



Rapport du Vérificateur général du Québec
à l'Assemblée nationale pour l'année 2016-2017

Hiver 2017

Étude

Portrait de la gouvernance et de la gestion des technologies de l'information au gouvernement du Québec

CHAPITRE

9

Sommaire

Objectifs de l'étude

L'importance des budgets consacrés aux technologies de l'information (TI) nous a amenés à réaliser une étude visant à dresser un portrait de la situation dans ce secteur d'activité. Cette étude n'est pas un audit. Elle présente les résultats d'une autoévaluation effectuée par les répondants des entités sélectionnées.

Le questionnaire d'autoévaluation a été transmis à 44 entités, soit 20 ministères, 19 organismes et 5 entreprises du gouvernement. Le taux de participation des premiers dirigeants responsables des TI est de 98 %.

Les objectifs poursuivis par l'étude sont les suivants :

- déterminer, à partir des résultats obtenus, les zones les plus vulnérables en matière de gouvernance et de gestion des TI au gouvernement du Québec ;
- permettre aux entités interrogées de se comparer ;
- orienter nos travaux d'audit de performance dans le secteur.

Le rapport entier est disponible au www.vgq.qc.ca.

Méthodologie

Pour concevoir le questionnaire d'autoévaluation, nous avons utilisé un modèle reconnu mondialement, soit le référentiel COBIT 5 proposé par l'ISACA (Information Systems Audit and Control Association), qui comprend 37 processus. Selon ce référentiel, tous les processus doivent atteindre les objectifs qui y sont associés pour produire un ensemble de résultats permettant la réalisation des objectifs globaux liés aux TI. Nous avons donc questionné les entités sur l'atteinte des objectifs liés à chacun des processus.

Pour chaque répondant, nous avons établi qu'un processus était vulnérable sur la base du principe du maillon le plus faible, soit lorsqu'un des objectifs y étant associés n'était pas atteint. Nous avons ensuite calculé la fréquence des réponses ainsi obtenues afin de classer les processus selon leur degré de vulnérabilité.

Il est important de mentionner qu'une autoévaluation repose sur le jugement du répondant ; celle-ci risque donc d'être subjective.

Observations

Nous présentons ci-dessous les principales observations concernant la gouvernance et la gestion des TI au gouvernement du Québec.

Les répondants estiment que les activités opérationnelles en matière de TI sont planifiées et réalisées comme il était prévu et que les problèmes liés aux TI sont résolus. Toutefois, ils ne sont pas certains que les investissements effectués dans le domaine génèrent une valeur optimale. Notre étude fait ressortir trois zones de vulnérabilité, soit la gouvernance des TI, leur alignement stratégique et la surveillance de leur performance.

Gouvernance des TI

La haute direction et les premiers dirigeants responsables des TI estiment ne pas avoir l'assurance :

- que le système de gouvernance fonctionne efficacement ;
- que chacun des investissements génère une valeur optimale ;
- que les risques critiques liés aux TI sont gérés efficacement et que leur impact est connu ;
- que les besoins en ressources sont comblés efficacement et que celles-ci sont utilisées de façon optimale.

Alignement stratégique des TI

Les premiers dirigeants responsables des TI perçoivent des enjeux à l'égard des processus de planification.

- Le choix des investissements semble approprié, mais les premiers dirigeants responsables des TI n'ont pas l'assurance qu'une surveillance appropriée est exercée, laquelle permet d'obtenir les bénéfices attendus.
- La compréhension des processus d'affaires, de l'information, des applications et des infrastructures en matière de TI ne semble pas suffisante pour soutenir efficacement l'organisation et pour permettre la réutilisation efficace des TI. Ces éléments ne semblent pas faire partie d'une architecture d'entreprise.
- L'innovation semble peu encouragée.
- Un profil de risque lié aux TI à jour et complet ne semble pas exister.
- La responsabilité de la livraison de la stratégie liée aux TI ne semble pas attribuée à quelqu'un.

Surveillance de la performance des TI

Selon les premiers dirigeants responsables des TI, la surveillance de la performance des TI semble déficiente car, pour chacun des trois processus y étant associés, au moins un objectif n'est pas atteint.

- L'approche ne semble pas efficace ni opérationnelle.
- Les processus ne semblent pas mesurés en fonction d'objectifs et d'indicateurs et, si ces derniers sont présents, ils ne semblent pas approuvés par les parties prenantes ou intégrés dans les systèmes de surveillance de l'organisation.
- La reddition de comptes portant sur la performance et la conformité ne semble pas toujours utile ni produite en temps opportun.
- Le système de contrôle interne ne semble pas être validé de manière indépendante pour s'assurer qu'il est opérationnel et efficace.

Notons qu'il s'agit d'un portrait global et qu'une vulnérabilité ne touche pas toutes les entités. De plus, un processus vulnérable ne s'explique pas de la même façon et n'a pas le même impact pour chaque entité concernée. Il n'est donc pas approprié de conclure que toutes les entités qui ont participé à l'étude sont touchées par les enjeux qui y sont soulevés. Par ailleurs, par souci de rentabilité et par respect des priorités, chaque entité décide du niveau d'exécution des processus et de la performance visée.

Des enjeux se posent à l'égard des processus jugés les plus vulnérables. Nous invitons la haute direction ou le conseil d'administration des entités interrogées à se questionner sur les raisons de la vulnérabilité de certains processus.

Bien que le Secrétariat du Conseil du trésor ait communiqué aux entités gouvernementales des orientations et des directives en matière de TI, des efforts additionnels semblent nécessaires pour mieux les guider.

Table des matières

1 Mise en contexte	6
2 Résultats de l'étude	10
2.1 Méthodologie	10
Répondants	
2.2 Analyse des résultats	12
Gouvernance des technologies de l'information	
Alignement stratégique des technologies de l'information	
Surveillance de la performance des technologies de l'information	
Autres résultats	
Conclusion	
 Annexes et sigles	 27

Équipe

Marcel Couture
Vérificateur général adjoint

Carole Bédard
Directrice d'audit
et responsable de mission

Patrice Watier
Directeur d'audit

Jean-François Bélanger
France Bêty

Selon le *Portrait de la main-d'œuvre en technologies de l'information de la fonction publique du Québec* publié au printemps 2016, il y avait, à la fin de 2015, plus de 8800 personnes qui travaillaient dans le domaine des TI pour les organismes dont le personnel est nommé en vertu de la *Loi sur la fonction publique*. Le tiers était des ressources externes.

Comme le prévoit la loi, le président du Conseil du trésor a déposé en 2016 un rapport concernant la mise en œuvre de celle-ci après les cinq premières années de son application. Ce rapport conclut que, même si des progrès sont toujours nécessaires, l'application de la loi permet d'avoir une meilleure connaissance des données financières, des projets et des activités menées à l'échelle gouvernementale.

1 Mise en contexte

1 Les technologies de l'information (TI) jouent un rôle de premier plan dans la prestation de services aux citoyens et aux entreprises, en plus de contribuer à la performance de l'État. Elles constituent des outils essentiels permettant au gouvernement de s'acquitter de ses responsabilités avec efficacité et efficience.

2 Selon le Secrétariat du Conseil du trésor (SCT), en 2015-2016, les budgets de dépenses et d'investissements dans ce domaine ont totalisé plus de 3 milliards de dollars pour les ministères, les organismes publics, Revenu Québec, le réseau de l'éducation et le réseau de la santé et des services sociaux. De cette somme, 73 % ont été consacrés à l'entretien et à l'exploitation des systèmes existants, alors que l'autre partie a été allouée au développement de nouveaux produits soutenant l'évolution des TI.

3 Comme nous l'avons annoncé dans le chapitre 1 du rapport déposé à l'Assemblée nationale à l'automne 2016, nous nous sommes intéressés à la gouvernance et à la gestion des technologies de l'information au gouvernement du Québec, compte tenu de leur importance pour le fonctionnement de l'État et des sommes investies dans le **domaine**.

Encadrement gouvernemental

4 Afin d'optimiser les ressources informationnelles, le gouvernement du Québec a posé des gestes dans le passé, notamment les suivants :

- l'adoption, en 2011, de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* ;
- la publication, en 2012, de la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* ;
- l'approbation par le Conseil du trésor, en 2012, des *Règles relatives aux demandes d'autorisation de projets et aux outils de gestion en ressources informationnelles*.

5 La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* précise les fonctions du dirigeant principal de l'information en matière de gestion et de gouvernance des TI. Outre son rôle de recommandation auprès du Conseil du trésor, le dirigeant principal de l'information est notamment chargé de mettre en œuvre les politiques et les directives établies conformément à la loi, d'en surveiller l'application et d'en coordonner l'exécution. Il est secondé par des dirigeants sectoriels de l'information et des dirigeants réseau de l'information qui veillent à l'application, par les organismes publics pour lesquels ils sont désignés, des règles de gouvernance et de gestion. L'annexe 1 présente les principales dispositions de la **loi**.

6 En 2015, comme des enjeux importants persistaient, une nouvelle stratégie gouvernementale en TI, intitulée *Rénover l'État par les technologies de l'information*, a été adoptée. Celle-ci mentionne que les outils de gouvernance et de gestion prévus dans la loi n'offrent pas la souplesse nécessaire au contexte évolutif des ressources informationnelles. Cette stratégie vise à revoir et à renforcer la gouvernance des TI, à gérer plus efficacement les talents, à adopter les meilleures pratiques et à rapprocher l'État des citoyens. D'ailleurs, afin d'élargir le rôle du dirigeant principal de l'information, un projet de modification de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* a été transmis au Conseil du trésor en novembre 2015 pour consultation auprès des organismes publics. Cette consultation est terminée et le SCT prévoit déposer un projet de loi à l'Assemblée nationale.

7 Il est important de noter que les dirigeants demeurent responsables de la gouvernance et de la gestion des TI dans leur organisation. Les orientations et les directives gouvernementales communiquées par le SCT ne dégagent pas les organisations de leurs responsabilités.

Normes et référentiels en technologies de l'information

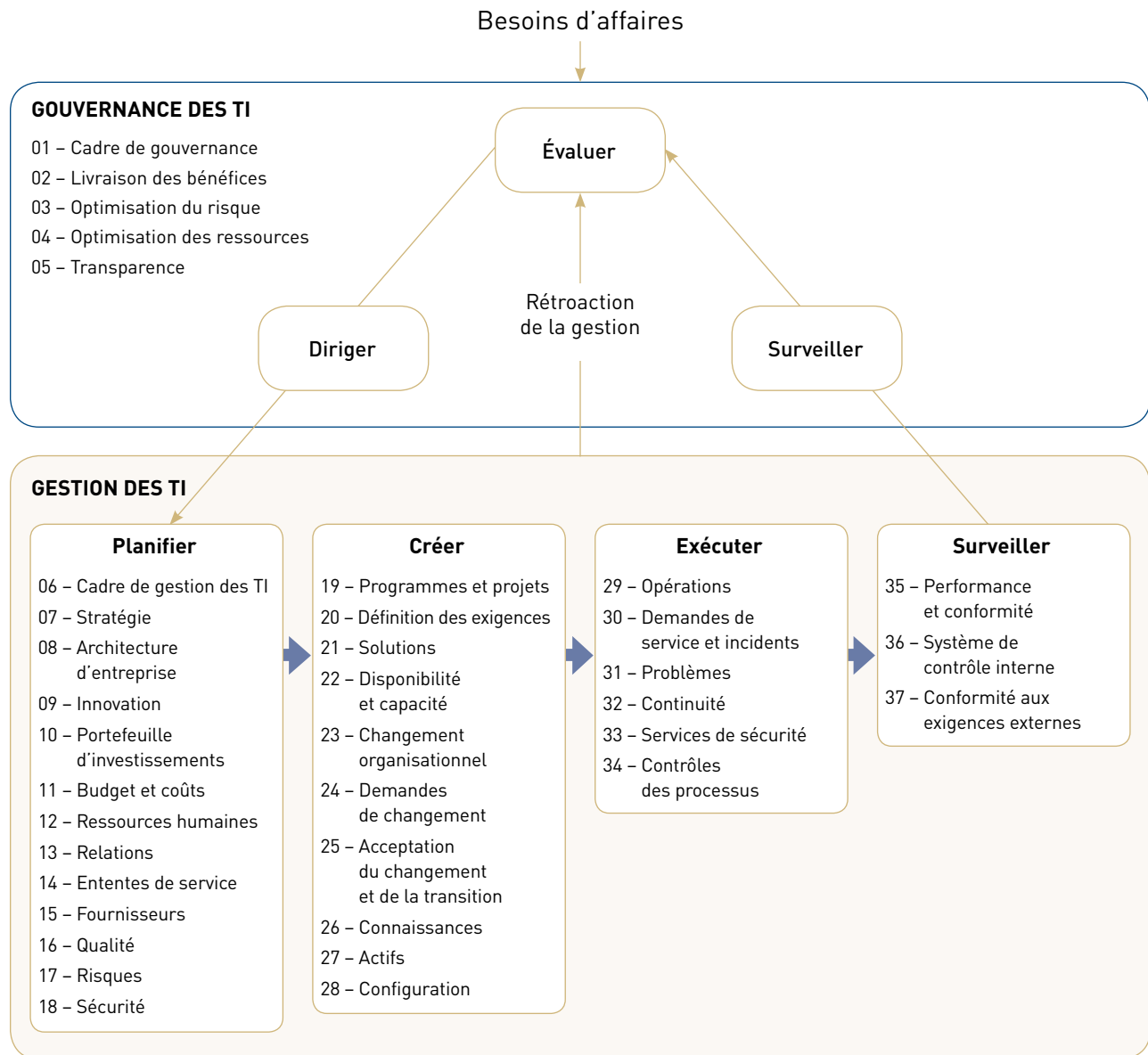
8 Il existe de nombreuses normes et bonnes pratiques dans le domaine des technologies de l'information. Le référentiel COBIT représente un des modèles de référence les plus reconnus en matière de gouvernance et de gestion des TI. Il est proposé par l'ISACA (Information Systems Audit and Control Association), une association regroupant plus de 140 000 professionnels de la gouvernance, de la sécurité, de la gestion des risques et de l'audit des TI qui proviennent de plus de 180 pays. Ce référentiel est utilisé notamment par plusieurs agences américaines, par le gouvernement de l'Alberta ainsi que par des vérificateurs législatifs, tels que ceux du Canada, de la Colombie-Britannique et de l'Australie.

9 La dernière version du référentiel, soit **COBIT 5**, comprend un modèle de référence qui présente l'ensemble des processus liés aux TI que l'on trouve habituellement dans une organisation. Selon ce référentiel, les besoins des **parties prenantes** doivent s'exprimer d'abord sous la forme d'objectifs d'affaires puis sous la forme d'objectifs liés aux TI. Pour atteindre ces objectifs, les organisations mettent notamment en place des processus qui se déclinent en pratiques et en activités. Le référentiel COBIT 5 détaille ces objectifs, ces processus, ces pratiques et ces activités. La figure 1 présente le modèle de référence COBIT 5.

Le référentiel COBIT 5 et plusieurs guides sont disponibles sur le site Web de l'ISACA.

Une partie prenante est toute personne qui détient une responsabilité ou qui a des attentes ou d'autres intérêts à l'égard de l'organisation, notamment les citoyens, les dirigeants, le personnel et les organismes de réglementation.

Figure 1 Modèle de référence COBIT 5



10 Le référentiel COBIT 5 établit une distinction claire entre la gouvernance et la gestion. Ces deux catégories englobent divers types d'activités, exigent différentes structures organisationnelles et répondent à divers besoins. Étant donné les responsabilités en matière de gouvernance (évaluer, diriger et surveiller), des interactions sont nécessaires entre les processus de gouvernance et de gestion afin d'obtenir un système de gouvernance efficace.

11 Il s'agit donc d'un modèle commun, compréhensible aussi bien par les premiers dirigeants responsables de l'exploitation des TI que par les gestionnaires des unités administratives, les auditeurs et les autres responsables des TI. Ce modèle comprend 37 processus qui sont regroupés en 2 grandes **catégories**, soit la gouvernance des TI et la gestion des TI, et cette dernière comporte 4 **sous-catégories** :

- Gouvernance des technologies de l'information : évaluation, direction et surveillance (5 processus) ;
- Gestion des technologies de l'information :
 - planifier : alignement, planification et organisation (13 processus) ;
 - créer : conception, acquisition et implantation (10 processus) ;
 - exécuter : livraison, service et soutien (6 processus) ;
 - surveiller : surveillance, évaluation et mesure (3 processus).

12 Un processus est défini comme un ensemble de pratiques qui sont influencées par les politiques et les procédures de l'organisation. Il reçoit des intrants (données, etc.) de différentes sources, y compris d'autres processus, les utilise et génère des extrants (produits, services, etc.) pour d'autres processus.

13 Comme le précise l'ISACA, le modèle proposé par le référentiel COBIT 5 est complet, mais il ne s'agit pas du seul modèle possible. Chaque organisation doit définir son propre ensemble de **processus** en tenant compte de sa situation.

14 Selon le référentiel, tous les processus doivent atteindre les objectifs qui y sont associés pour produire un ensemble de résultats permettant la réalisation des objectifs globaux liés aux TI. Toutefois, par souci de rentabilité et par respect des priorités, chaque entité décide du niveau d'exécution des processus et de la performance visée. Ce sont des choix légitimes, car chacune gère ses processus en fonction de sa situation, laquelle est déterminée par des facteurs internes et externes.

Plutôt que de parler de catégories et de sous-catégories, le référentiel COBIT 5 utilise les mots *fonction* (gouvernance et gestion) et *domaine* (planifier, créer, exécuter et surveiller).

À partir de maintenant, nous utilisons le mot *catégories* pour parler de catégories et de sous-catégories, afin d'alléger le texte.

Une entité peut organiser ses processus comme bon lui semble, pourvu que les objectifs de base en matière de gouvernance et de gestion des TI soient pris en compte.

2 Résultats de l'étude

15 Afin de brosser un portrait de la gouvernance et de la gestion des technologies de l'information au gouvernement du Québec, nous avons conçu un questionnaire en nous basant sur le référentiel COBIT 5.

16 L'étude que nous avons réalisée n'est pas un audit. Elle présente plutôt les résultats d'une autoévaluation effectuée par les répondants des entités sélectionnées, ce qui nous permet de dresser un portrait en matière de TI. Il est important de mentionner qu'une autoévaluation repose sur le jugement du répondant ; celle-ci risque donc d'être subjective.

17 Les objectifs poursuivis par l'étude sont les suivants :

- déterminer, à partir des résultats obtenus, les zones les plus vulnérables en matière de gouvernance et de gestion des TI au gouvernement du Québec ;
- permettre aux entités interrogées de se comparer ;
- orienter nos travaux d'audit de performance dans le secteur.

2.1 Méthodologie

18 Le référentiel COBIT 5 associe de 1 à 6 objectifs à atteindre à chacun des 37 processus figurant dans le modèle de référence. Nous avons donc conçu le **questionnaire** de manière à ce que les répondants puissent indiquer dans quelle mesure chacun de ces objectifs était atteint. Voici les choix de réponse qui étaient proposés :

- Jamais ou très rarement (0-15 % des situations) ;
- Rarement (> 15-50 % des situations) ;
- Souvent (> 50-85 % des situations) ;
- La plupart du temps ou toujours (> 85-100 % des situations) ;
- Ne sait pas ;
- Ne s'applique pas, car imparti à l'externe.

Le questionnaire en ligne, élaboré et géré en collaboration avec le CEFRIQ, a été transmis aux entités en octobre 2016.

19 Deux versions du questionnaire ont été élaborées. La version courte, qui s'adressait au plus haut dirigeant de l'entité, portait principalement sur les processus de gouvernance. L'autre version, plus détaillée, visait le premier dirigeant responsable des TI et traitait, en plus des processus de gouvernance, des processus de gestion des TI.

20 L'étude nous a permis de déterminer les zones pour lesquelles les entités peuvent être considérées comme plus vulnérables en matière de gouvernance et de gestion des TI. Pour chaque répondant, nous avons considéré qu'un processus était vulnérable sur la base du principe du maillon le plus faible, soit lorsqu'un des objectifs y étant liés n'était pas atteint. Cela est conforme aux orientations fournies par le référentiel COBIT 5. Un processus a donc été jugé vulnérable lorsque la réponse à l'une ou l'autre des questions associées à un objectif était « Jamais ou très rarement », « Rarement » ou « Ne sait pas ».

21 Aux fins de l'analyse des données et de la présentation d'un portrait global, nous avons ensuite calculé la fréquence des réponses ainsi obtenues afin de classer les processus selon leur degré de vulnérabilité. La méthodologie utilisée est détaillée à l'annexe 2.

Répondants

22 Les 44 entités sélectionnées sont des ministères (20), des organismes (19) et des **entreprises du gouvernement** (5). Nous avons retenu les entités pour lesquelles un minimum de 20 personnes (de l'interne et de l'externe) travaillaient dans le domaine des TI selon, notamment, le *Portrait de la main-d'œuvre en technologies de l'information de la fonction publique du Québec* réalisé par le SCT en date du 4 décembre 2015. Le tableau 1 présente le nombre de répondants et le taux de participation selon le type de répondants. La liste des entités est fournie à l'annexe 3.

Aux fins du présent rapport, nous utilisons la définition de l'expression *entreprises du gouvernement* qui est formulée dans la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

Tableau 1 Nombre de répondants et taux de participation

	Ministères		Organismes		Entreprises du gouvernement		Total	
	N ^{bre}	%	N ^{bre}	%	N ^{bre}	%	N ^{bre}	%
Hauts dirigeants	19	95	18	95	5	100	42	95
Premiers dirigeants responsables des TI	20	100	18	95	5	100	43	98

L'ETC est l'unité de mesure qui exprime le rapport entre la rémunération versée à une personne au cours d'un exercice et le traitement annuel correspondant à son classement.

Notons qu'il s'agit d'un portrait global et qu'une vulnérabilité ne touche pas toutes les entités. De plus, un processus vulnérable ne s'explique pas de la même façon et n'a pas le même impact pour chaque entité concernée. Il n'est donc pas approprié de conclure que toutes les entités qui ont participé à l'étude sont touchées par les enjeux qui y sont soulevés.

23 Globalement, il n'y a pas de différence observable entre les résultats portant sur les processus de gouvernance qui ont été obtenus pour les hauts dirigeants et ceux qui ont été compilés pour les premiers dirigeants responsables des TI. Les résultats présentés dans la section qui suit sont donc seulement ceux relatifs aux premiers dirigeants responsables des TI. Afin que les entités ayant répondu au questionnaire puissent se comparer, l'annexe 4 présente de manière globale, pour l'ensemble des organisations, la compilation des réponses brutes obtenues à chacune des questions. Chaque question portait sur un objectif lié à un processus.

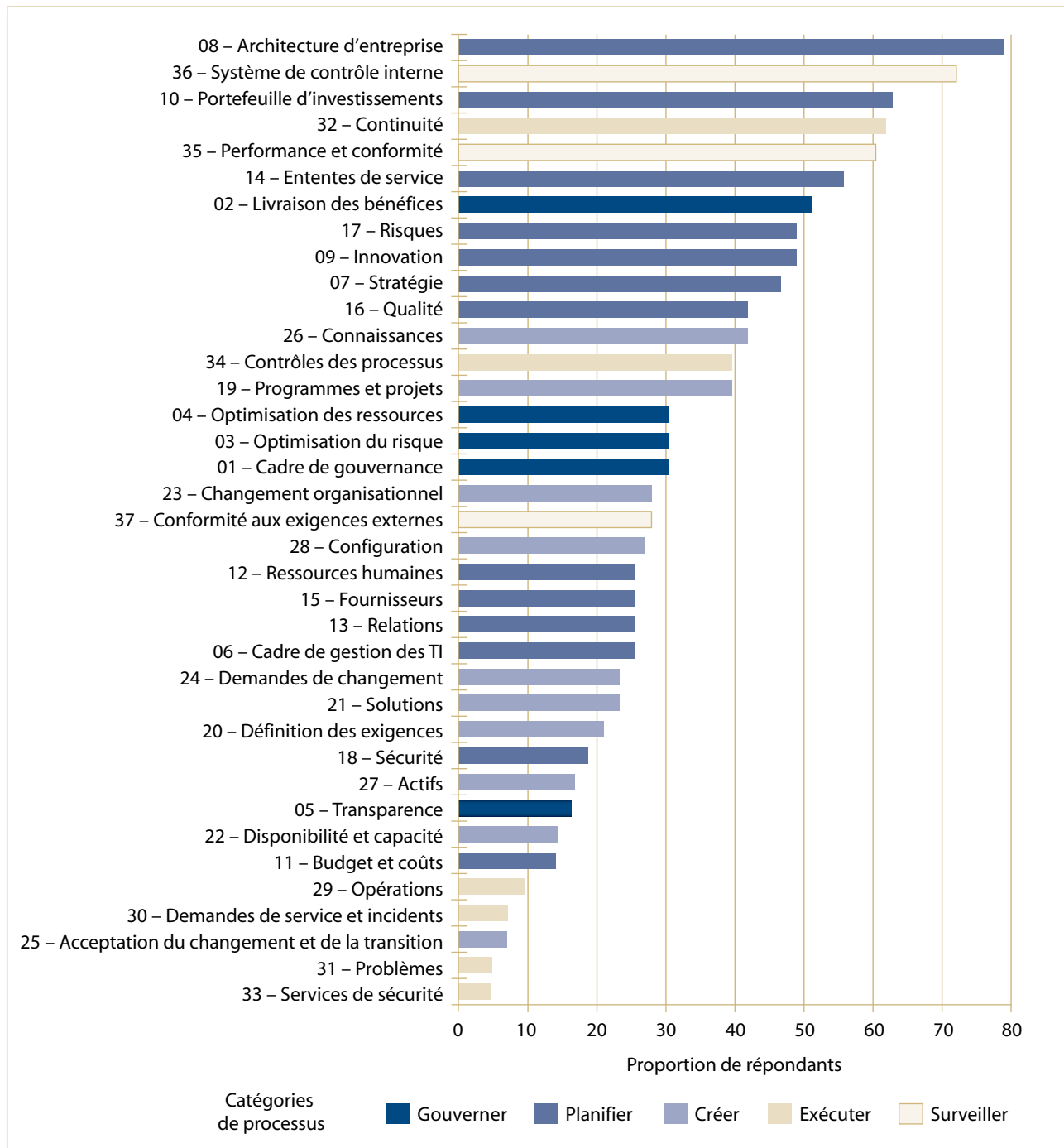
24 Il est à noter que nous avons également analysé les résultats de façon sommaire en fonction de l'importance du budget des entités et de leur nombre total d'équivalents temps complet (ETC). Aucune tendance observable n'est ressortie de cette analyse.

2.2 Analyse des résultats

25 Dans l'ensemble, les résultats montrent que la vulnérabilité se situe davantage sur le plan de la gouvernance, de la planification et de la surveillance que sur le plan des processus plus opérationnels, soit la création et l'exécution.

26 La figure 2 présente l'ensemble des processus en ordre décroissant de **vulnérabilité**, selon la proportion de répondants qui estiment qu'au moins un des objectifs liés à un processus n'est jamais, très rarement ou rarement atteint, ou qui ne le savent pas. Par exemple, la gestion du portefeuille d'investissements (processus n° 10) est un processus plus vulnérable : plus de 60 % des répondants considèrent qu'au moins un des objectifs qui y sont associés n'est pas atteint, alors que l'autre partie des répondants évalue que tous les objectifs liés à ce processus sont souvent, la plupart du temps ou toujours atteints.

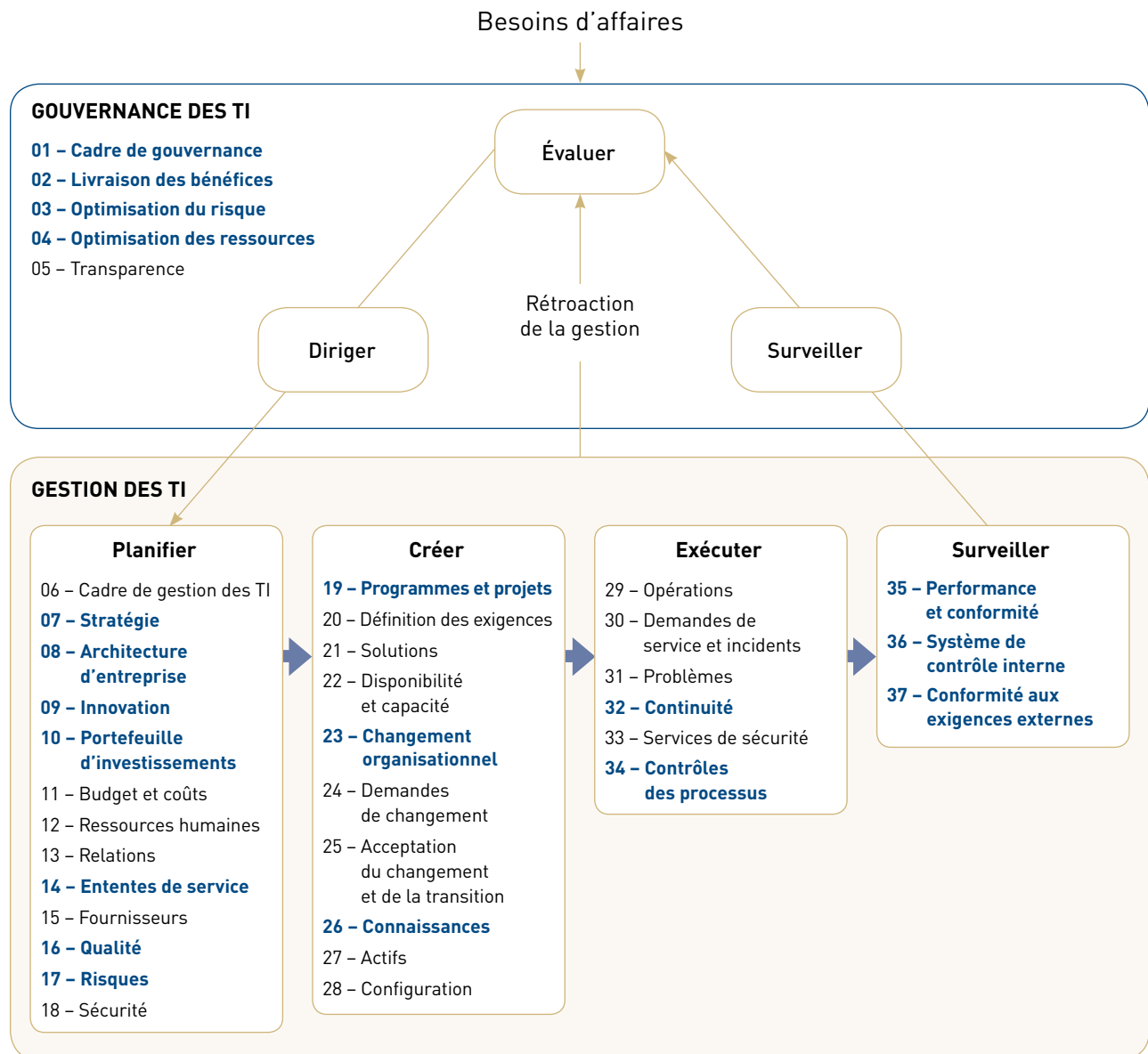
Figure 2 Ordre décroissant de vulnérabilité des processus¹ selon les réponses obtenues (en pourcentage²)



1. Le nom des processus, dans l'ensemble des figures du rapport ainsi que dans le texte, a été abrégé. De l'information plus détaillée sur les processus est présentée à l'annexe 4. Toutefois, il n'est pas possible de faire un rapprochement entre les résultats présentés dans la figure 2 et la compilation des réponses brutes obtenues au questionnaire géré par le CEFRIQ (annexe 4).
2. Il s'agit de la proportion de répondants qui estiment qu'au moins un des objectifs liés à un processus n'est jamais, très rarement ou rarement atteint, ou qui ne le savent pas.

27 La figure 3 situe les processus les plus vulnérables dans le modèle de référence COBIT 5. Aux fins de notre analyse, nous avons utilisé la médiane pour les déterminer. Ces processus sont mis en perspective par rapport à l'ensemble des 37 processus de gouvernance et de gestion des TI.

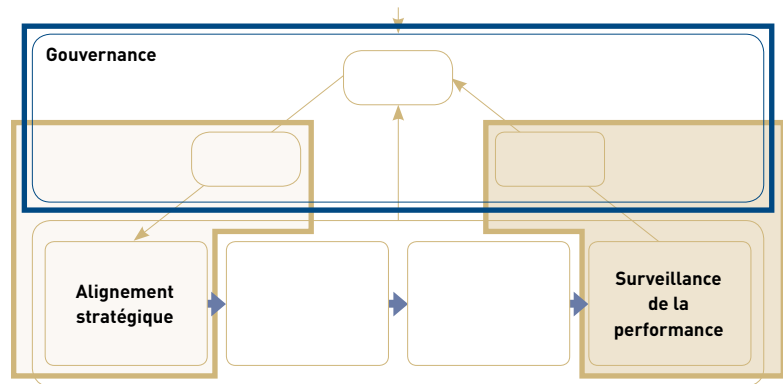
Figure 3 Processus les plus vulnérables présentés dans le modèle de référence COBIT 5



Processus les plus vulnérables

28 En fonction du nombre de processus les plus vulnérables par catégories, nous pouvons dégager trois zones de vulnérabilité :

- Gouvernance des TI (évaluer, diriger et surveiller). Les TI sont-elles optimisées et ajoutent-elles de la valeur à l'organisation ?
- Alignement stratégique des TI (diriger et planifier). Où devrions-nous investir en matière de TI et comment devrions-nous répartir les ressources ?
- Surveillance de la performance des TI (surveiller). Les processus de surveillance sont-ils efficaces et servent-ils à mesurer si les investissements et les actifs en TI permettent d'atteindre les objectifs fixés ?



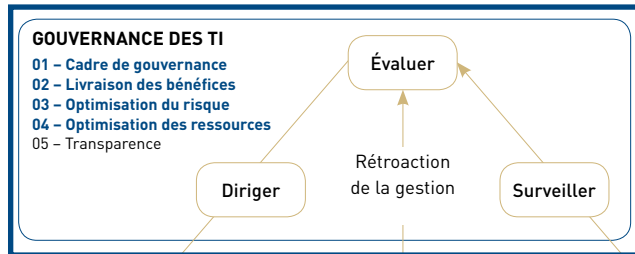
29 Les sous-sections qui suivent expliquent ces trois zones et leur impact potentiel sur les organisations.

Gouvernance des technologies de l'information

30 Selon le référentiel COBIT 5, le rôle des organisations est de créer de la valeur pour leurs parties prenantes. Cela signifie qu'elles doivent réaliser des bénéfices au meilleur coût, tout en optimisant la gestion des risques. Ces bénéfices peuvent prendre plusieurs formes. Pour les entreprises commerciales, ils peuvent être financiers, tandis que, pour la majorité des entités gouvernementales, ils peuvent se traduire par une meilleure prestation de services aux citoyens. Ainsi, la gouvernance des technologies de l'information consiste à évaluer les diverses options stratégiques, à diriger de même qu'à surveiller la performance et la conformité, et ce, dans le but de créer de la valeur.

31 Alors que les responsabilités relatives à la gouvernance des TI incombent à la haute direction et, s'il y a lieu, au conseil d'administration, celles liées à la planification, à la conception, à l'exécution de même qu'à la mise en place des mécanismes de surveillance des activités en matière de TI relèvent normalement de l'équipe de gestion des TI.

32 Les répondants ne sont pas certains que leur structure de gouvernance en matière de TI fonctionne efficacement, que les TI sont optimisées et qu'elles ajoutent de la valeur à leur organisation. Par ailleurs, ils n'ont pas la certitude que les risques critiques liés aux TI sont gérés de façon efficace et efficiente et que leur impact est connu. Ces résultats sont observés pour une plus grande proportion de ministères et d'organismes que d'entreprises du gouvernement.

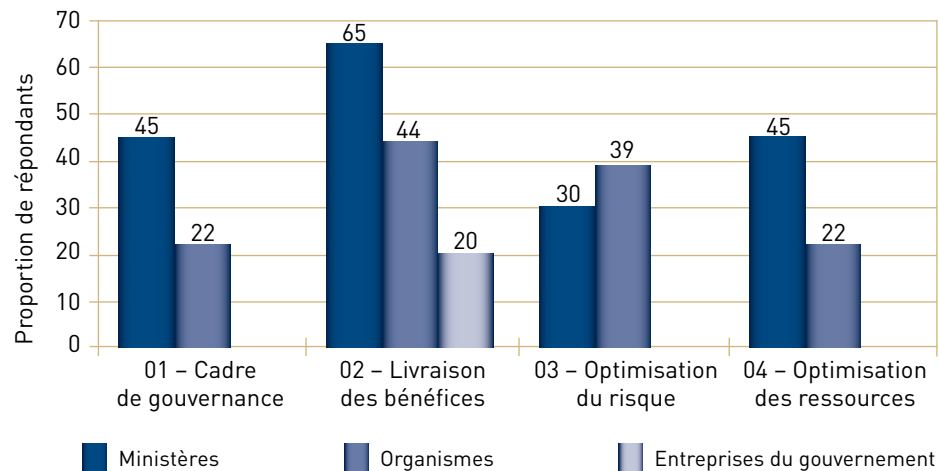


33 La première zone de vulnérabilité se compose de cinq processus, dont quatre sont considérés comme plus vulnérables.

34 La figure 4 présente les résultats liés aux processus de gouvernance les plus vulnérables selon le type d'entités. Par exemple, pour le processus n°2, 65% des ministères estiment qu'au moins un des objectifs relatifs à la livraison

des bénéfices (valeur ajoutée des TI) n'est jamais, très rarement ou rarement atteint, ou ils ne le savent pas. À l'inverse, 80% des entreprises du gouvernement sont d'avis que les objectifs liés à ce processus sont atteints dans la majorité des situations.

Figure 4 Processus les plus vulnérables en matière de gouvernance selon le type d'entités (en pourcentage¹)



1. Il s'agit de la proportion de répondants qui estiment qu'au moins un des objectifs liés à un processus n'est jamais, très rarement ou rarement atteint, ou qui ne le savent pas.

35 Une vulnérabilité en matière de gouvernance peut avoir un impact important sur l'organisation. Par exemple, une faible valeur ajoutée des TI (processus n°02) pour l'organisation peut limiter le potentiel de celle-ci de se renouveler, réduire sa capacité à atteindre ses objectifs et contribuer à maintenir des pratiques de gestion inefficaces. De plus, une sous-optimisation des ressources (processus n°04) peut être la cause de l'échec d'un projet en TI. En outre, s'il y a une sous-optimisation de la gestion des risques (processus n°03), des problèmes liés aux TI (brèches de sécurité, pannes de systèmes stratégiques, etc.) pourraient compromettre les objectifs stratégiques de l'organisation.

36 Des enjeux se posent à l'égard des processus considérés comme les plus vulnérables. Pour une meilleure gouvernance des TI, des questions devraient être formulées par la haute direction ou le conseil d'administration des entités ayant participé à l'étude. Voici des suggestions pouvant leur être utiles. Les processus sont présentés en ordre décroissant de vulnérabilité.

Processus	Questions
02 – Livraison des bénéfices	<ul style="list-style-type: none"> ■ Sommes-nous satisfaits de la valeur apportée par les TI par rapport aux coûts qu'elles génèrent? Avons-nous questionné les parties prenantes et le faisons-nous de façon régulière? ■ Comment nous assurons-nous que les investissements réalisés sont effectivement ceux qui sont planifiés et qu'ils apportent les bénéfices attendus? ■ Chaque initiative en TI (y compris les projets) franchit-elle toutes les étapes prévues, de la planification jusqu'au bilan?
01 – Cadre de gouvernance	<ul style="list-style-type: none"> ■ Comment nous assurons-nous que le fonctionnement du système de gouvernance des TI est efficace? Des évaluations indépendantes en matière de gouvernance des TI ont-elles été réalisées? ■ Comment traitons-nous du sujet de la gouvernance des TI? Toute l'information nécessaire est-elle produite et nous est-elle transmise en temps opportun?
04 – Optimisation des ressources (humaines, financières, matérielles)	<ul style="list-style-type: none"> ■ Comment nous assurons-nous que la façon de gérer les ressources permet de réduire les coûts et d'améliorer la prestation de services? Questionnons-nous les parties prenantes et ces dernières fournissent-elles une rétroaction? ■ Comment nous assurons-nous que les projets et les activités en TI sont peu à risque de rencontrer des problèmes de gestion des ressources? Nous assurons-nous que la planification des ressources tient compte de la situation de l'organisation? ■ Questionnons-nous le premier dirigeant responsable des TI sur la possibilité ou la pertinence de la réutilisation des TI? Nous assurons-nous que des évaluations sont réalisées?
03 – Optimisation du risque	<ul style="list-style-type: none"> ■ Connaissons-nous les risques liés aux TI et leur impact potentiel sur l'organisation? ■ Nous assurons-nous que les risques liés aux TI ne dépassent pas le seuil de tolérance au risque de l'organisation? ■ Comment nous assurons-nous que les projets tiennent compte des risques liés aux TI, que les plans d'action sont réalisés dans les délais et que les risques les plus critiques sont efficacement atténués?

Liens avec les autres processus

37 Les divers processus du référentiel sont liés et ils forment un cadre de gestion cohérent. Les extrants d'un processus deviennent les intrants d'autres processus. Ainsi, un processus vulnérable peut avoir un impact sur les processus qu'il alimente. Voici deux exemples :

- Optimisation des ressources (processus n°04). La haute direction ou le conseil d'administration d'une organisation doit préciser les principes directeurs concernant l'allocation des ressources et les stratégies privilégiées en matière d'approvisionnement. Les dirigeants doivent aussi donner leur accord sur la planification des ressources. Ces trois orientations sont des intrants pour le processus visant à définir la stratégie liée aux TI (processus n°07). Le manque d'orientations de la haute direction ou du conseil d'administration à cet égard nuira à l'alignement stratégique.
- Livraison des bénéfices (processus n°02). La haute direction ou le conseil d'administration doit spécifier les types d'investissements de même que les critères pondérés. Ces orientations guident le choix des investissements du portefeuille en TI (processus n°10). En l'absence d'orientations, ce choix pourrait ne pas être optimal, voire être remis en question par les parties prenantes.

Alignement stratégique des technologies de l'information

38 Une mauvaise gouvernance des TI peut nuire considérablement à une organisation, mais une bonne gouvernance ne peut pas, à elle seule, assurer le succès de celle-ci. Il est tout aussi important d'avoir un bon alignement stratégique des technologies de l'information.

39 L'alignement stratégique des TI a pour objectif d'harmoniser la stratégie de développement et de déploiement des TI avec la stratégie organisationnelle. Une organisation peut ainsi faire des choix technologiques judicieux qui lui permettront de tirer le maximum de bénéfices de ses investissements en TI et d'éviter que les retombées en la matière soient décevantes.

40 L'alignement stratégique des TI nécessite la connaissance des besoins de l'organisation ainsi que l'engagement des unités administratives, de la haute direction et, s'il y a lieu, du conseil d'administration. Le premier dirigeant responsable des TI s'assure de la réalisation de cet alignement.

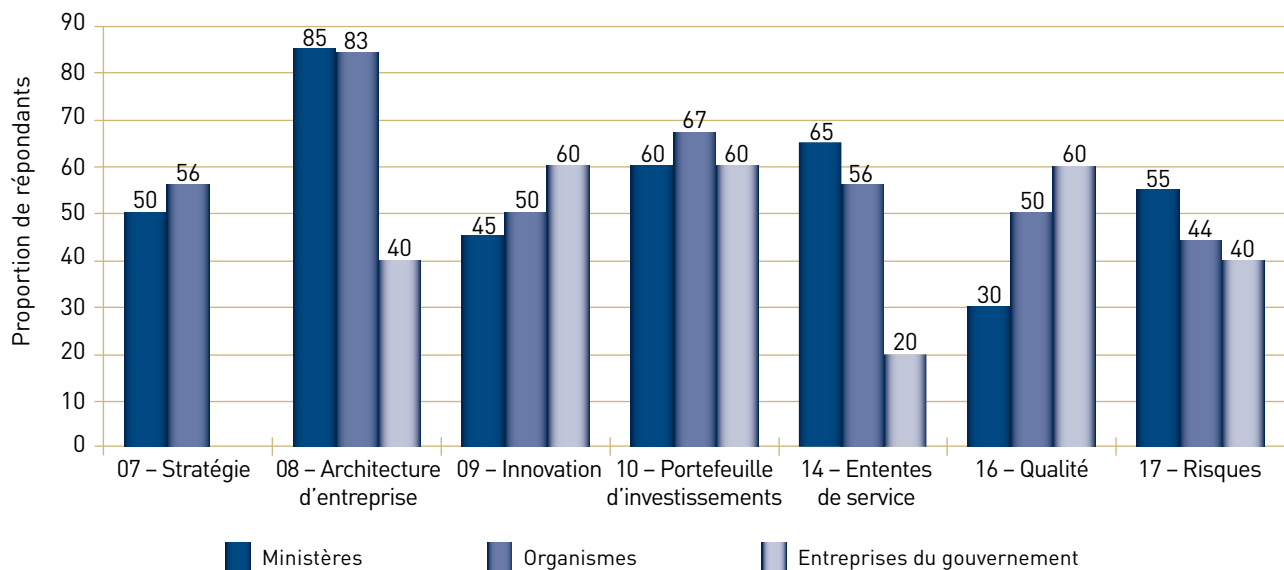
41 Plusieurs entités sont d'avis que les objectifs ne sont pas atteints pour les processus de planification, notamment ceux en lien avec l'alignement stratégique des TI. Malgré des efforts et des investissements parfois importants, elles ne semblent pas avoir attribué à quelqu'un de façon claire la responsabilité de la livraison de la stratégie liée aux TI. Elles ne semblent pas non plus disposer d'une architecture d'entreprise qui permet de soutenir efficacement l'organisation. D'autre part, elles estiment que la surveillance du portefeuille d'investissements n'est pas appropriée pour permettre d'obtenir les bénéfices attendus.

42 D'après les répondants, plus de la moitié des 13 processus de planification sont considérés comme plus vulnérables, dont plusieurs contribuent à l'alignement stratégique des TI.

43 La figure 5 présente les résultats relatifs aux processus de planification les plus vulnérables selon le type d'entités.



Figure 5 Processus les plus vulnérables en matière de planification selon le type d'entités (en pourcentage)¹



1. Il s'agit de la proportion de répondants qui estiment qu'au moins un des objectifs liés à un processus n'est jamais, très rarement ou rarement atteint, ou qui ne le savent pas.

L'architecture d'entreprise décrit l'état actuel d'une organisation selon différentes perspectives (processus d'affaires, information, applications, données, infra-structures). Cette connaissance est nécessaire pour aligner efficacement les TI sur les besoins de l'organisation.

44 Les résultats obtenus révèlent la vulnérabilité des processus qui permettent un alignement stratégique des TI, notamment la gestion de la stratégie, de l'architecture d'entreprise et du portefeuille d'investissements. Voici des raisons pour lesquelles ces processus sont importants :

- La gestion de la stratégie liée aux TI (processus n°07) permet d'avoir une vue d'ensemble actuelle de l'organisation et des TI, de définir des orientations en la matière et de proposer les actions nécessaires pour migrer vers l'environnement désiré. C'est un processus important, car il alimente plusieurs processus de gouvernance, de planification et de surveillance. De plus, la stratégie est elle-même alimentée par plusieurs processus. Par exemple, il est essentiel d'avoir une bonne **architecture d'entreprise** afin de disposer d'une compréhension adéquate de l'environnement actuel d'affaires et des TI, notamment en matière de processus d'affaires, d'information et d'applications.
- L'architecture d'entreprise (processus n°08) est utilisée pour prévoir les ressources et procéder aux modifications requises avant que les problèmes surviennent. Par exemple, elle sert à comprendre les processus, à déterminer où sont situés les goulots d'étranglement, à connaître les moments où il y a des temps d'attente, à préciser l'information nécessaire pour réaliser des activités ou encore à déterminer la nature et la puissance des technologies requises pour appuyer ces activités. L'architecture d'entreprise permet de soutenir efficacement une organisation.
- La gestion du portefeuille d'investissements (processus n°10) permet de faire les bons choix d'investissements en fonction notamment de la priorisation des dossiers d'affaires, des risques, des coûts, de la stratégie liée aux TI, de la situation actuelle de l'organisation et des sources de financement. Par la suite, il est important de surveiller la performance de ces investissements.

45 Des enjeux se posent à l'égard des processus considérés comme les plus vulnérables. Pour un meilleur alignement stratégique des TI, des questions devraient être formulées par la haute direction, le conseil d'administration ou le premier dirigeant responsable des TI des entités ayant participé à l'étude. Voici des suggestions pouvant leur être utiles. Les processus sont présentés en ordre décroissant de vulnérabilité.

Processus	Questions
08 – Architecture d'entreprise	<ul style="list-style-type: none"> ■ Possédons-nous une architecture d'entreprise ? Si oui, est-elle utilisée et permet-elle une réutilisation efficace des TI ? Autorisons-nous des exceptions aux normes et aux références d'architecture ? ■ Le personnel concerné travaillant dans le domaine des TI possède-t-il la connaissance de l'architecture, des outils et des méthodologies ? ■ Faisons-nous participer les parties prenantes, notamment à l'architecture des processus d'affaires ? Qu'en est-il lors d'un changement organisationnel ?
10 – Portefeuille d'investissements	<ul style="list-style-type: none"> ■ Avons-nous un système de surveillance approprié pour comparer les bénéfices obtenus à la suite des investissements réalisés avec les bénéfices attendus ? Ces bénéfices sont-ils mesurés ? Sont-ils comparés avec ce qui est prévu dans le dossier d'affaires ?
14 – Ententes de service	<ul style="list-style-type: none"> ■ Comment faisons-nous pour déterminer les attentes et le niveau de services requis au quotidien par l'organisation ? Est-ce consigné dans un document et connu ? ■ Comment évaluons-nous la satisfaction de la clientèle ? Est-elle en lien avec ce qui est attendu ?
09 – Innovation	<ul style="list-style-type: none"> ■ Encourageons-nous l'innovation dans l'organisation ? Cela fait-il partie de la culture organisationnelle ? ■ Comment l'innovation se traduit-elle chez le personnel ? Les attentes à l'égard du personnel sont-elles liées à des objectifs de performance en matière d'innovation ? ■ Les parties prenantes sont-elles consultées sur le niveau d'innovation (souhaité, perçu) ?
17 – Risques	<ul style="list-style-type: none"> ■ Existe-t-il un profil de risque à jour et complet en matière de TI ? Sinon, comment faisons-nous pour atténuer les risques ? ■ Comment nous assurons-nous que les processus d'affaires clés sont inclus dans le profil de risque ?
07 – Stratégie	<ul style="list-style-type: none"> ■ Qui est responsable de la livraison de la stratégie liée aux TI ? Des personnes précises ont-elles été désignées ? ■ Comment les résultats de la stratégie qui sont attendus se traduisent-ils chez le personnel ? Les avons-nous clairement indiqués dans les attentes en tant qu'objectifs de performance ? ■ Les mises à jour de la stratégie sont-elles communiquées aux personnes concernées ?
16 – Qualité	<ul style="list-style-type: none"> ■ Les processus liés aux TI font-ils l'objet d'au moins une exigence en termes de qualité ? Un rapport d'évaluation de la qualité est-il prévu ? ■ Établissons-nous, en collaboration avec les parties prenantes, des critères permettant d'évaluer l'atteinte des seuils de qualité ? Comment se traduisent-ils ?

Liens avec les autres processus

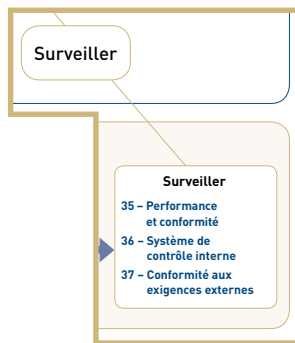
46 Certains de ces processus les plus vulnérables ont un impact sur les processus plus opérationnels, de même que sur la surveillance de la performance des TI et la gouvernance. Par exemple, le processus n°07 (gestion de la stratégie) et le processus n°16 (gestion de la qualité) alimentent la majorité des processus de gestion des TI, notamment la gestion des programmes et des projets (processus n°19). À l'inverse, le processus lié à la continuité (processus n°32), considéré comme plus vulnérable, alimente la stratégie (processus n°07).

Surveillance de la performance des technologies de l'information

47 La surveillance de la performance des technologies de l'information consiste à surveiller, à évaluer et à mesurer l'atteinte des résultats par rapport aux attentes et aux orientations de l'organisation, ainsi que l'application des bonnes pratiques. Elle vise plus particulièrement deux volets : le suivi global de la performance des TI et l'audit des mécanismes mis en place pour ce suivi.

48 Cette surveillance est une responsabilité conjointe de la haute direction, du premier dirigeant responsable des TI et, s'il y a lieu, du conseil d'administration.

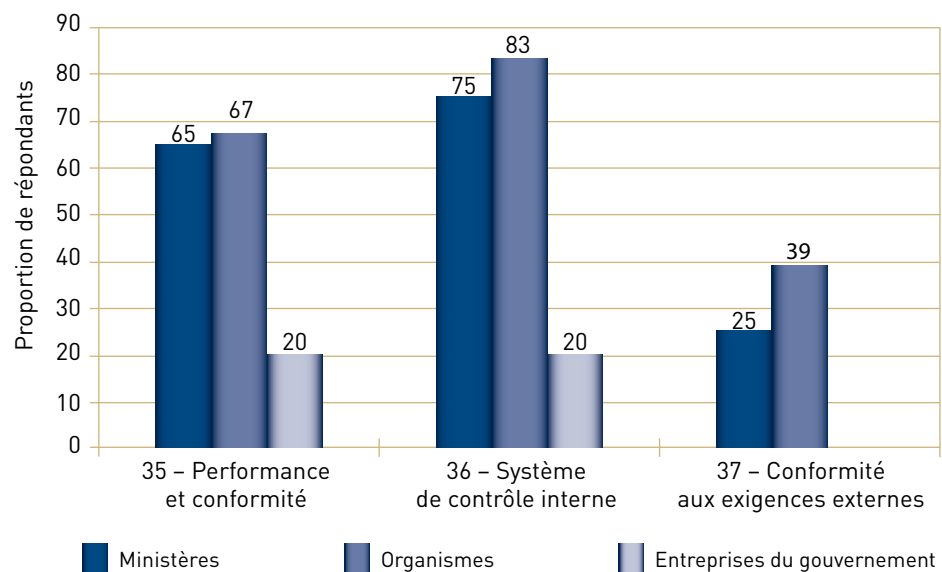
49 Les entités disent éprouver des difficultés en matière de surveillance de la performance des TI, plus particulièrement en ce qui concerne les audits permettant de s'assurer que les pratiques de surveillance fonctionnent efficacement. De plus, l'approche visant à surveiller, à évaluer et à informer ne semble pas efficace ni opérationnelle. Ces résultats sont observés pour une plus grande proportion de ministères et d'organismes que d'entreprises du gouvernement.



50 Pour la troisième zone de vulnérabilité, tous les processus qui la composent sont considérés comme plus vulnérables.

51 La figure 6 présente les résultats liés aux processus de surveillance de la performance selon le type d'entités.

Figure 6 Processus les plus vulnérables en matière de surveillance selon le type d'entités (en pourcentage¹)



1. Il s'agit de la proportion de répondants qui estiment qu'au moins un des objectifs liés à un processus n'est jamais, très rarement ou rarement atteint, ou qui ne le savent pas.

52 Des enjeux se posent à l'égard des processus considérés comme les plus vulnérables. Pour une meilleure surveillance de la performance des TI, des questions devraient être formulées par la haute direction, le conseil d'administration ou le premier dirigeant responsable des TI des entités ayant participé à l'étude. Voici des suggestions pouvant leur être utiles. Les processus sont présentés en ordre décroissant de vulnérabilité.

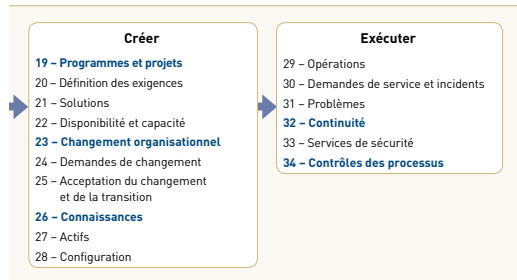
Processus	Questions
36 – Système de contrôle interne	<ul style="list-style-type: none">■ Avons-nous conçu un programme pour évaluer le système de contrôle interne relatif aux actifs en TI ? Ce programme tient-il compte de normes établies ? A-t-il été approuvé par la haute direction ?■ Comment vérifions-nous que le système de contrôle interne relatif aux actifs en TI est efficace et opérationnel ? Un avis indépendant a-t-il été demandé ?
35 – Performance et conformité	<ul style="list-style-type: none">■ Avons-nous mis en place un système de surveillance pour les TI ? Inclut-il des objectifs et des indicateurs approuvés ?■ Comment procédons-nous pour évaluer les processus liés aux TI et nous assurer qu'ils sont performants et conformes ? Avons-nous défini des objectifs et des indicateurs de mesure ?
37 – Conformité aux exigences externes	<ul style="list-style-type: none">■ Comment vérifions-nous que les exigences de conformité externes sont respectées ? Rencontrons-nous fréquemment des problèmes de conformité ? Comment sont-ils pris en charge et sont-ils résolus rapidement ?■ Avons-nous dressé un portrait des exigences de conformité externes ?

Liens avec les autres processus

53 Les processus de surveillance sont importants, car ils fournissent des intrants à la majorité des processus. En effet, ils permettent de produire en temps opportun l'information qui est requise par les décideurs afin d'optimiser, de réguler et d'améliorer de façon continue les autres processus. En l'absence de cette information, les décisions peuvent être fondées sur des données incomplètes, voire erronées. Dans ce contexte, il est difficile pour une organisation d'évaluer si les investissements et les actifs en TI permettent d'atteindre les objectifs qu'elle s'est fixés.

54 Une vulnérabilité importante à l'égard des processus de surveillance de la performance des TI signifie que des zones de faiblesse pourraient ne pas être détectées. Cela pourrait entraîner des difficultés liées au contrôle et à l'amélioration continue. Lorsqu'une organisation ne mesure pas ses résultats ou encore qu'elle n'est pas certaine que ce qui doit être mesuré l'est vraiment et que cela est effectué de la bonne manière, elle n'a pas l'assurance d'obtenir les résultats attendus. Cela peut avoir un impact direct sur la bonne gouvernance des TI ainsi que sur leur gestion. L'information obtenue et utilisée peut influencer sur la capacité de la haute direction ou du conseil d'administration à déterminer les orientations et les objectifs appropriés en matière de TI.

Autres résultats



55 Parmi les processus les plus vulnérables sur le plan opérationnel qui n'ont pas été abordés précédemment, mentionnons notamment la gestion de la continuité (processus n°32), la gestion des connaissances (processus n°26) et la gestion des programmes et des projets (processus n°19). Pour ce dernier processus, les résultats révèlent une vulnérabilité en ce qui concerne la suffisance des ressources pour la réalisation des activités prévues.

56 Par ailleurs, notons que les processus de gouvernance alimentent les processus de gestion, lesquels sont divisés en quatre catégories (planifier, créer, exécuter et surveiller), et que chacune d'elles alimente la catégorie suivante. Dans ce contexte, la vulnérabilité sur le plan de la gouvernance, de l'alignement stratégique et de la surveillance peut avoir une influence sur les processus plus opérationnels (créer et exécuter). Cela peut entraîner une mauvaise compréhension des défis qui se présentent sur le terrain et de leurs effets sur les priorités d'une entité. Il est possible de prévoir les besoins en TI, mais ceux-ci doivent être bien énoncés et faire partie d'une vision d'ensemble.

57 Pour illustrer la vulnérabilité en matière de TI et les conséquences qu'elle peut avoir sur les activités d'une entité, nous présentons à la page suivante un exemple concret, qui s'appuie sur un rapport d'audit produit par le Bureau du vérificateur général du Canada. Selon ce rapport, une entité avait notamment instauré un cadre de gestion des TI exhaustif en vue de renforcer sa gestion des investissements dans les TI. Cependant, les travaux d'audit ont démontré que des lacunes en matière de TI persistaient.

Lacunes	<p>Plusieurs lacunes ont été relevées lors de l'audit, notamment les suivantes :</p> <ul style="list-style-type: none">▪ l'absence d'une architecture d'entreprise ;▪ un portefeuille d'investissements partiel, car il n'inclut pas tous les projets de l'entité en matière de TI ;▪ le suivi du portefeuille d'investissements effectué en l'absence d'information importante (analyses de rentabilisation, évaluations des risques, plans détaillés des projets) ou à l'aide d'une information erronée (état d'avancement des projets, dates d'achèvement et demandes de modification) ;▪ l'approbation du démarrage des projets ou de la poursuite des travaux qui est obtenue même si les conditions préalables ne sont pas respectées ;▪ l'absence d'exigences liées aux TI ou la mauvaise définition de celles-ci ;▪ l'absence d'avantages mesurables avant le début de l'exécution des projets ;▪ l'absence d'un profil de risque global pour le portefeuille d'investissements dans les TI ;▪ l'information sur les projets présentée dans les tableaux de bord mensuels des projets et transmise à la haute direction (coûts, calendrier, portée des travaux) qui est incomplète et inexacte ;▪ l'absence de contrôles systématiques à l'égard de l'information communiquée à la haute direction au sujet des projets.
Conséquences	<p>Ces lacunes ont eu plusieurs conséquences, dont les suivantes :</p> <ul style="list-style-type: none">▪ L'entité a du mal à déterminer de manière intégrée l'ensemble des investissements nécessaires pour obtenir les résultats attendus à l'égard des besoins d'affaires.▪ Les systèmes informatiques se chevauchent et des solutions de rechange temporaires sont en place.▪ Les responsables ne peuvent démontrer que les projets concordent avec les orientations stratégiques, qu'ils répondent aux besoins opérationnels de l'entité et qu'ils ont le budget et les ressources nécessaires. Ces responsables ne peuvent pas non plus prouver qu'une fois mis en place, les projets répondent aux résultats attendus en termes d'économies prévues ou de coûts évités.▪ L'entité doit surmonter de nombreuses difficultés pendant l'étape de l'exécution des projets en raison du manque de clarté des exigences en matière de systèmes relatifs aux TI :<ul style="list-style-type: none">– dédoublement des efforts (systèmes semblables mis au point en parallèle) ;– aucune ventilation des coûts (entité qui n'est donc pas en mesure de dire quels travaux ont été reportés et à quel coût) ;– retards des projets (délais, coûts additionnels, risque d'inefficacité dans les opérations) ;– risque de ne pas obtenir les résultats attendus à l'égard des projets.▪ La haute direction ne dispose pas d'une vue d'ensemble fidèle et complète de l'état des projets, qui lui permettrait de prendre des décisions éclairées et de décider si un suivi plus rigoureux est nécessaire et si des mesures correctives s'imposent.

Source : Bureau du vérificateur général du Canada.

Conclusion

58 En résumé, les principaux éléments qui se dégagent de l'étude sont les suivants :

- La haute direction et les premiers dirigeants responsables des TI estiment ne pas avoir l'assurance que le système de gouvernance lié aux TI fonctionne efficacement.
- Les premiers dirigeants responsables des TI perçoivent des enjeux à l'égard des processus de planification, notamment ceux associés à l'alignement stratégique.
- Selon les premiers dirigeants responsables des TI, la surveillance de la performance des TI semble déficiente car, pour chacun des trois processus y étant associés, au moins un objectif n'est pas atteint.

59 Compte tenu des liens entre les processus et de l'influence qu'ont les catégories les unes sur les autres, il est difficile d'établir l'ordre d'importance des zones de vulnérabilité.

60 Les processus les plus vulnérables en matière de gouvernance des TI pourraient être l'une des causes de la vulnérabilité sur le plan de l'alignement stratégique. De plus, les déficiences en matière de surveillance des TI pourraient être responsables de la vulnérabilité sur le plan de la gouvernance.

61 L'encadrement gouvernemental mis en place au cours des dernières années au Québec a des effets limités pour le moment. Bien que la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* ait été adoptée en 2011 et que des outils aient été conçus par le SCT, nous observons, à la lumière de la présente étude, que des efforts additionnels semblent nécessaires pour orienter les entités. C'est d'ailleurs un des axes privilégiés dans la stratégie gouvernementale en TI, intitulée *Rénover l'État par les technologies de l'information*.

62 Cependant, les orientations et les directives gouvernementales communiquées par le SCT ne dégagent pas les entités de leurs responsabilités. Les dirigeants sont les premiers responsables de la gouvernance et de la gestion des TI dans leur organisation. Compte tenu du rôle de premier plan qu'ils jouent dans l'atteinte des objectifs, ils doivent trouver des solutions à l'égard des processus les plus vulnérables de leur organisation et participer à la mise en œuvre de celles-ci.

63 Les résultats de cette étude, qui n'est pas un audit, pourraient mener à la réalisation de travaux plus poussés afin de valider les possibles enjeux et d'investiguer en la matière. Comme il a été mentionné précédemment, les données accumulées nous permettront d'orienter nos travaux d'audit de performance dans le secteur des technologies de l'information.

Annexes et sigles

- Annexe 1** Dispositions de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*
- Annexe 2** Méthodologie
- Annexe 3** Entités sélectionnées
- Annexe 4** Fréquence des réponses obtenues pour chacun des objectifs

Sigles

ETC	Équivalent temps complet	SCT	Secrétariat du Conseil du trésor
ISACA	Information Systems Audit and Control Association	TI	Technologies de l'information

Annexe 1 Dispositions de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*

Objet et application de la loi

La loi établit un cadre et des règles de gouvernance et de gestion en matière de ressources informationnelles applicables aux organismes publics et aux entreprises du gouvernement. Le gouvernement a également le pouvoir, sur recommandation du Conseil du trésor, de soustraire un organisme public ou une entreprise du gouvernement à l'application de la loi.

Champ d'application

Voici un extrait des entités faisant partie du champ d'application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

Types d'entités	Définition	Extrait des entités assujetties à la loi
Organismes publics	<ul style="list-style-type: none"> ▪ Ministères ▪ Organismes budgétaires ▪ Organismes autres que budgétaires ▪ Autres organismes 	<ul style="list-style-type: none"> ▪ Ensemble des ministères ▪ Entités énumérées dans les annexes 1 et 2 de la <i>Loi sur l'administration financière</i>, sauf Revenu Québec ▪ Commission des normes, de l'équité, de la santé et de la sécurité du travail ▪ Conseil de gestion de l'assurance parentale, dans l'exercice de ses fonctions fiduciaires ▪ Retraite Québec ▪ Société de l'assurance automobile du Québec, dans l'exercice de ses fonctions fiduciaires ▪ Sûreté du Québec
Entreprises du gouvernement		<ul style="list-style-type: none"> ▪ Entités énumérées dans l'annexe 3 de la <i>Loi sur l'administration financière</i> ▪ Caisse de dépôt et placement du Québec ▪ Revenu Québec

Principales dispositions visant les organismes publics

Le gouvernement nomme, au sein du Secrétariat du Conseil du trésor, un dirigeant principal de l'information. Celui-ci a pour principales responsabilités de mettre en œuvre les politiques et les directives prises conformément à la loi, d'en surveiller l'application et d'en coordonner l'exécution.

Après avoir consulté le dirigeant principal de l'information, chaque sous-ministre ou dirigeant d'organisme public nomme un dirigeant sectoriel de l'information, lequel a pour principales fonctions d'assurer l'application des règles de gouvernance et de gestion établies en vertu de la loi, de voir à l'ensemble des activités en ressources informationnelles et de rendre des comptes au dirigeant principal de l'information à cet égard.

Dans les réseaux de l'éducation et de la santé et des services sociaux, un dirigeant réseau de l'information est nommé par le ministre responsable de chacun des secteurs. Les dirigeants réseau de l'information ont des fonctions semblables à celles assumées par les dirigeants sectoriels de l'information, mais ils doivent exercer leurs responsabilités auprès de plusieurs organismes (établissements de santé, commissions scolaires, etc.).

Le Conseil du trésor peut déterminer en outre les outils de gestion qu'un organisme public doit mettre en place aux fins de la gouvernance et de la gestion de ses ressources informationnelles, dont la planification triennale de ses projets et de ses activités en la matière et un bilan annuel de ses réalisations et des bénéfices réalisés.

Principales dispositions visant les entreprises du gouvernement

Les entreprises du gouvernement doivent adopter et rendre publique une politique qui tient compte, notamment, des objectifs énoncés dans la loi. Seul Revenu Québec doit communiquer au dirigeant principal de l'information des renseignements concernant l'ensemble de ses projets et de ses activités en ressources informationnelles.

Annexe 2 Méthodologie

Nos travaux ont été réalisés en collaboration avec le CEFRIQ, qui respecte les normes ISO en matière d'enquête effectuée sur le Web de même que les bonnes pratiques établies par l'Association de la recherche et de l'intelligence marketing (ARIM). Par ailleurs, nous avons été accompagnés par une consultante ayant une expertise et une expérience reconnues en matière de TI. Les travaux dont traite ce rapport ont été menés en vertu de la *Loi sur le vérificateur général* et conformément aux méthodes de travail en vigueur.

Questionnaire

Afin de valider les deux versions du questionnaire et notre démarche, nous avons réalisé un projet pilote en collaboration avec les deux types de répondants visés par notre étude. Leurs commentaires ont été pris en compte.

Chaque question portait sur un objectif lié à un processus et ne concernait que les activités internes associées aux TI dans les entités interrogées. Pour les activités confiées à une autre organisation, par exemple le Centre de services partagés du Québec, les entités pouvaient répondre « Ne s'applique pas, car imparti à l'externe ».

Il est important de souligner que notre étude ne visait pas à apprécier la qualité d'exécution de chacun des processus. Comme aucune vérification n'a été effectuée, nous n'avons pas l'assurance que l'atteinte des objectifs est bel et bien attribuable à une bonne exécution des processus.

Chaque répondant avait la possibilité de demander une copie de ses réponses afin qu'il puisse comparer ses résultats avec ceux des autres entités. À cette fin, l'annexe 4 présente globalement, pour l'ensemble des entités, la fréquence des réponses obtenues à chacune des questions.

Interprétation

Pour chaque répondant, nous avons considéré qu'un objectif n'était pas atteint lorsque la réponse obtenue à la question qui y était associée était « Jamais ou très rarement », « Rarement » ou « Ne sait pas ». Cette conception de la vulnérabilité est moins sévère que celle qui est proposée par le référentiel COBIT 5. En ce sens, nous avons exclu les réponses « Souvent » de notre analyse, alors que ce référentiel exclut seulement les réponses « La plupart du temps ou toujours ».

Les réponses « Ne s'applique pas, car imparti à l'externe » ont été exclues de notre analyse puisque les entités ne sont alors pas directement responsables de l'atteinte ou non de l'objectif concerné. Par contre, elles demeurent responsables de la gestion du fournisseur (processus n° 15).

Enfin, nous avons dégagé les principaux enjeux à l'égard des processus les plus vulnérables. Pour chaque processus, nous avons considéré les réponses obtenues à chacune des questions associées à un objectif pour trouver les principales raisons expliquant la vulnérabilité. Par exemple, pour le processus n° 07 (gérer la stratégie), 18 répondants ont indiqué que l'objectif n° 5 n'était pas atteint, ce qui est donc la principale cause de la vulnérabilité de ce processus.

Annexe 3 Entités sélectionnées

Ministères

Affaires municipales et Occupation du territoire	Forêts, Faune et Parcs
Agriculture, Pêcheries et Alimentation	Immigration, Diversité et Inclusion
Conseil exécutif	Justice
Culture et Communications	Relations internationales et Francophonie
Développement durable, Environnement et Lutte contre les changements climatiques	Santé et Services sociaux ¹
Économie, Science et Innovation	Secrétariat du Conseil du trésor
Éducation et Enseignement supérieur ¹	Sécurité publique
Énergie et Ressources naturelles	Tourisme
Famille	Transports, Mobilité durable et Électrification des transports
Finances	Travail, Emploi et Solidarité sociale

Organismes

Autorité des marchés financiers	La Financière agricole du Québec
Bibliothèque et Archives nationales du Québec	Office québécois de la langue française
Centre de services partagés du Québec	Régie de l'assurance maladie du Québec
Commission de la construction du Québec ²	Retraite Québec
Commission des normes, de l'équité, de la santé et de la sécurité du travail	Société de l'assurance automobile du Québec
Corporation d'urgences-santé	Société de télédiffusion du Québec (Télé-Québec)
Curateur public	Société d'habitation du Québec
Héma-Québec	Société québécoise des infrastructures
Institut de la statistique du Québec	Sûreté du Québec
	Tribunal administratif du travail

Entreprises du gouvernement

Hydro-Québec
Investissement Québec
Loto-Québec
Revenu Québec
Société des alcools du Québec

1. Les réseaux de l'éducation et de la santé et des services sociaux sont exclus de cette étude.

2. Cette entité est un organisme du gouvernement en vertu de la *Loi sur le vérificateur général*, mais elle n'est pas assujettie à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

Annexe 4 Fréquence des réponses obtenues pour chacun des objectifs

Nous présentons les sujets des questions qui ont été posées aux répondants ainsi que la fréquence des réponses obtenues pour chacun des objectifs. Voici l'ensemble des choix de réponse utilisés :

- J : Jamais ou très rarement (0-15 % des situations) ;
- R : Rarement (> 15-50 % des situations) ;
- S : Souvent (> 50-85 % des situations) ;
- T : La plupart du temps ou toujours (> 85-100 % des situations) ;
- NSP : Ne sait pas ;
- NA : Ne s'applique pas, car imparti à l'externe.

Mise en garde

Les données présentées dans l'annexe 4 sont la compilation des réponses brutes obtenues au questionnaire géré par le CEFRIQ. Elles ne permettent pas, à elles seules, d'arriver aux résultats présentés dans la figure 2, lesquels s'appuient sur une analyse des réponses fournies par chaque répondant. Rappelons que dès qu'un des objectifs liés à un processus n'est pas atteint, ce processus est considéré comme vulnérable.

La différence entre les données présentées dans la figure 2 et celles présentées dans cette annexe peut s'expliquer de la façon suivante :

- Une entité aurait pu mentionner que les trois objectifs liés à un processus donné ne sont jamais atteints, ce qui compte pour une entité dans la figure 2.
- Dans un autre cas, trois entités différentes auraient chacune pu indiquer qu'un de ces trois objectifs n'est jamais atteint, ce qui compte pour trois entités dans la figure 2.

Dans la figure 2, le calcul de la vulnérabilité s'effectue donc par entité et par processus. Toutefois, les données figurant dans les pages suivantes sont présentées par objectif, ce qui permettra aux entités de se comparer.

Objectifs	Nombre d'entités						Total
	J	R	S	T	NSP	NA	
Catégorie : Gouvernance des technologies de l'information (évaluation, direction et surveillance)							
01 – Assurer la définition et l'entretien d'un cadre de gouvernance							
1. Le modèle de prise de décision stratégique en matière de TI est efficace et aligné sur l'environnement interne et externe de l'organisation, et sur les exigences des parties prenantes.	1	5	20	17	-	-	43
2. Le système de gouvernance des TI est implanté.	1	3	19	20	-	-	43
3. L'assurance que le système de gouvernance pour les TI fonctionne efficacement est obtenue.	5	7	17	13	1	-	43
02 – Assurer la livraison des bénéfices							
1. L'organisation optimise la valeur de son portefeuille d'initiatives, de services et d'actifs en matière de TI.	1	8	22	12	-	-	43
2. Les pratiques de gestion de valeur sont efficaces.	2	12	10	18	1	-	43
3. Chaque investissement en TI génère une valeur optimale.	4	14	20	4	1	-	43
03 – Assurer l'optimisation du risque							
1. Les seuils de risque sont définis et communiqués, et les principaux risques liés aux TI sont connus.	1	5	15	22	-	-	43
2. L'organisation gère efficacement et avec efficience les risques critiques liés aux TI.	2	6	12	23	-	-	43
3. Les risques de l'organisation liés aux TI ne dépassent pas son seuil de tolérance et l'impact des risques sur la valeur de l'organisation est connu et géré.	-	9	16	17	1	-	43
04 – Assurer l'optimisation des ressources							
1. Les besoins en ressources sont comblés de façon optimale.	2	8	26	7	-	-	43
2. Les ressources sont allouées pour répondre au mieux aux priorités de l'organisation en respectant les contraintes budgétaires.	1	5	13	24	-	-	43
3. L'utilisation optimale des ressources est obtenue tout au long de leur cycle de vie.	2	7	24	10	-	-	43
05 – Assurer la transparence envers les parties prenantes							
1. Les rapports soumis sont conformes aux exigences des parties prenantes qui approuvent les objectifs, les indicateurs et les actions correctives nécessaires.	1	2	15	22	3	-	43
2. Les rapports sont précis, complets et livrés en temps opportun.	1	-	14	26	2	-	43
3. La communication est efficace et les parties prenantes qui approuvent les objectifs, les indicateurs et les actions correctives sont satisfaites.	-	1	21	19	2	-	43

Objectifs	Nombre d'entités						
	J	R	S	T	NSP	NA	Total
Catégorie : Planifier (alignement, planification et organisation)							
06 – Gérer le cadre de gestion des TI							
1. Un ensemble efficace de politiques est défini et maintenu.	1	7	24	11	-	-	43
2. Chacun connaît les politiques et la façon dont elles doivent être appliquées.	1	8	24	10	-	-	43
07 – Gérer la stratégie							
1. Tous les aspects de la stratégie TI sont alignés sur la stratégie organisationnelle.	-	5	15	23	-	-	43
2. La stratégie TI est rentable, appropriée, réaliste, réalisable, centrée sur l'organisation et équilibrée.	-	6	25	12	-	-	43
3. Des objectifs à court terme clairs et concrets peuvent découler d'initiatives à long terme et peuvent ensuite être traduits en plans opérationnels.	-	5	15	23	-	-	43
4. Les TI sont un générateur de valeur pour l'organisation.	1	6	15	21	-	-	43
5. Il y a une prise de conscience de la stratégie TI et une assignation claire de la responsabilité de sa livraison.	1	17	16	9	-	-	43
08 – Gérer l'architecture d'entreprise							
1. L'architecture et les normes soutiennent efficacement l'organisation.	4	16	16	7	-	-	43
2. Un portefeuille de services d'architecture d'entreprise soutient le changement de l'organisation.	10	16	9	8	-	-	43
3. Des architectures de domaine ou fédérées, appropriées et à jour, existent afin de fournir de l'information fiable sur l'architecture.	9	13	13	7	1	-	43
4. Un cadre et une méthodologie d'architecture d'entreprise, ainsi qu'un registre d'architecture intégré, sont utilisés pour permettre la réutilisation efficace dans l'organisation.	11	17	10	5	-	-	43
09 – Gérer l'innovation							
1. La valeur de l'organisation est créée grâce à la qualification et à l'utilisation des avancées et des innovations technologiques, des méthodes et des solutions les plus appropriées.	-	10	18	15	-	-	43
2. Les objectifs de l'organisation sont atteints avec davantage de qualité ou à coût moindre à la suite de l'identification et de la mise en œuvre de solutions innovantes.	1	6	21	15	-	-	43
3. L'innovation est encouragée et favorisée, et fait partie de la culture de l'organisation.	2	16	14	11	-	-	43

Objectifs	Nombre d'entités						Total
	J	R	S	T	NSP	NA	
10 – Gérer le portefeuille d'investissements							
1. Une combinaison appropriée d'investissements est définie et alignée sur la stratégie organisationnelle.	–	4	14	25	–	–	43
2. Les sources de financement des investissements sont identifiées et disponibles.	–	2	15	26	–	–	43
3. Les dossiers d'affaires sont évalués et priorisés avant que les fonds soient alloués.	2	4	3	34	–	–	43
4. Il existe une vue complète et précise de la performance du portefeuille d'investissements.	4	4	9	26	–	–	43
5. Les changements au programme d'investissements se reflètent dans les portefeuilles des services TI, des actifs et des ressources.	2	7	11	23	–	–	43
6. Une surveillance appropriée permet d'obtenir les bénéfices attendus.	7	19	6	11	–	–	43
11 – Gérer le budget et les coûts							
1. Un budget TI transparent et complet reflète fidèlement les dépenses prévues.	–	1	12	30	–	–	43
2. L'allocation des ressources pour les initiatives TI se base en priorité sur les besoins de l'organisation.	1	3	8	31	–	–	43
3. Les coûts des services TI sont répartis d'une manière équitable.	–	3	7	33	–	–	43
4. Les budgets peuvent être comparés avec précision aux coûts réels.	–	2	6	35	–	–	43
12 – Gérer les ressources humaines							
1. La structure organisationnelle en TI et les liens entre la direction des TI et les autres sont flexibles et réactifs.	–	7	17	19	–	–	43
2. Les ressources humaines sont gérées de manière efficace et efficiente.	1	7	15	20	–	–	43
13 – Gérer les relations							
1. Les stratégies, les plans et les exigences d'affaires sont bien compris, documentés et approuvés.	–	5	16	22	–	–	43
2. De bonnes relations existent entre les unités d'affaires et les TI.	–	3	23	17	–	–	43
3. Les parties prenantes d'affaires connaissent les opportunités amenées par les TI.	3	6	18	16	–	–	43
14 – Gérer les ententes de service							
1. L'organisation peut utiliser efficacement les services TI tels que définis dans un catalogue.	6	14	16	4	3	–	43
2. Les ententes de service reflètent les besoins de l'organisation et les capacités des TI.	7	8	19	7	2	–	43
3. Les services TI sont exécutés comme il est stipulé dans les ententes de service.	5	6	11	21	–	–	43

Objectifs	Nombre d'entités						Total
	J	R	S	T	NSP	NA	
15 – Gérer les fournisseurs							
1. Les fournisseurs effectuent ce qui a été convenu.	–	1	11	31	–	–	43
2. Les risques liés aux fournisseurs sont évalués et traités de façon adéquate.	–	9	10	24	–	–	43
3. Les relations avec les fournisseurs sont efficaces.	–	6	8	29	–	–	43
16 – Gérer la qualité							
1. Les parties prenantes sont satisfaites de la qualité des solutions et des services.	1	6	23	13	–	–	43
2. Les résultats des projets et des services livrés correspondent au niveau de qualité attendu.	–	5	23	15	–	–	43
3. Des exigences de qualité sont intégrées dans tous les processus.	2	15	18	8	–	–	43
17 – Gérer les risques							
1. Les risques TI sont définis, analysés, gérés et communiqués.	1	4	19	19	–	–	43
2. Il existe un profil de risque à jour et complet.	5	10	11	13	4	–	43
3. Toutes les actions majeures de gestion des risques sont gérées et sous contrôle.	2	8	15	18	–	–	43
4. Les actions de gestion des risques ont les impacts prévus lorsqu'elles sont exécutées.	2	6	15	20	–	–	43
18 – Gérer la sécurité							
1. Un système est en place qui tient compte des exigences de l'organisation en matière de sécurité de l'information et y répond efficacement.	–	3	9	31	–	–	43
2. Un plan de sécurité a été établi, accepté et communiqué dans toute l'organisation.	–	8	14	21	–	–	43
3. Des solutions de sécurité de l'information sont déployées et exploitées de manière uniforme dans toute l'organisation.	1	4	12	25	–	1	43
Catégorie : Créer (conception, acquisition et implantation)							
19 – Gérer les programmes et les projets							
1. Les parties prenantes concernées sont impliquées dans les programmes et les projets.	–	1	8	33	1	–	43
2. La portée et les résultats des programmes et des projets sont viables et alignés sur les objectifs.	–	5	7	31	–	–	43
3. Les programmes et les projets atteindront vraisemblablement les résultats attendus.	–	2	13	28	–	–	43
4. Les activités liées aux programmes et aux projets sont réalisées selon la planification.	–	4	17	22	–	–	43
5. Les ressources pour les programmes et les projets sont suffisantes pour réaliser les activités selon les plans.	–	12	20	11	–	–	43
6. Les bénéfices escomptés des programmes et des projets sont atteints et acceptés.	2	6	19	16	–	–	43

Objectifs	Nombre d'entités						Total
	J	R	S	T	NSP	NA	
20 – Gérer la définition des exigences							
1. Les exigences d'affaires fonctionnelles et techniques reflètent les attentes et les besoins de l'organisation.	1	3	22	17	-	-	43
2. Les solutions proposées satisfont les exigences d'affaires fonctionnelles, techniques et de conformité.	-	3	16	24	-	-	43
3. Le risque lié aux exigences est pris en charge dans les solutions proposées.	2	6	18	17	-	-	43
4. Les exigences et les solutions proposées respectent les objectifs des dossiers d'affaires (valeur attendue et coûts probables).	1	2	15	25	-	-	43
21 – Gérer l'identification et la conception des solutions							
1. Les cahiers des charges, incluant les éléments pertinents, répondent aux besoins de l'organisation, sont conformes aux normes et tiennent compte de tous les risques connus.	-	3	17	23	-	-	43
2. Les solutions sont conformes aux cahiers des charges et aux normes organisationnelles et intègrent les contrôles, la sécurité et les audits appropriés.	-	4	16	22	1	-	43
3. Les solutions sont d'une qualité acceptable et sont testées avec succès.	-	1	21	20	1	-	43
4. Les changements approuvés aux exigences sont correctement intégrés dans la solution.	-	1	16	24	2	-	43
5. Les activités d'entretien répondent avec succès aux besoins d'affaires et technologiques.	-	2	12	29	-	-	43
22 – Gérer la disponibilité et la capacité							
1. La planification de la disponibilité des environnements TI tient compte des exigences critiques des unités d'affaires en matière de capacité.	-	2	13	27	-	1	43
2. La capacité, la performance et la disponibilité rencontrent les exigences.	-	5	13	24	-	1	43
3. Les problèmes de disponibilité, de performance et de capacité sont signalés et systématiquement résolus.	-	2	7	33	-	1	43
23 – Gérer le changement organisationnel							
1. Le désir des parties prenantes pour le changement a été compris.	-	3	17	22	1	-	43
2. L'équipe de mise en œuvre est compétente et en mesure de conduire le changement.	-	5	15	21	2	-	43
3. Les parties prenantes comprennent et acceptent le changement souhaité.	-	5	20	16	2	-	43
4. Les parties prenantes sont habilitées à effectuer le changement.	-	6	17	19	1	-	43
5. Les parties prenantes sont en mesure d'exercer, d'utiliser et de maintenir le changement.	-	6	14	21	2	-	43
6. Le changement est intégré et soutenu.	-	5	24	13	1	-	43

Objectifs	Nombre d'entités						
	J	R	S	T	NSP	NA	Total
24 – Gérer les demandes de changement							
1. Les changements autorisés sont effectués au moment opportun et en minimisant les erreurs.	-	1	19	22	-	1	43
2. Les études d'impact révèlent l'effet du changement sur l'ensemble des composantes concernées.	1	4	16	22	-	-	43
3. L'ensemble des changements d'urgence est examiné et autorisé après le changement.	1	3	9	28	1	1	43
4. Les principales parties prenantes sont tenues informées de tous les aspects du changement.	-	6	21	16	-	-	43
25 – Gérer l'acceptation du changement et de la transition							
1. Les tests d'acceptation respectent l'approbation des parties prenantes et tiennent compte de tous les aspects des plans de conversion et de mise en œuvre.	-	2	8	33	-	-	43
2. Les versions sont prêtes à passer en mode production avec le soutien et la collaboration des parties prenantes.	-	2	8	33	-	-	43
3. Le passage en production des versions est effectué avec succès; les versions sont stables et conformes aux attentes.	-	-	15	28	-	-	43
4. Les leçons apprises contribuent aux futures livraisons.	-	1	18	24	-	-	43
26 – Gérer les connaissances							
1. Les sources d'information sont identifiées et classées.	-	16	19	7	1	-	43
2. Les connaissances sont utilisées et partagées.	-	13	18	11	1	-	43
3. Le partage des connaissances fait partie intégrante de la culture de l'organisation.	1	13	23	5	1	-	43
4. Les connaissances sont mises à jour et améliorées pour répondre aux exigences.	2	10	19	11	1	-	43
27 – Gérer les actifs TI (qui sont sous la gestion de l'organisation)							
1. Les licences sont conformes et alignées sur les besoins d'affaires.	-	2	6	33	-	2	43
2. Les actifs sont maintenus à un niveau optimal.	-	6	16	20	-	1	43
28 – Gérer la configuration (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. Le référentiel de configuration est exact, complet et à jour.	-	6	15	15	5	2	43

Objectifs	Nombre d'entités						Total
	J	R	S	T	NSP	NA	
Catégorie : Exécuter (livraison, service et soutien)							
29 – Gérer les opérations (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. Les activités opérationnelles sont exécutées comme prévu et planifiées.	-	1	16	25	-	1	43
2. Les opérations sont surveillées, mesurées, rapportées et restaurées.	-	4	12	26	-	1	43
30 – Gérer les demandes de service et les incidents (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. Les services soutenus par les TI sont disponibles pour leur utilisation.	-	1	5	36	-	1	43
2. Les incidents sont réglés selon les niveaux de services convenus.	-	-	9	33	-	1	43
3. Les demandes de service sont traitées conformément aux niveaux de services convenus et à la satisfaction des utilisateurs.	-	3	11	28	-	1	43
31 – Gérer les problèmes (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. Les problèmes liés aux TI sont résolus afin qu'ils ne se reproduisent pas.	-	2	14	26	-	1	43
32 – Gérer la continuité (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. L'information d'affaires critique est disponible conformément aux niveaux minimums de services requis.	-	-	7	34	-	2	43
2. Les services essentiels sont suffisamment robustes pour assurer la continuité des services.	1	2	10	28	-	2	43
3. L'efficacité du plan de continuité est vérifiée par des tests de continuité de services.	7	10	14	11	-	1	43
4. Un plan de continuité à jour reflète les exigences d'affaires actuelles.	8	5	13	16	-	1	43
5. Les intervenants internes et externes sont formés selon le plan de continuité.	9	8	13	10	2	1	43
33 – Gérer les services de sécurité (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. La sécurité des réseaux et des communications répond aux besoins d'affaires.	-	-	7	34	-	2	43
2. L'information traitée, stockée ou transmise par des dispositifs de points de terminaison (poste de travail, tablette, portable, etc.) est protégée.	-	2	10	29	-	2	43
3. Chaque utilisateur a un identifiant unique et détient des droits d'accès en fonction de son rôle dans son unité d'affaires.	-	-	6	36	-	1	43
4. Des mesures physiques ont été mises en place pour protéger l'information contre des accès non autorisés, des dommages et des interférences pendant son traitement, son stockage et sa transmission.	-	-	8	32	1	2	43
5. L'information électronique est correctement sécurisée pendant son stockage, sa transmission et sa destruction.	-	-	5	37	-	1	43

Objectifs	Nombre d'entités						Total
	J	R	S	T	NSP	NA	
34 – Gérer les contrôles des processus (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. La couverture et l'efficacité des contrôles clés pour répondre aux besoins de l'organisation en matière de traitement de l'information sont complètes.	1	6	12	17	7	–	43
2. L'inventaire des rôles, des responsabilités et des droits d'accès est aligné sur les besoins d'affaires autorisés.	–	4	16	23	–	–	43
3. Les transactions d'affaires sont entièrement conservées et journalisées lorsque cela est requis.	–	6	12	24	1	–	43
Catégorie : Surveiller (surveillance, évaluation et mesure)							
35 – Surveiller, évaluer et mesurer la performance et la conformité en TI							
1. Les objectifs et les indicateurs sont approuvés par les parties prenantes.	2	11	23	4	3	–	43
2. Les processus sont mesurés en fonction des objectifs et des indicateurs convenus.	3	14	17	6	3	–	43
3. L'approche de l'organisation pour surveiller, évaluer et informer est efficace et opérationnelle.	2	14	15	8	4	–	43
4. Les objectifs et les indicateurs sont intégrés dans les systèmes de surveillance de l'organisation.	2	18	14	5	4	–	43
5. La reddition de comptes portant sur la performance et la conformité est utile et produite en temps opportun.	3	11	16	10	3	–	43
36 – Surveiller, évaluer et mesurer le système de contrôle interne (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. Les processus, les ressources et l'information répondent aux exigences du système de contrôle interne de l'organisation.	2	6	17	9	9	–	43
2. Toutes les initiatives d'assurance sont planifiées et exécutées de façon efficace.	3	6	9	4	20	1	43
3. Valider de façon indépendante que le système de contrôle interne fourni est opérationnel et efficace.	6	8	13	7	8	1	43
4. Le contrôle interne est mis en place et les faiblesses sont identifiées et rapportées.	1	9	15	12	5	1	43
37 – Surveiller, évaluer et mesurer la conformité aux exigences externes (pour les actifs TI qui sont sous la gestion de l'organisation)							
1. Toutes les exigences de conformité externes sont identifiées.	3	3	15	18	4	–	43
2. Les exigences de conformité externes sont adéquatement prises en charge.	2	3	11	21	6	–	43