Pratique recommandée en sécurité de l'information

PR-066

Guide d'élaboration d'un tableau de bord de sécurité de l'information

Québec

Guide d’élaboration d’un tableau de bord de sécurité de l’information

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

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

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

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

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

Dépôt légal – 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71117-9

Table des matières

Remerciements

Le Sous-secrétariat du dirigeant principal de l'information remercie l'équipe de réalisation et le groupe de travail interministériel pour leur participation et le travail accompli.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Roza Lami, chargé de projet
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Daniel Guimont
Commission des lésions professionnelles

Dany Michaud
Commission de protection du territoire agricole du Québec

Claude Côté
Commission des transports du Québec

Daniel Carpentier
Contrôleur des finances

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

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

Jacques Blouin
Régie de l'assurance-maladie du Québec

Christian Marcotte
Société de l'assurance automobile du Québec

Daniel Landry
Sureté du Québec

Notes à l'intention du lecteur

Note 1 : Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document.

Note 2 : Le terme « organisme public » ou « organisme » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux.
[Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].

Note 3 : Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.

1. Introduction

La gestion axée sur les résultats fait partie des préoccupations des organisations souhaitant améliorer la qualité et la performance de leurs processus, activités ou services. Une telle gestion requiert l'établissement de mesures de performance à l'aide d'indicateurs regroupés dans des tableaux de bord afin de pouvoir apprécier l'atteinte des objectifs fixés et de prendre des décisions appuyées sur les résultats obtenus.

Conscient de la valeur ajoutée que peuvent apporter les tableaux de bord dans le cadre d'une démarche d'amélioration en sécurité de l'information, le dirigeant principal de l'information (DPI) met le présent guide à la disposition des organismes publics (OP) en vue de les appuyer dans le cadre de l'élaboration d'un tableau de suivi des réalisations en matière de sécurité de l'information, particulièrement celles liées aux obligations découlant de la directive sur la sécurité de l'information gouvernementale et de l'approche stratégique gouvernementale 2014-2017 en sécurité de l'information.

1.1 Contexte

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et entreprises du gouvernement (LRQ, chapitre G-1.03) précise, à l'alinéa 3) de l'article 10, que les organismes publics doivent « rendre compte au dirigeant principal de l'information de l'état d'avancement de même que des résultats des projets et des autres activités en matière de ressources informationnelles [...] ».

Par ailleurs, la Directive sur la sécurité de l'information gouvernementale précise, au paragraphe b) de l'article 7, que les organismes publics doivent déposer au DPI un bilan de sécurité de l'information.

Cette directive est appuyée par trois documents structurants :

- ✓ **L'Approche stratégique gouvernementale en sécurité de l'information 2014 – 2017**, qui définit la mission du gouvernement du Québec en matière de sécurité de l'information et détermine les éléments essentiels à la réalisation de la vision de l'encadrement de la sécurité de l'information gouvernementale. Elle fixe les cibles gouvernementales à atteindre en matière de sécurité de l'information pour les trois prochaines années et définit les indicateurs gouvernementaux de suivi du degré d'atteinte de ces cibles.
- ✓ **Le Cadre gouvernemental de gestion de la sécurité de l'information**, qui complète les dispositions de la directive sur la sécurité de l'information gouvernementale, en précisant l'organisation fonctionnelle de la sécurité de l'information dans l'Administration du Québec ainsi que les rôles et les responsabilités sur les plans gouvernemental et sectoriel.
- ✓ **Le Cadre de gestion des risques et des incidents à portée gouvernementale**, qui présente une approche novatrice de gestion des risques et des incidents susceptibles de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale.

1.2 But

Le présent guide vise à fournir des éléments d'aide (démarche, fiches descriptives d'indicateurs, etc.) à la construction d'un tableau de bord en matière de sécurité de l'information, pour assurer le suivi régulier du degré d'atteinte des cibles sectorielles découlant des cibles gouvernementales et pour évaluer la conformité aux obligations fixées par la Directive sur la sécurité de l'information gouvernementale.

1.3 Portée

Le présent guide :

- ✓ décrit les principaux concepts et définitions liés aux tableaux de bord;
- ✓ couvre l'ensemble des étapes nécessaires à l'élaboration et à la mise en œuvre d'un tableau de bord en sécurité de l'information, tout en mettant l'accent sur les étapes de sélection et de construction d'indicateurs;
- ✓ présente une grille synthèse d'indicateurs sectoriels concourant à l'atteinte des cibles gouvernementales;
- ✓ présente l'ensemble des fiches descriptives d'indicateurs sectoriels découlant des cibles gouvernementales ainsi qu'un exemple de tableau de bord illustrant cinq cibles parmi celles présentées dans les fiches descriptives.

1.4 Public cible

Le présent guide s'adresse principalement aux :

- ✓ détenteurs de l'information;
- ✓ principaux intervenants en sécurité de l'information (ROSI[1], COSI[2], COGI[3]);
- ✓ autres intervenants dans des domaines connexes à la sécurité de l'information (vérificateur interne, responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP), responsable de la gestion des technologies de l'information, responsable de la sécurité physique, responsable de la gestion documentaire, etc.).

1.5 Organisation du document

Outre la présente introduction, le document se décline en trois chapitres :

- ✓ Concepts et définitions, qui présente les principaux concepts et définitions liés aux tableaux de bord;
- ✓ Démarche de construction d'un tableau de bord en sécurité de l'information, qui présente l'ensemble des étapes nécessaires à l'élaboration et à la mise en œuvre d'un tableau de bord;

1. ROSI : Responsable organisationnel de la sécurité de l'information.
2. COSI : Conseiller organisationnel en sécurité de l'information.
3. COGI : Coordonnateur organisationnel de gestion des incidents.

- ✓ Résultat de l'application de la démarche - tableau de bord, qui présente une grille synthèse d'indicateurs sectoriels découlant d'indicateurs gouvernementaux en matière de sécurité de l'information et un exemple de tableau de bord.

2. Concepts et définitions

Le présent chapitre décrit brièvement les principaux concepts et définitions liés aux tableaux de bord de pilotage en général, avec un point focal sur la sécurité de l'information.

2.1 Mesure de performance

Définition

La mesure de performance est un processus continu de collecte de données, d'interprétation et de rapport concernant les aspects critiques des activités ou des interventions d'une personne, d'un groupe ou d'une organisation. Elle permet de suivre les activités et les processus et de vérifier si les résultats obtenus sont en lien avec ce qui était attendu. Elle vise notamment à documenter les progrès vers l'atteinte des objectifs préétablis[4].

Types de mesure de performance

Le NIST[5] définit trois types de mesure de performance : la mesure de mise en œuvre, la mesure d'efficacité et d'efficience, et la mesure d'impact.

- ✓ La mesure de mise en œuvre permet de suivre la progression de la mise en œuvre d'une action, d'un programme, d'une procédure ou d'une politique de sécurité de l'information (p. ex. « Le pourcentage des prestations de services électroniques utilisant le service d'authentification gouvernementale »).
- ✓ La mesure d'efficacité et d'efficience permet d'apprécier si la mise en œuvre d'une action ou d'un processus produit exactement les résultats attendus avec les moyens prévus (p. ex. « Le pourcentage des postes de travail pour lesquels les mises à jour de sécurité de l'information ont été déployées le mois dernier »).
- ✓ La mesure d'impact permet d'exprimer l'impact de la sécurité de l'information sur la mission de l'organisation (p. ex. « Le pourcentage de satisfaction des citoyens sur la protection de leurs données »).

4. Source : http://www.tresor.gouv.qc.ca/fileadmin/PDF/publications/glossaire_termes_usuels.pdf
5. *National Institute of Standards and Technology*

2.2 Indicateur de performance

Définition

Un indicateur de performance est une information ou une mesure permettant de juger des progrès accomplis en vue de l'atteinte d'un objectif. Un indicateur de performance peut être associé à un objectif opérationnel, organisationnel, ou lié à une intervention donnée. Il permet de mesurer le succès en matière d'efficacité, d'efficience ou de qualité[6].

Rôle d'un indicateur

Selon le contexte d'utilisation et l'objectif pour lequel il est choisi, un indicateur peut avoir plusieurs rôles. Il peut être utilisé :

- ✓ comme élément de suivi de la performance de la mise en œuvre des mesures de sécurité de l'information ou des plans d'action en sécurité de l'information;
- ✓ pour appuyer le processus de reddition de comptes de l'atteinte des cibles et objectifs gouvernementaux;
- ✓ pour justifier l'utilisation d'un budget additionnel ou d'un besoin en ressources complémentaires;
- ✓ pour soutenir les démarches d'amélioration du niveau de sécurité de l'information de l'organisme, notamment pour ce qui est de la gestion des risques et de la conformité aux normes et exigences en matière de sécurité de l'information.

Caractéristiques d'un indicateur

- ✓ Pertinent : Il doit répondre à un objectif ou à une préoccupation et permettre d'identifier simplement des problèmes pour lesquels des actions de prévention ou de correction existent.
- ✓ Précis : Il doit être précis dans sa définition, sa mesure et ses paramètres, et doit être compréhensible et compris de tous.
- ✓ Faisable : On doit pouvoir obtenir des données fiables à un coût raisonnable. Il doit être facile à élaborer et à calculer.
- ✓ Convivial : Sa mesure doit être accessible et son interprétation, facile pour l'utilisateur.

2.3 Axe de performance

Définition

Un axe de performance se rattache aux orientations stratégiques d'un organisme et présente l'axe de progrès que le gestionnaire désire suivre. Un axe de performance regroupe les indicateurs liés aux objectifs qui le sous-tendent. Ces regroupements favorisent la juste interprétation des résultats par l'auditoire concerné, soit les gestionnaires et les responsables de la sécurité de l'information (p. ex. le ROSI). Un exemple d'axe de performance serait de renforcer l'encadrement de la sécurité de l'information.

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

2.4 Tableau de bord

Définition

Un tableau de bord est un ensemble d'indicateurs de pilotage, construits de façon périodique, à l'intention d'un intervenant responsable, afin de guider ses décisions et ses actions en vue d'atteindre les objectifs de performance[7].

C'est un outil de mesure de la performance facilitant le pilotage proactif d'une ou de plusieurs activités, dans le cadre d'une démarche d'amélioration. Un tableau de bord se veut un outil d'aide à la décision.

Caractéristiques

- ✓ est constitué d'un certain nombre d'indicateurs essentiels et pertinents;
- ✓ met en évidence les résultats significatifs, les exceptions[8], les écarts et les tendances;
- ✓ fournit une vue cohérente en regroupant les indicateurs de façon parlante;
- ✓ présente les indicateurs de manière compréhensible, évocatrice et attrayante (visualisation facile)[9].

Note : Dans la suite du présent guide, l'expression « objectif de performance » est utilisée plutôt que l'expression « objectif de performance en sécurité de l'information », et ce, dans le but d'alléger le texte.

7. Source : http://gestionentreprisesofppt.blogspot.ca/2011/08/tableau-de-bord-et-reporting.html
8. Une situation d'exception peut-être, par exemple, un indicateur qui demeure inchangé au sein d'un axe de performance en pleine croissance ou encore un indicateur qui plonge subitement.
9 Source : JOBIN. La gestion axée sur les résultats : un levier pour une plus grande performance des établissements de santé, 2005.

3. Démarche de construction d'un tableau de bord en sécurité de l'information

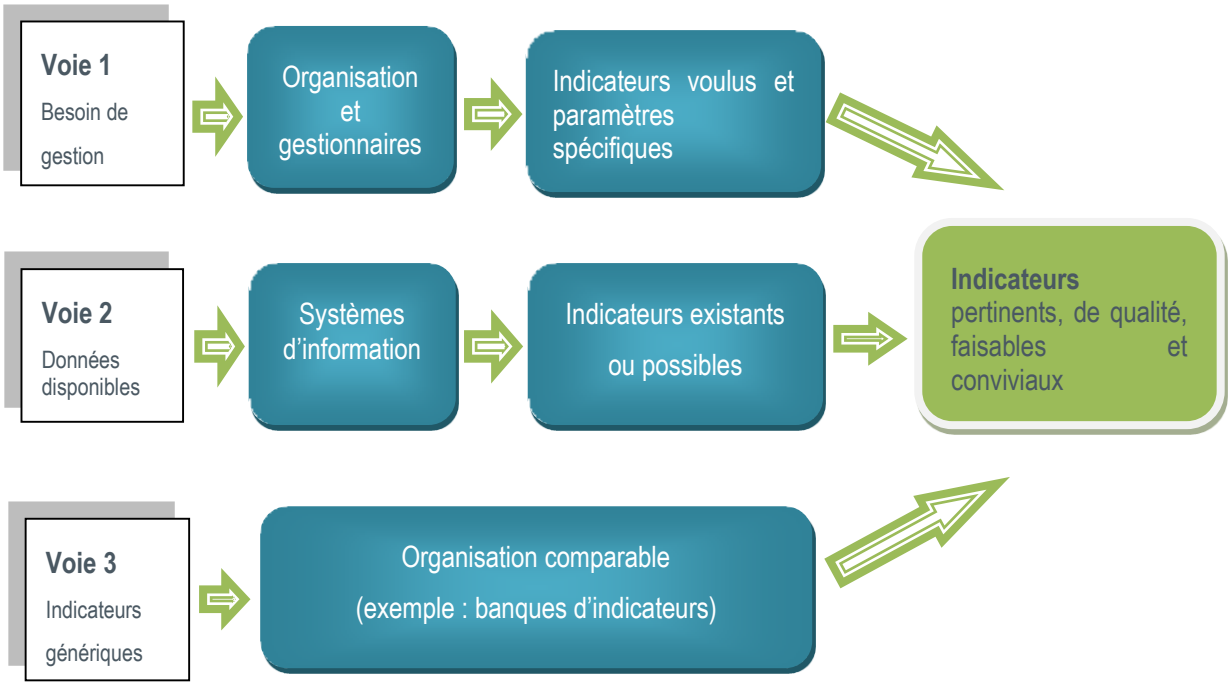
Le présent chapitre décrit une démarche de construction d'un tableau de bord en sécurité de l'information. Pour ce faire, il présente d'abord les voies de construction généralement empruntées pour élaborer les indicateurs. Il présente ensuite une vue d'ensemble des étapes de la démarche et, finalement, une description des activités qui les composent.

Il est à noter que la démarche tient compte des orientations et objectifs gouvernementaux définis dans l'approche stratégique gouvernementale 2014-2017 de sécurité de l'information et qu'elle se veut participative (nécessite l'apport de différents acteurs concernés par le tableau de bord)

Voies de construction d'indicateurs

Un tableau de bord se construit à partir d'indicateurs de performance. En général, comme l'illustre la figure 1, présentée ci-après, trois voies peuvent être empruntées pour élaborer des indicateurs.

Figure 1 : Voies de construction d'indicateurs de mesure[10]



Chacune des voies présente des avantages et des inconvénients, comme le décrit le tableau présenté ci-après.

Tableau 1 : Avantages et inconvénients des voies de construction d'indicateurs

10. Source d'inspiration : VOYER, Pierre. Tableau de bord de gestion et indicateurs de performance, 2e édition.

Voie	Avantage	Inconvénient
Voie 1 : Besoin de gestion	Les indicateurs sont cohérents par rapport aux objectifs de performance; Permet d'assurer la pertinence des indicateurs.	La formulation des objectifs de performance est assez exigeante et prend du temps; Exige de vérifier systématiquement la faisabilité.
Voie 2 : Données disponibles	Les indicateurs sont performants sur le plan technique[11] et sont faciles à produire, car ils reposent sur des données disponibles.	Cette voie, empruntée seule, risque de limiter le champ d'indicateurs aux seules données disponibles; Les indicateurs sont parfois peu pertinents.
Voie 3 : Indicateurs génériques	S'inspirer des listes d'indicateurs génériques; La construction des indicateurs est accélérée.	Les indicateurs ne suffisent pas toujours.

La démarche proposée dans le présent guide emprunte la voie 1. Toutefois, sans perdre de vue l'importance de prendre en compte les besoins d'affaires propres à l'organisme, il est possible de s'inspirer d'indicateurs préconçus et présentés à l'Annexe II, et ce, afin d'accélérer les travaux.

11. Le fait de produire les mesures des indicateurs construits à partir de la voie 2 est généralement performant, car ils reposent sur des données déjà produites par les systèmes d'information visés.

Vue d'ensemble de la démarche

La démarche préconisée se déroule en six étapes, présentées dans le tableau suivant.

Figure 2 : Élaboration d'un tableau de bord en sécurité de l'information (vue d'ensemble des étapes)

Étapes	Étape 1 Détermination des axes de performance	Étape 2 Détermination des points d'intervention	Étape 3 Définition des objectifs et des cibles en sécurité de l'information	Étape 4 Sélection et priorisation d'indicateurs	Étape 5 Construction d'indicateurs	Étape 6 Construction et exploitation du tableau de bord
Activités	Analyse du contexte	Identification des processus et activités	Identification des cibles et des objectifs gouvernementaux	Constitution d'une base d'indicateurs	Préparation des paramètres de définition d'indicateurs	Conception
	Identification des orientations stratégiques	Détermination des acteurs clés	Détermination des cibles et des objectifs sectoriels	Élaboration des critères de sélection et de priorisation	Préparation des paramètres de collecte, d'analyse et de calcul	Alimentation
	Sélection des axes de performance			Sélection et priorisation des indicateurs	Collecte des données et analyse des résultats	Mise à jour
					Représentation des indicateurs	

Les sections suivantes décrivent chacune des étapes

3.1 Étape 1 : Détermination des axes de performance

Les axes de performance se rattachent aux orientations de l'organisme en matière de sécurité de l'information et regroupent les indicateurs associés à ces dernières. Afin de faciliter le choix de ces axes, trois activités doivent être réalisées :

- ✓ Analyser le contexte;
- ✓ Identifier les orientations stratégiques gouvernementales et sectorielles en lien avec les besoins et les objectifs du tableau de bord;
- ✓ Sélectionner les axes de performance.

À la fin de cette étape, une liste d'axes de performance est produite.

3.1.1 Analyse du contexte

L'analyse du contexte vise à recueillir toute l'information pertinente et à en prendre connaissance, ce qui permettra de cerner les besoins, les attentes, les enjeux et les objectifs liés au tableau de bord ainsi que le niveau d'importance accordé à ce dernier. Pour ce faire, les questions suivantes sont appropriées :

- ✓ Qui sont les demandeurs?
- ✓ Quelles sont les utilisations prévues?
- ✓ Quels sont les objectifs du tableau de bord?
- ✓ A-t-on l'aval de la direction?
- ✓ Existe-t-il déjà des tableaux de bord en sécurité de l'information dans l'organisme public (OP)?

Les réponses obtenues précisent l'étendue et la portée du tableau de bord. Au terme de cette activité, une vision claire et partagée du tableau de bord doit être dégagée, en ce qui a trait aux besoins et aux objectifs liés à ce dernier.

3.1.2 Identification des orientations stratégiques

L'identification des orientations stratégiques en matière de sécurité de l'information permet non seulement d'assurer que les objectifs du tableau de bord sont en lien avec la mission, la vision et les enjeux de l'OP, mais, aussi, de faciliter la sélection des axes de performance. Pour ce faire, un exercice de rapprochement doit être fait entre les orientations gouvernementales, les orientations propres à l'OP ainsi que les besoins et les objectifs du tableau de bord.

3.1.4 Sélection des axes de performance

La sélection des axes de performance se fait sur la base de critères à élaborer. Ces derniers portent en général sur les attentes de la clientèle (citoyens, entreprises, utilisateurs, gestionnaires), l'évaluation des vulnérabilités en matière de sécurité de l'information et le niveau de maturité de l'OP. À titre indicatif, les critères présentés ci-après pourraient être considérés :

- ✓ l'impact sur les attentes de la clientèle;
- ✓ le degré d'atténuation des vulnérabilités de l'OP en matière de sécurité de l'information;
- ✓ l'impact organisationnel;
- ✓ la capacité[12] de l'OP à suivre l'axe de performance.

Une fois les critères déterminés, la sélection des axes de performance consiste à identifier, parmi les orientations stratégiques retenues au terme de l'activité précédente, celles qui répondent à ces critères.

3.2 Étape 2 : Détermination des points d'intervention

Les points d'intervention sont des processus, activités ou acteurs concernés au premier plan par le suivi des axes de performance choisis. Ils permettent de définir et d'affiner les objectifs de performance, en vue de favoriser l'efficience de la démarche d'amélioration. Afin de les déterminer, deux activités doivent être réalisées :

- ✓ identifier les processus et les activités de sécurité de l'information par axe de performance;
- ✓ désigner ou déterminer les acteurs clés.

À la fin de cette étape, une liste de processus, d'activités et d'acteurs est produite.

3.2.1 Identification des processus et des activités

Cette activité consiste à identifier tous les processus et activités (y compris ceux ou celles gérés par des partenaires) dont la performance conditionnera le suivi des axes de performance identifiés à l'étape précédente. Pour ce faire, il est possible de prendre appui sur une cartographie des processus et activités de gestion de la sécurité de l'information; à partir de celle-ci, il convient alors de vérifier, pour chacun des processus et activités, la possibilité d'obtenir de l'information pertinente pour le suivi des axes de performance retenus.

12. La capacité est liée à la maturité de l'OP. Par exemple, pour qu'un OP puisse suivre un axe de performance, les processus qui conditionnent l'amélioration de cet axe doivent être suffisamment matures (documentés, répétables, etc.).

À titre d'exemple :

Tableau 2 : Processus et activités par axe de performance

Axe de performance	Processus/activités
Atteindre un niveau de maturité adéquat en sécurité de l'information	✓ Gérer les incidents de sécurité de l'information ✓ Gérer les risques de sécurité de l'information
Renforcer l'encadrement de la sécurité de l'information	✓ Adopter une politique de sécurité de l'information ✓ Identifier les actifs critiques pour lesquels des mesures de contingence sont mises en place
Sensibiliser le personnel à la sécurité de l'information	✓ Sensibiliser et former le personnel en matière de sécurité de l'information

3.2.2 Détermination des acteurs clés

Cette activité consiste à désigner les acteurs pouvant décliner leur vision de la performance des processus et activités retenus précédemment. La participation active de ces derniers est essentielle à l'élaboration du tableau de bord et au suivi des réalisations en matière de sécurité de l'information.

3.3 Étape 3 : Définition des objectifs et des cibles en sécurité de l'information

À cette étape, il est question de définir les objectifs de sécurité de l'information en lien avec les axes de performance retenus et d'y associer des cibles à atteindre. Ce travail est effectué par les acteurs clés désignés à l'étape précédente. Deux activités doivent être réalisées :

- ✓ définir des objectifs en sécurité de l'information, par processus ou par activité;
- ✓ associer, à chaque objectif en sécurité de l'information, une ou plusieurs cibles à atteindre.

À la fin de cette étape, une liste d'objectifs et de cibles en sécurité de l'information par axe de performance est produite.

3.3.1 Identification des cibles et des objectifs gouvernementaux

Cette activité consiste à parcourir les cibles et les objectifs gouvernementaux et à retenir ceux qui sont en lien avec les activités et processus établis au terme de l'étape 2.

3.3.2 Détermination des cibles et des objectifs sectoriels

Dans le cadre de cette activité, l'OP doit déterminer les cibles et les objectifs sectoriels[13] en sécurité de l'information qui découlent des cibles et des objectifs gouvernementaux. Pour faciliter la réalisation de cette activité, de l'information sommaire est fournie dans la zone « CIBLE et SEUIL SECTORIELS » de chacune des fiches descriptives d'indicateurs fournies à l'Annexe II.

L'OP pourrait également définir ses propres objectifs et cibles en matière de sécurité de l'information. À cette fin, il pourrait prendre en compte :

- ✓ les orientations gouvernementales en matière de sécurité de l'information;
- ✓ le niveau de maturité de l'organisme;
- ✓ l'importance de la sécurité de l'information dans les activités de l'organisme;
- ✓ les aspects légaux, réglementaires et contractuels;
- ✓ les bénéfices prévus en matière de sécurité de l'information.

Les objectifs retenus en matière de sécurité de l'information doivent être précis, mesurables et cohérents par rapport aux axes de performance associés. À titre d'exemple, l'objectif sectoriel « Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information » pourrait découler de l'objectif gouvernemental « Taux d'OP ayant mis en œuvre un processus formel de gestion des risques de sécurité de l'information ».

3.4 Étape 4 : Sélection et priorisation des indicateurs

Cette étape consiste à déterminer les indicateurs, à partir des objectifs en sécurité de l'information définis à l'étape précédente, et à établir des priorités parmi les indicateurs possibles. Pour y parvenir, trois activités doivent être réalisées :

- ✓ constituer une base d'indicateurs;
- ✓ élaborer des critères de sélection et de priorisation;
- ✓ sélectionner les indicateurs et les mettre en ordre de priorité, sur la base des critères élaborés.

À la fin de cette étape, une liste d'indicateurs, classés par ordre de priorité, est produite.

3.4.1 Constitution d'une base d'indicateurs

Cette activité se subdivise en deux sous-activités : l'inventaire et l'analyse des indicateurs existants et la détermination des nouveaux indicateurs.

Inventaire et analyse des indicateurs existants

Afin de mettre à profit les efforts déjà consacrés à l'élaboration d'indicateurs (que ces derniers soient opérationnels ou non) et surtout de gagner en temps, il convient de faire un inventaire des indicateurs existants et de les analyser. L'analyse consiste à vérifier si l'objectif de l'indicateur est

13. Il est nécessaire de classer l'organisme selon sa taille et son degré d'exposition aux risques afin d'interpréter les cibles et objectifs sectoriels; Les critères de classement sont précisés dans le document « approche stratégique gouvernementale 2014–2017 en sécurité de l'information ».

en lien avec les objectifs en sécurité de l'information définis à l'étape précédente et à le retenir, le cas échéant.

Détermination des nouveaux indicateurs

À la suite de la sous-activité précédente, il convient de compléter la liste afin de constituer une base d'indicateurs complète. Pour ce faire, il est important de s'assurer que, pour chaque objectif, au moins un indicateur de mesure est déterminé.

3.4.2 Élaboration des critères de sélection

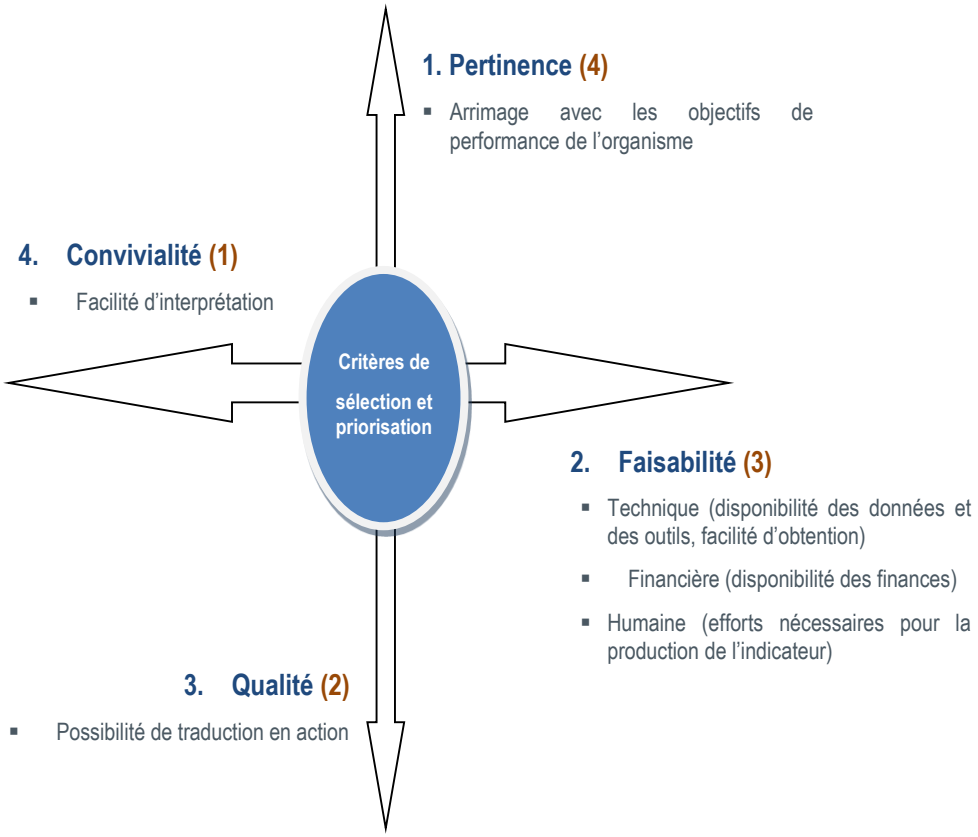
Les critères de sélection permettent de choisir, de façon objective, les indicateurs à retenir à partir de la base constituée. Il revient à chaque OP de déterminer ses propres critères de sélection et de priorisation. À titre d'exemple, les critères présentés ci-après pourraient être utilisés pour sélectionner les indicateurs et les mettre en ordre de priorité :

- ✓ **Pertinence** : L'indicateur doit répondre à un objectif;
- ✓ **Faisabilité** : On doit pouvoir calculer l'indicateur sans difficulté majeure;
- ✓ **Qualité** : L'indicateur doit permettre une prise de décision;
- ✓ **Convivialité** : L'indicateur doit être facile à interpréter.

3.4.3 Sélection et priorisation des indicateurs

La sélection des indicateurs consiste à choisir ceux qui répondent le mieux à l'ensemble des critères élaborés à l'activité précédente. À titre illustratif, une approche de sélection et de priorisation est présentée à la figure suivante.

Figure 3 : Critères de sélection et priorisation d'indicateurs[14]



Le chiffre qui se trouve entre parenthèses, à la suite de chaque critère, représente son poids. Chaque indicateur répondant à un critère se voit attribuer le poids de ce dernier. Le poids total de l'indicateur est obtenu en faisant la somme du poids de chaque critère auquel il répond. Les indicateurs ayant un poids supérieur ou égal à 7 sont sélectionnés et priorisés par ordre de grandeur de poids. Ainsi, ceux ayant un poids très élevé auront une priorité supérieure.

3.5 Étape 5 : Construction des indicateurs

Cette étape consiste à produire les indicateurs retenus et priorisés au terme de l'étape précédente. Pour ce faire, quatre activités doivent être réalisées :

- ✓ préparer les paramètres de définition d'indicateurs;
- ✓ préparer les paramètres de collecte et d'analyse des données ainsi que ceux du calcul des résultats;
- ✓ procéder à la collecte des données et analyser les résultats;
- ✓ représenter les indicateurs.

À la fin de cette étape, des indicateurs de performance sont représentés. Il est à noter que l'Annexe II présente des exemples d'indicateurs pouvant aider à la compréhension de la présente section.

14. Source d'inspiration : VOYER, Pierre. Tableau de bord de gestion et indicateurs de performance, 2e édition.

3.5.1 Préparation des paramètres de définition d'indicateurs

Les paramètres de définition d'indicateurs présentés dans le tableau suivant permettent de définir et de documenter ces derniers. Ces paramètres sont considérés comme des éléments d'entrée pour l'élaboration des fiches descriptives d'indicateurs; la valeur de ceux-ci est à déterminer pour chaque indicateur.

Tableau 3 : Paramètres de définition d'indicateurs

Paramètre	Description
Numéro	Permet d'identifier de manière unique l'indicateur (par exemple, «Ind 24 »).
Libellé	Appellation de l'indicateur (par exemple, « Nombre d'incidents de sécurité de l'information à portée gouvernementale identifiés au cours des six derniers mois »).
Objectif	Objectif précis de la mesure (par exemple, « réduire le nombre d'incidents de sécurité de l'information à portée gouvernementale »).
Cible	Cible visée par l'objectif lié à l'indicateur (par exemple, « 10 % de réduction des incidents de sécurité de l'information à portée gouvernementale par semestre »).
Responsable de production	Personne (morale ou physique) chargée de produire l'indicateur (par exemple, « le ROSI » ou « le COSI »).
Date de production	Date à laquelle l'indicateur a été produit.
Destinataires	Personnes (morales ou physiques) qui utiliseront l'indicateur (par exemple, « le ROSI », « le COSI » ou « le conseil d'administration »).

3.5.2 Préparation des paramètres de collecte, d'analyse et de calcul

Les paramètres de collecte et d'analyse des données ainsi que ceux du calcul des résultats sont des éléments d'information préalables à la production des indicateurs. Ils sont regroupés dans le tableau suivant.

Tableau 4 : Paramètres de collecte et d’analyse des données ainsi que ceux du calcul des résultats

Paramètre	Description
Mesure	Unité de mesure (par exemple, « pourcentage » ou « nombre »).
Type de mesure	Préciser si la mesure est de base ou dérivée (obtenue à partir de plusieurs mesures de base).
Élément de calcul	Variables nécessaires au calcul de l'indicateur.
Algorithme de calcul	Algorithme permettant de calculer l'indicateur, à partir des éléments de calcul.
Formule/pondération	Expression servant de base ou alors affectation d'une valeur à un élément de calcul, afin de calculer l'indicateur (par exemple, « nombre d'actifs critiques/nombre total d'actifs »).
Fréquence de collecte	Périodicité de la collecte des données (par exemple, « mensuelle », « annuelle », « bisannuelle », etc.).
Responsable d'alimentation	Personne (morale ou physique) chargée de procéder à la collecte des données (par exemple, « le service de support aux utilisateurs », etc.).

Méthode de collecte	Méthode qui sera utilisée pour procéder à la collecte des données nécessaires à la production de l'indicateur (par exemple, « manuelle » ou « automatique »).
Propriétaire des données	Personne (morale ou physique) qui détient les données dont on doit faire la collecte (par exemple, « le responsable de la gestion de risques », etc.).
Source de données	Source des données dont on doit faire la collecte (par exemple, « base de données », « rapports de gestion de risques », etc.).
Format d'illustration	Méthode d'illustration de l'indicateur (par exemple, « tableau », « graphique », etc.).
Règle d'interprétation	Comment interpréter l'indicateur pour assurer la compréhension uniforme des destinataires.

Ces paramètres doivent être établis pour chaque indicateur. Ils servent à compléter les fiches descriptives d'indicateurs. Il est à noter qu'un modèle de fiche d'indicateur est proposé à l'Annexe I et que des fiches décrivant les indicateurs sectoriels découlant des indicateurs gouvernementaux sont fournies à l'Annexe II. Ces fiches permettent d'apprécier, de manière uniforme, le niveau d'atteinte des cibles et objectifs gouvernementaux en matière de sécurité de l'information.

3.5.3 Collecte des données et analyse des résultats

Collecte des données et calcul des résultats

Il convient, au moment de réaliser cette activité, de confirmer que les conditions de collecte et de traitement prévues sont toujours en place[15], ce qui permettra d'assurer la stabilité et la reproductivité, au fil du temps, de l'information produite.

À titre indicatif, les ressources nécessaires à la collecte des données et au calcul des résultats se composent des éléments suivants :

- ✓ fiches d'indicateurs sur lesquelles on retrouve de l'information telle que la méthode de collecte, la fréquence de collecte, etc.;
- ✓ outils d'enregistrement et d'analyse des données tels que des fiches d'entrevues, des chiffriers, des bases de données, etc.;
- ✓ infrastructures qui serviront à produire des données, telles que des ordinateurs, des routeurs, des pare-feu, etc.;
- ✓ ressources à partir desquelles les données seront extraites, telles que les bases de données, les services, etc.

On doit procéder à la collecte des données nécessaires au calcul de chaque indicateur, les intégrer à un outil (par exemple, un chiffrier) et effecteur les calculs à partir de ces données.

Analyse des résultats

Cette sous-activité consiste à faire une comparaison entre les résultats obtenus et les cibles fixées, en vue d'identifier les écarts.

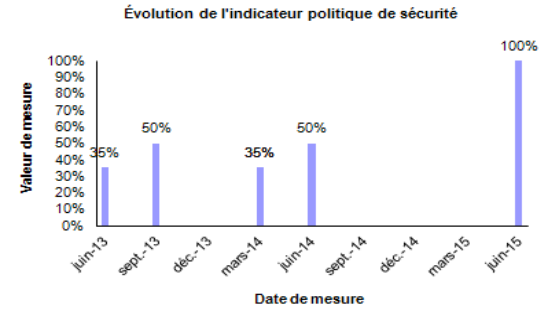
3.5.4 Représentation des indicateurs

Cette activité consiste à extraire et à utiliser l'information nécessaire à la représentation de chaque indicateur, conformément au format précisé dans sa fiche descriptive. Cette information se limite souvent au nom de l'indicateur, à sa mesure et à la cible associée. Cependant, on peut, au besoin, ajouter d'autres éléments d'information pertinents, comme la date de production, l'objectif, l'écart, etc. Il est approprié de conserver une représentation légère de l'indicateur, afin de faciliter sa consultation. À titre indicatif, la figure suivante décrit une structure type de présentation d'un indicateur.

Tableau 5 : Exemple de structure de présentation d'un indicateur

15. Par exemple, il est possible qu'un serveur de fichiers journaux (log files) prévu comme source de données lors de la sélection et de la priorisation des indicateurs soit indisponible lors de la collecte de données.

Libellé de l'indicateur		
Éléments de calcul	**Choix/Réponse**	**Valeur (%)**
Élément de calcul 1	Oui	35 %
Élément de calcul 2	Oui	15 %
…	Non	0 %
…		
Élément de calcul n		
Mesure	50 %	
Cible	100 %	



Interprétation	

3.6 Étape 6 : Construction et exploitation du tableau de bord

À la suite de l'élaboration des indicateurs retenus, la dernière étape consiste à réaliser et à mettre en œuvre le tableau de bord. Pour y parvenir, trois activités doivent être exécutées :

- ✓ concevoir le tableau de bord;
- ✓ alimenter le tableau de bord;
- ✓ mettre à jour le tableau de bord.

À la fin de cette étape, un tableau de bord à jour est produit.

3.6.1 Conception du tableau de bord

Cette activité consiste à concevoir un tableau de bord et à y intégrer les indicateurs nécessaires. Pour ce faire, il faudra tenir compte des grands principes visuels, ergonomiques et analytiques tels que :

- ✓ la navigation (entre les indicateurs et à l'intérieur d'un indicateur);
- ✓ le choix des couleurs, de manière à faciliter la lecture;
- ✓ la disposition des éléments (axe de performance, indicateurs, boutons d'action, infobulles, etc.), de manière à faciliter l'analyse et la compréhension de la performance des axes choisis.

La conception pourrait se faire progressivement, afin d'intégrer au fur et à mesure certaines préférences (couleurs, dispositions, etc.) du destinataire. Il est important que la version finale du tableau de bord soit validée par ce dernier.

L'agencement des indicateurs dans le tableau de bord devra également être effectué en tenant compte de la structure logique de navigation. À titre indicatif, il peut être intéressant de prévoir une page par indicateur, dans laquelle on retrouvera toute l'information (identification, cible, seuil, éléments de calcul, etc.) associée, et une page de synthèse, qui présentera uniquement l'illustration des indicateurs associés à un ou plusieurs axes de performance.

3.6.2 Alimentation

L'alimentation du tableau de bord consiste à produire de nouvelles valeurs des indicateurs qui le composent. Elle doit se faire selon les périodes définies dans les fiches descriptives ou à la demande du gestionnaire visé. À cette fin, l'OP aura besoin d'outils tels que :

- ✓ les fiches d'indicateurs dans lesquelles on trouve l'information utile au calcul des nouvelles valeurs (source de données, méthode de collecte, etc.);
- ✓ le matériel informatique (ordinateur, logiciel, etc.).

3.6.3 Mise à jour

La mise à jour du tableau de bord doit se faire sur une base régulière ou à la suite d'un changement majeur pouvant remettre en question l'exactitude de l'information qui s'y trouve. La mise à jour consiste à revoir la structure du tableau de bord, afin de s'assurer que les objectifs en matière de sécurité de l'information pour lesquels il a été réalisé sont toujours d'actualité. Parmi les événements pouvant nécessiter la mise à jour d'un tableau de bord, citons, à titre d'exemple :

- ✓ une évolution du contexte, des besoins ou des objectifs de sécurité de l'information;

- ✓ un constat d'inefficacité d'un indicateur, c'est-à-dire qu'il ne reflète pas la réalité qu'il est supposé mesurer ou que son résultat, quel qu'il soit, ne permet pas de prendre une décision;
- ✓ une inadéquation des indicateurs par rapport aux objectifs de sécurité de l'information, c'est-à-dire qu'ils ne contribuent pas à leur mesure;
- ✓ un changement organisationnel (responsables, structures, etc.);

Outre les changements majeurs nécessitant la mise à jour d'un tableau de bord, il est conseillé d'en faire une revue selon une périodicité définie. À cette fin, il revient à chaque OP de définir cette périodicité en fonction de ses objectifs en matière de sécurité de l'information. Par exemple, une révision aux deux ans pourrait être envisagée afin de vérifier la pertinence des indicateurs déjà existants et la nécessité d'introduire de nouveaux indicateurs pour mieux répondre aux besoins des gestionnaires.

4. Résultat de l'application de la démarche - tableau de bord

Le chapitre 4 a pour objectif de présenter un exemple de tableau de bord (outil) réalisé à la suite de l'application de la démarche décrite au chapitre précédent. Pour y parvenir, il présente d'abord une grille synthèse des indicateurs sectoriels concourant à l'atteinte des cibles gouvernementales. Il décrit ensuite l'exemple d'outil, en présentant ses fonctionnalités et ses modalités d'utilisation.

4.1 Grille de suivi des cibles gouvernementales

Cette section présente une grille synthèse d'indicateurs sectoriels concourant à l'atteinte des cibles gouvernementales définies dans l'approche stratégique gouvernementale 2014-2017. La grille présentée ci-après vise à fournir à un OP l'information permettant une compréhension rapide des attentes gouvernementales par rapport à ses cibles.

Tableau 6 : Grille d'indicateurs sectoriels de suivi des cibles gouvernementales

Orientation 1 : Renforcer l'encadrement de la sécurité de l'information

Objectif 1.1 : Gérer efficacement la sécurité de l'information gouvernementale

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'OP ayant adopté une politique et un cadre de gestion de la sécurité de l'information	100 % des OP d'ici le 31 mars 2015	Degré de conformité à l'obligation portant sur la politique de sécurité de l'information (Ind1a)	Un OP est conforme à l'obligation portant sur la politique de sécurité de l'information si sa politique en matière de sécurité de l'information est : ✓ élaborée et mise en œuvre et qu'elle a été adoptée il y a moins de 3 ans; ✓ dans le cas où elle a été adoptée il y a plus de 3 ans, elle doit être réévaluée et révisée au besoin.
		Degré de conformité à l'obligation portant sur le cadre de gestion de la sécurité de l'information (Ind1b)	Un OP est conforme à l'obligation portant sur le cadre de gestion de la sécurité de l'information (SI) si son cadre de gestion de la SI est : ✓ élaboré et mis en œuvre et qu'il a été adopté il y a moins de 3 ans; ✓ dans le cas où il a été adopté il y a plus de 3 ans, il doit être réévalué et révisé au besoin.
Taux d'OP ayant désigné leurs principaux intervenants en sécurité de l'information (ROSI, COGI)	100 % des OP d'ici le 31 mars 2015	Degré de conformité à l'obligation portant sur la désignation d'un ROSI (Ind2a)	Un OP est conforme à l'obligation portant sur la désignation d'un ROSI : ✓ s'il a désigné un ROSI qui est un employé régulier de l'organisme et qui appartient à la classe d'emploi de niveau cadre ou de niveau supérieur; ou ✓ s'il a pris une entente avec un autre OP du même ministère afin que le ROSI de cet OP agisse pour son compte.
		Degré de conformité à l'obligation portant sur la désignation d'un COGI (Ind2b)	Un OP est conforme à l'obligation portant sur la désignation d'un COGI : ✓ s'il a désigné un COGI qui est un employé régulier de l'organisme et qui appartient à la classe d'emploi de niveau professionnel ou de niveau supérieur; ou ✓ s'il a pris une entente avec un autre OP du même ministère afin que le COGI de cet OP agisse pour son compte.
Taux de participation de chacun des OP invités aux activités gouvernementales de concertation	65 % annuellement pour chacun des OP	Taux de participation, sur invitation, de l'OP aux rencontres de la table des ROSI et au réseau des COSI depuis le 1er avril de l'année en cours (Ind3)	Ce taux de participation est calculé selon : ✓ le nombre de participations aux rencontres de la table des ROSI et au réseau des COSI depuis le 1er avril de l'année en cours, divisé par le nombre d'invitations à participer à ces rencontres depuis le 1er avril de l'année en cours (100 %) Pour que l'OP soit conforme aux exigences gouvernementales, ce taux doit être supérieur à 65 %. Ce ratio traduit la participation annuelle d'un OP à au moins 4 rencontres sur 5. L'OP doit participer à au moins 2/3 des rencontres du réseau des COSI et aux 2 rencontres de la table des ROSI chaque année.

Objectif 1.2 : Évaluer les risques à portée gouvernementale

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'OP ayant identifié leurs actifs critiques	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP d'ici le 31 mars 2016	Degré de conformité à l'exigence portant sur l'identification des actifs critiques (Ind4)	Un OP est conforme à l'exigence portant sur l'identification de ses actifs critiques si : ✓ les actifs critiques de l'OP sont identifiés (50 %); ✓ les actifs critiques identifiés sont validés à l'échelle de l'OP (20 %); ✓ les actifs critiques identifiés sont documentés (20 %); ✓ une revue périodique de l'inventaire des actifs critiques est réalisée (10 %).
Taux d'actifs critiques identifiés pour lesquels des mesures de contingence sont mises en place	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP, d'ici le 31 mars 2016	Taux d'actifs critiques identifiés pour lesquels les mesures de contingence sont mises en place (Ind5)	Ce taux est calculé selon : ✓ le nombre d'actifs critiques pour lesquels les mesures de contingence sont mises en place, divisé par le nombre total d'actifs critiques. Pour que l'OP soit conforme aux exigences gouvernementales, ce taux doit être de 100 % à la date cible.

Orientation 2 : Atteindre un niveau de maturité adéquat en sécurité de l’information

Objectif 2.1 : Mettre en œuvre des processus formels de gestion de la sécurité de l’information

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'OP ayant mis en œuvre un processus formel de gestion des risques de sécurité de l'information	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information (Ind6)	Un OP est conforme à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information si : ✓ le processus de gestion des risques est clairement défini et connu des intervenants concernés (15 %); ✓ l'analyse du contexte organisationnel (enjeux de sécurité de l'information) est réalisée (10 %); ✓ l'identification des risques de sécurité de l'information est réalisée (20 %); ✓ l'analyse et l'évaluation des risques sont réalisées (20 %); ✓ les traitements des risques identifiés sont planifiés ou réalisés (20 %); ✓ un suivi et une revue périodiques des risques sont prévus et mis en œuvre (15 %).
Taux d'OP ayant mis en œuvre un processus formel de gestion des incidents	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des incidents (Ind7)	Un OP est conforme à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des incidents de sécurité de l'information si : ✓ le processus de gestion des incidents est clairement défini et connu des intervenants concernés (15 %); ✓ les activités de prévention des incidents sont en place (15 %); ✓ les activités de détection des incidents sont en place (20 %); ✓ les activités de réaction aux incidents sont prévues (25 %); ✓ les activités de rétablissement après incidents sont prévues (15 %); ✓ les activités de suivi des incidents (documentation et recommandations) sont prévues (10 %).
Taux d'OP ayant mis en œuvre un processus formel de gestion de l'accès à l'information	✓ 75 % des OP de grande taille et 25 % des OP de taille moyenne, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, 75 % des OP de taille moyenne et 50 % des OP de petite taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion de l'accès à l'information (Ind8)	Un OP est conforme à l'obligation portant sur la mise en œuvre d'un processus formel de gestion de l'accès à l'information si : ✓ le processus de gestion des accès est clairement défini et connu des intervenants concernés (15 %); ✓ les droits d'accès et les privilèges spéciaux sont attribués et mis à jour de façon formelle (45 %); ✓ les activités de contrôle des accès sont clairement définies et mises en œuvre (25 %); ✓ les droits d'accès et les privilèges spéciaux sont révisés périodiquement ou à la suite d'un changement majeur (15 %).

Objectif 2.2 : Se conformer aux bonnes pratiques de sécurité de l'information

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'OP ayant intégré les clauses contractuelles de sécurité de l'information à leurs ententes ou leurs contrats	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur l'intégration des clauses contractuelles de sécurité de l'information aux contrats et ententes (Ind9)	Un OP est conforme à l'obligation portant sur l'intégration des clauses contractuelles de sécurité de l'information aux contrats et ententes établis si : ✓ les clauses sur le respect des règles[16] de sécurité sont intégrées aux ententes et contrats conclus à partir de la date de mise en vigueur de la directive sur la sécurité de l'information (15 %); ✓ les clauses sur les mesures[17] de sécurité sont intégrées aux ententes et contrats conclus à partir de la date de mise en vigueur de la directive sur la sécurité de l'information (15 %); ✓ les clauses sur la sécurité des accès[18] sont intégrées aux ententes et contrats conclus à partir de la date de mise en vigueur de la directive sur la sécurité de l'information (20 %); ✓ les clauses sur la confidentialité[19] sont intégrées aux ententes et contrats conclus à partir de la date de mise en vigueur de la directive sur la sécurité de l'information (50 %).
Taux d'OP ayant effectué un audit en sécurité de l'information au cours des deux dernières années	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la réalisation d'un audit en sécurité de l'information (Ind10)	Un OP est conforme à l'obligation portant sur la réalisation d'un audit de sécurité de l'information si : ✓ le plan d'audit est clairement défini (15 %); ✓ la collecte de données est effectuée (20 %); ✓ l'analyse des données est effectuée (20 %); ✓ le rapport d'audit est rédigé et les recommandations sont formulées (15 %); ✓ les priorités d'actions et les échéanciers sont définis (10 %); ✓ le rapport d'audit date de moins de 2 ans (10 %); ✓ un audit est réalisé à la suite de changements majeurs susceptibles d'avoir des conséquences sur la SI (10 %).

16. Clause sur le respect des règles de sécurité : Le prestataire de services s'engage à respecter les politiques, les directives et les autres règles de sécurité applicables à l'information gouvernementale et déterminées par le ministre ou le dirigeant de l'organisme. À cet égard, il s'engage à ce que toute personne qui participe à la réalisation du contrat les respecte.
17. Clause sur les mesures de sécurité : Le prestataire de services s'engage à prendre les mesures nécessaires afin d'assurer, en tout temps, la sécurité de l'information gouvernementale en fonction de la valeur de cette information, déterminée par le ministre ou le dirigeant d'organisme, et d'informer ce dernier des mesures prises.
18. Clause sur la sécurité des accès : Le prestataire de services s'engage à restreindre l'accès à l'information gouvernementale aux seules personnes qui doivent y avoir accès aux fins de la réalisation du contrat. De même, il s'engage à ce que toute personne qui participe à la réalisation du contrat n'ait accès qu'à l'information nécessaire à la réalisation de celui-ci. Il s'engage également à assurer la sécurité des moyens d'identification qui sont remis afin d'accéder à cette information.
19. Clause sur la confidentialité : Le prestataire de services s'engage à ce que ni lui ni aucune autre personne qui participe à la réalisation du contrat ne divulguent, sans y être dûment autorisés par le ministre ou le dirigeant de l'organisme, l'information gouvernementale dont ils ont eu connaissance dans la réalisation du contrat, de même que les travaux, y compris les données, les analyses ou les résultats, réalisés en vertu du contrat.

Taux d'OP qui effectuent, annuellement, des tests d'intrusions et de vulnérabilités en sécurité de l'information	100 % des OP fortement exposés aux risques et de ceux de grande taille, d'ici le 31 mars 2015 75 % des OP de taille moyenne et 50 % des OP de petite taille, d'ici le 31 mars 2016 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la réalisation des tests d'intrusions et de vulnérabilités en sécurité de l'information (Ind11)	Un OP est conforme à l'obligation portant sur la réalisation des tests d'intrusions et de vulnérabilités en sécurité de l'information si : ✓ le plan des tests d'intrusions et de vulnérabilités est clairement défini (20 %); ✓ la phase de découverte des vulnérabilités est réalisée (20 %); ✓ la phase d'exploitation des vulnérabilités (tests d'intrusions) est réalisée (20 %); ✓ le rapport des tests d'intrusions et des vulnérabilités est rédigé et les recommandations sont formulées (10 %); ✓ les priorités d'actions et les échéanciers sont définis (10 %); ✓ le rapport des tests d'intrusions et de vulnérabilités date de moins d'un an (10 %); ✓ des tests d'intrusions et de vulnérabilités sont réalisés à la suite de changements majeurs susceptibles d'avoir des conséquences sur la SI (10 %).
Taux d'OP ayant mis en place un registre d'autorité	100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 100 % des OP de grande taille, d'ici le 31 mars 2016 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la mise en place d'un registre d'autorité (Ind12)	Un OP est conforme à l'obligation portant sur la mise en place d'un registre d'autorité si : ✓ le contenu du registre est clairement défini[20] (35 %); ✓ les règles de mise à jour du registre sont établies (15 %); ✓ le registre d'autorité est mis en œuvre (50 %).
Taux d'OP ayant adopté une architecture de sécurité de l'information	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur l'adoption d'une architecture de sécurité de l'information (Ind13)	Un OP est conforme à l'obligation portant sur l'adoption d'une architecture de sécurité de l'information si : ✓ une architecture de sécurité documentée existe (20 %); ✓ un cadre d'architecture de SI et une méthodologie sont utilisés (15 %); ✓ les travaux d'architecture, de la conception à l'implantation, sont intégrés au programme de sécurité de l'OP ou à la planification triennale des travaux de sécurité (20 %); ✓ l'architecture de sécurité est arrimée au processus d'amélioration continue de la sécurité de l'OP (15 %); ✓ les orientations, les principes, les normes et les standards de sécurité en usage découlent de l'architecture de sécurité (15 %); ✓ les mesures de sécurité découlent des orientations, des principes, des normes et des standards définis à l'architecture (15 %).

20. Le « guide d'élaboration du registre d'autorité » fournit une information détaillée sur le contenu d'un registre d'autorité.

Orientation 3 : Renforcer la cybersécurité de l'information

Objectif 3.1 : Participer activement au réseau d'alerte gouvernemental

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux de participation des OP au réseau d'alerte gouvernemental	✓ 100 % des OP fortement exposés aux risques ainsi que ceux de grande taille, d'ici le 31 mars 2015 ✓ 100 % des OP, d'ici le 31 mars 2016	Taux de participation au réseau d'alerte gouvernemental depuis avril 2014 (Ind14)	Ce taux de participation est calculé selon : ✓ un participant de l'OP au réseau d'alerte est désigné dans la liste « alerte.ra » (15 %); ✓ le nombre de conférences organisées par le réseau d'alerte auxquelles l'OP a participé depuis avril 2014, divisé par le nombre de conférences organisées par le réseau d'alerte depuis avril 2014 (85 %). Pour que l'OP soit conforme aux exigences gouvernementales, ce taux doit être supérieur à 75 %.

Orientation 4 : Développer l'offre de service d'authentification gouvernementale

Objectif 4.1 : Augmenter l'utilisation des services d'authentification gouvernementale

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'adhésion à clicSÉQUR	80 % des nouvelles prestations électroniques de services (PES) transactionnelles utilisent clicSÉQUR	Taux d'adhésion des nouvelles PES à clicSÉQUR (Ind15)	Ce taux d'adhésion est calculé selon : ✓ le nombre de nouvelles PES transactionnelles depuis avril 2014 utilisant ClicSÉQUR, divisé par le nombre de nouvelles PES transactionnelles depuis avril 2014 (100 %). Pour que l'OP soit conforme aux exigences gouvernementales, ce taux doit être supérieur à 80 %.

Orientation 5 : Développer et maintenir les compétences en sécurité

Objectif 5.1 : Sensibiliser le personnel à la sécurité de l'information

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'OP ayant mis en place un plan de sensibilisation de l'ensemble du personnel en matière de sécurité de l'information	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la mise en œuvre d'un plan de sensibilisation de l'ensemble du personnel en matière de sécurité de l'information (Ind16)	Un OP est conforme à l'obligation portant sur la mise en œuvre d'un plan de sensibilisation formel en matière de sécurité de l'information pour l'ensemble du personnel si : ✓ les besoins en sécurité sont évalués pour les différents groupes d'utilisateurs (25 %); ✓ le plan de sensibilisation est adapté aux besoins des différents groupes d'utilisateurs (25 %); ✓ le plan de sensibilisation est adopté et mis en œuvre (40 %); ✓ le plan de sensibilisation est révisé périodiquement (10 %).
Taux d'OP ayant offert une première session de sensibilisation à la sécurité de l'information à l'ensemble du personnel	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Taux du personnel ayant suivi une première session de sensibilisation à la sécurité de l'information (Ind17)	Ce taux est calculé selon : ✓ l'effectif ayant suivi la première session de sensibilisation, divisé par l'effectif total (100 %), à condition que le plan de sensibilisation soit clairement défini et que la première session de sensibilisation soit démarrée. Pour que l'OP soit conforme aux exigences gouvernementales, ce taux doit être égal à 100 %.

Objectif 5.2 : Accroître l'expertise et le savoir-faire en sécurité de l'information

Indicateur gouvernemental	Cible gouvernementale	Indicateur sectoriel	Règles de conformité de l'OP à l'égard des cibles gouvernementales
Taux d'OP ayant mis en œuvre un programme formel de formation de l'ensemble du personnel	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'obligation portant sur la mise en œuvre d'un programme formel de formation pour l'ensemble du personnel en matière de sécurité de l'information (Ind18)	Un OP est conforme à l'obligation portant sur la mise en œuvre d'un programme formel de formation en matière de sécurité de l'information pour l'ensemble du personnel si : ✓ les besoins en sécurité sont évalués pour les différents groupes d'utilisateurs (25 %); ✓ le programme de formation est adapté aux besoins des différents groupes d'utilisateurs (25 %); ✓ le programme de formation est adopté et mis en œuvre (40 %); ✓ le programme de formation est révisé périodiquement (10 %).
Taux des ROSI ayant suivi une formation générale en sécurité de l'information	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'exigence portant sur la formation générale en matière de sécurité de l'information du ROSI (Ind19)	Un OP est conforme à cette exigence si le ROSI a des connaissances générales en sécurité de l'information ou a suivi un programme de formation générale en sécurité de l'information visant à vulgariser les différents domaines de sécurité de l'information conformément à la norme ISO/IEC 27002.
Taux des COGI ayant suivi une formation sur les bonnes pratiques de sécurité de l'information, dont la gestion des risques, des incidents ou de l'accès à l'information	✓ 100 % des OP fortement exposés aux risques, d'ici le 31 mars 2015 ✓ 100 % des OP de grande taille et 50 % des OP de taille moyenne et de petite taille, d'ici le 31 mars 2016 ✓ 100 % des OP, d'ici le 31 mars 2017	Degré de conformité à l'exigence portant sur la formation sur les bonnes pratiques de sécurité de l'information du COGI (Ind20)	Un OP est conforme à cette exigence si le COGI a des connaissances générales en sécurité de l'information ou a suivi un programme de formation sur les bonnes pratiques de sécurité de l'information comme le préconisent les normes ISO/IEC 27001 et 27002.

4.2 Description de l'outil

L'outil se présente sous la forme d'un chiffrier *Excel* illustrant graphiquement une vue d'ensemble des indicateurs sectoriels concourant à l'atteinte des cibles gouvernementales et organisés par axe de performance.

Structure

L'outil comporte une page d'identification, une vue principale, une vue par axe de performance et une vue détail par indicateur.

- ✓ Page d'identification : permet de choisir de consulter ou d'alimenter le tableau de bord. Elle est illustrée à la figure 4, présentée ci-après.

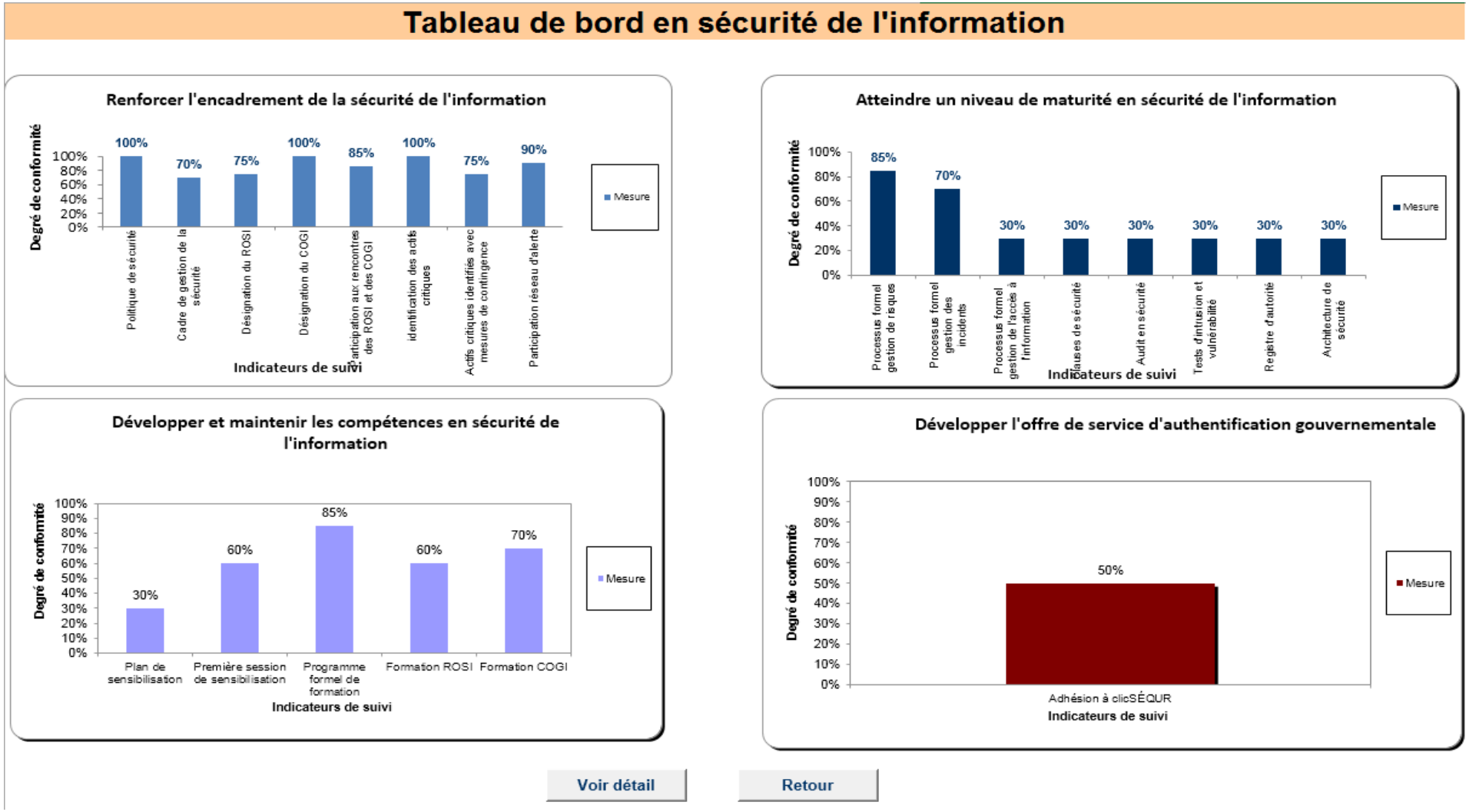
Figure 4 : Page d'identification

Vue principale : comporte quatre quadrants, présentant graphiquement les indicateurs sectoriels associés à chacun des axes de performance. Ces quatre quadrants sont les suivants :

- ✓ Renforcer l'encadrement de la sécurité de l'information;
- ✓ Atteindre un niveau de maturité adéquat en sécurité de l'information;
- ✓ Développer l'offre de service d'authentification gouvernementale;
- ✓ Développer et maintenir les compétences en sécurité de l'information.

La vue principale est illustrée à la figure 5, présentée ci-après.

Figure 5 : Vue principale

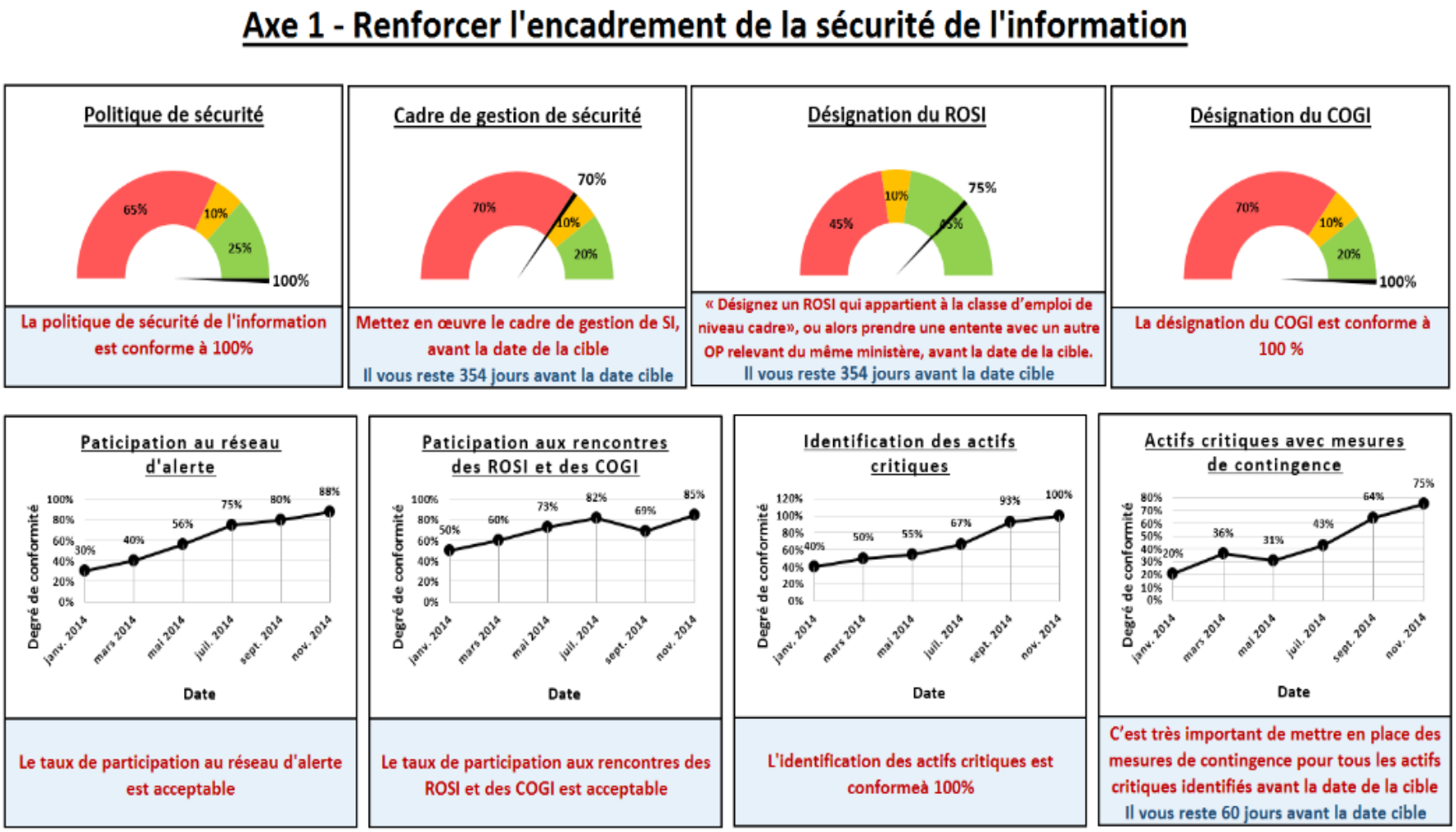


Un clic sur l'un des quadrants permet d'accéder à la vue par axe de performance.

- ✓ Vue par axe de performance : fournit une illustration graphique de chaque indicateur représentant l'axe de performance choisi. Des précisions telles que le degré de conformité de chaque indicateur par rapport à la cible visée et le temps qui reste pour atteindre la cible sont affichées.

La vue pour l'axe de performance « Renforcer l'encadrement de la sécurité de l'information » est illustrée à la figure 6, présentée ci-après.

Figure 6 : Vue par axe de performance



Un clic sur l'un des graphiques d'un indicateur sur la page de la vue par axe de performance permet d'accéder à la vue détail de cet indicateur.

- ✓ Vue détail par indicateur : permet d'observer la progression vers l'atteinte de la cible liée à l'indicateur, selon des dates de collecte de données relatives à cet indicateur.

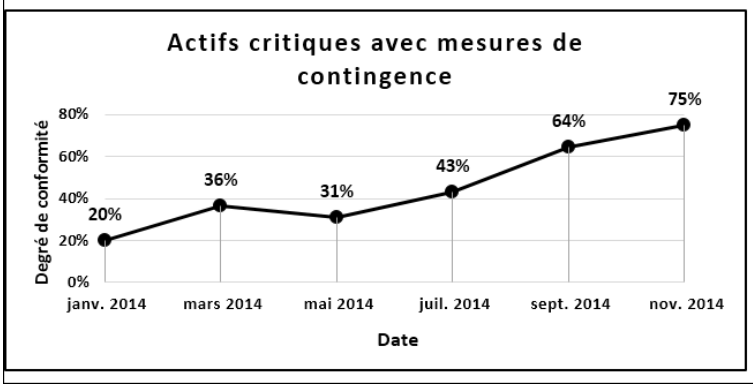
La vue détail de l'indicateur « Actifs critiques avec mesures de contingence » est illustrée à la figure 7, présentée ci-après.

Figure 7 : Vue détail par indicateur

Actifs critiques avec mesures de contingence

Date (aaaa-mm-jj)	Nombre d'actifs critiques identifiés avec mesures de contingence en place	Nombre d'actifs critiques identifiés	Pourcentage
2014-01-01	2	10	20%
2014-03-01	4	11	36%
2014-05-01	4	13	31%
2014-07-01	6	14	43%
2014-09-01	9	14	64%
2014-11-01	12	16	75%

Mesure actuelle	75%
Seuil	100%
Cible	100%



C'est très important de mettre en place des mesures de contingence pour tous les actifs critiques identifiés avant la date de la cible

Il vous reste 60 jours avant la date cible

Retour

ANNEXE I **Modèle de fiche descriptive d'indicateur**

Fiche descriptive d'indicateur numéro xx

Nº indicateur :	
Désignation :	
Libellé :	
Description :	
Objectif :	
Destinataires :	
Date de production :	
Éléments de référence gouvernementale	
Orientation gouvernementale :	
Objectif gouvernemental :	
Cible gouvernementale :	
Cible sectorielle et seuil d'alerte	
Cible sectorielle :	
Seuil d'alerte :	
Calcul de l'indicateur	
Mesure (unité) :	**Type de mesure :**
Éléments de calcul :	
Algorithme de calcul :	
Formule/Pondération :	
Collecte des données et rapport	
Responsable d'alimentation :	**Propriétaire des données :**
Fréquence de collecte :	**Source de données :**
Méthode de collecte :	**Date de collecte :**
Format d'illustration :	**Règle d'interprétation :**

Description des champs

Champ	Description
Indicateur sectoriel	
Nº indicateur	Permet d'attribuer un numéro à l'indicateur. Ce numéro permet de l'identifier de manière unique.
Désignation	Permet de nommer l'indicateur.
Libellé	Permet d'exprimer textuellement l'indicateur.
Description	Permet de décrire l'indicateur.
Objectif	Permet de préciser l'objectif de l'indicateur pour l'OP.
Destinataires	Permet de préciser à qui est destiné l'indicateur.
Date de production	Permet de préciser la date de production de l'indicateur.
Éléments de référence gouvernementale	
Orientation gouvernementale	Permet de préciser l'orientation gouvernementale en rapport avec l'indicateur.
Objectif gouvernemental	Objectif gouvernemental en rapport avec l'indicateur.
Cible gouvernementale	Permet de préciser la cible gouvernementale à atteindre.
Cible et seuil sectoriels	
Cible sectorielle	Permet de préciser la cible sectorielle à atteindre.
Seuil d'alerte	Permet de préciser le seuil d'alerte de l'indicateur.
Calcul de l'indicateur	
Mesure	Permet de préciser la mesure de l'indicateur. Les valeurs possibles sont : « moyenne », « nombre », « pourcentage ».
Type de mesure	Permet de préciser si la mesure est de base (obtenue d'une seule source) ou dérivée (obtenue de plusieurs sources de données). Deux valeurs sont possibles : « base **»** ou « dérivée ».
Éléments de calcul	Permet de préciser les éléments nécessaires à la formule de calcul de l'indicateur.
Algorithme de calcul	Permet de préciser l'algorithme de calcul de la valeur de l'indicateur.
Formule/Pondération	Permet de préciser la formule ou la pondération (des activités liées à l'indicateur) utilisée pour calculer la valeur de l'indicateur.
Collecte des données et rapports	

Responsable d'alimentation	Permet de désigner le responsable de la collecte des données utiles au calcul de la valeur de l'indicateur.
Propriétaire des données	Permet de désigner le contact du propriétaire de la ou des données devant faire l'objet d'une collecte.
Fréquence de collecte	Permet de préciser la fréquence de collecte des données. Les valeurs possibles sont : « heure », « quotidienne », « hebdomadaire », « mensuelle », « bimensuelle », « trimestrielle », « semestrielle », « annuelle ».
Date de collecte	Permet de préciser la date où on a procédé à la collecte des données.
Méthode de collecte	Permet de préciser la méthode de collecte. Les valeurs possibles sont : « automatique » et « manuelle ».
Source de données	Permet de préciser la source des données devant faire l'objet d'une collecte.
Format d'illustration	Permet de préciser le type et le format de représentation de l'indicateur.
Règle d'interprétation	Permet de préciser comment interpréter l'illustration de l'indicateur.

ANNEXE II **Fiches descriptives d’indicateurs de suivi des cibles gouvernementales**

Fiche descriptive d’indicateur numéro 1a

Nº indicateur : 1a

Désignation : Ind1a

Libellé : Degré de conformité à l'obligation portant sur la politique de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « Adopter et mettre en œuvre une politique de sécurité de l'information, la maintenir à jour et assurer son application ».

Objectif : Adopter et mettre en œuvre une politique de sécurité de l'information et s'assurer de sa mise à jour.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Gérer efficacement la sécurité de l'information gouvernementale.

Cible gouvernementale :

- ✓ 100 % des OP auront adopté une politique de sécurité de l'information d'ici le 31 mars 2015.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind1a = 100 % d'ici le 31 mars 2015

Seuil d'alerte : Ind1a <= 75 %

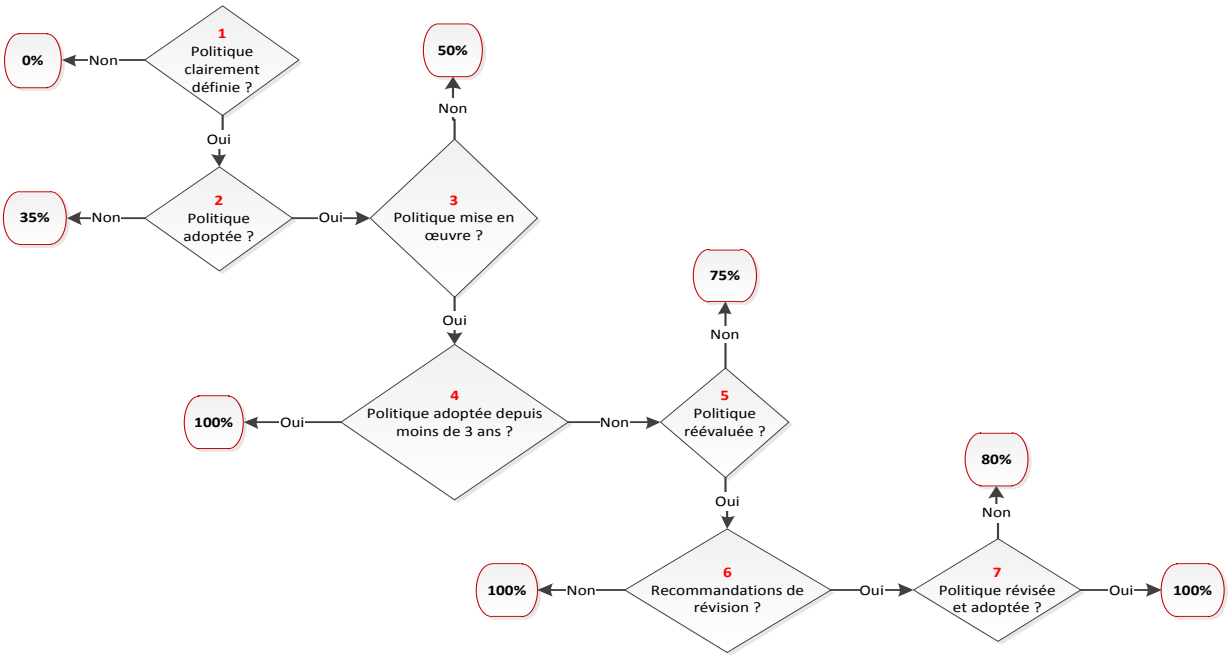
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Politique de SI clairement définie (O/N)
2. Politique de SI adoptée (O/N)
3. Politique de SI mise en œuvre (O/N)
4. Politique adoptée il y a moins de 3 ans (O/N)
5. Politique de SI réévaluée (O/N)
6. Recommandations de révision (O/N)
7. Politique de SI révisée et adoptée (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la politique de sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind1a = 0 %

Si ((1 = « Oui ») et (2 = « Non ») alors Ind1a = 35 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non ») alors Ind1a = 50 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») alors Ind1a = 100 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Non ») alors Ind1a = 75 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Oui ») et (6 = « Non ») alors Ind1a = 100 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Non ») alors Ind1a = 80 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Oui ») alors Ind1a = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « plan d'action », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	✓ Si Ind1a = 0 %, Alarme : « Définissez clairement la politique de SI, avant le 31 mars 2015 ». ✓ SI Ind1a = 35 %, Alarme : « Adoptez la politique de SI, avant le 31 mars 2015 ». ✓ SI Ind1a = 50 %, Alarme : « Mettez en œuvre la politique de SI, avant le 31 mars 2015 ». ✓ Si Ind1a = 75 %, Alarme : « Évaluez la politique de SI, avant le 31 mars 2015 ». ✓ Si Ind1a = 80 %, Signal : « Révisez la politique de SI, avant le 31 mars 2015 ». ✓ Si Ind1a = 100 %, Signal : « La politique de SI est conforme à 100 % ». ✓ Si ((Date_Système > « 31 mars 2015 ») et (Ind1a <100 %)) Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 1b

Nº indicateur : 1b

Désignation : Ind1b

Libellé : Degré de conformité à l'obligation portant sur le cadre de gestion de la sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permettra d'apprécier le degré de conformité de l'organisme public à l'obligation « Adopter et mettre en œuvre un cadre de gestion de la sécurité de l'information, le maintenir à jour et assurer son application ».

Objectif : Adopter et mettre en œuvre un cadre de gestion de la sécurité de l'information et s'assurer de sa mise à jour.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Gérer efficacement la sécurité de l'information gouvernementale.

Cible gouvernementale :

- ✓ 100 % des OP auront adopté un cadre de gestion de la sécurité de l'information d'ici le 31 mars 2015.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind1b = 100 d'ici le 31 mars 2015

Seuil d'alerte : Ind1b <= 75 %

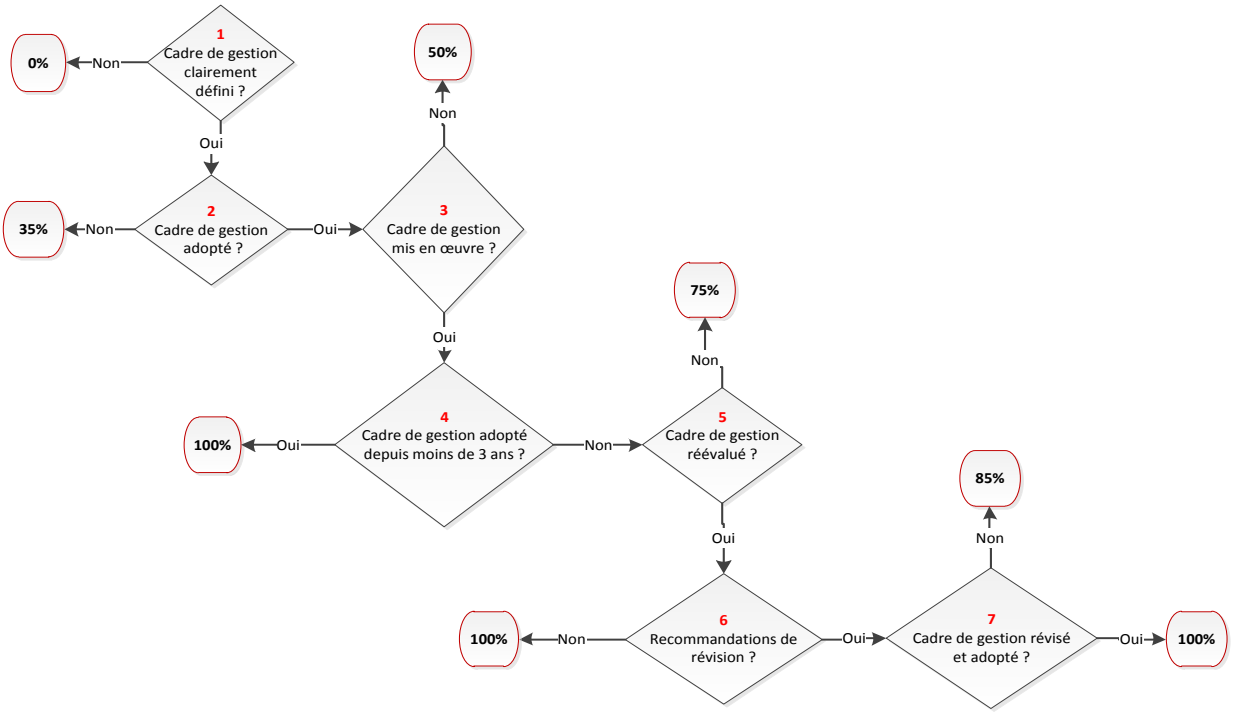
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Cadre de gestion de SI clairement défini (O/N)
2. Cadre de gestion de SI adopté (O/N)
3. Cadre de gestion de SI mis en œuvre (O/N)
4. Cadre adopté il y a moins de 3 ans (O/N)
5. Cadre de gestion de SI réévalué (O/N)
6. Recommandations de révision (O/N)
7. Cadre de gestion de SI révisé et adopté (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur le cadre de gestion de la sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind1b = 0 %

Si ((1 = « Oui ») et (2 = « Non »)) alors Ind1b = 35 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind1b = 50 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui »)) alors Ind1b = 100 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Non »)) alors Ind1b = 75 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Oui ») et (6 = « Non »)) alors Ind1b = 100 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Non »)) alors Ind1b = 85 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Oui »)) alors Ind1b = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « plan d'action », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	✓ Si Ind1b = 0 %, Alarme : « Définissez clairement le cadre de gestion de SI, avant le 31 mars 2015 ». ✓ SI Ind1b = 35 %, Alarme : « Adoptez le cadre de gestion de SI, avant le 31 mars 2015 ». ✓ SI Ind1b = 50 %, Alarme : « Mettez en œuvre le cadre de gestion de SI, avant le 31 mars 2015 ». ✓ Si Ind1b = 75 %, Alarme : « Évaluez le cadre de gestion de SI, avant le 31 mars 2015 ». ✓ Si Ind1b = 85 %, Signal : « Révisez le cadre de gestion de SI, avant le 31 mars 2015 ». ✓ Si Ind1b = 100 %, Signal : « Le cadre de gestion de SI est conforme à 100 % ». ✓ Si ((Date_Système > « 31 mars 2015 ») et (Ind1b <100 %)) Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 2a

Nº indicateur : 2a

Désignation : Ind2a

Libellé : Degré de conformité à l'obligation portant sur la désignation d'un responsable organisationnel de la sécurité de l'information (ROSI).

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « Désigner un responsable organisationnel de la sécurité de l'information pour le représenter en matière de sécurité de l'information auprès de l'organisation et auprès du dirigeant principal de l'information. Ce responsable doit être un employé régulier de l'organisme public et appartenir à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur ».

Objectif : S'assurer que le ROSI est désigné, qu'il est employé régulier de l'organisme et qu'il appartient à la classe d'emploi de niveau cadre, ou qu'une entente a été établie avec un autre organisme public de son ministère pour que le ROSI agisse à son compte.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Gérer efficacement la sécurité de l'information gouvernementale.

Cible gouvernementale :

- ✓ 100 % des OP auront désigné leurs principaux intervenants en sécurité de l'information (ROSI et COGI) d'ici le 31 mars 2015.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind2a = 100 % d'ici le 31 mars 2015

Seuil d'alerte : Ind2a < 100 %

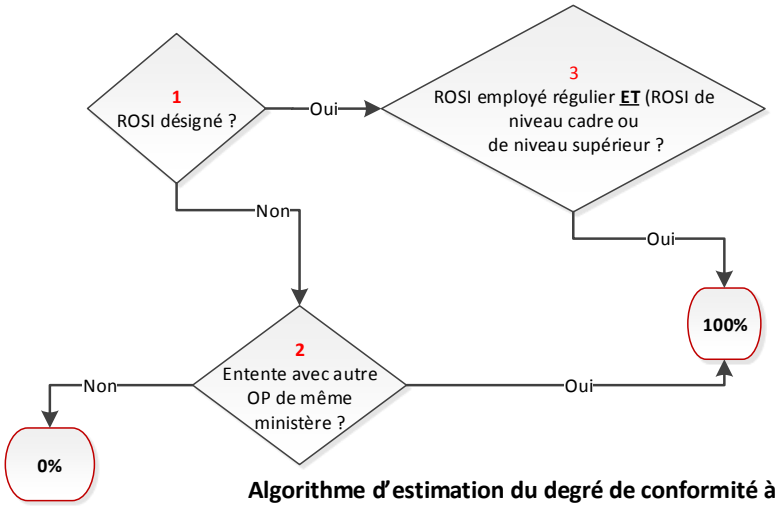
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. ROSI désigné (O/N)
2. Entente avec un autre OP relevant du même ministère (O/N)
3. ROSI employé régulier ET (ROSI de niveau cadre ou de niveau supérieur) (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la désignation d'un ROSI

Formule/Pondération :

Si ((1 = « Non ») et (2 = « Non ») alors Ind2a = 0 %

Si ((1 = « Non ») et (2 = « Oui ») alors Ind2a = 100 %

Si ((1 = « Oui ») et (3 = « Oui ») alors Ind2a = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** RH
Fréquence de collecte : semestrielle	**Source de données :** ROSI, RH
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « participation aux activités gouvernementales de concertation », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (0 %, 25 %, 50 %, 75 %, 100 %).	**Règle d'interprétation :** ✓ Si Ind2a = 0 %, Alarme : « Désignez un ROSI qui est employé régulier et appartient à la classe d'emploi de niveau cadre ou de niveau supérieur » ou alors prenez une entente avec un autre OP relevant du même ministère, avant le 31 mars 2015. ✓ Si Ind2a = 100 %, Signal : « La désignation du ROSI est conforme à 100 % ». ✓ Si ((Date_Système > « 31 mars 2015 ») et (Ind2a <100 %)) Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 2b

Nº indicateur : 2b

Désignation : Ind2b

Libellé : Degré de conformité à l'obligation portant sur la désignation d'un coordonnateur organisationnel de gestion des incidents (COGI).

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « Désigner un coordonnateur organisationnel de gestion des incidents pour le représenter auprès du réseau d'alerte gouvernemental et y participer activement. Ce coordonnateur doit être un employé régulier de l'organisme public et appartenir à la classe d'emploi de niveau professionnel ou à une classe d'emploi de niveau supérieur ».

Objectif : S'assurer que le COGI est désigné, qu'il est employé régulier de l'organisme et qu'il appartient à la classe d'emploi de niveau professionnel, ou qu'une entente a été établie avec un autre organisme public de son ministère pour que le COGI agisse à son compte.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Gérer efficacement la sécurité de l'information gouvernementale.

Cible gouvernementale :

- ✓ 100 % des OP auront désigné leurs principaux intervenants en sécurité de l'information (ROSI et COGI) d'ici le 31 mars 2015.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

100 % d'ici le 31 mars 2015

Seuil d'alerte : Ind2b < 100 %

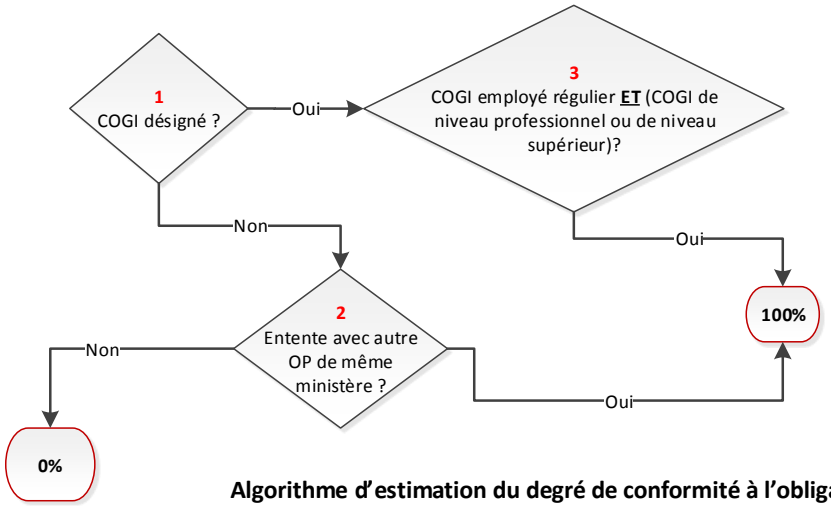
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. COGI désigné (O/N)
2. Entente avec un autre OP relevant du même ministère (O/N)
3. COGI employé régulier ET (COGI de niveau professionnel ou de niveau supérieur) (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la désignation d'un COGI

Formule/Pondération :

Si ((1 = « Non ») et (2 = « Non ») alors Ind2b = 0 %

Si ((1 = « Non ») et (2 = « Oui ») alors Ind2b = 100 %

Si ((1 = « Oui ») et (3 = « Oui ») alors Ind2b = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** RH
Fréquence de collecte : semestrielle	**Source de données :** ROSI, RH
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « participation aux activités gouvernementales de concertation », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si Ind2b = 0 %, Alarme : « Désignez un COGI qui est employé régulier et appartient à la classe d'emploi de niveau professionnel ou de niveau supérieur » ou alors prenez une entente avec un autre OP relevant du même ministère, avant le 31 mars 2015 ». ✓ Si Ind2b = 100 %, Signal : « La désignation du COGI est conforme à 100 % ». ✓ Si ((Date_Système > « 31 mars 2015 ») et (Ind2b <100 %)) Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 3

Nº indicateur : 3

Désignation : Ind3

Libellé : Taux de participation, sur invitation, de l'organisme public aux rencontres de la table des ROSI et du réseau des COSI depuis le 1er avril dernier.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le taux de participation de l'organisme public aux activités gouvernementales de concertation, depuis le 1er avril jusqu'au 31 mars.

Objectif : S'assurer de contribuer aux activités gouvernementales de concertation.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Gérer efficacement la sécurité de l'information gouvernementale.

Cible gouvernementale :

- ✓ 65 % annuellement pour chacun des organismes publics.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind3 >= 65 % chaque année

Seuil d'alerte : Ind3 < 65 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

A. Nombre d'invitations à participer aux rencontres de la table des ROSI et du réseau des COSI depuis le 1er avril dernier

B. Nombre de participations aux rencontres de la table des ROSI et du réseau des COSI depuis le 1er avril dernier

Algorithme de calcul : s. o.

Formule/Pondération :

Ind3 = (B / A) x 100, avec A > 0 et B <= A

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : semestrielle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « diagramme linéaire » dont l'axe des ordonnées représentera le taux de participation et l'axe des abscisses, les dates de collecte semestrielle. Le diagramme devra afficher le taux de participation sur une période choisie par l'organisme. Au niveau de la fenêtre principale du tableau de bord, cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « participation aux rencontres de la table des ROSI et du réseau des COSI », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, 100 %)	✓ Si Ind3 = 0 %, Alarme : « C'est très important de participer aux rencontres de la table des ROSI et du réseau des COSI ». ✓ Si Ind3 < 65 % et Ind3 # 0, Alarme : « C'est très important de participer davantage aux rencontres de la table des ROSI et du réseau des COSI ». ✓ Si Ind3 >= 65 %, Signal : « Le taux de participation aux rencontres de la table des ROSI et du réseau des COSI est acceptable ».

Fiche descriptive d’indicateur numéro 4

Nº indicateur : 4

Désignation : Ind4

Libellé : Degré de conformité à l'exigence portant sur l'identification des actifs critiques.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'OP à l'exigence portant sur l'identification des actifs critiques.

Objectif : S'assurer que tous les actifs critiques sont identifiés.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Évaluer les risques à portée gouvernementale.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront identifié leurs actifs critiques d'ici le 31 mars 2015.
- ✓ 100 % des OP auront identifié leurs actifs critiques d'ici le 31 mars 2016.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind4 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind4 = 100 % d'ici le 31 mars 2016 si l'OP n'est pas fortement exposé aux risques

Seuil d'alerte : Ind4 < 100 %

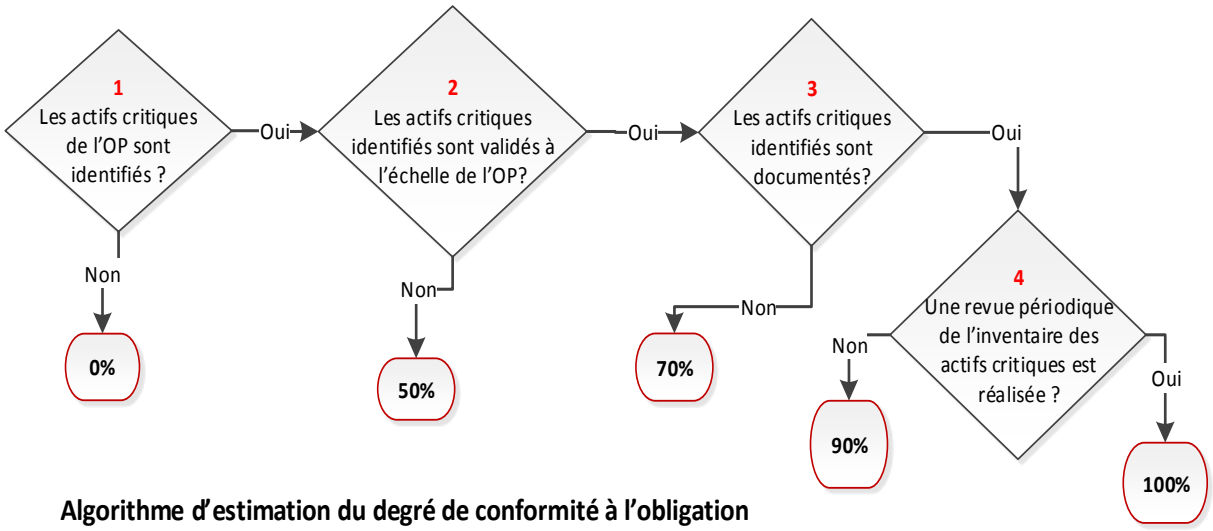
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Les actifs critiques de l'OP sont identifiés (O/N)
2. Les actifs critiques identifiés sont validés à l'échelle de l'OP (O/N)
3. Les actifs critiques identifiés sont documentés (O/N)
4. Une revue périodique de l'inventaire des actifs critiques est réalisée (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur l'identification des actifs critiques de l'OP

Formule/Pondération :

Si ((1 = « Non ») alors Ind4 = 0 %

Si ((1 = « Oui ») et (2 = « Non »)) alors Ind4 = 50 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind4 = 70 %

((1 = « Oui ») et (2 = « Non ») et (3 = « Oui ») et (4 = « Non »)) alors Ind4 = 90 %

((1 = « Oui ») et (2 = « Non ») et (3 = « Oui ») et (4 = « Oui »)) alors Ind4 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « participation aux activités gouvernementales de concertation », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, 100 %).	✓ Si OP fortement exposé aux risques alors Date cible = « 31 mars 2015 », Si non Date cible = « 31 mars 2016 ». ✓ Si Ind4 = 0 %, Alarme : « C'est très important d'identifier vos actifs critiques, avant la date cible ». ✓ Si Ind4 < 100 % et Ind4 # 0, Alarme : « L'ensemble de vos actifs doivent être catégorisés pour pouvoir identifier vos actifs critiques, avant la date cible ». ✓ Si Ind4 = 50 %, Alarme : « L'ensemble des actifs critiques identifiés doivent être validés à l'échelle de l'organisme, avant la date cible ». ✓ Si Ind4 = 70 %, Alarme : « L'ensemble des actifs critiques identifiés doivent être documentés, avant la date cible ». ✓ Si Ind4 = 90 %, Alarme : « Les actifs critiques identifiés doivent être revus périodiquement, avant la date cible ». ✓ Si Ind4 = 100 %, Signal : « L'identification des actifs critiques est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind4 <100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 5

Nº indicateur : 5

Désignation : Ind5

Libellé : Taux d'actifs critiques identifiés pour lesquels les mesures de contingence sont mises en place.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le taux d'actifs critiques pour lesquels des mesures de contingence sont mises en place.

Objectif : S'assurer que les mesures de contingence nécessaires pour les actifs critiques sont mises en place.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Évaluer les risques à portée gouvernementale.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront mis en place les mesures de contingence pour tous leurs actifs critiques identifiés d'ici le 31 mars 2015.
- ✓ Tous les OP (100 %) auront mis en place les mesures de contingence pour tous leurs actifs critiques identifiés d'ici le 31 mars 2016.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind5 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind5 = 100 % d'ici le 31 mars 2016 si l'OP n'est pas fortement exposé aux risques

Seuil d'alerte : Ind5 < 100 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure** : dérivée

Éléments de calcul :

A. Nombre d'actifs critiques identifiés

B. Nombre d'actifs critiques identifiés avec mesures de contingence mises en place

Algorithme de calcul :

s. o.

Formule/Pondération :

(B / A) x 100, avec A > 0 et B <= A

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : bimensuelle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « diagramme linéaire » dont l'axe des ordonnées représentera le taux d'actifs critiques identifiés avec mesures de contingence mises en place et l'axe des abscisses, les dates de collecte trimestrielle. Le diagramme devra afficher le taux d'actifs critiques identifiés avec mesures de contingence mises en place sur une période choisie par l'organisme. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « politique de sécurité de l'information », « cadre de gestion », « participation aux activités gouvernementales de concertation », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, 100 %).	✓ Si OP fortement exposé aux risques alors Date_cible = « 31 mars 2015 », Si non Date_cible = « 31 mars 2016 ». ✓ Si Ind5 = 0 %, Alarme : « C'est très important de mettre en place les mesures de contingence pour tous les actifs critiques identifiés avant la Date_cible ». ✓ Si Ind5 <100 % et Ind5 # 0, Alarme : « C'est très important de continuer à mettre en place les mesures de contingence pour tous les actifs critiques identifiés avant la Date_cible ». ✓ Si Ind5 = 100 %, Signal : « La mise en place des mesures de contingence pour les actifs critiques identifiés est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind5<100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 6

Nº indicateur : 6

Désignation : Ind6

Libellé : Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer de la mise en œuvre d'un processus formel de sécurité de l'information permettant d'assurer la gestion des risques ».

Objectif : S'assurer qu'un processus formel de gestion des risques est mis en œuvre, comme le décrit le cadre de gestion des risques et incidents à portée gouvernementale.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, responsable de gestion des risques, COGI, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Mettre en œuvre des processus formels de gestion de la sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront mis en œuvre un processus formel de gestion des risques d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront mis en œuvre un processus formel de gestion des risques d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront mis en œuvre un processus formel de gestion des risques d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind6 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind6 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind6 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind6 < 70 %

Calcul de l'indicateur

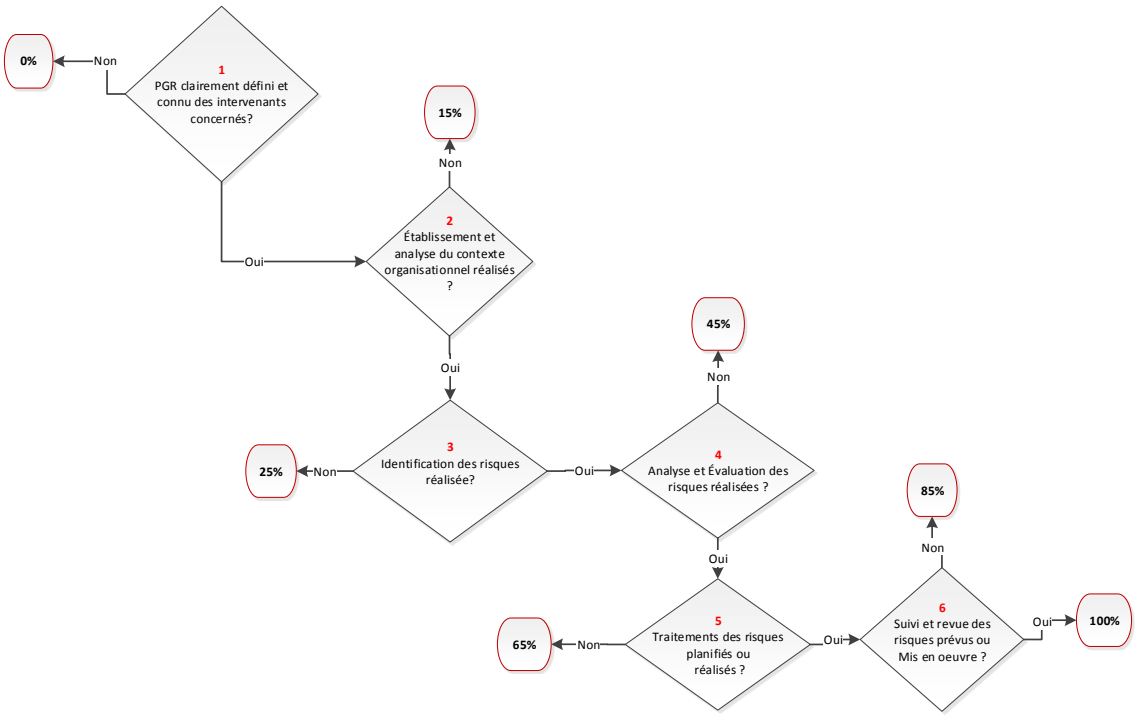
Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

PGR = Processus de gestion des risques

1. PGR de SI clairement défini et connu des intervenants concernés (O/N)
2. Établissement et analyse du contexte organisationnel réalisés (O/N)
3. Identification des risques réalisée (O/N)
4. Analyse et évaluation des risques réalisées (O/N)
5. Traitements des risques planifiés ou réalisés (O/N)
6. Suivi et revue des risques prévus et mis en œuvre (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des risques de sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind6 = 0 %

Si ((1 = « Oui ») et (2 = « Non »)) alors Ind6 = 15 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind6 = 25 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non »)) alors Ind6 = 45 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Non »)) alors Ind6 = 65 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Non »)) alors Ind6 = 85 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui »)) alors Ind6 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, responsable de la gestion des risques
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « gestion de risques », « gestion d'incidents », « audit de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (20 %, 50 %, 70 %, etc.).	✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015 Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind6 = 0 %, Alarme : « Définissez clairement le PGR de SI, avant la Date_cible ». ✓ Si Ind6 = 15 %, Alarme : « Établissez et analysez le contexte organisationnel, avant la Date_cible ». ✓ Si Ind6 = 25 %, Alarme : « Identifiez les risques, avant la Date_cible ». ✓ Si Ind6 = 45 %, Alarme : « Analysez et évaluez les risques, avant la Date_cible ». ✓ Si Ind6 = 65 %, Alarme : « Planifiez et réalisez les traitements des risques, avant la Date_cible ». ✓ Si Ind6 = 85 %, Alarme : « Suivez et révisez les risques, avant la Date_cible ». ✓ Si Ind6 = 100 %, Signal : « La mise en œuvre du processus de gestion des risques de SI est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind6 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 7

Nº indicateur : 7

Désignation : Ind7

Libellé : Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des incidents de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer de la mise en œuvre d'un processus formel de sécurité de l'information permettant d'assurer la gestion des incidents ».

Objectif : S'assurer qu'un processus formel de gestion des incidents est mis en œuvre, comme le décrit le cadre de gestion des risques et incidents à portée gouvernementale.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, responsable de la gestion des incidents, COGI, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Mettre en œuvre des processus formels de gestion de la sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront mis en œuvre un processus formel de gestion des incidents d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront mis en œuvre un processus formel de gestion des incidents d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront mis en œuvre un processus formel de gestion des incidents d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind7 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind7 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind7 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind7 < 90 %

Calcul de l'indicateur

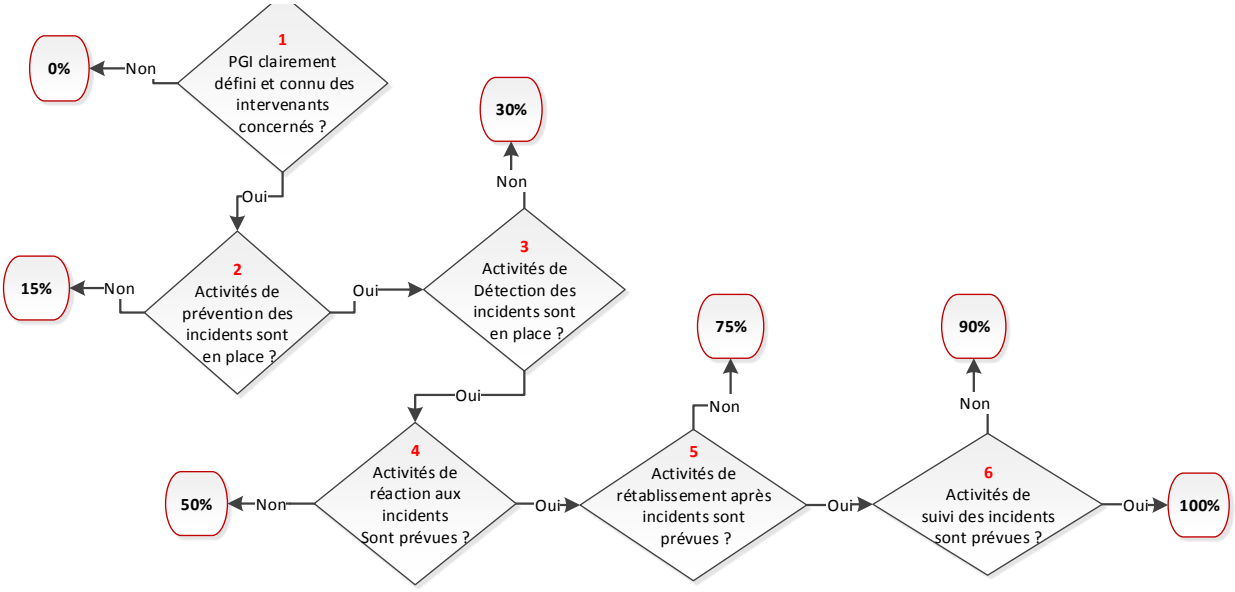
Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

PGI = Processus de gestion des incidents

1. PGI clairement défini et connu des intervenants concernés (O/N)
2. Activités de prévention des incidents sont en place (O/N)
3. Activités de détection des incidents sont en place (O/N)
4. Activités de réaction aux incidents sont prévues (O/N)
5. Activités de rétablissement après incidents sont prévues (O/N)
6. Activités de suivi des incidents sont prévues (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion des incidents de sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind7 = 0 %

Si (1 = « Oui ») et (2 = « Non »)) alors Ind7 = 15 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind7 = 30 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non »)) alors Ind7 = 50 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Non »)) alors Ind7 = 75 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Non »)) alors Ind7 = 90 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui »)) alors Ind7 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** COGI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, COGI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « gestion de risques », « gestion des incidents », « audit de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (20 %, 50 %, 70 %, etc.).	✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind7 = 0 %, Alarme : « Définissez clairement le PGI de SI avant la Date_cible ». ✓ SI Ind7 = 15 %, Alarme : «Mettez en place les activités de prévention avant la Date_cible ». ✓ SI Ind7 = 30 %, Alarme : « Mettez en place les activités de détection avant la Date_cible ». ✓ Si Ind7 = 50 %, Alarme : « Prévoyez les activités de réaction aux incidents avant la Date_cible ». ✓ SI Ind7 = 75 %, Alarme : « Prévoyez les activités de rétablissement après incident avant la Date_cible ». ✓ Si Ind7 = 90 %, Alarme : « Prévoyez les activités de suivi des incidents avant la Date_cible ». ✓ Si Ind7 = 100 %, Signal : « La mise en œuvre du processus de gestion des incidents de SI est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind7 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 8

Nº indicateur : 8

Désignation : Ind8

Libellé : Degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion de l'accès à l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer de la mise en œuvre d'un processus formel de sécurité de l'information permettant d'assurer la gestion de l'accès à l'information ».

Objectif : S'assurer qu'un processus formel de gestion de l'accès à l'information est mis en œuvre.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Mettre en œuvre des processus formels de gestion de la sécurité de l'information.

Cible gouvernementale :

- ✓ 75 % des OP de grande taille et 25 % des OP de taille moyenne auront mis en œuvre un processus formel de gestion de l'accès à l'information d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille, 75 % des OP de taille moyenne et 50 % des OP de petite taille auront mis en œuvre un processus formel de gestion de l'accès à l'information d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront mis en œuvre un processus formel de gestion de l'accès à l'information d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind8 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind8 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind8 < 85 %

Calcul de l'indicateur

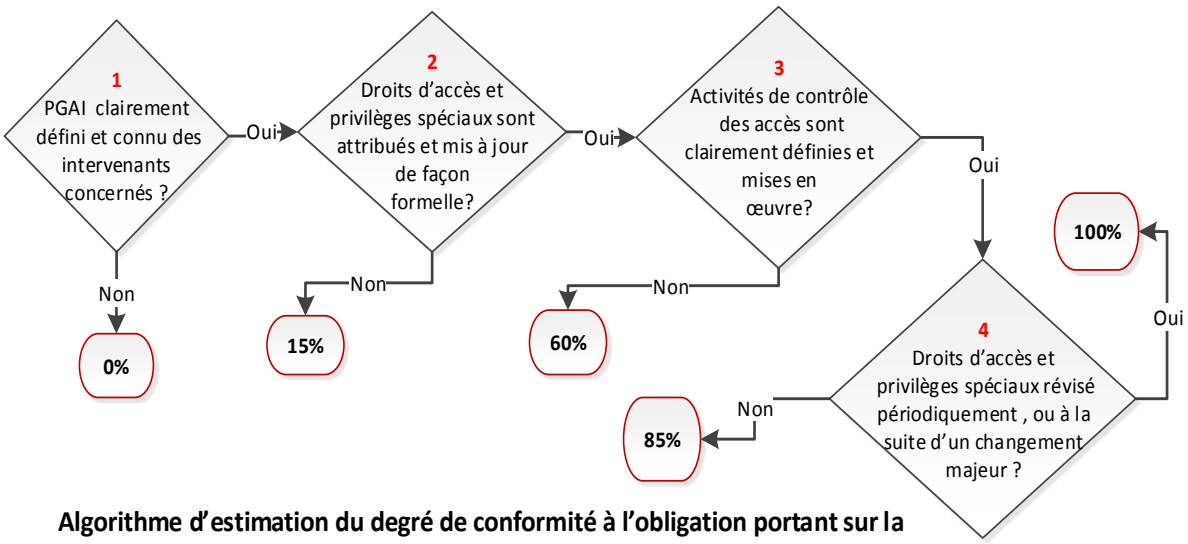
Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

PGAI = Processus de gestion de l'accès à l'information

1. PGAI clairement défini et connu des intervenants concernés (O/N)
2. Droits d'accès et privilèges spéciaux sont attribués et mis à jour de façon formelle (identités, rôles, profils, politique des mots de passe, séparation des pouvoirs, journalisation, etc.) (O/N)
3. Les activités de contrôle des accès sont clairement définies et mises en œuvre (O/N)
4. Droits d'accès et privilèges spéciaux révisés périodiquement ou à la suite d'un changement majeur (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la mise en œuvre d'un processus formel de gestion de l'accès à l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind8 = 0 %

Si (1 = « Oui ») et (2 = « Non »)) alors Ind8 = 15 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind8 = 60 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non »)) alors Ind8 = 85 %

Si (1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui »)) alors Ind8 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, COGI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « gestion de risques », « gestion des incidents », « audit de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (20 %, 50 %, 70 %, etc.).	**Règle d'interprétation :** ✓ Si OP de grande taille alors Date_cible = 31 mars 2016, Sinon Date_cible = 31 mars 2017. ✓ Si Ind8 = 0 %, Alarme : « Définir clairement un processus de contrôle des accès, avant la Date_cible ». ✓ Si Ind8 = 15 %, Alarme : « Gérez de façon formelle les droits d'accès et les privilèges spéciaux, avant la Date_cible ». ✓ Si Ind8 = 60 %, Alarme : « Définir clairement les activités de contrôle des accès, avant la Date_cible ». ✓ Si Ind8 = 85 %, Alarme : « Révisez les droits d'accès et les privilèges spéciaux périodiquement, ou à la suite d'un changement majeur, avant la Date_cible ». ✓ Si Ind8 = 100 %, Signal : « La mise en œuvre du processus de gestion des accès à l'information est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind8 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 9

Nº indicateur : 9

Désignation : Ind9

Libellé : Degré de conformité à l'obligation portant sur l'intégration des clauses contractuelles de sécurité de l'information, dans les contrats et ententes.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer que les ententes de service et les contrats, conclus avec les prestataires de services, les partenaires et les mandataires, stipulent des clauses garantissant le respect des exigences de sécurité de l'information ».

Objectif : S'assurer que les clauses contractuelles de sécurité de l'information sont intégrées aux ententes et aux contrats conclus avec les prestataires de services, les partenaires et les mandataires.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, Service de gestion des contrats et ententes, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Se conformer aux bonnes pratiques de sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront intégré les clauses contractuelles de sécurité de l'information à leurs ententes ou leurs contrats d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront intégré les clauses contractuelles de sécurité de l'information à leurs ententes ou leurs contrats d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront intégré les clauses contractuelles de sécurité de l'information à leurs ententes ou leurs contrats d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind9 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind9 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind9 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind9 < 85 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

A. Nombre de contrats et ententes conclus depuis la date de la mise en œuvre de la directive
B. Nombre de contrats et ententes incluant les clauses sur le « respect des règles de sécurité de l'information »
C. Nombre de contrats et ententes incluant les clauses sur les « mesures de sécurité de l'information »
D. Nombre de contrats et ententes incluant les clauses sur la « sécurité des accès »
E. Nombre de contrats et ententes incluant les clauses sur la « confidentialité »

Algorithme de calcul :

s. o.

Formule/Pondération :

Ind9 = (B / A) * 15% + (C / A) * 15% + (C / A) * 20% + (E / A) * 50%, avec A > 0

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Service de gestion des contrats et ententes
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, Service de gestion des contrats et ententes
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « diagramme linéaire » dont l'axe des ordonnées représentera le taux d'intégration des clauses contractuelles de sécurité de l'information aux contrats et ententes conclus depuis la date de mise en vigueur de la directive (janvier 2014) et l'axe des abscisses, les dates de collecte trimestrielle couvrant une période choisie par l'OP ou allant au moins jusqu'à la date ciblée dans l'approche stratégique (Date_cible). Au niveau de la fenêtre principale du tableau de bord, cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « audit de sécurité de l'information », « tests d'intrusions et de vulnérabilités », « architecture de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind9 = 0 %, Alarme : « C'est très important d'intégrer les clauses contractuelles de sécurité de l'information à vos ententes et contrats, avant ou à la Date_cible ». ✓ SI Ind9 < 85 % et Ind9 # 0, Alarme : « C'est très important d'intégrer davantage de clauses contractuelles de sécurité de l'information à vos ententes et contrats, avant ou à la Date_cible ». ✓ SI 85 % < Ind9 < 100%, Signal : « Le taux d'intégration des clauses contractuelles de sécurité de l'information aux ententes et contrats est acceptable ». ✓ Si Ind9 < 100 %, Signal : « L'intégration des clauses contractuelles de sécurité de l'information aux ententes et contrats est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind9 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 10

Nº indicateur : 10

Désignation : Ind10

Libellé : Degré de conformité à l'obligation portant sur la réalisation d'un audit en sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer de la réalisation d'un audit de sécurité de l'information, selon une périodicité bisannuelle ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégager les priorités d'action ainsi que les échéanciers afférents ».

Objectif : S'assurer de réaliser au moins un audit en sécurité de l'information tous les deux ans, ou à la suite d'un changement majeur.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Se conformer aux bonnes pratiques de sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront effectué un audit de sécurité de l'information au cours des deux dernières années d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront effectué un audit de sécurité de l'information au cours des deux dernières années d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront effectué un audit de sécurité de l'information au cours des deux dernières années d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind10 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind10 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind10 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind10 < 80 %

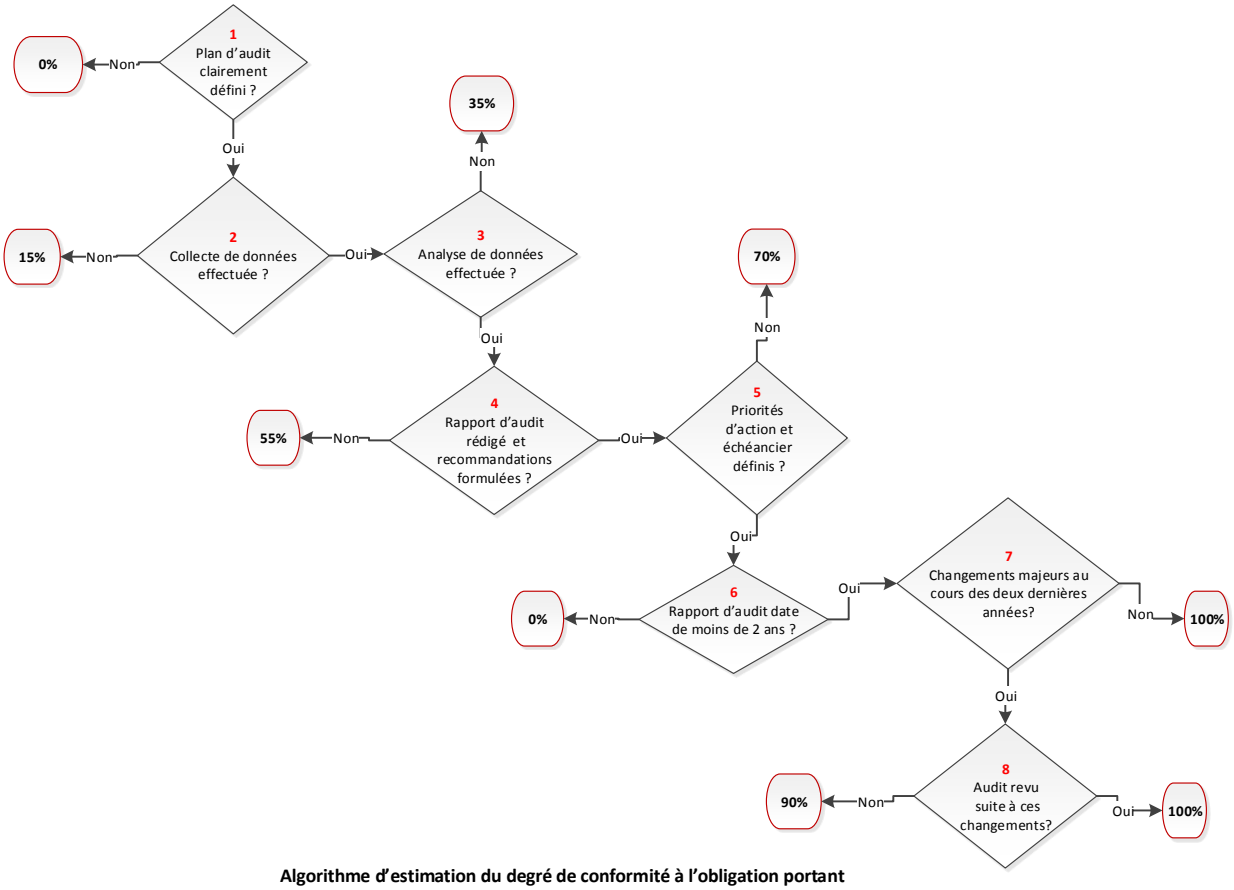
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Plan d'audit clairement défini (O/N)
2. Collecte de données effectuée (O/N)
3. Analyse de données effectuée (O/N)
4. Rapport d'audit rédigé et recommandations formulées (O/N)
5. Priorités d'action et échéanciers définis (O/N)
6. Rapport d'audit date de moins de deux ans (O/N)
7. Changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, survenu au cours des deux dernières années (O/N)
8. Audit revu à la suite de ces changements (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la réalisation d'un audit de sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind10 = 0 %

Si ((1 = « Oui ») et (2 = « Non »)) alors Ind10 = 15 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind10 = 35 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non »)) alors Ind10 = 55 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Non »)) alors Ind10 = 70 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Non »)) alors Ind10 = 0 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Non »)) alors Ind10 = 100 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Oui ») et (8 = « Non »)) alors Ind10 = 90 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Oui ») et (8 = « Oui »)) alors Ind10 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, Service de sécurité de l'information
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « audit de sécurité de l'information », « tests d'intrusions et de vulnérabilités », « architecture de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind10 = 0 %, Alarme : « Définissez clairement un plan d'audit en sécurité de l'information, avant ou à la date de la cible ». ✓ SI Ind10 = 15 %, Alarme : « Réalisez la collecte des données pour l'audit, avant la Date_cible ». ✓ Si Ind10 = 35 %, Alarme : « Réalisez l'analyse de données pour l'audit, avant la Date_cible ». ✓ Si Ind10 = 55 %, Alarme : « Rédigez le rapport d'audit et formulez les recommandations, avant la Date_cible ». ✓ Si Ind10 = 70 %, Alarme : « Définissez les priorités d'action et les échéanciers afférents, avant la Date_cible ». ✓ Si Ind10 = 90 %, Alarme : « Révisez l'audit à la suite de changements majeurs au cours des 2 dernières années, avant la Date_cible ». ✓ Si Ind10 = 100 %, Signal : « La réalisation de l'audit en sécurité de l'information est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind10 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 11

Nº indicateur : 11

Désignation : Ind11

Libellé : Degré de conformité à l'obligation portant sur la réalisation des tests d'intrusion et de vulnérabilité en sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer de la réalisation de tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégager les priorités d'action ainsi que les échéanciers afférents ».

Objectif : S'assurer de réaliser au moins un test d'intrusion et de vulnérabilité en sécurité de l'information chaque année, ou à la suite d'un changement majeur.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Se conformer aux bonnes pratiques de sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront effectué annuellement un test d'intrusion et de vulnérabilité en sécurité de l'information d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront effectué annuellement un test d'intrusion et de vulnérabilité en sécurité de l'information d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront effectué annuellement un test d'intrusion et de vulnérabilité en sécurité de l'information d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind11 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind11 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind11 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind11 < 80 %

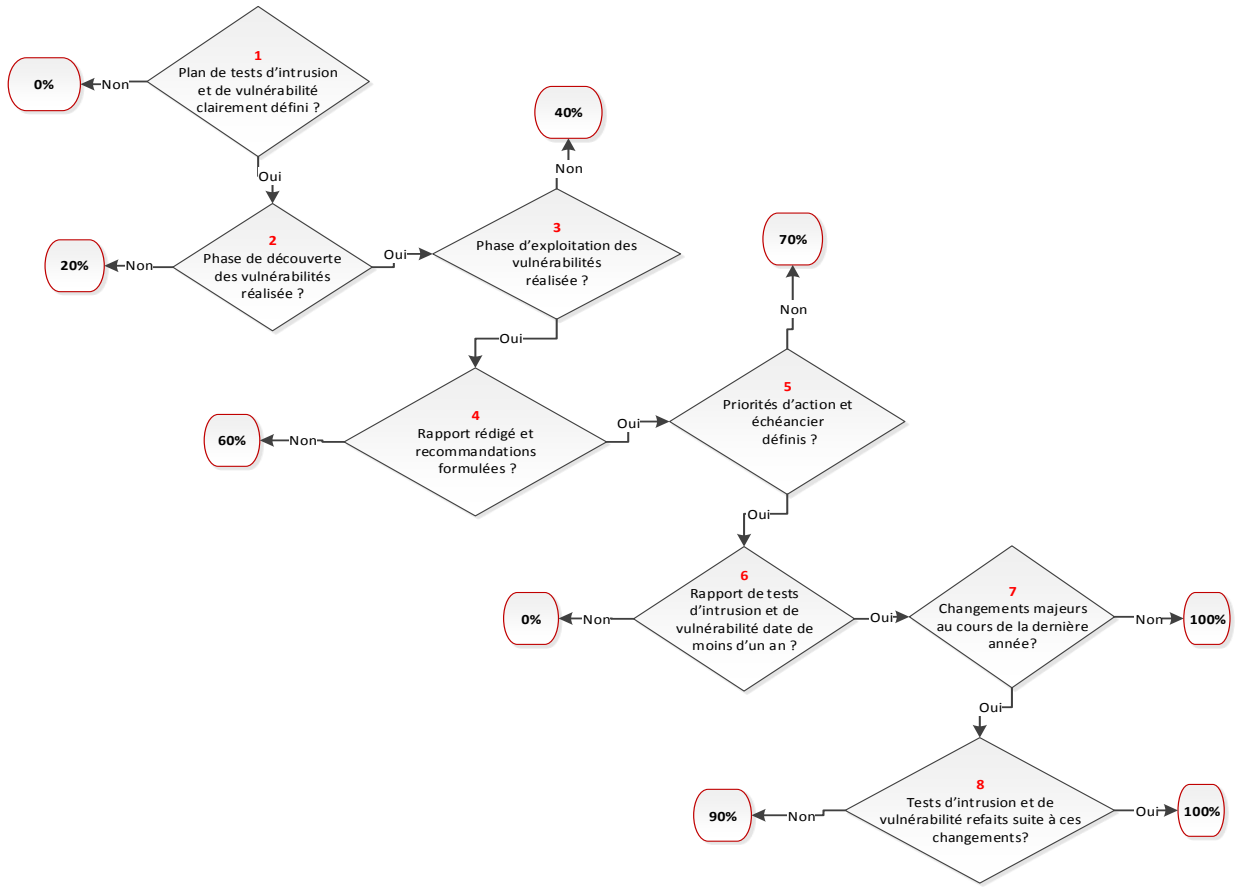
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Plan de tests d'intrusion et de vulnérabilité clairement défini (O/N)
2. Phase de découverte des vulnérabilités réalisée (O/N)
3. Phase d'exploitation des vulnérabilités réalisée (O/N)
4. Rapport des tests d'intrusion et de vulnérabilité rédigé et recommandations formulées (O/N)
5. Priorités d'action et échéanciers définis (O/N)
6. Rapport de tests d'intrusion et de vulnérabilité date de moins d'un an (O/N)
7. Changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information, survenu depuis moins d'un an (O/N)
8. Tests d'intrusion et de vulnérabilité refaits à la suite de ces changements (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la réalisation de tests d'intrusion et de vulnérabilité en sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind11 = 0 %

Si ((1 = « Oui ») et (2 = « Non ») alors Ind11 = 20 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non ») alors Ind11 = 40 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») alors Ind11 = 60 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Non ») alors Ind11 = 70 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Non ») alors Ind11 = 0 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Non ») alors Ind11 = 100 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Oui ») et (8 = « Non ») alors Ind11 = 90 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») et (5 = « Oui ») et (6 = « Oui ») et (7 = « Oui ») et (8 = « Oui ») alors Ind11 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « audit en sécurité de l'information », « tests d'intrusion et de vulnérabilité », « architecture de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind11 = 0 %, Alarme : « Définissez annuellement et clairement un plan de test d'intrusion et de vulnérabilité, avant la Date_cible ». ✓ Si Ind11 = 20 %, Alarme : «Réalisez la phase de découverte des vulnérabilités, avant la Date_cible ». ✓ Si Ind11 = 40 %, Alarme : « Réalisez la phase d'exploitation des vulnérabilités avant la Date_cible ». ✓ Si Ind11 = 60 %, Alarme : « Rédigez le rapport des tests et formulez les recommandations, avant la Date_cible ». ✓ Si Ind11 = 70 %, Alarme : « Définissez les priorités d'action et les échéanciers afférents, avant la Date_cible ». ✓ Si Ind11 = 90 %, Alarme : « Refaites les tests d'intrusion et de vulnérabilité à la suite des changements majeurs de la dernière année, avant la Date_cible ». ✓ Si Ind11 = 100 %, Signal : « La réalisation des tests d'intrusion et de vulnérabilité en sécurité de l'information est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind10 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 12

Nº indicateur : 12

Désignation : Ind12

Libellé : Degré de conformité à l'obligation portant sur la mise en place d'un registre d'autorité de la sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « S'assurer de la mise en place d'un registre d'autorité de la sécurité de l'information. Sont notamment consignés, dans ce registre, les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information ».

Objectif : S'assurer de mettre en place un registre d'autorité dans lequel sont consignés les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés, ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Se conformer aux bonnes pratiques de sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront mis en place un registre d'autorité de la sécurité de l'information d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront mis en place un registre d'autorité de la sécurité de l'information d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront mis en place un registre d'autorité de la sécurité de l'information d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind12 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind12 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind12 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind12 < = 100 %

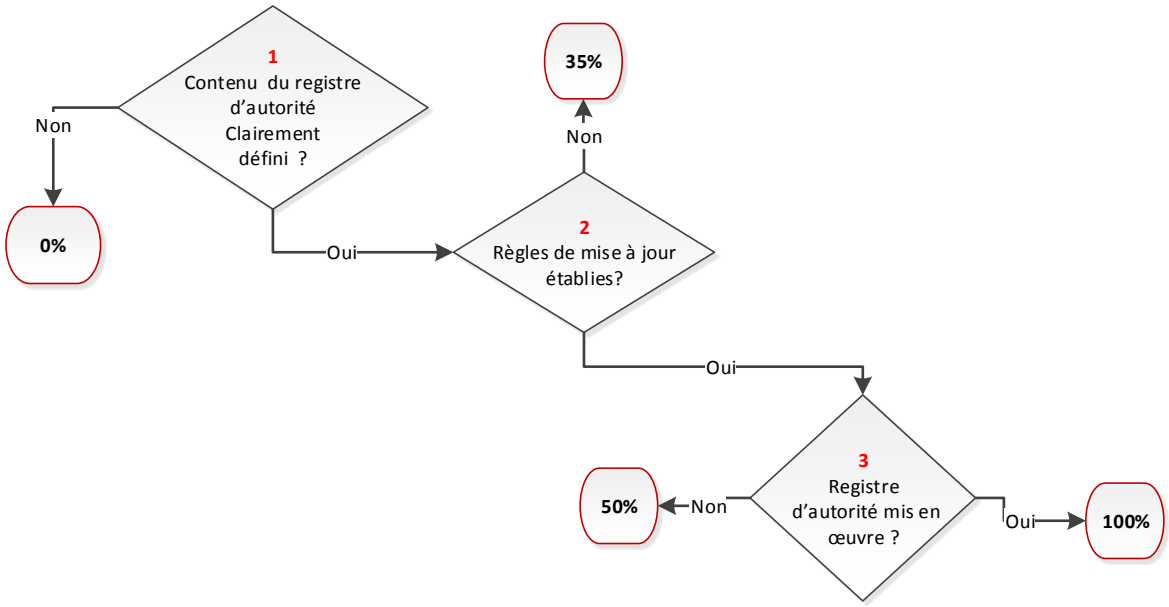
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Contenu du registre d'autorité clairement défini (O/N)
2. Règles de mise à jour du registre établies (O/N)
3. Registre d'autorité mis en œuvre (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la mise en place d'un registre d'autorité de la sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind12 = 0 %

Si ((1 = « Oui ») et (2 = « Non »)) alors Ind12 = 35 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind12= 50 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui »)) alors Ind12 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Au niveau de la fenêtre principale du tableau de bord, cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « audit en sécurité de l'information », « tests d'intrusion et de vulnérabilité », « architecture de sécurité de l'information », etc.) et, pour axe des , le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind12 = 0 %, Alarme : « Définissez clairement le contenu du registre d'autorité, avant la Date_cible ». ✓ Si Ind12 = 35 %, Alarme : « Établissez les règles de mise à jour du registre d'autorité, avant la Date_cible ». ✓ Si Ind12 = 50 %, Alarme : « Mettez en œuvre le registre d'autorité, avant la Date_cible ». ✓ Si Ind12 = 100 %, Signal : « La mise en place du registre d'autorité est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind10 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 13

Nº indicateur : 13

Désignation : Ind13

Libellé : Degré de conformité à l'exigence portant sur l'adoption d'une architecture de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'exigence d'adopter une architecture de sécurité de l'information.

Objectif : Adopter et mettre en place une architecture de sécurité de l'information et s'assurer de sa mise à jour.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Atteindre un niveau de maturité adéquat en sécurité de l'information.

Objectif gouvernemental : Se conformer aux bonnes pratiques de sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront adopté une architecture de sécurité de l'information d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront adopté une architecture de sécurité de l'information d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront adopté une architecture de sécurité de l'information d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind13 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind13 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind13 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind13 <= 75 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

A. Existe-t-il une architecture de sécurité de l'information documentée? (Oui = 1, Non = 0)

B. Un cadre d'architecture de SI et une méthodologie sont-ils utilisés? (Oui = 1, Non = 0)

C. Les travaux d'architecture (de la conception à l'implantation) sont-ils intégrés au programme de sécurité de l'information de l'OP ou à la planification triennale des travaux? (Oui = 1, Non = 0)

D. L'architecture de sécurité de l'information est-elle arrimée au processus d'amélioration continue de la sécurité de l'information de l'OP? (Oui = 1, Non = 0)

E. Les orientations, les principes, les normes et les standards de sécurité de l'information en usage découlent-ils de l'architecture de sécurité de l'information? (Oui = 1, Non = 0)

F. Les mesures de sécurité de l'information découlent-elles des orientations, des principes, des normes et des standards définis à l'architecture? (Oui = 1, Non = 0)

Algorithme de calcul :

Répondre aux questions énumérées dans la section « Éléments de calcul » et attribuer la valeur correspondante à chaque réponse.

Formule/Pondération :

Ind13 = A*20 % + B*15 % + C*20 % + D*15 % + E*15 % + F*15 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** ROSI, architecte de sécurité de l'information
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, architecte de sécurité de l'information
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Au niveau de la fenêtre principale du tableau de bord, cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Atteindre un niveau de maturité adéquat en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « audit de sécurité de l'information », « tests d'intrusion et de vulnérabilité », « architecture de sécurité de l'information », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (35 %, 50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. ✓ Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si ((Ind13 < 100 %) et ((Date_Système < Date_cible)), alors : ▪ Si A = « Non » : Signal : « Il est important d'avoir une architecture de sécurité documentée, avant la date de la cible ». ▪ Si B = « Non » : Signal : « Il est important d'utiliser un cadre d'architecture et une méthodologie, avant la date de la cible ». ▪ Si C = « Non » : Signal : « Il est important d'intégrer les travaux d'architecture au programme de sécurité de l'information, ou à la planification triennale, avant la date de la cible ». ▪ Si D = « Non » : Signal : « L'architecture de sécurité documentée doit être arrimée au processus d'amélioration continue de la sécurité de l'information, avant la date de la cible ». ▪ Si E = « Non » : Signal : « Les orientations, principes, normes et standards de sécurité de l'information en usage doivent découler de l'architecture de sécurité, avant la date de la cible ». ▪ Si F = « Non » : Signal : « Les mesures de sécurité de l'information doivent découler des orientations, principes, normes et standards définis à l'architecture, avant la date de la cible ». ✓ Si Ind13 = 100 %, Signal : « L'architecture de SI est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind13 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 14

Nº indicateur : 14

Désignation : Ind14

Libellé : Taux de participation de l'organisme public au réseau d'alerte gouvernemental depuis le 1er avril 2014.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le taux de participation de l'organisme public au réseau d'alerte gouvernemental, depuis le 1er avril 2014.

Objectif : S'assurer de contribuer aux activités du réseau d'alerte gouvernemental.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Renforcer l'encadrement de la sécurité de l'information.

Objectif gouvernemental : Participer activement au réseau d'alerte gouvernemental.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques ainsi que ceux de grande taille auront participé au réseau d'alerte gouvernemental d'ici le 31 mars 2015;
- ✓ Tous les OP (100 %) auront participé au réseau d'alerte gouvernemental d'ici le 31 mars 2016.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind14 > 75 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques ou si l'OP est de grande taille

Ind14 > 75 % d'ici le 31 mars 2016 pour tout OP

Seuil d'alerte : Ind14 < 75 %

Calcul de l'indicateur

Mesure (unité) : %

Type de mesure : dérivée

Éléments de calcul :

A. L'OP a-t-il désigné un participant au réseau d'alerte dans la liste « alerte.ra »? (Oui = 15 %, Non = 0 %)
B. Nombre de conférences organisées par le réseau d'alerte depuis le 1er avril 2014
C. Nombre de conférences auxquelles l'OP a participé depuis le 1er avril 2014

Algorithme de calcul :

Répondre à la question A de la section « Éléments de calcul » et attribuer la valeur correspondante.

Formule/Pondération :

Ind14 = [(C / B) x 85 %] + [A], avec B > 0, C <= B

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** COGI
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, COGI
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « diagramme linéaire » dont l'axe des ordonnées représentera les taux de participation au réseau d'alerte gouvernemental de sécurité de l'information et l'axe des abscisses, les dates de collecte trimestrielle couvrant une période choisie par l'OP ou débutant le 1er avril 2014. Au niveau de la fenêtre principale du tableau de bord, cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Renforcer l'encadrement de la sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « participation au réseau d'alerte gouvernemental », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, 100 %).	✓ Si (OP fortement exposé aux risques ou OP de grande taille) alors Date_cible = 31 mars 2015. Sinon (Date_cible = 31 mars 2016). ✓ Si Ind14 = 0 %, Alarme : « C'est très important de désigner un participant au réseau d'alerte gouvernemental et de participer à ce réseau avant la Date_cible ». ✓ Si (Ind14 < 75 % et Ind14 # 0), Alarme : « C'est très important de participer davantage au réseau d'alerte gouvernemental ». ✓ Si Ind14 >= 75 %, Signal : « Le taux de participation au réseau d'alerte gouvernemental est acceptable ». ✓ Si ((Date_Système > Date_cible) et (Ind14 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 15

Nº indicateur : 15

Désignation : Ind15

Libellé : Taux d'adhésion des nouvelles PES transactionnelles à clicSÉQUR.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le taux d'adhésion des nouvelles PES transactionnelles au service d'authentification gouvernementale clicSÉQUR depuis le 1er avril de l'année en cours.

Objectif : S'assurer de l'adhésion des nouvelles PES transactionnelles au service d'authentification gouvernementale.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Développer l'offre de service d'authentification gouvernementale.

Objectif gouvernemental : Augmenter l'utilisation des services d'authentification gouvernementale par les organismes publics.

Cible gouvernementale :

✓ 80 % des nouvelles PES transactionnelles utilisent clicSÉQUR.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind15 = 100 %

Seuil d'alerte : Ind15 < 80 %

Calcul de l'indicateur

Mesure (unité) : %

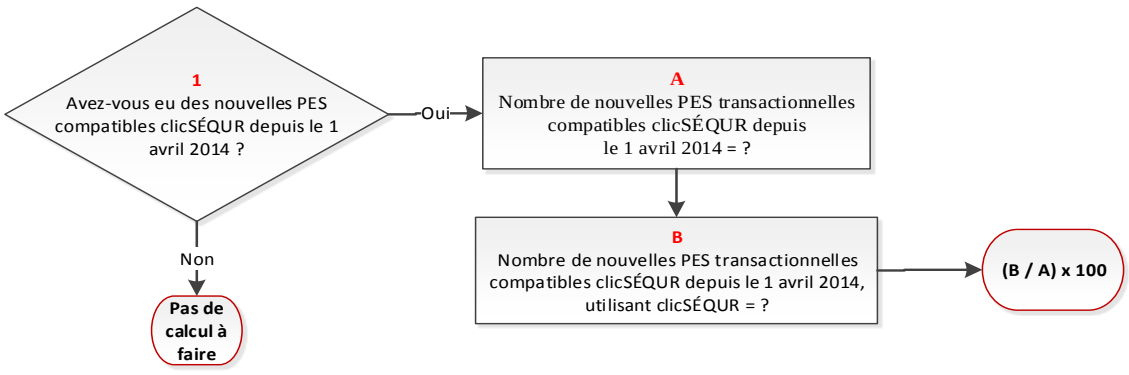
Type de mesure : dérivée

Éléments de calcul :

A. Nombre de nouvelles PES transactionnelles adhérant à clicSÉQUR depuis le 1er avril 2014

B. Nombre de nouvelles PES transactionnelles adhérant à clicSÉQUR depuis le 1er avril 2014, utilisant clicSÉQUR.

Algorithme de calcul :



Algorithme d'estimation du taux d'adhésion des nouvelles PES transactionnelles à clicSÉQUR

Formule/Pondération :

Si (1 = « Non ») alors Ind15 = «-1 »

Si (1 = « Oui »), alors Ind15 = (B / A) x 100, avec A > 0 et B <= A

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Détenteur des prestations électroniques de services
Fréquence de collecte : semestrielle	**Source de données :** Service de prestation électronique de services
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « diagramme linéaire » dont l'axe des ordonnées représentera le taux d'adhésion des nouvelles PES transactionnelles à ClicSÉQUR et l'axe des abscisses, les dates de collecte semestrielle. Le diagramme devra afficher le taux d'adhésion sur une période choisie par l'OP. Au niveau de la fenêtre principale du tableau de bord, il sera représenté par une barre dans le diagramme à barres représentant les objectifs de l'orientation « Développer l'offre de service d'authentification gouvernementale ».	**Règle d'interprétation :** ✓ Si Ind15 = « -1 », Signal : « Aucune PES » ✓ Si Ind15 = 0 %, Alarme : « Il est important d'intégrer le service d'authentification gouvernementale aux nouvelles PES transactionnelles compatibles avec clicSÉQUR ». ✓ Si Ind15 < 80 % et Ind15 # 0 %, Alarme : « Il est important d'intégrer le service d'authentification gouvernementale à toutes les nouvelles PES transactionnelles compatibles avec clicSÉQUR ». ✓ Si Ind15 >= 80 %, Alarme : « Le taux d'intégration du service d'authentification gouvernementale aux nouvelles PES transactionnelles compatibles avec clicSÉQUR est acceptable ».

Fiche descriptive d’indicateur numéro 16

Nº indicateur : 16

Désignation : Ind16

Libellé : Degré de conformité à l'obligation portant sur la mise en place d'un plan de sensibilisation de l'ensemble du personnel en matière de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « Définir et mettre en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information ».

Objectif : S'assurer que l'ensemble du personnel est sensibilisé en matière de sécurité de l'information.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Développer et maintenir les compétences en sécurité de l'information.

Objectif gouvernemental : Sensibiliser le personnel à la sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront mis en place un plan de sensibilisation en matière de sécurité de l'information pour l'ensemble de leur personnel d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront mis en place un plan de sensibilisation en matière de sécurité de l'information pour l'ensemble de leur personnel d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront mis en place un plan de sensibilisation en matière de sécurité de l'information pour l'ensemble de leur personnel d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind16 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind16 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind16 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind16 < 75 %

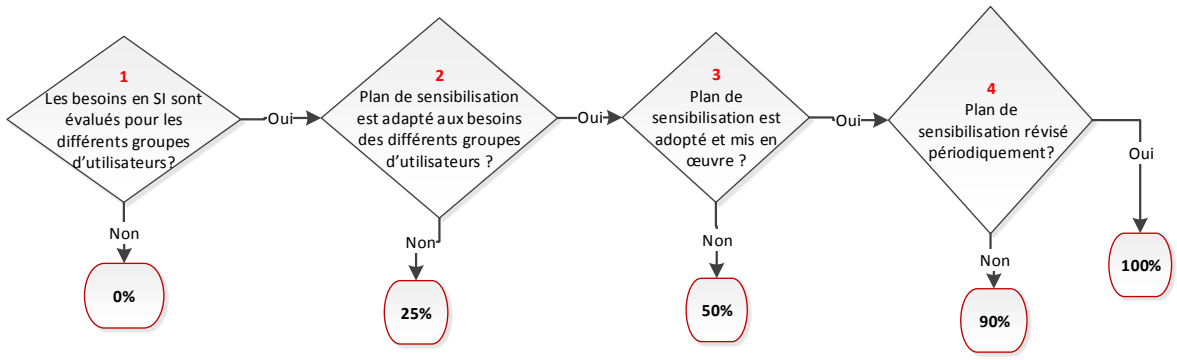
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Les besoins en sécurité sont évalués pour les différents groupes d'utilisateurs (O/N)
2. Le plan de sensibilisation est adapté aux besoins des différents groupes d'utilisateurs (O/N)
3. Le plan de sensibilisation est adopté et mis en œuvre (O/N)
4. Le plan de sensibilisation est révisé périodiquement (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'exigence portant sur la mise en place d'un plan de sensibilisation de l'ensemble du personnel en matière de sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind16 = 0 %

Si ((1 = « Oui ») et (2 = « Non »)) alors Ind16 = 25 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non »)) alors Ind16 = 50 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non »)) alors Ind16 = 90 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui »)) alors Ind16 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Service de formation
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, Service de formation
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Développer et maintenir les compétences en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « formation ROSI », « formation COGI », « sensibilisation du personnel », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind16 = 0 %, Alarme : « Définissez les besoins en SI pour les différents groupes d'utilisateurs, avant la Date_cible ». ✓ Si Ind16 = 25 %, Alarme : « Adaptez le plan de sensibilisation aux besoins des différents groupes d'utilisateurs, avant la Date_cible ». ✓ Si Ind16 = 50 %, Alarme : « Adoptez et mettez en œuvre le plan de sensibilisation avant la Date_cible ». ✓ Si Ind16 = 90 %, Alarme : « Le plan de sensibilisation doit être révisé périodiquement avant la Date_cible ». ✓ Si Ind16 = 100 %, Signal : « La mise en place du plan de sensibilisation de l'ensemble du personnel est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind16 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 17

Nº indicateur : 17

Désignation : Ind17

Libellé : Taux du personnel ayant suivi une première session de sensibilisation à la sécurité de l'information de l'ensemble du personnel.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité à l'exigence de réaliser une première session de sensibilisation à la sécurité de l'information de l'ensemble du personnel.

Objectif : S'assurer que l'ensemble du personnel a suivi une première session de sensibilisation à la sécurité de l'information avant la date ciblée dans l'approche stratégique gouvernementale.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Développer et maintenir les compétences en sécurité de l'information.

Objectif gouvernemental : Sensibiliser le personnel à la sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront offert une première session de sensibilisation à la sécurité de l'information à l'ensemble du personnel d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront offert une première session de sensibilisation à la sécurité de l'information à l'ensemble du personnel d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront offert une première session de sensibilisation à la sécurité de l'information à l'ensemble du personnel d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind17 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind17 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind17 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind17 < 100 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

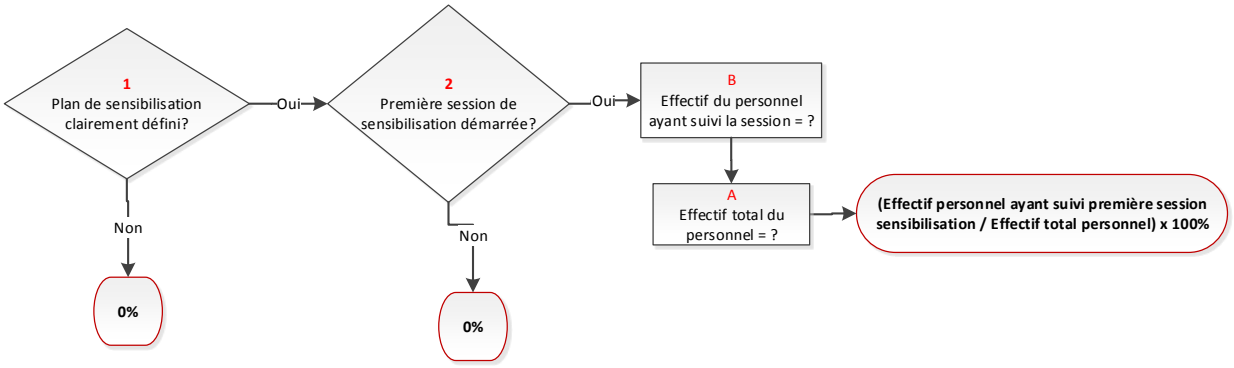
Éléments de calcul :

1. Plan de sensibilisation clairement défini (O/N)
2. Première session de sensibilisation démarrée (O/N)

A. EffectifTotalPersonnel

B. EffectifPersonnel_AyantSuiviPremièreSessionSensibilisation_SI

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'exigence portant sur la réalisation d'une première session de sensibilisation du personnel à la sécurité de l'information

Formule/Pondération :

Si (1 = « Non ») alors Ind17 = 0 %

Si (1 = « Oui ») et (2 = « Non »)) alors Ind17 = 0 %

Si (1 = « Oui ») et (2 = « Oui »)) alors Ind17 = (B/A) x 100 %, avec A > 0 et B <= A

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Service de formation, RH
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, Service de formation
Méthode de collecte : manuelle, automatique	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « diagramme linéaire » dont l'axe des ordonnées représentera le taux du personnel ayant suivi une première session de sensibilisation et l'axe des abscisses, les dates de collecte trimestrielle sur une période choisie par l'OP. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Développer et maintenir les compétences en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « formation ROSI », « formation COGI », « sensibilisation personnel », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind17 = 0 %, Alarme : « Définissez clairement un plan de sensibilisation du personnel et démarrez la première session de sensibilisation, avant la Date_cible ». ✓ Si Ind17 > 0 %, et Ind18 < 100 %, Alarme : « Il est important que l'ensemble du personnel suive la première session de sensibilisation, avant la Date_cible ». ✓ Si Ind17 = 100 %, Signal : « Le taux de sensibilisation de l'ensemble du personnel est conforme ». ✓ Si ((Date_Système > Date_cible) et (Ind17 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 18

Nº indicateur : 18

Désignation : Ind18

Libellé : Degré de conformité à l'obligation portant sur le programme formel de formation de l'ensemble du personnel.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'obligation « Définir et mettre en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information ».

Objectif : S'assurer que l'ensemble du personnel est formé en matière de sécurité de l'information.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Développer et maintenir les compétences en sécurité de l'information.

Objectif gouvernemental : Accroître l'expertise et le savoir-faire en sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des OP fortement exposés aux risques auront mis en œuvre un programme formel de formation de l'ensemble du personnel d'ici le 31 mars 2015;
- ✓ 100 % des OP de grande taille auront mis en œuvre un programme formel de formation de l'ensemble du personnel d'ici le 31 mars 2016;
- ✓ Tous les OP (100 %) auront mis en œuvre un programme formel de formation de l'ensemble du personnel d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind18 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind18 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind18 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind18 < 75 %

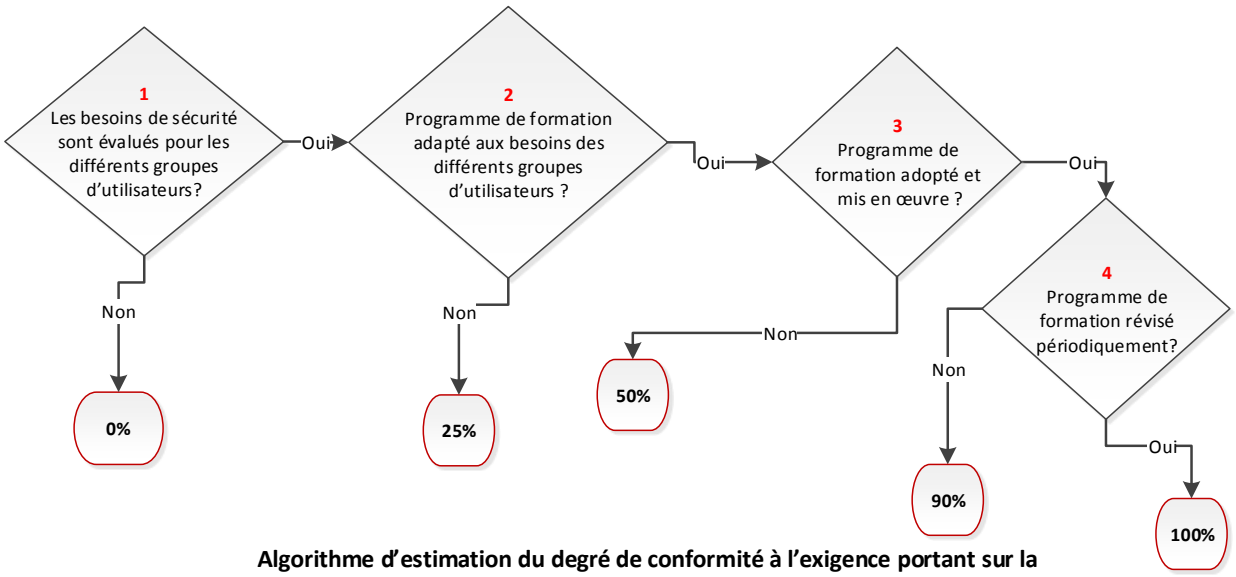
Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

Éléments de calcul :

1. Les besoins en sécurité sont évalués pour les différents groupes d'utilisateurs (O/N)
2. Le programme de formation est adapté aux besoins des différents groupes d'utilisateurs (O/N)
3. Le programme de formation est adopté et mis en œuvre (O/N)
4. Le programme de formation est révisé périodiquement (O/N)

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'exigence portant sur la mise en œuvre d'un programme formel de formation de l'ensemble du personnel

Formule/Pondération :

Si (1 = « Non ») alors Ind18 = 0 %

Si ((1 = « Oui ») et (2 = « Non ») alors Ind18 = 25 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Non ») alors Ind18 = 50 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Non ») alors Ind18 = 90 %

Si ((1 = « Oui ») et (2 = « Oui ») et (3 = « Oui ») et (4 = « Oui ») alors Ind18 = 100 %

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Service de formation
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, Service de formation
Méthode de collecte : manuelle, automatique	**Date de collecte :** jj/mm/aaaa

Format d'illustration :	**Règle d'interprétation :**
Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Développer et maintenir les compétences en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « formation ROSI », « formation COGI », « sensibilisation personnel », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, etc.).	✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind18 = 0 %, Alarme : « Définissez les besoins en SI pour les différents groupes d'utilisateurs, avant la Date_cible ». ✓ Si Ind18 = 25 %, Alarme : « Adaptez le programme de formation aux besoins des différents groupes d'utilisateurs, avant la Date_cible ». ✓ Si Ind18 = 50 %, Alarme : « Adoptez et mettez en œuvre le programme de formation avant la Date_cible ». ✓ Si Ind18 = 90 %, Alarme : « Le programme de formation doit être révisé périodiquement avant la Date_cible ». ✓ Si Ind18 = 100 %, Signal : « La mise en place du programme de formation de l'ensemble du personnel est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind18< 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 19

Nº indicateur : 19

Désignation : nd19

Libellé : Degré de conformité à l'exigence portant sur la formation générale du ROSI en matière de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'exigence sur la formation du ROSI.

Objectif : S'assurer que le ROSI développe et maintient ses connaissances et compétences en sécurité de l'information.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Développer et maintenir les compétences en sécurité de l'information.

Objectif gouvernemental : Accroître l'expertise et le savoir-faire en sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des ROSI des OP fortement exposés aux risques auront suivi au moins une formation générale en sécurité de l'information d'ici le 31 mars 2015;
- ✓ 100 % des ROSI des OP de grande taille auront suivi au moins une formation générale en sécurité de l'information d'ici le 31 mars 2016;
- ✓ 100 % des ROSI de tous les OP auront suivi au moins une formation générale en sécurité de l'information d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind19 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind19 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind19 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind19 < 100 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

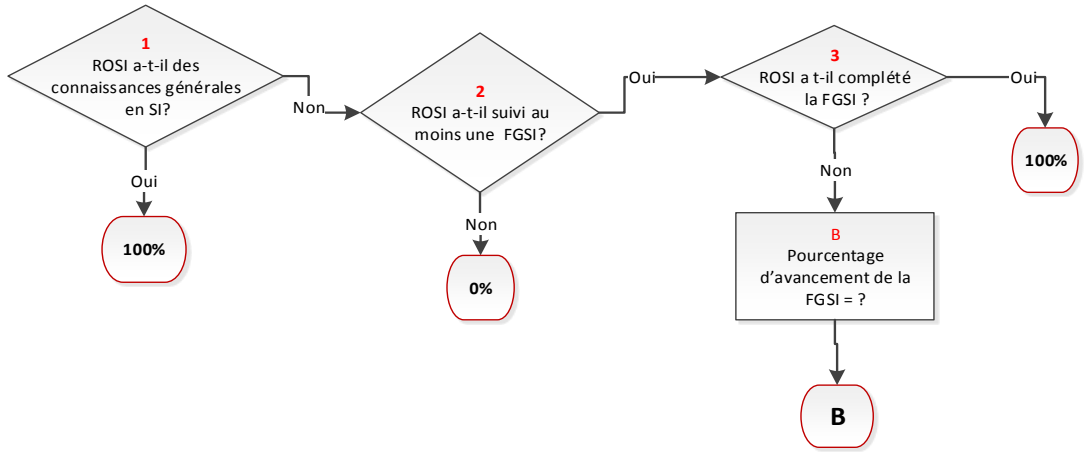
Éléments de calcul :

FGSI = Formation générale en sécurité de l'information

1. Le ROSI a-t-il des connaissances générales en sécurité de l'information? (O/N)
2. Le ROSI a-t-il suivi au moins une FGSI? (O/N)
3. Le ROSI a-t-il complété la FGSI? (O/N)

B. Pourcentage d'avancement de la FGSI

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la participation du ROSI à une formation générale en sécurité de l'information

Formule/Pondération :

Si (1 = « Oui ») alors Ind19 = 100 %

Si ((1 = « Non ») et (2 = « Non »)) alors Ind19 = 0 %

Si ((1 = « Non ») et (2 = « Oui ») et (3 = « Oui »)) alors Ind19 = 100 %

Si ((1 = « Non ») et (2 = « Oui ») et (3 = « Non »)) alors Ind19 = B

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Service de formation
Fréquence de collecte : trimestrielle	**Source de données :** ROSI, Service de formation
Méthode de collecte : manuelle	**Date de collecte :** : jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Développer et maintenir les compétences en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « formation ROSI », « formation COGI », « sensibilisation du personnel », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind19 = 0 %, Alarme : « Le ROSI doit suivre au moins une formation générale en SI, avant la Date_cible ». ✓ Si ((Ind19 < 100 %) et ((Date_Système < Date_cible)), Alarme : « Le ROSI doit compléter au moins une formation générale en SI, avant la Date_cible ». ✓ Si Ind19 = 100 %, Signal : « La formation du ROSI est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind19 < 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

Fiche descriptive d’indicateur numéro 20

Nº indicateur : 20

Désignation : Ind20

Libellé : Degré de conformité à l'exigence portant sur la formation du COGI sur les bonnes pratiques de sécurité de l'information.

Description : La valeur de l'indicateur, exprimée en pourcentage, permet d'apprécier le degré de conformité de l'organisme public à l'exigence sur la formation du COGI.

Objectif : S'assurer que le COGI développe et maintient ses connaissances et compétences en sécurité de l'information.

Destinataires : ROSI, comité de sécurité de l'information, vérificateur interne, autres.

Date de production : jj/mm/aaaa

Éléments de référence gouvernementale

Orientation gouvernementale : Développer et maintenir les compétences en sécurité de l'information.

Objectif gouvernemental : Accroître l'expertise et le savoir-faire en sécurité de l'information.

Cible gouvernementale :

- ✓ 100 % des COGI des OP fortement exposés aux risques auront suivi au moins une formation sur les bonnes pratiques de sécurité de l'information d'ici le 31 mars 2015;
- ✓ 100 % des COGI des OP de grande taille auront suivi au moins une formation sur les bonnes pratiques de sécurité de l'information d'ici le 31 mars 2016;
- ✓ 100 % des COGI des tous les OP auront suivi au moins une formation sur les bonnes pratiques de sécurité de l'information d'ici le 31 mars 2017.

Cible sectorielle et seuil d'alerte

Cible sectorielle :

Ind20 = 100 % d'ici le 31 mars 2015 si l'OP est fortement exposé aux risques

Ind20 = 100 % d'ici le 31 mars 2016 si l'OP est de grande taille

Ind20 = 100 % d'ici le 31 mars 2017 pour tout OP

Seuil d'alerte : Ind20 < 100 %

Calcul de l'indicateur

Mesure (unité) : %	**Type de mesure :** dérivée

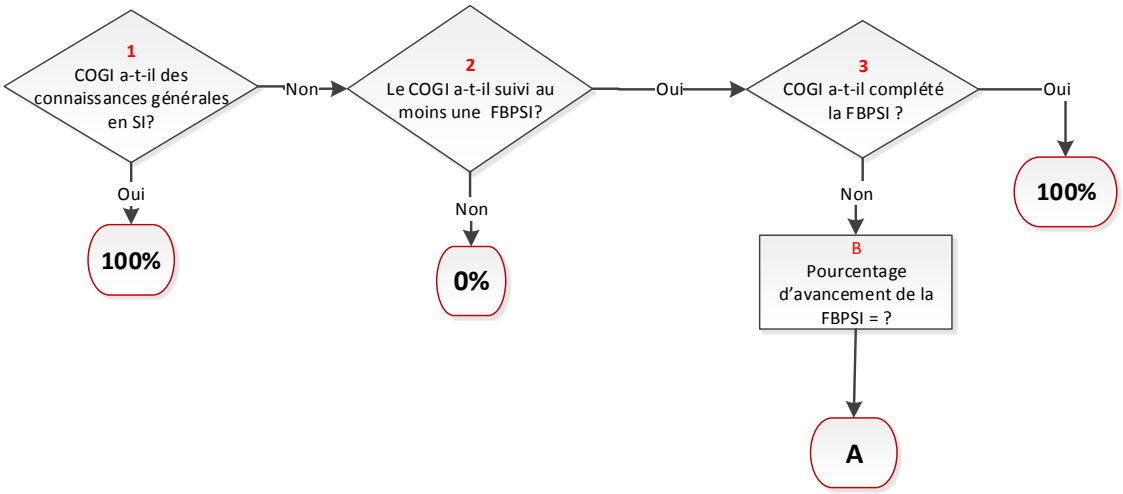
Éléments de calcul :

FBPSI = Formation sur les bonnes pratiques de sécurité de l'information

1. Le COGI a-t-il des connaissances générales en sécurité de l'information? (O/N)
2. Le COGI a-t-il suivi au moins une FBPSI? (O/N)
3. Le COGI a-t-il complété la FBPSI? (O/N)

A. Pourcentage d'avancement de la FBPSI

Algorithme de calcul :



Algorithme d'estimation du degré de conformité à l'obligation portant sur la participation du COGI à une formation sur les bonnes pratiques de sécurité de l'information

Formule/Pondération :

Si (1 = « Oui ») alors Ind20 = 100 %

Si ((1 = « Non ») et (2 = « Non ») alors Ind20 = 0 %

Si ((1 = « Non ») et (2 = « Oui») et (3 = « Oui ») alors Ind20 = 100 %

Si ((1 = « Non ») et (2 = « Oui ») et (3 = « Non ») alors Ind20 = A

Collecte des données et rapport

Responsable d'alimentation : ROSI	**Propriétaire des données :** Service de formation
Fréquence de collecte : trimestrielle	**Source de données :** COGI, Service de formation
Méthode de collecte : manuelle	**Date de collecte :** jj/mm/aaaa
Format d'illustration : Cet indicateur sera représenté par un « tachymètre » pour refléter le degré de sa conformité à l'exigence gouvernementale. Cet indicateur sera représenté par une barre dans le diagramme à barres représentant l'ensemble des indicateurs estimant le degré d'atteinte des objectifs liés à l'orientation gouvernementale « Développer et maintenir les compétences en sécurité de l'information ». Ce diagramme aura, pour axe des abscisses, les indicateurs liés à cette orientation (par exemple, « formation ROSI », « formation COGI », « sensibilisation personnel », etc.) et, pour axe des ordonnées, le pourcentage d'atteinte (50 %, 75 %, etc.).	**Règle d'interprétation :** ✓ Si OP fortement exposé aux risques alors Date_cible = 31 mars 2015. Sinon ((Si OP de grande taille alors Date_cible = 31 mars 2016), Sinon Date_cible = 31 mars 2017). ✓ Si Ind20 = 0 %, Alarme : « Le COGI doit suivre au moins une formation sur les bonnes pratiques en SI, avant la Date_cible ». ✓ Si ((Ind20 < 100 %) et ((Date_Système < Date_cible)), Alarme : « Le COGI doit compléter au moins une formation sur les bonnes pratiques en SI, avant la Date_cible ». ✓ Si Ind20 = 100 %, Signal : « La formation du COGI sur les bonnes pratiques en SI est conforme à 100 % ». ✓ Si ((Date_Système > Date_cible) et (Ind20< 100 %)), Alarme : « Attention! Vous avez dépassé la date cible pour cet indicateur ».

ANNEXE III **Références**

BLAIS, Sébastien. Tableau de bord équilibré (*balanced scorecard*) : de l'incarnation tangible de la stratégie à l'architecture de l'information de gestion, février 2011, [en ligne] [http://regiondequebec.iiba.org/download/Presentation%20Sebastien%20Blais.pdf] (le 23 février 2011)

FERNANDEZ, Alain. L'essentiel du tableau de bord, 3e édition, juin 2011.

MARR, Bernard. *How to Design Key Performance Indicators, Management Case Study, Advanced Performance Institute*, juin 2010.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Performance Measurement Guide for Information Security*, *Special Publication* 800-55, Revision 1, juillet 2008.

SECRÉTARIAT DU CONSEIL DU TRÉSOR (SCT). Approche stratégique gouvernementale en sécurité de l'information 2014-2017, décembre 2013.

SECRÉTARIAT DU CONSEIL DU TRÉSOR (SCT). Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information, décembre 2013.

SECRÉTARIAT DU CONSEIL DU TRÉSOR (SCT). Cadre gouvernemental de gestion de la sécurité de l'information, décembre 2013.

SECRÉTARIAT DU CONSEIL DU TRÉSOR (SCT). Directive sur la sécurité de l'information gouvernementale, janvier 2014.

VOYER, Pierre. Tableau de bord de gestion et indicateurs de performance, Presses de l'Université du Québec, 2e édition, 2006.

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique