveillance et d'assistance aux consommateurs de produits et services financiers au Québec. Elle a pour mission d'appliquer les lois relatives à l'encadrement du secteur financier québécois, notamment dans les domaines des assurances, des valeurs mobilières, instruments dérivés, des institutions de dépôt – sauf les banques – et de la distribution de produits et services financiers, incluant le courtage hypothécaire ainsi que celui de l'évolution du crédit.

Dans l'exercice de sa mission et ses responsabilités, l'Autorité, détient des actifs informationnels pour lesquels elle assure la mise en place d'un cadre de gouvernance efficient.

Ce cadre vise à assurer le respect des exigences légales auxquelles l'Autorité est assujettie et l'enlignement sur les politiques et directives gouvernementales applicables, notamment. Il vise aussi à renforcer la résilience de l'Autorité face aux risques informationnels.

Il tient compte notamment des principes énoncés dans la Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications publiée par l'Autorité (la « Ligne directrice de l'Autorité sur les risques TI ») pour la mise en place de mesures contribuant à prévenir la matérialisation d'un incident de sécurité majeur et à limiter ses impacts.

L'Autorité se dote ainsi d'une gouvernance forte et intégrée par laquelle elle :

- détermine les stratégies, politiques et procédures de mise en œuvre des principes de saine gestion; et
- voit à leur application en regard de la nature, de la taille, de la complexité des activités et du profil de risque.

La protection et la sécurité de l'information sont au cœur de cette gouvernance, tant dans la gestion que dans l'utilisation et l'exploitation des actifs informationnels de l'Autorité.

Par ailleurs, l'accès à l'information et sa diffusion constituent des activités incontournables pour une organisation gouvernementale moderne. Celles-ci permettent à un organisme public de faire connaître, en toute transparence, des renseignements liés à ses fonctions et ses différentes actions.

En parallèle, la protection des renseignements personnels est une composante essentielle de l'action gouvernementale dans laquelle l'Autorité s'investit afin d'assurer le respect du droit à la vie privée.

La gouvernance et la valorisation des données ainsi que la gouvernance et la gestion des ressources informationnelles sont également des éléments cruciaux qui font partie intégrante de la gouvernance des actifs informationnels et sont hautement stratégiques dans la réalisation de la mission de l'Autorité.

Le tout est soutenu par une saine gouvernance et gestion de l'information pour assurer une utilisation adéquate des actifs informationnels de l'Autorité ainsi que leur exploitation optimale.

La *Politique-cadre de gouvernance des actifs informationnels de l'Autorité* (la « Politique-cadre ») est la pièce de gouvernance maîtresse qui chapeaute les autres pièces de gouvernance relatives à ses actifs informationnels. Ensemble, elles forment le cadre de gouvernance des actifs informationnels de l'Autorité (le « Cadre de gouvernance ») dont la cartographie est présentée en annexe.

Elle vise à établir une vision commune de la gouvernance de l'ensemble des actifs informationnels de l'Autorité dans une perspective de cohérence organisationnelle.

La Politique-cadre annule et remplace la version 2.0 du *Cadre de gouvernance relatif à l'actif informationnel de l'Autorité* approuvée le 21 décembre 2012 par la décision nº 2012-PDG-0231.

Les termes utilisés dans la présente Politique-cadre ont le sens qui leur est attribué dans le *Lexique commun relatif à la gouvernance des actifs informationnels*. Il est disponible sur l'intranet et sur le portail électronique du conseil d'administration de l'Autorité.

2. CADRE LÉGAL, ADMINISTRATIF ET NORMATIF

À titre d'organisme public, l'Autorité est soumise à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* RLRQ, c. A-2.1 (la « Loi sur l'accès ») ainsi qu'aux règlements pris en vertu de celle-ci, notamment le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, r.2 (le « Règlement sur la diffusion »).

Cette loi favorise la transparence organisationnelle et prévoit les mesures à suivre par les organismes publics en matière d'accès à l'information et de protection des renseignements personnels. Elle loi établit également un équilibre entre le droit à l'information et le droit à la vie privée.

Les restrictions aux droits d'accès généraux prévues à la Loi sur l'accès ainsi qu'à certaines dispositions de la loi constitutive de l'Autorité, à savoir la *Loi sur l'encadrement du secteur financier,* RLRQ, c. E-6.1 (la « Loi sur l'encadrement »), et aux lois qu'elle administre protègent la confidentialité de certains renseignements ou actifs informationnels.

Les renseignements détenus par l'Autorité dans le cadre de l'exercice de ses pouvoirs d'encadrement et d'application de la loi, à la suite d'une inspection ou une enquête notamment, bénéficient d'une protection additionnelle et spécifique du fait que certaines dispositions législatives restreignent leur divulgation et leur accès.

En outre, le Code civil du Québec, la *Loi sur les archives*, RLRQ, c. A-21.1, *Loi sur la gouvernance des sociétés d'État*, RLRQ, c. G-1.02, la Directive gouvernementale sur la sécurité de l'information, décret numéro 1514-2021 (la « Directive gouvernementale ») prise en application de l'article 20 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03 (pour laquelle l'Autorité bénéficie du décret d'exclusion 1091-2012 du 21 novembre 2012, modifié par l'article 25 du PL 135 (2017, C. 28)), la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1 (la « LCCJTI »), les textes réglementaires, les lignes directrices et directives constituent les fondements légaux et administratifs des pièces de gouvernance relatives aux actifs informationnels de l'Autorité.

La présente Politique-cadre et les pièces de gouvernance qui s'y rattachent s'inspirent par ailleurs des meilleures pratiques, notamment de la norme ISO 24143:2022 *Information et documentation – Gouvernance de l'information – Concept et principes*, de la norme ISO 15489 *Information et documentation - Gestion des documents d'activité* et du Manuel du professionnel en AIPRP de l'Association des professionnels en accès à l'information et en protection de la vie privée (« AAPI »), des normes ISO 27000 en sécurité de l'information, des standards du *National Institute of Standards and Technology* (« NIST ») et du *Center for Internet Security* (« CIS ») ainsi que des publications du *SANS Institute*. En matière de gouvernance et gestion des ressources informationnelles, l'Autorité prend appui sur les pratiques du *Information Technology Infrastructure Library* (« *ITIL* ») et du *Scaled Agile Framework* (« *SAFe* »).

3. ÉNONCÉS GÉNÉRAUX

L'Autorité reconnaît que les actifs informationnels, sous toutes leurs formes, qu'il s'agisse d'information, de documents au sens de l'article 3 de la LCCJTI, de connaissances, de données, de composantes technologiques, systèmes informatiques ou autres ressources informationnelles, sont essentiels à ses opérations courantes.

Elle reconnaît également qu'elle est tributaire d'un certain nombre d'actifs informationnels qui sont stratégiques pour l'accomplissement de sa mission et l'atteinte des résultats attendus. À ce titre, non seulement doivent-ils faire l'objet d'une utilisation appropriée, d'une gestion efficace et d'une protection adéquate tout au long de leur cycle de vie, mais ils doivent aussi être optimisés et valorisés.

Dans un contexte de croissance de la masse d'information, de l'ouverture à son partage, des nouvelles exigences de la gestion des connaissances, de l'évolution rapide et constante des technologies et des exigences en matière de sécurité, l'Autorité met en place une structure de gouvernance de ses actifs informationnels qui tient compte de l'évolution des technologies qui s'opère dans la société et de la transformation numérique de l'organisation.

4. STRUCTURE DE GOUVERNANCE

La Politique-cadre présente la structure générale de la gouvernance de même que ses principes directeurs et jette les bases de la collaboration et de la coordination des actions de l'ensemble des secteurs opérationnels impliqués. Cette gouvernance a aussi pour objectif de permettre l'évaluation de la maturité de notre organisation et de faire évoluer son écosystème pour s'adapter aux enjeux voire les anticiper.

Les pièces qui composent le Cadre de gouvernance sont fondées sur les énoncés généraux à l'effet que ces actifs sont essentiels à ses opérations courantes, doivent faire l'objet d'une utilisation et d'une protection adéquate. De même, ils visent tant les relations envers les tiers que celles entre les membres du personnel, ces derniers ayant accès uniquement aux ressources qui leur sont nécessaires et permises dans l'exécution de leurs fonctions.

L'Autorité a adopté des politiques qui visent à définir les principes selon lesquels doit être traitée l'information au sein de l'organisation, le tout en application du cadre juridique applicable :

4.1 Politique visant la gouvernance de l'information

L'Autorité doit adopter une *Politique de gouvernance de l'information* pour exprimer sa position sur l'application des pratiques de gestion des connaissances, de l'information, des documents et des données considérées comme essentielles à l'accès, à la consultation, à l'exploitation, à la modification, au transfert, à la conservation, à la communication ou transmission, à la protection et à la conservation ou la destruction de l'information.

Une telle politique vise à établir la stratégie par laquelle l'Autorité entend s'acquitter de ses obligations relatives à la gouvernance de l'information et à définir ses axes d'intervention pour encadrer et coordonner le déroulement de l'ensemble des activités liées à l'information détenue et générée au sein de l'Autorité. Elle vise aussi à promouvoir la saine gestion des connaissances qui en découlent.

Également, l'objectif de cette politique est d'appuyer la position de l'Autorité quant à l'importance de la valorisation des données pour la réalisation de sa mission et de présenter les risques et opportunités qui s'offrent aux différentes lignes d'affaires afin que les choix en matière de valorisation représentent un équilibre entre les risques et bénéfices pour chacune d'elles.

4.2 Politique visant la sécurité de l'information

L'Autorité possède un cadre de gouvernance spécifiquement dédié à la sécurité de l'information qu'elle détient pour assurer sa conformité avec les lois et encadrements gouvernementaux. Ces orientations sont en phase avec les priorités et directives gouvernementales en la matière.

La *Politique de sécurité de l'information* établit la stratégie et les axes d'intervention par lesquels l'Autorité entend assurer la sécurité de l'information afin de préserver la disponibilité, l'intégrité et la confidentialité des actifs informationnels qu'elle détient ou qu'elle génère dans le cadre de ses opérations.

Le *Cadre de gestion de la protection et de la sécurité de l'information* complète cette politique en définissant la structure de gestion et les rôles et responsabilités des intervenants en matière de protection et de sécurité de l'information. Il établit les priorités d'intervention tant pour la protection des renseignements personnels que la sécurité de l'information. On y prévoit notamment la mise en place du Comité de protection et de sécurité de l'information (le « CPSI ») dont le mandat est d'appuyer le Président-directeur général et le Comité de gestion intégré des risques (le « CGIR ») dans les orientations stratégiques, les plans et pratiques en matière de sécurité de l'information.

Ces documents et ceux qui en découlent (ex. directives, règles, procédures, guides, etc.) ont pour objectif d'établir une vision commune des mesures qui contribuent à la sécurité des actifs informationnels de l'Autorité. Ils assurent la cohérence et la coordination des interventions en cette matière et intègrent le modèle des trois lignes instauré par *The Institute of Internal Auditors* et promu par la Ligne directrice de l'Autorité sur les risques TI. Ces documents sont aussi en adéquation avec le processus d'escalade des incidents de sécurité de l'information en vigueur à l'Autorité et formalisé par la règle visant à structurer sa mise en œuvre.

4.3 Politique visant l'accès à l'information détenue par l'Autorité et garantissant la protection des renseignements personnels

La Loi sur l'accès établit les mesures à suivre par les organismes publics québécois en matière d'accès et de protection des renseignements personnels de même que les renseignements autrement confidentiels. Cette loi établit aussi un équilibre entre le droit à l'information, les valeurs organisationnelles de transparence et d'imputabilité et le droit à la vie privée. Au sein de l'Autorité, ces droits occupent une place primordiale.

L'Autorité, conformément à la Loi sur l'accès, a procédé à la désignation du Secrétaire général adjoint pour exercer les fonctions de responsable de l'accès aux documents et de la protection des renseignements personnels au sein de l'organisation.

De même, une *Politique d'accès à l'information et de protection des renseignements personnels* est implantée au sein de l'Autorité. Cette politique vise à développer une culture d'accès à l'information et à la protection des renseignements personnels et à établir un encadrement à la fois clair et efficace de l'exécution des obligations de l'Autorité en la matière. Le *Cadre de gestion de la protection et de la sécurité de l'information* qui met en œuvre cette politique définit les rôles et les responsabilités dévolus aux membres du personnel en cette matière, car ceux-ci doivent contribuer au développement, à la mise en œuvre et à l'évolution d'une véritable culture de l'accès à l'information et de la protection des renseignements personnels.

Cette politique prévoit que le CPSI, mis en place au sein de l'Autorité conformément à la Loi sur l'accès agit notamment à l'égard des responsabilités édictées à l'article 2 du Règlement sur la diffusion.

4.4 Politique visant la gouvernance et la gestion des ressources informationnelles (TI)

Finalement, l'Autorité s'est dotée d'une *Politique de gouvernance et gestion des ressources informationnelles* enlignée sur les objectifs du gouvernement qui prônent l'adoption de règles claires pour une utilisation optimale des ressources informationnelles, plus particulièrement dans le cadre des projets liés aux technologies de l'information (« TI »).

Cette politique prévoit la mise en place du Comité de gouvernance des technologies de l'information (le « CGTI ») pour la prise en charge les responsabilités qui incombent à l'Autorité et coordonner les processus, l'allocation budgétaire et la reddition afférente.

Ces politiques sont complétées par des cadres de gestion qui établissent les structures fonctionnelles nécessaires à la gestion et à la mise en œuvre de la gouvernance des actifs informationnels afin d'atteindre les orientations et objectifs qui y sont définis en plus de décrire les rôles et responsabilités des divers intervenants au sein de l'Autorité, en complément de ceux décrits dans les politiques et dans la présente Politique-cadre.

Des directives, règles, guides et procédures précisant les dispositions à respecter et les modalités d'application complètent ce corpus de pièces de gouvernance.

Les pièces qui composent le Cadre de gouvernance ainsi que les documents produits en soutien à leur mise en œuvre permettent aux utilisateurs de saisir clairement la portée de leurs obligations et de leurs responsabilités tout en les sensibilisant aux risques associés à l'usage des technologies de l'information.

5. CHAMP D'APPLICATION

Le Cadre de gouvernance s'applique aux utilisateurs, c'est-à-dire tous les membres du personnel de l'Autorité, membres de son conseil d'administration, membres du Conseil consultatif des consommateurs de produits et utilisateurs de services financiers institué par l'article 58.1 de la Loi sur l'encadrement ainsi que toute personne, entité ou partenaire qui, par un engagement contractuel ou autre, accède, collecte, héberge ou traite de l'information détenue ou générée par l'Autorité à partir de ses locaux ou de n'importe quel autre endroit prévu à ces fins.

Le Cadre de gouvernance vise toute activité impliquant la création, la collecte, l'utilisation, le traitement, l'exploitation, la communication, la conservation ou la destruction d'une information ou d'un actif informationnel détenu par l'Autorité, qu'elle soit conduite dans ses locaux ou de n'importe quel autre endroit prévu à ces fins.

Le Cadre de gouvernance s'applique à tout actif informationnel détenu par l'Autorité dans la réalisation de sa mission ou par un mandataire, sans égard à sa localisation, conformément à la Loi sur l'accès et la LCCJTI.

Il s'applique également à tout autre actif informationnel de l'Autorité, notamment à une banque d'information électronique, un système ou un support d'information, une technologie de l'information, un service infonuagique, une installation ou un ensemble d'éléments, acquis ou constitué par l'Autorité.

Le Cadre de gouvernance s'applique tout au long du cycle de vie de chacun des actifs informationnels détenus par l'Autorité.

6. PRINCIPES DIRECTEURS

La gouvernance des actifs informationnels de l'Autorité repose sur des principes directeurs destinés à orienter l'élaboration des différentes pièces de gouvernance ainsi que la prise de décisions et d'actions à l'Autorité. Ils sont définis comme suit :

- **Imputabilité :** Superviser la gouvernance des actifs informationnels et déléguer aux personnes appropriées la responsabilité de la gestion de l'information et des risques qui y sont reliés.
- **Transparence :** Favoriser la transparence, dans le respect du droit à la vie privée et de la protection des renseignements personnels et autres règles de confidentialité applicables.
- **Disponibilité :** Conserver ses actifs informationnels d'une manière appropriée et qui garantit leur récupération rapide, efficace et précise selon la nature de l'information.
- **Intégrité :** S'assurer que les actifs informationnels générés ou gérés pour l'organisation ont une garantie d'authenticité et de fiabilité adéquate.
- **Protection :** Assurer l'application de mesures de protection proportionnelles à la valeur de l'information et aux risques encourus au niveau de la disponibilité, de l'intégrité et de la confidentialité des actifs informationnels.

- **Conformité :** Se conformer aux lois applicables, aux autres règles contraignantes et aux politiques de l'organisation.
- **Conservation :** Conserver ses actifs informationnels en tenant compte de ses aspects juridiques, réglementaires, financiers, opérationnels et historiques et ce, tout au long de leur cycle de vie.
- **Disposition :** Assurer une disposition sûre et appropriée pour les actifs informationnels dont la conservation n'est plus requise, en conformité avec les lois applicables et les politiques de l'organisation.
- **Qualité :** Assurer un haut degré de précision, d'exhaustivité, d'homogénéité, de fiabilité et d'actualité des informations que conserve l'Autorité afin de permettre leur bonne organisation et de faciliter leur exploitation.
- **Valorisation :** Mettre en place et maintenir un processus de collecte, de traitement et d'analyse de données permettant l'utilisation pertinente et optimale de celles-ci dans la réalisation de la mission de l'Autorité.

7. RÔLES ET RESPONSABLITÉS

Les fonctions stratégiques et transversales en matière de gouvernance des actifs informationnels à l'Autorité sont les suivantes :

Conseil d'administration

Le conseil d'administration (le « CA ») obtient l'assurance raisonnable que l'organisation agit en conformité du cadre législatif et réglementaire applicable. Il s'assure aussi que le Cadre de gouvernance est respecté et mis à jour périodiquement. Il doit aussi s'assurer que l'organisation met en place les mesures de contrôle adéquates.

En matière de gouvernance de l'information (fonction gouvernance et gestion de l'information et fonction gouvernance et valorisation des données) (« GI ») :

Le CA s'assure :

- que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement organisationnel respectant les bonnes pratiques et exigences en matière de gouvernance et de gestion de l'information;
- de l'évaluation régulière des structures, rôles et responsabilités de GI afin de permettre le développement et l'amélioration continue de la gouvernance.

Également, il approuve la Politique GI.

En matière de sécurité de l'information et protection des renseignements personnels (« PSI ») :

Le CA doit évaluer l'intégrité des contrôles internes, des contrôles de la divulgation de l'information, des systèmes d'information ainsi que des risques associés à la sécurité et aux technologies de l'information.

Il s'assure :

- que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement organisationnel éthique et sécuritaire;
- de l'évaluation régulière des structures, rôles et responsabilités de PSI afin de permettre le développement et l'amélioration continue de la gouvernance des actifs informationnels;
- d'une fonction de 2e ligne qui supervise la gestion des risques de sécurité de l'information (« SI »);
- que la fonction audit interne (3e ligne de la SI) ait la capacité de revoir et fournir une assurance indépendante des rôles respectifs des 1re et 2e lignes et que les processus et contrôles sont en place;
- que les autres rôles et responsabilités des fonctions de gestion de la SI soient clairement définis dans l'établissement et le maintien de la gouvernance des actifs informationnels;
- d'être notifié des incidents de sécurité majeurs, conformément à la règle formalisant le processus d'escalade en vigueur à l'Autorité.

Également, il :

- reçoit la reddition de comptes périodique relativement aux incidents majeurs de sécurité dont les cyberévénements et risques résiduels importants acceptés par le CGIR de l'Autorité;
- est informé des stratégies d'appétit aux risques SI de même que des stratégies de gestion pour les risques les plus critiques à la réalisation de la mission de l'Autorité;
- approuve les politiques de l'Autorité en matière de PSI.

En matière de gouvernance et gestion des ressources informationnelles - TI (« GGRI ») :

Le CA s'assure :

- que la haute direction s'assure de la priorisation et du financement des initiatives en lien avec le plan stratégique et les opérations courantes de l'Autorité;
- de l'évaluation régulière des structures, rôles et responsabilités de GGRI afin de permettre le développement et l'amélioration continue de la gouvernance.

Également, il approuve la Politique GGRI.

Président-directeur général

Le Président-directeur général (« PDG ») est imputable de l'application de la présente Politique-cadre.

En matière de GI :

Le PDG est imputable de l'application de la *Politique de gouvernance de l'information* (la « Politique GI ») et des pièces de gouvernance afférentes.

En matière de PSI :

Le PDG est le premier et ultime responsable de la PSI à l'Autorité.

Le PDG est imputable :

- du respect du cadre législatif et réglementaire ainsi que des orientations stratégiques édictées dans la *Politique d'accès à l'information et de protection des renseignements personnels* (la « Politique AIPRP »);
- du respect du cadre législatif et réglementaire ainsi que des orientations stratégiques, des plans d'intervention et des pratiques édictées dans la *Politique de sécurité de l'information* (la « Politique SI »), le *Cadre de gestion de la protection et de la sécurité de l'information* (le « CGPSI ») et les directives applicables à la PSI au sein de l'Autorité;
- de la mise en place de mesures permettant de réduire les risques de SI à un niveau acceptable par l'organisation.

Il désigne les détenteurs des actifs informationnels, qui sont des employés de niveau cadre, qui ont pour responsabilité de s'assurer de la SI, et des ressources qui la sous-tendent, relevant de l'autorité de leur unité administrative. À cet égard, il effectue une désignation formelle des responsables suivants :

- Dirigeant de l'information (« DI »);
- Chef délégué à la sécurité de l'information (« CDSI »);
- Chef de la sécurité de l'information organisationnelle (« CSIO »);
- Responsable opérationnel de cyberdéfense (« ROCD »); et
- Responsable de l'accès aux documents et de la protection des renseignements personnels (« RADPRP »).

Il s'assure de la mise en œuvre des responsabilités et des obligations attribuées par la Loi sur l'accès et le Règlement sur la diffusion et met sur pied le CPSI pour le soutenir.

Le PDG veille à la sensibilisation et à la formation des membres du personnel sur les obligations et les pratiques en matière d'accès à l'information et de PSI.

En matière de GGRI :

Le PDG est imputable de l'application de la *Politique de gouvernance et gestion des ressources informationnelles* (la « Politique GGRI ») et des pièces de gouvernance afférentes.

Comité de direction

Le comité de direction (le « CODIR ») est l'instance qui recommande au comité de gouvernance et d'éthique du CA l'approbation par le CA de la Politique GI et les stratégies qui en découlent. Il reçoit aussi la reddition afférente.

Également, le CODIR met en place le Comité directeur de la gouvernance et de la valorisation des données (le « CDGVD ») afin de fédérer les efforts des multiples parties prenantes impactant ou étant impactées par la gouvernance et la valorisation des données (structurées et non structurées). Plus particulièrement, il confie à ce comité le mandat d'élaborer une vision commune en matière de gouvernance et de valorisation des données et contribuer à créer une culture de la donnée au sein de l'Autorité.

Afin de délimiter clairement son rôle en matière de PSI, le CODIR met en place le CGIR et lui confie les responsabilités énumérées dans la présente Politique-cadre. C'est par cette instance qu'il s'acquitte des responsabilités qui lui sont confiées en matière de PSI.

Enfin, la responsabilité de la GGRI incombe au CODIR. Celui-ci nomme le CGTI à cet égard et lui confie le mandat de la mise en place et du suivi de la GGRI.

Comité de gestion intégrée des risques

Le Comité de gestion intégrée des risques (le « CGIR ») appuie le PDG dans son rôle de premier responsable de la PSI de l'Autorité. Il reçoit les avis, plans d'intervention, recommandations et orientations soumis par le CPSI et fait un suivi sur l'état des risques en SI.

Le CGIR est consulté pour toutes les questions d'importance. Une reddition lui est faite concernant les enjeux majeurs. La reddition en matière de gestion des incidents est aussi communiquée trimestriellement.

Le CGIR valide le niveau de risque acceptable de même que les stratégies de gestion pour les risques les plus critiques à la réalisation de la mission de l'Autorité, conformément à la *Politique de gestion intégrée des risques* de l'Autorité. Il recommande le tout au comité d'audit pour approbation du CA.

Le CGIR approuve :

- la feuille de route ainsi que les statuts de mise en œuvre et les indicateurs de performance de la SI avec les impacts d'affaires afférents;
- les dérogations aux encadrements de l'Autorité en matière de sécurité de l'information et révise périodiquement ces dérogations;
- l'allocation de ressources pour réaliser les stratégies de SI (budget annuel au CODIR).

De plus, il :

- effectue le suivi de la gestion des risques de SI présentée par le VPFTT, propriétaire de ce risque;
- prend les décisions sur les points de vue divergents quant aux requis de sécurité des différents secteurs d'affaires, sur recommandation du CPSI.

Également, il obtient l'assurance que :

- la Politique SI a été développée, qu'elle définit adéquatement les objectifs et les règles à suivre pour la protection de la confidentialité, l'intégrité, l'authentification, l'irrévocabilité et la disponibilité des informations, qu'elle est documentée, diffusée et mise en œuvre;
- la Politique SI s'applique à toutes les activités incluant l'information de l'Autorité traitée chez les intervenants externes;
- des responsables ont été désignés pour chaque actif informationnel et que les contrôles déployés pour protéger ces actifs sont proportionnels à leur criticité et sensibilité;
- les gestionnaires responsables du développement de l'encadrement des risques SI on la compétence requise et il voit à l'assignation :
  - d'un responsable pour les systèmes informatiques et les technologies de l'information qui soutiennent les objectifs de l'entreprise (« DPTI »);
  - d'un responsable tel un chef de la sécurité de l'information (« CISO »), ou autre personne de la 2e ligne pour la surveillance du déploiement de l'encadrement relatif à la sécurité de l'information et à la sécurité physique des infrastructures technologiques (« DGIR »);
  - d'un responsable tel un chef des données ou autre personne de la 2e ligne, lequel surveille l'encadrement approuvé à l'égard de la collecte, l'utilisation, la communication, la conservation et la destruction des données à travers l'Autorité (Chef des données et de l'analytique avancée (« CDAA »)).
- les contrôles en place sont efficaces conséquemment à la conduite de régimes d'essais systématiques adéquats.

Enfin, le CGIR est l'instance qui recommande :

- au comité d'audit et au comité de gouvernance et d'éthique du CA l'approbation par le CA de la Politique-cadre;
- au comité d'audit du CA l'approbation par le CA de la Politique SI, des orientations et stratégies et des objectifs incluant l'appétit pour le risque, compte tenu des coûts et bénéfices liés à la SI et de manière cohérente avec les objectifs stratégiques organisationnels approuvés;
- au comité de gouvernance et d'éthique du CA l'approbation par le CA de la Politique AIPRP.

et qui approuve le CGPSI et les directives qui en découlent.

La personne qui préside le CGIR est responsable de faire la reddition de compte au CA des risques résiduels importants acceptés par le CGIR en PSI.

Comité de gouvernance des technologies de l'information

Le Comité de gouvernance des technologies de l'information (le « CGTI »), bien que ne faisant pas partie des comités de l'Autorité liés à la SI, a la responsabilité d'assurer la sécurité des actifs informationnels reposants sur les actifs TI en budgétant des ressources suffisantes et en intégrant la SI dans ses initiatives.

Le CGTI :

- approuve les critères de priorisation, sélectionne les investissements et assure le suivi des projets touchant les ressources informationnelles;
- met en place et assure le suivi de la gouvernance et de la gestion des ressources informationnelles (« GGRI »);
- recommande au comité d'audit du CA l'approbation par le CA de la Politique GGRI.

Le CGTI est sous la responsabilité du VPFTT.

Chef de l'Audit Interne

Le Chef de l'Audit interne fournit une assurance indépendante et objective sur la suffisance et l'efficacité de la gouvernance, les processus de gestion des risques et les mécanismes de contrôle interne, l'efficience et l'efficacité des opérations, la protection des actifs informationnels et la fiabilité et l'intégrité de leurs processus de divulgation en tenant compte du positionnement de l'appétit pour les risques de sécurité par le CGIR.

À cet égard, ses responsabilités sont les suivantes :

- effectuer la revue de la conception et de l'efficacité des contrôles de sécurité de l'information, incluant les contrôles maintenus par les parties externes.;
- revoir les assurances fournies par une partie externe et qui ont le potentiel de nuire aux activités de l'Autorité;
- surveiller et évaluer l'environnement de contrôle :
  - les autoévaluations;
  - les revues d'assurance; et
  - l'identification des déficiences dans les contrôles, la conformité des processus supportés par les TI aux lois, règlements et obligations contractuelles, etc.
- effectuer des tests, simulation pour valider l'efficacité des contrôles;
- examiner les indicateurs de gestion qui sont utilisés pour la reddition de compte sur la sécurité de l'information;
- revoir les travaux effectués par la fonction de gestion des risques et par le DGIR.

Le Chef de l'Audit interne, représentant de la 3e ligne de la SI, est un invité permanent, mais non décisionnel du CPSI.

Secrétaire et directeur général des affaires juridiques

En matière de GI :

Les responsabilités du Secrétaire et directeur général des affaires juridiques (« DGSAJ ») sont les suivantes :

- affecter les ressources requises à la conception, au développement, à l'implantation, à la mise à jour et à l'évaluation d'un système de gestion de l'information et à l'application effective et efficace du système de gestion de l'information;
- assurer le respect des procédures, normes et règles à suivre provenant de Bibliothèque et Archives nationales du Québec;
- promouvoir les meilleures pratiques de gestion de l'information, par toute mesure appropriée, afin de sensibiliser son personnel à l'importance d'une gestion efficace et rentable des documents;
- soumettre, conjointement avec le VPFTT, la Politique GI à l'approbation du CODIR;
- faire, conjointement avec le VPFTT, le suivi et la reddition annuelle de la Politique GI au CODIR et au CA.

En matière de PSI :

Le DGSAJ intervient au niveau de la 2e ligne de la SI, notamment en soulevant au CGIR tout risque en matière de protection des renseignements personnels (« PRP ») dont ceux de non-conformité.

Le DGSAJ coordonne les interventions des domaines de responsabilités de son secteur avec la PRP, en tenant compte des besoins et priorités de l'organisation et en assure une saine gestion.

À ce titre, ses responsabilités sont les suivantes :

- soumettre pour approbation au CGIR la Politique-cadre et faire la reddition afférente au CGIR et au CA;
- soumettre pour approbation au CGIR la Politique AIPRP, les orientations et stratégies, incluant l'appétit pour le risque lié à la PRP, compte tenu des coûts et bénéfices et faire la reddition afférente au CGIR et au CA;
- s'assurer que les rôles et responsabilités des intervenants de la PRP sont clairement définis;
- définir des objectifs clairs de PRP;
- effectuer auprès du CGIR le suivi de la gestion des risques PRP en tant que propriétaire et responsable de ces risques (présente les risques inhérents et résiduels, proposer les indicateurs de performance, une feuille de route et présenter le statut sur la mise en œuvre);
- présenter au CA les stratégies liées à la PRP approuvées au CGIR ainsi que les statuts sur leur mise en œuvre;
- assurer qu'il n'y a pas de différence entre l'approche aux risques PRP et la véritable approche mise en œuvre;
- informer le CA sur les procédures d'escalade lors de brèches ou d'incidents de sécurité impliquant la PRP, conformément à la règle applicable en la matière;
- surveiller le déploiement de l'encadrement relatif à la PRP, tel qu'approuvé par le CGIR;

- obtenir l'assurance que :
  - la Politique AIPRP a été développée, documentée, diffusée et qu'elle définit bien les principes et les règles à suivre;
  - les contrôles déployés pour protéger les actifs informationnels sont proportionnels à la criticité et la sensibilité desdits actifs;
  - les contrôles en place sont efficaces conséquemment à la conduite de régimes d'essais systématiques adéquats.
- assurer l'efficacité des processus d'escalade sur les conflits d'intérêts potentiels;
- expliquer au CGIR les principales différences entre les propositions présentées et la position des membres du CPSI (points de vue divergents);
- inclure dans la feuille de route différents types d'évaluation, de tests et de revues périodiques à être réalisés par le Chef de l'Audit interne et par des experts indépendants;
- communiquer au RADPRP les décisions prises par le CGIR sur les enjeux qui ont été escaladés;
- agir comme médiateur pour réconcilier des divergences entre les requis de PRP des différentes divisions et présente au CGIR les problématiques non résolues;
- suggérer au CODIR une allocation de ressources pour réaliser les stratégies de PRP.

Responsable de l'accès aux documents et de la protection des renseignements personnels

En matière de GI :

Le Responsable de l'accès aux documents et de la protection des renseignements personnels (« RADPRP ») est responsable de la gouvernance et de l'organisation de l'accès à l'information. Il bénéficie d'une indépendance de fonction. Il s'appuie sur l'équipe de la gouvernance et de la gestion de l'information et sur celle de la gouvernance et de la valorisation des données pour s'assurer de la saine gestion des risques en matière d'accès à l'information et de protection des renseignements personnels (« AIPRP ») ainsi que de la conformité règlementaire de l'information consignées ou détenues dans l'organisation.

À ce titre, ses responsabilités sont, notamment, de :

- s'assurer que l'Autorité établisse un plan de classification de ses documents et qu'elle respecte ce plan;
- s'assurer que l'Autorité établisse un calendrier de conservation, qu'elle le fasse approuver par BAnQ et qu'elle respect ce calendrier;
- s'assurer que l'Autorité diffuse l'information prescrite dans le respect du Règlement sur la diffusion;
- insérer dans le rapport annuel de gestion de l'Autorité une mention qui atteste de la diffusion des documents conformément au Règlement sur la diffusion;
- disposer avec diligence des demandes d'accès aux documents détenus par l'Autorité ainsi que des demandes de rectification et demandes de révision, conformément à la Loi sur l'accès et à la *Politique d'accès à l'information et de protection des renseignements personnels* de l'Autorité.

En matière de PSI :

Le RADPRP se rapporte au PDG. Il est membre du CPSI et est le premier répondant pour tout ce qui se rapporte à la PRP. Il doit aussi communiquer et se coordonner étroitement avec les intervenants clés de l'Autorité en PSI pour répondre aux exigences de Loi sur l'accès.

Le RADPRP est responsable de surveiller l'application de la Loi sur l'accès et du Règlement sur la diffusion dans le cadre des activités de l'Autorité qui concernent, notamment, la collecte, l'utilisation, la communication, la conservation, l'anonymisation ou la destruction des renseignements personnels.

Il intervient au niveau de la 1re ligne de la SI et participe à l'évaluation des risques et des mesures de sécurité requises compte tenu, notamment, de la confidentialité, de la finalité, de la qualité, de la répartition et du type de support des renseignements personnels.

Il a l'obligation d'aviser la Commission d'accès à l'information (la « CAI ») et la personne concernée de tout incident de confidentialité impliquant un renseignement personnel présentant un risque de préjudice sérieux et de tenir un registre à cet effet.

Il collabore avec les divers intervenants en PSI afin de s'assurer de l'efficacité des mesures de sécurité propres à assurer la PRP. À cet égard, il collabore avec le Directeur de la sécurité de l'information (« DSI ») et le Directeur de la gestion intégrée des risques (« DGIR ») à :

- la rédaction de politiques et directives en matière de PRP et à développer et communiquer la formation continue à cet égard;
- la définition des mesures propres à assurer la PRP dans la réalisation des projets TI qui créent, recueillent, utilisent, transfèrent, traitent, exploitent, communiquent, conservent ou détruisent des renseignements personnels.

L'étendue des responsabilités, le niveau d'autorité et les droits de décision sont pour le RADPRP, entre autres, les suivants :

- exercer un rôle-conseil auprès des unités administratives, notamment en examinant, au regard de la conformité avec la Loi sur l'accès et le Règlement sur la diffusion, tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels et informer le CPSI de l'incidence d'un tel projet sur les renseignements personnels;
- procéder à une évaluation des facteurs relatifs à la vie privée (« EFVP ») de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels et informer le CPSI de l'incidence d'un tel projet sur la vie privée des personnes concernées;
- s'assurer de la mise en application des mesures de PRP identifiées lors des EFVP;
- proposer au président du CPSI les enjeux de SI liés à la PRP, pour l'information tant numérique que non numérique, à adresser par les membres du comité;
- mettre en place un processus de reddition entre lui et le DGSAJ pour que celui-ci puisse faire une reddition en tant que membre du CGIR lors d'enjeux de SI liés à la PRP;
- assister les détenteurs des actifs informationnels dans l'identification des risques PRP, faire rapport au CPSI des risques importants non mitigés qui ont été portés à sa

connaissance et, au besoin, se coordonner avec le DGSAJ pour que celui-ci puisse inclure ces risques dans sa reddition au CGIR;

- conseiller les détenteurs de renseignements personnels sur les mesures requises pour respecter les obligations légales tout au long du cycle de vie des actifs informationnels et veiller à la sensibilisation et à la formation des membres du personnel en cette matière.

Responsable de la gouvernance et de la gestion de l'information

Le Responsable de la gouvernance et de la gestion de l'information (« RGGI ») se rapporte au Secrétaire général adjoint. Il a le mandat d'élaborer et de mettre en œuvre d'une stratégie de gouvernance et de gestion de l'information consignée ou détenue pour l'ensemble de l'organisation (la « gouvernance et la gestion de l'information »).

À cet effet, le titulaire est responsable de deux sphères d'activités distinctes et transversales en lien avec l'information :

- Mise en place et maintien d'un cadre de gestion;
- Gestion opérationnelle d'une équipe centralisée de spécialistes en gestion d'information.

Le titulaire et son équipe soutiennent l'organisation dans sa transformation numérique en exerçant un rôle-conseil auprès des autres secteurs de l'Autorité en matière de gestion de l'information.

En matière de GI :

Les responsabilités du RGGI sont les suivantes :

- assurer un rôle de leadership et coordonner les initiatives inhérentes à la gouvernance et à la gestion de l'information;
- assurer une gouvernance et une gestion de l'information tout au long de son cycle de vie en raison de son statut d'actif pour l'organisation;
- élaborer les orientations stratégiques et le programme d'activités transversales en matière de gouvernance et de gestion de l'information consignée;
- élaborer et mettre en place des systèmes et des méthodes de travail qui visent à traiter, à déterminer la valeur et à exploiter l'information véhiculée par les actifs informationnels ainsi qu'à justifier les supports appropriés;
- effectuer, en collaboration avec la Direction des technologies de l'information, les études d'intégration des moyens bureautiques et informatiques et superviser la mise en application des systèmes de traitement et d'exploitation retenus à la suite de ces études;
- établir, tenir à jour et appliquer des outils de gestion de l'information consignée tels que :
  - plan de classification;
  - index de repérage;
  - matrice de maturité.
- établir, tenir à jour et appliquer un calendrier de conservation des documents et le faire approuver par Bibliothèque et Archives nationales du Québec;
- élaborer et mettre en place, en collaboration avec le RADPRP et le DSI, les systèmes et les mécanismes qui visent à assurer la diffusion systématique des documents, la protection

des documents essentiels de l'organisation, la mise en application des mesures de sécurité et d'accès à l'information et de PRP;

- évaluer les résultats obtenus après l'implantation des systèmes de traitement et d'exploitation;
- participer à l'identification des risques en matière de gestion d'information ainsi qu'à la définition et à la mise en œuvre de stratégie et de procédures permettant l'application de mesures d'atténuation;
- appliquer des mesures de protection de l'information en fonction des exigences liées aux risques informationnels et aux processus de qualité.

En matière de PSI :

Le RGGI élabore et met en place, en collaboration avec le RADPRP et le DPTI ou son représentant, les systèmes et les mécanismes qui visent à assurer les valeurs administratives, financières et légales ainsi que la pérennité, l'intégrité et la confidentialité des documents officiels sur support électronique et papier, ainsi que la mise en application des mesures de sécurité et d'accès à l'information et de PRP.

Il gère les incidents de sécurité de l'information reliés aux documents de toute nature en s'intégrant à la directive et au processus de gestion des incidents de l'Autorité.

À titre de responsable de la gestion documentaire au sens du Règlement sur la diffusion, il est appelé à siéger au CPSI de façon *ad hoc*, lorsque les sujets à l'ordre du jour requièrent son expertise concernant la gouvernance et la gestion de l'information.

L'étendue des responsabilités, le niveau d'autorité et les droits de décision sont pour le RGGI, entre autres, les suivantes :

- s'assurer que la consultation de certains documents de nature confidentielle s'effectue selon les paramètres d'accessibilité déterminés par l'Autorité. Il peut, dans ce cadre :
  - refuser la consultation de l'un ou l'autre de ces documents;
  - recommander, au besoin, qu'une action soit entreprise pour préserver les documents dont l'entreposage comporte des dangers de perte d'intégrité ou d'élimination.

Vice-président stratégie et risques

En matière de PSI :

Présidant le CGIR, le Vice-président stratégie et risques (« VPSR ») a les responsabilités suivantes :

- intervenir au niveau de la 2e ligne;
- favoriser une collaboration active entre les trois lignes;
- faire la promotion d'une gestion intégrée des risques en SI selon une approche holistique
- surveiller l'efficacité et la cohérence globale des dispositifs de contrôles mis en œuvre en matière de SI;
- approuver les scénarios, considérés à partir des analyses d'impact d'affaires, des plans de reprise et de continuité des activités ainsi que le plan de la mise à l'essai (tests);

- encourager la communication par une reddition de comptes périodique au CGIR, incluant la performance globale des plans de traitement des risques SI auprès des instances de décision et des comités internes;
- présenter au CA la reddition de compte des risques résiduels importants acceptés par le CGIR en PSI.

Chef des données et de l'analytique avancée

Le Chef des données et de l'analytique avancée (« CDAA » (ou *CDO*)) est responsable de l'élaboration et de la mise en œuvre d'une gouvernance des données et d'une stratégie de valorisation des données pour l'ensemble de l'organisation.

Le CDAA est responsable de deux sphères d'activités distinctes et transversales en lien avec les données :

- Mise en place et maintien d'une structure de gouvernance et de valorisation des données;
- Gestion d'une équipe centralisée de scientifiques de données responsables du développement de solutions d'analytiques avancées répondant à des problématiques complexes et communes à plusieurs lignes d'affaires, générant ainsi des économies d'échelle importantes.

Le CDAA et son équipe amènent l'organisation vers une culture axée sur les données.

De plus, le CDAA et son équipe d'experts exercent un rôle-conseil auprès des autres secteurs de l'Autorité en matière de gouvernance et de valorisation des données.

<u>En matière de GI</u> :

Les responsabilités du CDAA sont les suivantes :

- élaborer les orientations stratégiques et du plan d'activités de sa direction et des activités transversales de l'Autorité en matière de gouvernance et de valorisation des données;
- assurer un rôle de leadership en matière de gouvernance des données :
  - élaborer et recommander un plan d'activités pour mettre en œuvre la gouvernance des données à l'Autorité, en tenant compte des orientations établies par l'organisation en matière de technologies de l'information et de valorisation des données;
  - établir les directives en matière d'utilisation responsable des données, incluant les aspects liés à la classification, la protection et la confidentialité des données, ainsi que la gestion de leur cycle de vie et de leur exploitation éthique;
  - optimiser, en conformité avec ces directives, le partage des données entre les lignes d'affaires de l'organisation;
  - élaborer et mettre en œuvre des standards et des outils de gestion de gouvernance de données, incluant les gabarits de documentation des données;
  - développer et garder à jour une cartographie des données de l'Autorité, afin notamment d'assurer la traçabilité des données utilisées à l'interne, sur la base du développement d'un lexique commun des données;

- élaborer des règles et des balises sur l'intégrité et la qualité des données, et sur les mécanismes à mettre en place pour corriger les données à l'entrée, pour mesurer leur qualité et identifier éventuellement des problématiques (mécanismes de validation automatiques);
- identifier les indicateurs de performance clés à suivre afin d'évaluer la progression du déploiement de la gouvernance des données à l'Autorité;
- participer au déploiement du plan de communication associé à la gestion des données et, d'une façon plus large, à la gestion du changement nécessaire à la création d'une culture de la donnée dans l'ensemble de l'organisation.

- assurer un rôle de leadership en matière de valorisation des données :
  - élaborer et mettre en œuvre une stratégie d'appui à la valorisation des données à l'échelle de l'organisation, alignée sur un modèle fédéré, qui répond à la fois aux besoins organisationnels et spécifiques des lignes d'affaires (qui peuvent avoir une capacité et des besoins différents);
  - assurer un leadership technique et intellectuel en matière de valorisation des données, incluant les aspects éthiques reliés à l'exploitation des données, afin de promouvoir dans l'organisation des approches et solutions cohérentes et conformes aux meilleures pratiques;
  - surveiller et évaluer les derniers développements en matière de technologies, d'outils et d'approches en lien avec la valorisation et la sécurité des données afin de recommander des initiatives ou investissements ayant des avantages pour l'organisation, compte tenu des besoins actuels ou émergents;
  - procéder à l'identification et au tri des projets, des initiatives et opportunités pour exploiter les données, et recommander une priorisation en se basant sur les ressources disponibles et une compréhension des priorités actuelles et émergentes des lignes d'affaires et de l'organisation dans son ensemble;
  - jouer un rôle majeur dans l'élaboration et la mise en œuvre d'une stratégie de formation sur la valorisation des données pour l'ensemble de l'organisation.
- assurer une vigie en matière de gouvernance et de valorisation des données.

<u>En matière de PSI</u> :

Le CDAA a les responsabilités suivantes :

- surveiller, conjointement avec le DPTI, la mise en œuvre de l'encadrement approuvé par le CGIR à l'égard de la collecte, l'utilisation, la communication, la conservation et la destruction des données numériques et non en conformité avec les obligations légales de l'Autorité, notamment la Loi sur l'accès lorsqu'il s'agit de renseignements personnels. Cette responsabilité s'applique particulièrement dans le contexte de développement en milieu utilisateur (DMU);
- collaborer avec le DSI et le DPTI pour définir les principes et les règles à suivre pour la protection de la confidentialité, l'intégrité, l'authentification, l'irrévocabilité et la disponibilité des informations dans les activités de l'Autorité et celles qu'il encadre;
- assumer la responsabilité principale de l'intégrité des données, il agit de concert avec les autres intervenants incluant le DSI et le DPTI;

- assurer avec le DSI la coordination et la cohérence des actions de sécurité de l'information menées au sein de l'Autorité par d'autres intervenants dont les détenteurs des actifs informationnels ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la PRP, de la gestion de l'information, de la gouvernance et de la valorisation des données et de l'éthique;
- consulter le RADPRP pour toute question relative à la PRP en lien avec les initiatives de valorisation des données pour s'assurer de leur conformité à la Loi sur l'accès.

Vice-président finances, talents et technologies

En matière de GI :

Les responsabilités du Vice-président finances, talents et technologies (« VPFTT ») sont les suivantes :

- encadrer, coordonner et valoriser l'utilisation optimale des données numériques;
- identifier et mitiger les risques liés à la valorisation des données en milieu utilisateur;
- soutenir les secteurs dans leur valorisation des données;
- soumettre, conjointement avec le DGSAJ, la Politique GI à l'approbation du CODIR;
- faire, conjointement avec le DGSAJ, le suivi et la reddition annuelle de la Politique GI au CODIR et au CA.

En matière de PSI :

Le VPFTT coordonne les interventions des domaines de responsabilités de son secteur avec la PSI, en tenant compte des besoins et priorités de l'organisation et en assure une saine gestion.

La 1re ligne de la SI relève principalement du DPTI, sous la supervision du VPFTT.

Le VPFTT est porteur des domaines de responsabilités suivants en lien avec la SI :

- Les ressources informationnelles :
  - Encadrement des technologies de l'information
  - Encadrement de la sécurité de l'information
  - Gouvernance et gestion de projet
- Les autres services administratifs :
  - Gestion et formation des ressources humaines
  - Gestion des ressources matérielles, dont l'établissement des ententes contractuelles
  - Gestion des locaux incluant la sécurité physique et les infrastructures requises pour l'hébergement des technologies de l'information
  - Sécurité des personnes
  - Gestion des budgets (planification et suivi)

Dans le cadre de ses fonctions relatives à la gouvernance de la SI, le VPFTT est responsable de:

- s'assurer que les rôles et responsabilités des intervenants de la SI soient clairement définis;
- s'assurer que la Politique SI a été développée, documentée, diffusée et qu'elle définit bien les principes et les règles à suivre pour la protection de la confidentialité, l'intégrité, l'authentification, l'irrévocabilité et la disponibilité des informations;
- soumettre pour approbation au CGIR la Politique SI, les orientations et stratégies, incluant l'appétit pour le risque, compte tenu des coûts et bénéfices, ainsi que le CGPSI;
- approuver l'élaboration de l'architecture technologique et de SI et de son intégration à l'architecture d'entreprise;
- effectuer auprès du CGIR le suivi de la gestion des risques de SI en tant que propriétaire et responsable de ces risques (présente les risques inhérents et résiduels, proposer les indicateurs de performance, une feuille de route et présenter le statut sur la mise en œuvre);
- présenter au CA les stratégies liées à la SI approuvées au CGIR ainsi que les statuts sur leur mise en œuvre;
- assurer qu'il n'y a pas de différence entre l'approche aux risques SI et la véritable approche mise en œuvre;
- s'assurer que les procédures d'escalade au CA sont suivies, conformément au plan de gestion de crise de l'Autorité auquel réfère la règle relative au processus d'escalade d'incident de sécurité de l'information;
- surveiller le déploiement de l'encadrement relatif à la SI et à la sécurité physique des infrastructures technologiques, tel qu'approuvé par le CGIR;
- obtenir l'assurance que :
    - les contrôles déployés pour protéger les actifs informationnels sont proportionnels à la criticité et la sensibilité desdits actifs;
    - les contrôles en place sont efficaces conséquemment à la conduite de régimes d'essais systématiques adéquats.
- assurer l'efficacité des processus d'escalade sur les conflits d'intérêts potentiels :
- superviser le DSI par une ligne en pointillée (*dotted line*);
- inclure dans la feuille de route différents types d'évaluation, de tests et de revues périodiques à être réalisés par le Chef de l'Audit interne et par des experts indépendants;
- communiquer au DPTI les décisions prises par le CGIR sur les enjeux qui ont été escaladés;
- expliquer au CGIR les principales différences entre les propositions présentées et la position des membres du CPSI (points de vue divergents);
- agir comme médiateur pour réconcilier des divergences entre les requis de sécurité des différentes divisions et présenter au CGIR les problématiques non résolues;
- suggérer au CODIR une allocation de ressources pour réaliser les stratégies de SI;
- agir en tant que responsable des situations d'urgence et incidents majeurs (dont les cyberévénements) et en faire la reddition au CGIR et au CA;

- convoquer la cellule de crise, au besoin, conformément au plan de gestion de crise de l'Autorité auquel réfère la règle relative au processus d'escalade d'incident de sécurité de l'information.

En matière de GGRI :

Le VPFTT est responsable de soumettre pour approbation au CGTI la Politique GGRI, les orientations et stratégies, compte tenu des coûts et bénéfices. Il en fait également la reddition annuelle afférente au CA.

Directeur principal des technologies de l'information, occupant les fonctions de **:**

- **Dirigeant de l'information,**
- **Chef délégué de la sécurité de l'information**, et
- **Président du CPSI**

En matière de PSI :

Le Directeur principal des technologies de l'information (« DPTI ») veille à l'application des règles de gouvernance et de gestion, notamment les règles inhérentes à la sécurité de l'information établies.

De plus, il agit à titre de Dirigeant de l'information (« DI ») et CDSI auprès du chef gouvernemental de la sécurité de l'information tel que décrit dans la Directive gouvernementale.

Il assure la 1re ligne de la SI, sous la supervision du VPFTT.

À cet effet, il a les responsabilités suivantes :

- assurer le suivi de la mise en œuvre des recommandations émises par le ministre de la Cybersécurité et du Numérique ou par le sous-ministre de la Cybersécurité et du Numérique en sa qualité de Dirigeant principal de l'information;
- mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par l'Autorité, dont le développement et la mise à l'essai (tests) des plans de reprise informatiques;
- 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 PRP, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information;
- présider le CPSI avec un langage accessible aux gens d'affaires de façon à susciter l'engagement des participants et à réconcilier les différents points de vue;
- assurer la transparence dans la reddition de compte au CPSI;
- recommander au VPFTT les encadrements, les orientations et stratégies liées à la SI et le seuil d'appétit pour le risque en justifiant les propositions de risques résiduels plus élevés et en identifiant et expliquant au VPFTT les différences avec les propositions des membres du CPSI (points de vue divergents);

- effectuer auprès du VPFTT, en collaboration avec le DSI, le suivi des risques de SI en tant que responsable de la gestion de ces risques (proposer les indicateurs de performance, une feuille de route et faire le suivi des plans d'action);
- superviser le déploiement de l'encadrement relatif à la SI et à la sécurité physique des infrastructures technologiques puis préparer les statuts sur leur mise en œuvre;
- s'assurer que :
  - les contrôles déployés pour protéger les actifs informationnels sont proportionnels à la criticité et la sensibilité des dits actifs;
  - les contrôles en place sont efficaces conséquemment à la conduite de régimes d'essais systématiques adéquats.
  - le DSI collabore avec le CDAA et de l'analytique avancée pour que les encadrements liés à la SI soient développés, documentés, diffusés et qu'ils définissent bien les principes et les règles à suivre pour la protection de la confidentialité, l'intégrité, l'authentification, l'irrévocabilité et la disponibilité des informations.
- superviser le DSI dans l'élaboration de l'architecture technologique et de SI et de son intégration à l'architecture d'entreprise;
- superviser la mise en œuvre de l'encadrement approuvé par le CGIR à l'égard de la collecte, l'utilisation, la communication, la conservation et la destruction des données, numériques et non numériques, en conformité avec la Loi sur l'accès lorsqu'il s'agit de renseignements personnels (responsabilité partagée avec le CDAA);
- s'assurer du bon fonctionnement de la fonction SI;
- recueillir et évaluer les indicateurs et les objectifs liés à la SI.
- effectuer, conjointement avec le DSI, la reddition au VPFTT et au CPSI, en temps opportun et de manière systématique et transparente;
- évaluer les risques de la SI, notamment, il doit :
  - identifier les risques de sécurité de l'information liés à la perte de confidentialité, d'intégrité et de disponibilité des informations et identifie les responsables des risques;
  - faire le lien entre les scénarios de risques et leurs impacts potentiels sur les actifs informationnels et sur les processus d'affaires afin que l'ensemble des parties intéressées comprennent les effets des évènements indésirables liés aux technologies de l'information et des communications;
  - établir et tenir à jour les critères de risque de SI incluant les critères d'acceptation des risques et les critères de réalisation des évaluations des risques de SI;
  - déterminer les mesures nécessaires à la mise en œuvre des options de mitigation des risques de SI;
  - comparer les mesures déterminées avec les meilleures pratiques existantes et vérifier qu'aucune mesure nécessaire n'a été omise;
  - produire une déclaration d'applicabilité répertoriant les mesures et la justification de leur inclusion ou exclusion en fonction de l'appétit pour le risque approuvé.
- encadrer et coordonner l'utilisation optimale des infrastructures technologiques et des espaces de stockage;
- assurer la sécurité des infrastructures sur lesquelles résident les documents numériques et les bases de données;

- gérer la sécurité des accès logistiques sur les infrastructures;
- gérer les droits d'utilisation des logiciels de gestion de l'information;
- assurer une veille technologique pour éviter la désuétude des technologies;
- mettre à la disposition des unités administratives des espaces de stockage pour l'entreposage et l'archivage des documents numériques, en collaboration avec le RGGI.

L'étendue des responsabilités, le niveau d'autorité et les droits de décision sont pour le DPTI, entre autres, les suivantes :

- assumer les responsabilités d'orientation, de planification et d'encadrement des ressources informationnelles;
- s'assurer que les actions engagées sont conformes aux objectifs d'affaires de l'Autorité;
- veiller à optimiser les sommes consacrées aux ressources informationnelles, dont celles en matière de PRP;
- coordonner et promouvoir la transformation organisationnelle;
- veiller à la pérennité des actifs informationnels;
- participer aux instances de concertation gouvernementale;
- veiller au respect des normes gouvernementales et la mise en œuvre des obligations applicables à l'Autorité en matière de sécurité de l'information.

L'étendue des responsabilités, le niveau d'autorité et les droits de décision sont pour le DI comme président du CPSI, entre autres, les suivantes :

- assumer un rôle de leader organisationnel en PSI à l'Autorité au sein des diverses instances de concertation;
- s'assurer de :
  - la gestion des enjeux et des dossiers reliés à l'encadrement stratégique de la sécurité de l'information de l'Autorité;
  - l'arrimage des orientations et des plans d'action en PSI avec la planification stratégique de l'Autorité;
  - la coordination et la cohérence des actions de PSI menées au sein de l'Autorité par d'autres intervenants dont le DSI, les détenteurs des actifs informationnels ainsi que par les autres membres du CPSI;
  - la contribution des principaux intervenants de l'Autorité au processus de gestion des risques et des incidents de sécurité de l'information.

<u>En matière de GGRI</u> :

Le DPTI a les responsabilités suivantes :

- coordonner la GGRI;
- siéger au CGTI en tant que membre permanent;
- agir comme délégué de l'Autorité pour les relations avec le ministère de la Cybersécurité et du Numérique et le Secrétariat du Conseil du Trésor;
- faire une reddition au CGTI.

Directeur du Bureau de projets d'entreprise

La Direction du Bureau de projets d'entreprise est le bureau de projets d'entreprise (le « BPE ») de l'Autorité.

Le Directeur du Bureau de projets d'entreprise (« DBPE »), à titre de responsable du BPE, doit conseiller le CODIR, prioriser les travaux du portefeuille d'entreprise, assurer une saine gestion des risques liés aux projets du BPE, accompagner les équipes de projets afin d'assurer un déroulement optimal et le respect du cadre normatif applicable, présenter la vision globale des initiatives de l'organisation et en faire la reddition.

En matière de GGRI :

Le DBPE a les responsabilités suivantes :

- gérer la planification financière de la Direction principale des technologies de l'information et du BPE et en assure le suivi;
- assumer la gestion du processus de gouvernance des TI de l'Autorité;
- produire et maintenir à jour les indicateurs de gestion liés aux investissements en RI;
- assurer la mise en place, le maintien et le développement des processus opérationnels et administratifs nécessaires pour soutenir efficacement la gestion des investissements en RI tout au long de leur cycle de vie;
- collaborer au respect des politiques, cadres de gestions, directives, règles et procédures qui s'appliquent à la gestion et à la gouvernance des RI;
- prioriser les dossiers d'affaires liés aux investissements et en assurer la préparation;
- collaborer à l'évolution de la GGRI;
- préparer le matériel destiné au CGTI en vue de la présentation des dossiers et de la reddition par le DPTI;
- siéger au CGTI en tant que membre permanent.

Détenteur des actifs informationnels

Chacun des gestionnaires de l'organisation est un détenteur des actifs informationnels (« détenteur »).

En matière de GI :

Le détenteur a les responsabilités suivantes :

- identifier les séries documentaires essentielles afin de déterminer la durée de vie des documents ainsi que la confidentialité et les niveaux de protection à appliquer sur les documents;
- approuver le déclassement des documents semi-actifs et le versement des documents inactifs de son unité administrative;
- approuver la destruction des actifs informationnels en conformité avec le calendrier de conservation;

- assurer l'organisation, la conservation, la protection et la destruction des actifs informationnels sous sa responsabilité;
- être informé des incidents touchant les actifs informationnels sous sa responsabilité.

En matière de PSI :

Les membres du CODIR, à titre de détenteurs des actifs informationnels situés au plus haut niveau hiérarchique, sont responsables d'assurer la sécurité de l'information relevant de leur unité administrative respective.

Ils s'acquittent de cette responsabilité de 1re ligne en déterminant les responsabilités qu'ils souhaitent assumer directement et celles qu'ils confient à l'exécution de l'un ou l'autre des gestionnaires de leur équipe.

Ainsi, tous les gestionnaires de l'Autorité sont réputés être les détenteurs des actifs informationnels nécessaires à l'exercice de leurs fonctions ainsi que celles qu'assument les membres du personnel qui relèvent d'eux.

À cet effet, le détenteur des actifs informationnels a les responsabilités suivantes :

- s'assurer que la collecte d'information est restreinte aux besoins réels;
- restreindre l'accès aux méthodes d'extraction des données aux besoins réels en tenant compte des évaluations de risque de fuite d'information;
- accorder les privilèges d'accès sur la base des principes « besoin de savoir », « moindre privilège » et « ségrégation des tâches » tel qu'établi en matière de gouvernance des données à l'Autorité et en conformité avec la Loi sur l'accès;
- procéder à la revue périodique des accès qui sont sous son autorité pour s'assurer que l'information soit accessible uniquement aux personnes qui en ont un besoin réel, qu'elle est utilisée pour les fins pour lesquelles elle a été recueillie et qu'elle est détruite lorsqu'elle n'est plus requise;
- assurer le respect de la gouvernance des actifs informationnels ainsi que l'application des contrôles tels que conçus;
- identifier les risques de sécurité d'information dans ses processus, effectuer la gestion et le suivi des risques résiduels et faire rapport au CPSI de tous les risques significatifs non mitigés;
- assumer la responsabilité ultime d'assurer l'adéquation des mesures de sécurité par rapport aux risques encourus et l'application efficace de ces mesures pour réduire le risque résiduel à un niveau faible (à moins d'exception approuvée par le CGIR).

Le détenteur est le responsable de certains processus et applications d'affaires de l'Autorité. Il communique le niveau des risques d'affaires/opérationnels applicables aux informations sur tous ses supports, aux applications et aux actifs informationnels dont il est responsable;

Il appuie le DSI dans la mise en application des mesures de PSI dans son unité administrative.

Le détenteur a la responsabilité de contrôler les coûts et bénéfices de sécurité applicables et de définir les exigences de sécurité pour les actifs informationnels sous sa responsabilité et pour son secteur d'activité.

Également, le détenteur est responsable de :

- définir et approuver la valeur de l'information et des actifs informationnels relevant de sa responsabilité en tenant compte des enjeux et des besoins de disponibilité, d'intégrité et de confidentialité liés à ses obligations légales et les impératifs d'affaires (catégorisation/cote DIC);
- prendre en compte les risques de SI associés aux actifs informationnels et s'assurer de l'application des mesures d'atténuation des risques dans les processus d'affaires et les systèmes d'information relevant de son secteur d'activité;
- participer, au besoin, à l'approbation des orientations stratégiques et recommandations des plans en PSI les concernant;
- signaler tout changement dans les processus et/ou les stratégies d'affaires (c.-à-d. nouveaux produits ou services) au CDAA.

8. RESPECT DE LA POLITIQUE-CADRE

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition, conformément à la législation applicable et aux codes d'éthique et de déontologie en vigueur à l'Autorité

Les utilisateurs doivent respecter la présente Politique-cadre et les pièces de gouvernance qui en découlent.

Tout utilisateur qui contrevient à la présente Politique-cadre ou aux pièces de gouvernance qui en découlent peut faire l'objet d'une mesure administrative, disciplinaire ou autre mesure légale applicable, pouvant aller jusqu'à une fin d'emploi ou à une fin de contrat, selon le cas.

Afin d'assurer une saine gestion des ressources ainsi que l'utilisation adéquate de ses actifs informationnels, l'Autorité peut effectuer certaines mesures de surveillance par l'intermédiaire des outils de travail mis à la disposition des utilisateurs et des moyens relatifs à la sécurité. Ces mesures de surveillance sont encadrées et effectuées selon les paramètres fixés par le droit applicable et l'ensemble des politiques et directives de l'organisation.

9. DIFFUSION

Cette Politique-cadre est publiée sur l'intranet de l'Autorité.

Pour toute information, question ou demande en lien avec cette Politique-cadre, tout membre du personnel peut communiquer avec son gestionnaire ou avec le Secrétariat général à l'adresse suivante : secretariat@lautorite.qc.ca

10. SUIVI ET RÉVISION

Le suivi et la présentation d'un bilan annuel au CGIR et au CA relativement à l'application de la présente Politique-cadre sont effectués par le DGSAJ.

Une révision complète de cette Politique-cadre et de toute pièce de gouvernance qui en découle doit être faite périodiquement pour s'assurer d'être adaptée au cadre légal et normatif applicable ainsi qu'aux bonnes pratiques en gouvernance des actifs informationnels. Cette révision doit minimalement être effectuée tous les cinq ans.

Une mise à jour doit aussi être effectuée lors de changements organisationnels ou stratégiques majeurs ou lorsque jugé opportun par le CA, son comité d'audit, le CODIR ou les comités institutionnels de l'Autorité dont le mandat concerne la gouvernance des actifs informationnels.

11. APPROBATION ET HISTORIQUE DES RÉVISIONS

Version N°	**Recommandation au comité d'audit et au comité de gouvernance et d'éthique du CA**	**Recommandation au CA**	**Approbation par le CA**
01	CODIR (tenant lieu de CGIR) : 13 juin 2022	Comité de gouvernance et d'éthique : 22 septembre 2022 Comité d'audit : 4 octobre 2022	5 octobre 2022 Résolution 2022-CA-0029
Version administrative produite par le Secrétariat général le 16 avril 2024			

12. ENTRÉE EN VIGUEUR

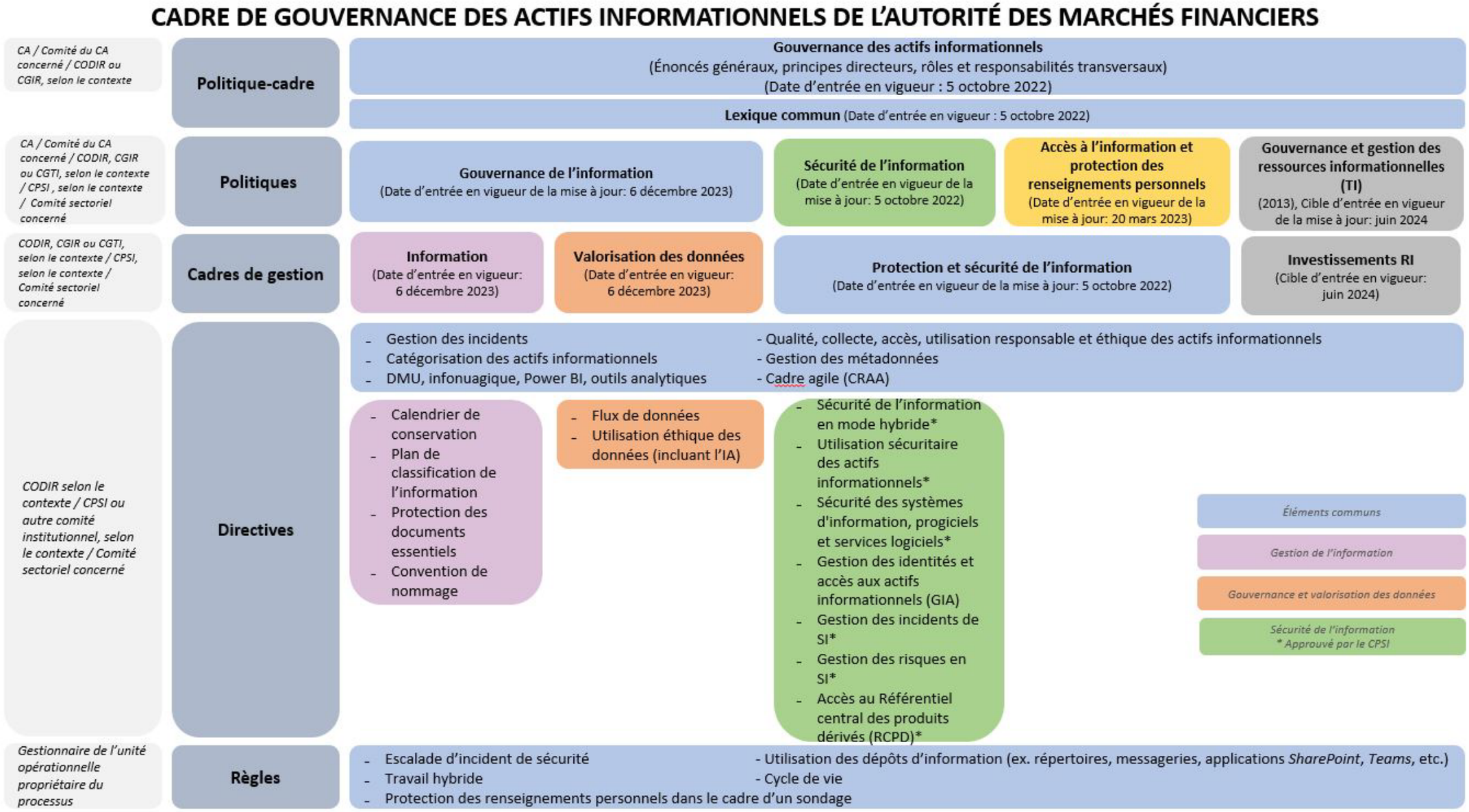
La Politique-cadre entre en vigueur à la date de son approbation par le conseil d'administration le 5 octobre 2022.

LISTE D'ACRONYMES

AAPI	Association des professionnels en accès à l'information et en protection de la vie privée
AIPRP	Politique d'accès à l'information et de protection des renseignements personnels
BAnQ	Bibliothèque de l'Assemblée nationale du Québec
CA	Conseil d'administration
CAI	Commission d'accès à l'Information
CDAA	Chef des données et de l'analytique avancée
CDSI	Chef délégué à la sécurité de l'information
CDGVD	Comité directeur de la gouvernance et de la valorisation des données
CGIR	Comité de gestion intégrée des risques
CGPSI	Cadre de gestion de la protection et de la sécurité de l'information
CGTI	Comité de gouvernance des technologies de l'information
CPSI	Comité de protection et de sécurité de l'information
CIS	Center for Internet Security
CISO	Chef de la sécurité de l'information (*Chief Information Officer*)
CSIO	Chef de la sécurité de l'information organisationnelle
CODIR	Comité de direction
DI	Dirigeant de l'information
DSI	Directeur de la sécurité de l'information
DGIR	Direction de la gestion intégrée des risques
DGSAJ	Direction générale du secrétariat et des affaires juridiques
DMU	Développement en milieu utilisateur
DPTI	Directeur principal des technologies de l'information
EFVP	Évaluation des facteurs relatifs à la vie privée

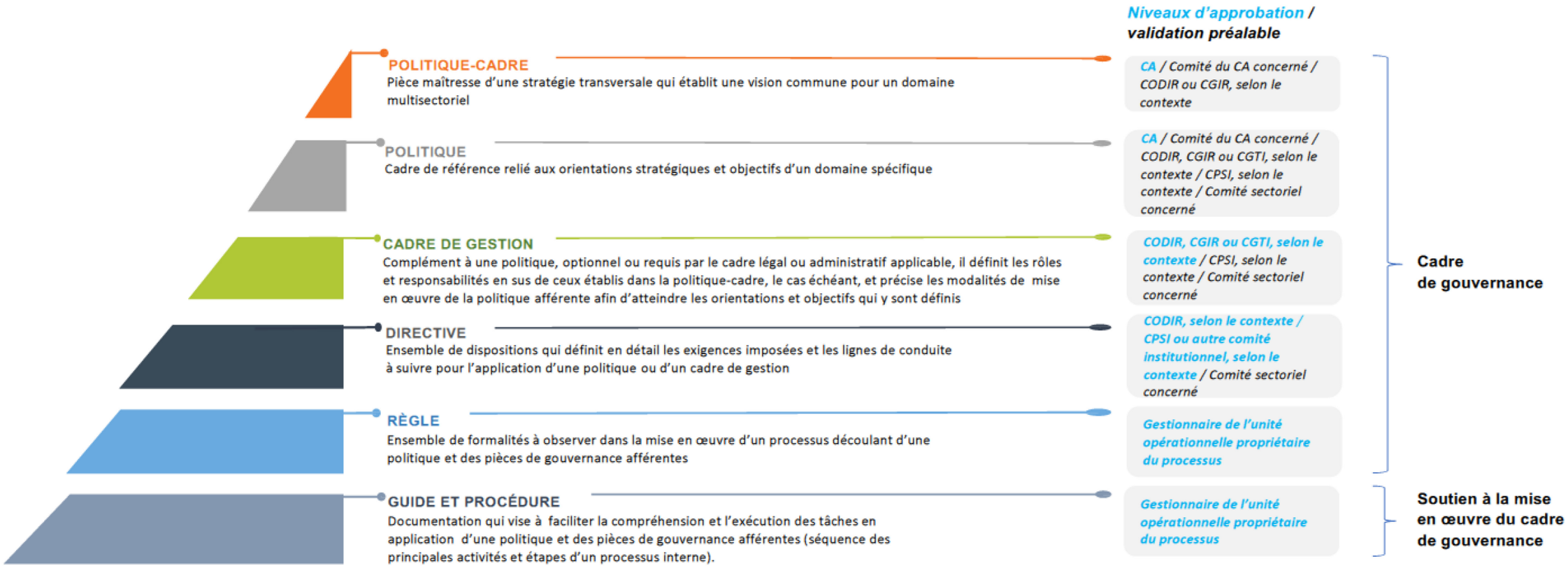
GGRI	Gouvernance et gestion des ressources informationnelles
GI	Gestion de l'information
ITIL	Information Technology Infrastructure Library
LCCJTI	Loi concernant le cadre juridique des technologies de l'information
NIST	National Institute of Standards and Technology
Politique GI	Politique de gouvernance de l'information
Politique SI	Politique de la sécurité de l'information
PSI	Protection des renseignements et sécurité de l'information
PRP	Protection des renseignements personnels
RADPRP	Responsable de l'accès aux documents et de la protection des renseignements personnels
RGGI	Responsable de la gouvernance et de la gestion de l'information
ROCD	Responsable opérationnel de cyberdéfense
SAFe	Scaled Agile Framework Canadian Securities Administrators / Autorités canadiennes en valeurs mobilières
SI	Sécurité de l'information
TI	Technologies de l'information
VPFTT	Vice-président finances, talents et technologies
VPSR	Vice-président stratégie et risques

ANNEXE – Cartographie de la gouvernance des actifs informationnels de l'Autorité



QUI APPROUVE QUOI?

À l'Autorité, un cadre de gouvernance est composé de divers documents de régie d'entreprise (pièces de gouvernance) qui concernent l'ensemble des membres du personnel et dont le respect est attendu de tous



Note:

- Puisque tous les membres du CODIR siègent au CGIR et au CGTI, l'approbation ou la validation par l'une ou l'autre de ces instances est réputée être celle du CODIR lorsque la pièce de gouvernance visée relève de leur mandat respectif.
- Lorsque l'échéancier d'un projet de pièce de gouvernance qui relève du mandat du CGIR ou du CGTI ne coïncide pas avec le calendrier de leurs séances respectives, le dossier peut être présenté au CODIR, pour approbation ou validation, selon le cas.

APPROUVÉ PAR LE CODIR (CGIR) – 13 juin 2022