Segment Sécurité

Cadre de référence d'une architecture de sécurité de l'information (ASI) d'un organisme public

Architecture d'entreprise gouvernementale 3.3

ENSEMBLE on fait avancer le Québec

Québec

Segment Sécurité

Cadre de référence de l'architecture de sécurité de l'information (ASI) d'un organisme public

Architecture d’entreprise gouvernementale 3.3

Cette publication a été réalisée
par le Dirigeant principal de l'information
et produite en collaboration avec la Direction des communications.

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

Direction des communications du ministère du Conseil exécutif et du Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

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

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

Dépôt légal – juin 2017
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-78889-8 (en ligne)

Table des matières

Liste des figures

Liste des sigles et des acronymes

AEG	Architecture d’entreprise gouvernementale
ASIG	Architecture de sécurité de l’information gouvernementale
ASI	Architecture de sécurité de l'information
ASIM	Architecture de sécurité de l'information ministérielle
DPI	Dirigeant principal de l'information
OP	Organisme public
RI	Ressources informationnelles
SCT	Secrétariat du Conseil du trésor
SI	Sécurité de l'information
TI	Technologies de l’information

Historique des changements

Version de l'AEG	Date de publication	Modifications
3.3	Juin 2017	Publication de la première édition

La version en vigueur est accessible à l'adresse suivante :

http://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/

Avis au lecteur

Note 1 : Le terme *organisme public* désigne un ministère ou un organisme, qu'il soit budgétaire ou autre, ainsi que tout organisme du réseau de l'éducation et de l'enseignement supérieur ou du réseau de la santé et des services sociaux.

Note 2 : Bien que les éléments du présent document soient applicables à la plupart des organismes publics, il convient pour chacun d'eux de les adapter à son contexte et aux risques qui lui sont propres.

Public cible

Responsables organisationnels de la sécurité de l'information (ROSI)

Conseillères et conseillers organisationnels de la sécurité de l'information (COSI)

Conseillères et conseillers organisationnels de la gestion des incidents (COGI)

Architectes de sécurité de l'information

Spécialistes en sécurité de l'information

Responsables des technologies de l'information

Architectes d'entreprise

Gestionnaires

1. Introduction

Le présent cadre de référence est produit afin de servir de modèle et de canevas aux organismes publics pour les aider à concevoir et à réaliser leur propre architecture de sécurité de l'information. Il présente les différentes phases de sa mise en œuvre ainsi que ses principales composantes.

L'architecture de sécurité de l'information consiste à mettre en place un système qui tient compte des besoins de l'organisme public en matière de sécurité de l'information.

L'objectif ultime de ce document est de permettre aux organismes publics de prendre en considération les préoccupations de sécurité dès l'émergence de nouveaux projets ainsi que l'évolution de leurs orientations stratégiques, afin de mieux assurer la sécurité de l'information et la protection des renseignements personnels.

1.1 Qu'est-ce qu'une architecture de sécurité de l'information (ASI) d'un organisme public?

L'architecture de sécurité de l'information est un outil stratégique qui définit la vision et les orientations en sécurité de l'information de l'organisme public. Elle est alignée sur les orientations gouvernementales et tient compte des objectifs d'affaires de l'organisme public et des risques de sécurité encourus.

Elle permet de circonscrire les préoccupations de l'organisme public en matière de disponibilité, d'intégrité et de confidentialité de l'information et, ainsi, de contribuer à l'élaboration et à la mise en œuvre d'un programme (plan directeur) de sécurité de l'information cohérent et intégré.

1.2 Contexte

La sécurité de l'information est au cœur des préoccupations du Gouvernement du Québec.

La directive sur la sécurité de l'information gouvernementale, adoptée en 2014, précise en effet qu'un organisme public doit assurer la sécurité de l'information qu'il détient dans le cadre de sa prestation de services. Elle stipule, entre autres, le niveau d'imputabilité et de responsabilité de la sécurité de l'information gouvernementale dévolu aux organismes publics.

« Les organismes publics doivent assurer la sécurité de l'information gouvernementale conformément aux principes directeurs suivants :

- ✓ Responsabilité et imputabilité
- ✓ Évolution
- ✓ Universalité
- ✓ Éthique[1] »

[1] Directive sur la sécurité de l'information gouvernementale 5 a, b, c, d

Parmi les documents qui sont en appui à cette directive, l'approche stratégique prévoit notamment que les organismes publics doivent définir une architecture qui vise à formaliser leur vision de la sécurité de l'information, celle-ci s'inscrivant idéalement dans l'architecture d'entreprise de l'organisation. Ils doivent également s'assurer de l'adéquation des mesures de sécurité en vigueur par rapport aux risques encourus.

Cette exigence de la mise en place d'une architecture de sécurité de l'information s'appuie sur les meilleures pratiques du marché et sur les normes internationales. Ces dernières stipulent qu'une telle architecture constitue un outil important permettant justement aux organismes publics de mieux répondre à leurs obligations en matière de sécurité de l'information, d'avoir une meilleure vision de la situation et de mieux planifier les investissements en ce domaine.

Enfin, l'état de situation gouvernemental en sécurité de l'information (produit sur une base bisannuelle) questionne les organismes publics sur la mise en place, de façon formelle, d'une architecture de sécurité de l'information. Certains organismes confirment ne pas avoir encore mis en place une telle architecture .

Ainsi, afin de mettre en place une architecture de sécurité de l'information adaptée à sa mission et à ses objectifs, l'organisme public doit s'appuyer, entre autres, sur le cadre légal et réglementaire, sur la tolérance au risque, sur l'évaluation du bilan de maturité en sécurité de l'information ainsi que sur l'alignement stratégique avec les besoins d'affaires.

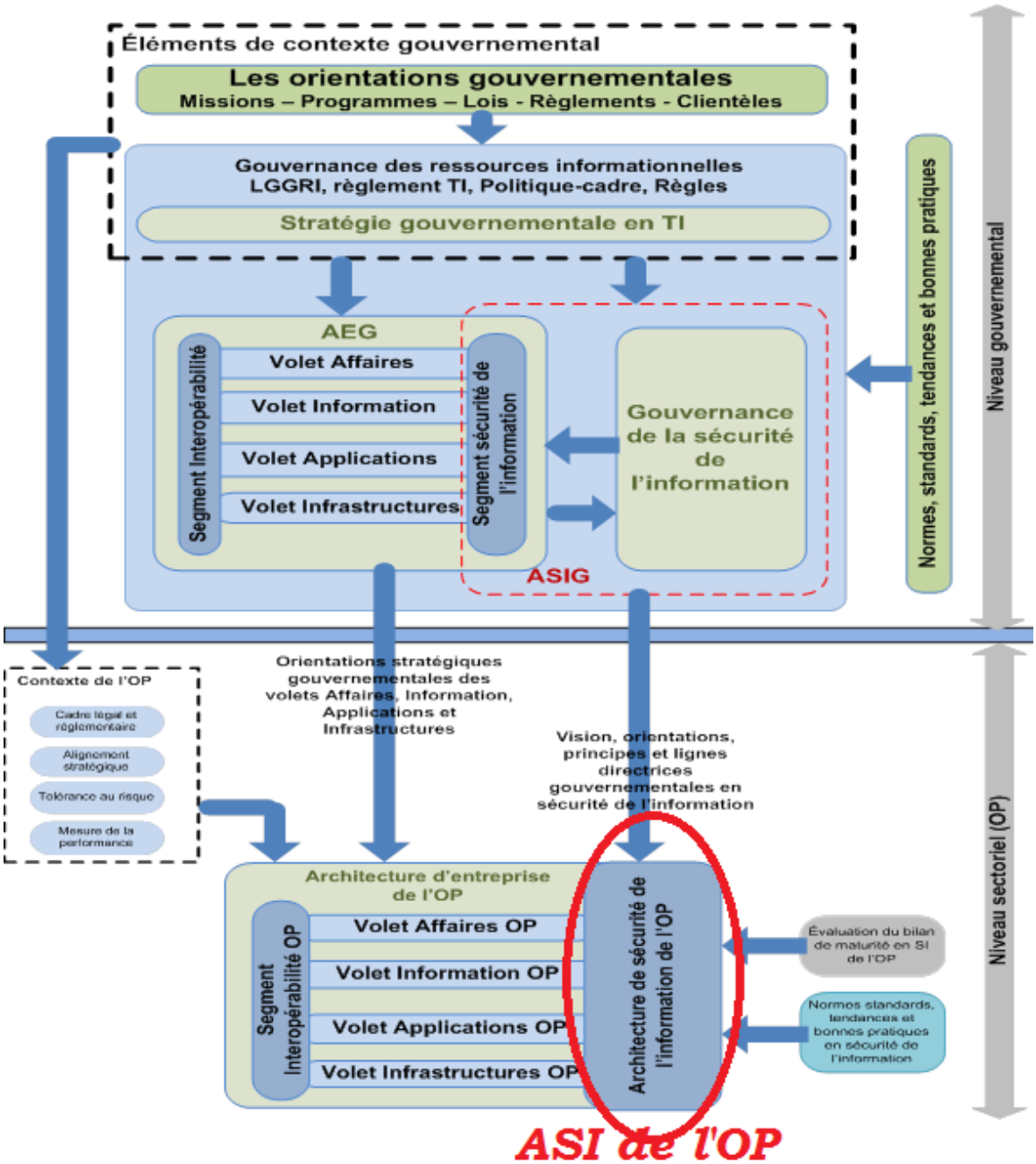
1.3 Quels sont les bénéfices d'une ASI?

Les principaux avantages d'une architecture de sécurité de l'information sont :

- ✓ de permettre d'aligner les initiatives, les stratégies et les activités de l'organisme public pour atteindre la vision commune en sécurité de l'information;
- ✓ d'offrir une vue d'ensemble permettant d'examiner la dimension stratégique des solutions mises en place et d'en assurer la compatibilité et l'interopérabilité;
- ✓ de produire un cadre de principes, de processus et d'outils de gestion communs qui supportent des solutions de sécurité appropriées aux exigences d'affaires et de démontrer aux parties prenantes l'intention vis-à-vis de la sécurité de l'information, de la gestion du risque et de la conformité réglementaire;
- ✓ de procurer à l'organisme public un plan directeur de ce qui doit se faire en matière de sécurité de l'information et d'établir des définitions communes dans la terminologie de sécurité de l'information;
- ✓ d'induire un langage commun et compréhensible pour les communications internes et de fournir la base d'une amélioration continue mesurable des processus de sécurité et des activités, en formalisant la gestion de processus.

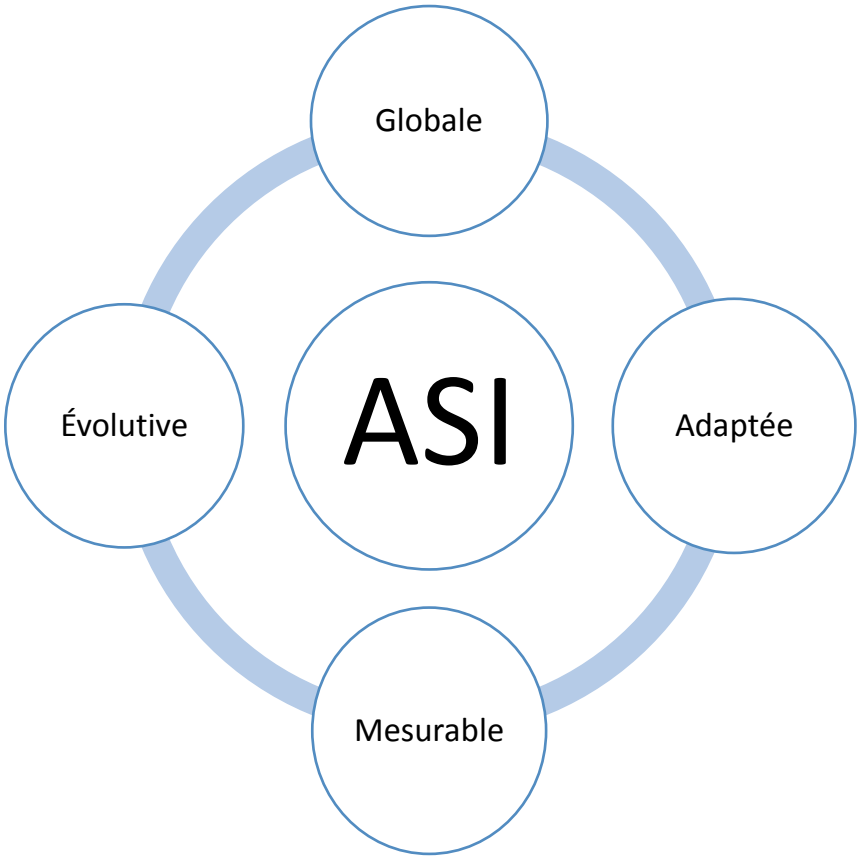
2. Positionnement de l'ASI d'un organisme public par rapport à l'ASI gouvernementale (ASIG)

Figure 1 : Lien entre l'ASI gouvernementale (ASIG) et celle d'un organisme public



3. Quelles sont les caractéristiques d'une ASI?

Figure 2 : Caractéristiques d'une ASI



Une architecture de sécurité de l'information viable doit être :

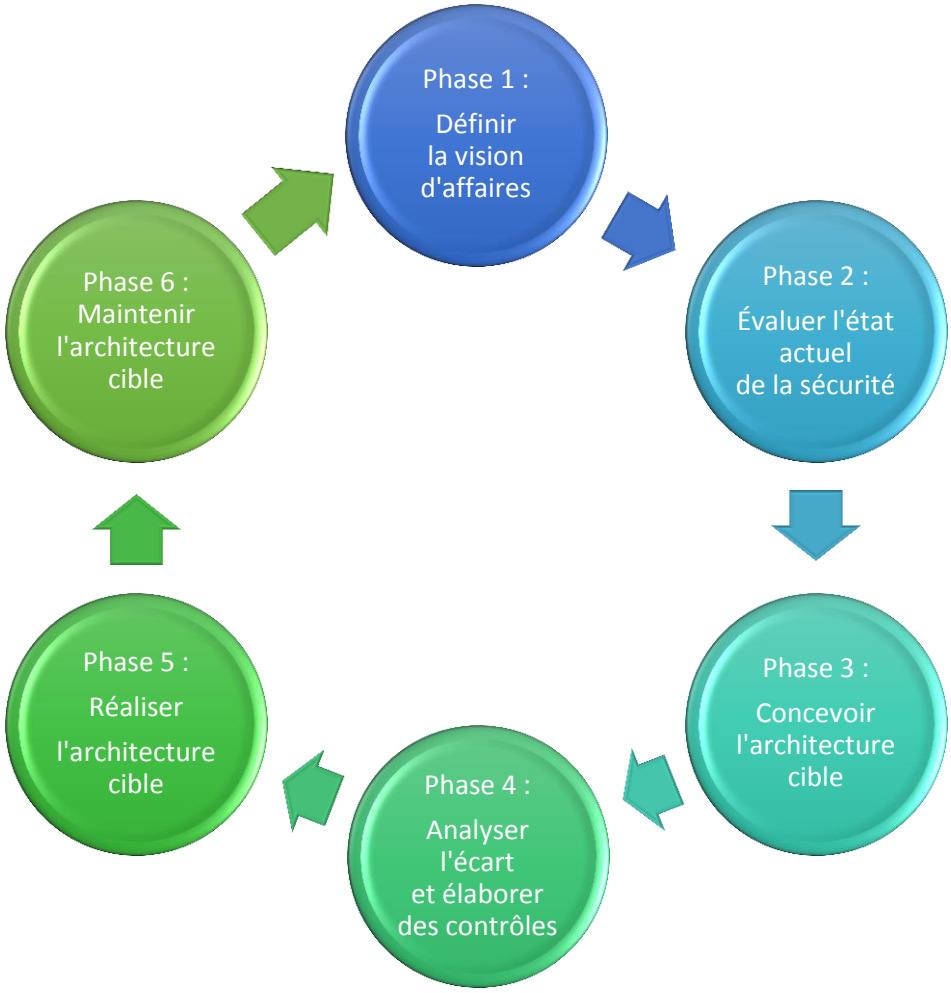
- globale : elle doit aborder la gouvernance d'entreprise, les problèmes stratégiques et de gestion, le niveau tactique et opérationnel, la politique de gestion de la sécurité de l'information, les problèmes de ressources humaines, les problèmes d'administration, les normes de sécurité d'information, les problèmes technologiques, les installations physiques, les différentes autres architectures de l'organisme public, etc.
- adaptée : elle doit être spécifique aux réalités et aux risques de l'organisme public.
- mesurable : il doit être possible de déterminer les indicateurs de succès et de jauger le niveau de maturité de l'architecture de sécurité.
- évolutive : elle doit être itérative et suivre un ensemble de phases afin d'assurer une amélioration continue et de prendre en compte les nouvelles réalités (nouveaux objectifs d'affaires, risques émergents, nouveaux services…) de l'organisme public.

4. Comment mettre en place une ASI?

L'architecture de sécurité de l'information s'appuie sur des exigences visant à réduire les risques reliés à la sécurité de l'information.

La démarche de mise en place d'une architecture de sécurité de l'information se décline en six phases :

Figure 3 : Phases de la démarche de mise en place de l'ASIM



Tout d'abord, l'organisme public définit sa vision et évalue son état actuel de la sécurité avant de concevoir son architecture cible. Ensuite, il analyse l'écart entre l'état actuel et l'état cible, puis élabore les mesures de sécurité pertinentes afin de réaliser l'architecture cible. Enfin, il faut effectuer un suivi de l'architecture en utilisant des métriques permettant de contrôler la cible.

4.1 Définir la vision d'affaires

Un des critères fondamentaux de la sécurité de l'information est son alignement avec les objectifs d'affaires.

Cette vision d'affaires aura les attributs suivants :

- ✓ Aligner la sécurité de l'information sur les objectifs d'affaires

La vision doit permettre de soutenir les orientations stratégiques de l'organisme public. Les exigences de sécurité de l'information devraient être pratiques et offrir une réduction réelle et mesurable des risques.

- ✓ Avoir une approche basée sur le risque

Les contrôles de sécurité de l'information sont souvent mis en œuvre avec peu d'évaluation, quand il y en a, des risques actuels et des menaces pour l'organisme public, ce qui entraine la non-protection des actifs critiques ou une surprotection inutile. Les professionnels de la sécurité de l'information doivent comprendre les affaires, les objectifs, l'environnement réglementaire et d'exploitation, les menaces potentielles, les impacts du risque, la flexibilité opérationnelle et la résilience. C'est à partir de ce moment seulement qu'ils pourront sélectionner les contrôles appropriés pour mitiger le risque efficacement.

- ✓ Observer un équilibre entre les organismes publics, les personnes, les processus et la technologie

Une gestion de risque efficace requiert un support de l'organisme public, des personnes compétentes et des processus efficients ainsi que la sélection d'une technologie appropriée. Chaque élément influence et soutient les autres en interagissant souvent avec eux de manière complexe. Ainsi, il est crucial d'atteindre un équilibre. Si l'un d'eux est déficient, la sécurité de l'information s'en trouve diminuée.

- ✓ Assurer la convergence des stratégies de sécurité

Pour maximiser le retour sur investissement, toutes les fonctions de sécurité doivent être alignées et se soutenir mutuellement. Les fonctions de sécurité non alignées sont un gaspillage et elles entravent l'identification et l'atténuation du risque.

- ✓ Maintenir une neutralité technique et environnementale

La vision doit être indépendante de toute technologie particulière ou de changements techniques dans le temps. De même, elle devrait être applicable dans les industries, dans les géographies et dans les systèmes réglementaires et juridiques.

Après avoir défini la vision d'affaires, il est important d'obtenir l'engagement et l'adhésion de la haute direction afin de poursuivre les différentes activités de mise en place de l'architecture de sécurité.

4.2 Évaluer l'état actuel de la sécurité

Le but de cette phase est de répondre à cette question : Où l'organisme public en est-il aujourd'hui avec la sécurité de l'information?

Répondre à cette question consiste à effectuer une première évaluation afin de créer une situation de référence à laquelle l'architecture cible va pouvoir se mesurer.

Il s'agit, en fait, d'évaluer les risques auxquels les actifs de l'organisation sont exposés et de certifier que les contrôles de sécurité actuellement mis en oeuvre sont adéquats ou qu'ils rencontrent les niveaux acceptables de risque.

Cette évaluation implique, sans s'y limiter :

- ✓ l'identification du personnel clé, avec lequel il faut s'entretenir pour rassembler l'information,

- ✓ l’identification des composantes de sécurité critiques et non critiques,
- ✓ la détermination des contrôles appropriés en place,
- ✓ l’identification des menaces et des vulnérabilités,
- ✓ la gestion des identités et des accès,
- ✓ l'identification des incidents de sécurité,
- ✓ la conduite d’une analyse de risque.

Les recommandations issues de cette phase peuvent être utilisées pour apporter les modifications nécessaires à la conception et à l’implémentation d’une politique ou à l’amélioration des politiques existantes et pour ajouter des contrôles de sécurité.

4.3 Concevoir l’architecture cible

Cette phase répond à cette question : Vers où l'organisme public veut-il aller?

La conception de l’architecture cible passe par la prise en compte des orientations stratégiques contenues dans la vision d'affaires, de la mission, des buts et des objectifs de l'organisme public. Elle peut dépendre aussi des recommandations issues de l'évaluation de l'état actuel.

Il est important de concevoir l'architecture de sécurité de l'information, dans le but de mettre en œuvre la sécurité dans toutes les architectures identifiées (affaires, information, applications, infrastructure, etc.).

Cette phase détaille les différentes composantes de l'architecture de sécurité de l'information. Elle en donne les éléments de gouvernance et les principales exigences de sécurité, comme le montre la section 5 de ce document.

4.4 Analyser l’écart et élaborer des mesures

Cette phase répond à cette question : Que manque-t-il à l'organisme public pour atteindre sa cible?

Elle permet d’analyser l'écart entre l’architecture cible et l’état actuel, qu'une architecture de sécurité soit déjà en place ou non. En fonction de ce résultat, l'organisme public va produire, revoir ou réviser la politique globale de sécurité de l’information qui traduit les objectifs stratégiques, les contrôles de sécurité liés aux différents volets de l’architecture d’entreprise ainsi que les politiques et les procédures de sécurité opérationnelles qui ont pour objectif de traiter ce qui doit être protégé.

Cette analyse permet de mieux faire la transition de l'architecture actuelle vers l'architecture cible et elle provient des réponses aux questions suivantes :

- ✓ Quels sont les nouveaux contrôles que l'organisme public veut mettre en place?
- ✓ Quels sont les contrôles à supprimer?
- ✓ Quels sont les contrôles à modifier?
- ✓ Quels contrôles vont-ils rester inchangés?

Comme vu plus haut, les résultats de cette analyse doivent cependant être confrontés avec la vision d'affaires de l'organisme public afin de juger de leur pertinence. Cette analyse va au-delà des systèmes; elle prend aussi en compte tout le cadre normatif de la sécurité de l'information.

4.5 Réaliser l’architecture cible

Cette phase répond à cette question : Comment l'organisme public compte-t-il mettre en oeuvre son architecture de sécurité de l'information?

C’est à cette étape qu’il faut concrétiser l'architecture cible, en mettant en place toutes les actions indiquées lors de la phase de conception.

L'organisme public passe en revue l'ensemble des éléments de gouvernance pour s'assurer qu'ils sont en place et aussi que les contrôles de sécurité sont pertinents et qu’ils s'adaptent aux résultats de l'analyse de risque.

Une fois réalisée, l’architecture cible sera soumise à la ou au responsable organisationnel de la sécurité de l'information (ROSI) pour validation et à la haute direction pour approbation.

4.6 Maintenir l’architecture cible

Cette phase répond à ces deux questions : Comment l'organisme public va-t-il s'assurer qu'il a implémenté la bonne architecture de sécurité de l'information? Comment continue-t-il à s'améliorer?

Les objectifs sont :

- ✓ de s’assurer que les ressources mises en œuvre à l'étape de réalisation et que les résultats obtenus après celle-ci correspondent bien à ce qui a été prévu à l'étape de la conception;
- ✓ d’ajuster les écarts et de vérifier que les contrôles mis en place sont pertinents dans le temps;
- ✓ de rechercher des pistes d'amélioration tant que le niveau de performance attendu n'est pas atteint.

Pour ce faire, il faut surveiller et revoir les performances de l'architecture cible afin de déterminer les actions correctrices en vue d'une amélioration continue. Il faut aussi maintenir et améliorer l'architecture cible en exécutant les actions correctrices sur la base des résultats des mesures de performance et en réévaluant les contrôles mis en place de même que les éléments de gouvernance.

Il faut veiller à :

- ✓ utiliser des métriques pour voir si l'architecture rencontre certains critères établis dans la phase de conception;
- ✓ vérifier si les contrôles sont implantés correctement;
- ✓ identifier les causes d'écart entre l'architecture conçue et celle qui est implantée;
- ✓ formaliser les éléments d'encadrement de la sécurité une fois que le niveau attendu est atteint;
- ✓ réviser de manière périodique l'étape de définition de la vision pour assurer une évolution permanente de l'architecture.

5. De quoi est composée une ASI?

Idéalement, une architecture de sécurité de l'information est composée de deux parties :

- ✓ Une partie « gouvernance » qui s’assure que la sécurité s’aligne sur les objectifs d’affaires de l’organisme public et sur les orientations gouvernementales en sécurité de l'information;

- ✓ Une partie « exigences de sécurité » qui définit les différentes familles de contrôle que l'organisme public compte appliquer afin de s'assurer de la disponibilité, la confidentialité et l'intégrité de l'information. Dans le cas où l'organisme public dispose d'une architecture d'entreprise, ces contrôles seront liés aux volets Affaires, Information, Applications et Infrastructure de celle-ci.

Ces éléments de gouvernance ainsi que ces contrôles de sécurité ne sont pas exhaustifs. L'organisme public pourra en ajouter (ou en retirer) selon son contexte et sa mission. Il peut se référer aux documents cités en référence pour connaitre les contrôles subsidiaires.

5.1 Éléments de gouvernance

5.1.1 Cadre normatif de sécurité

Dans un organisme public, le cadre normatif est principalement composé d'une politique, d'un cadre de gestion, de directives, de guides, de processus et de procédures.

La politique de sécurité de l'information témoigne de l'importance accordée par l'organisme public à la protection de l'information gouvernementale. Elle énonce des principes généraux et fixe des responsabilités à l'endroit de certains intervenants clés.

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

La directive vise à préciser, pour un domaine d'application particulier de sécurité de l'information (sécurité des locaux et des équipements, échanges sécuritaires de l'information, etc.), les dispositions à respecter aux fins d'assurer la sécurité de l'information.

Le guide vise à faciliter l'application des prescriptions d'une politique, d'une directive ou, éventuellement, d'une norme, sans en avoir le caractère contraignant

La procédure est un ensemble d'étapes à franchir, de moyens à prendre et de méthodes à suivre dans l'exécution d'une tâche.

Documents de référence :

- ✓ *Guide d'élaboration d'un cadre de gestion de la sécurité de l'information (PR-075)*
- ✓ *Guide d'élaboration d'une politique de sécurité de l'information (PR-074)*
- ✓ *Guide d'élaboration et de mise en œuvre d'un processus de gestion des risques de sécurité de l'information (PR-062)*
- ✓ *ISO 27001, management de la sécurité de l'information*
- ✓ *COBIT 5 for Information Security*

5.1.2 Gestion du risque

Le cadre de gestion du risque s'assure que les risques sont identifiés et gérés et que la tolérance au risque est comprise et communiquée. La gestion des risques détermine les exigences de sécurité.

Les organismes publics évaluent périodiquement les risques qui peuvent survenir durant le traitement, le stockage et la transmission de ses informations ainsi que les risques liés aux opérations.

Il s'agit d'identifier les menaces pertinentes pour l'organisme public, les vulnérabilités internes et externes, l'impact et la probabilité qu'un dommage survienne.

Documents de référence :

- ✓ *Guide de mise en œuvre d'un cadre de gestion des risques de sécurité de l'information à portée gouvernementale (PR-063)*
- ✓ *Élaboration et mise en œuvre d'un processus de gestion des risques de sécurité de l'information (PR-062)*
- ✓ *NIST SP 800-30, Risk Management Guide*
- ✓ *ISO 27005, technologies de l'information – techniques de sécurité – gestion des risques liés à la sécurité de l'information*
- ✓ *COBIT 5 for Information Risk*

5.1.3 Sensibilisation et formation

L'utilisateur est souvent considéré comme le maillon le plus important de la sécurité de l'information. Sensibiliser les utilisateurs sur leurs responsabilités en sécurité et leur apprendre les bonnes pratiques peut changer leur environnement.

Les organismes publics sont responsables de s'assurer que les gestionnaires et les utilisateurs sont conscients des risques de sécurité associés à leurs activités et que le personnel est adéquatement formé pour s'acquitter de ses tâches et de ses responsabilités liées à la sécurité de l'information.

Documents de référence :

- ✓ *Guide de sensibilisation à la sécurité de l'information (PR-070)* du SCT
- ✓ *NIST SP 800-50, Building an Information Technology Security Awareness*

5.2 Exigences de sécurité

Pour assurer la disponibilité, la confidentialité et l'intégrité de l'information, des exigences minimales de sécurité sont requises. Ces exigences sont la base d'un programme de sécurité équilibré et adressent les différents volets de l'architecture d'entreprise de l'organisme public.

5.2.1 Continuité des affaires

La planification de la continuité des affaires est une politique de gestion et une procédure utilisées par les gestionnaires pour guider la réponse organisationnelle devant une perte perçue de la capacité de mission. Elle permet de déterminer l'action à effectuer si un événement majeur arrive.

Les organismes publics sont invités à établir, à maintenir et à implémenter de manière efficace des plans de continuité des activités (PCA). Ainsi, ils vont faire des sauvegardes de leurs opérations et prévoir la reprise après sinistre des systèmes organisationnels afin de s'assurer de la disponibilité des ressources informationnelles critiques et de la continuité des opérations dans des situations d'urgence.

Documents de référence :

- ✓ *Guide de gestion de la continuité des services (PR-059)* du SCT
- ✓ *NIST SP 800-34, Contingency Planning Guide*

- ✓ *ISO 27002 ch. 17, aspects de la sécurité de l'information dans la gestion de la continuité d'activité*
- ✓ *COBIT 5, processus facilitants*

5.2.2 Conformité

Il est conseillé d'identifier les législations applicables, car les textes peuvent formuler des exigences concernant la sécurité des systèmes d'information que l'organisme se doit de respecter sous peine de poursuites judiciaires ou de pénalités contractuelles.

Les organismes publics sont invités à mettre en place un processus de gestion des licences ainsi que des dispositifs pour éviter l'installation illicite de logiciels.

Documents de référence :

- ✓ *Cadre légal et administratif du Gouvernement Québec*
- ✓ *ISO 27002 ch. 18, conformité*
- ✓ *COBIT 5, processus facilitants*

5.2.3 Sécurité liée aux ressources humaines

De nombreuses questions importantes en matière de sécurité de l'information concernent les utilisateurs, les concepteurs, les responsables de la mise en œuvre et les gestionnaires. Un large éventail de problèmes de sécurité se rapporte à la façon dont ces personnes interagissent avec les composants du système ainsi qu'avec l'accès et les autorisations nécessaires pour faire leur travail.

Les organismes publics sont invités à veiller à ce que les personnes occupant des postes de responsabilité (y compris les tiers fournisseurs de services) soient dignes de confiance et qu'ils respectent les critères de sécurité établis pour ces postes. Ils vont veiller à ce que les informations et les systèmes organisationnels soient protégés avant, pendant et après la prise de fonction. Ils doivent pouvoir sanctionner le personnel qui ne respecte pas les politiques et les procédures de sécurité de l'organisme public.

Documents de référence :

- ✓ *Guide établissant les critères de désignation des principaux intervenants en sécurité de l'information (PR-076)*
- ✓ *ISO 27002 ch. 7, sécurité des ressources humaines*
- ✓ *COBIT 5, processus facilitants*

5.2.4 Relations avec les fournisseurs

Les organismes publics sont invités à rédiger une politique de sécurité destinée aux fournisseurs et à insérer des articles relatifs à la sécurité des SI et à la protection des renseignements personnels dans les contrats pour que les fournisseurs s'engagent dans le domaine.

Le fournisseur doit être en mesure d'apporter la preuve qu'il respecte ses engagements en matière de sécurité.

Documents de référence :

- ✓ *ISO 27002 ch. 15, relations avec les fournisseurs*
- ✓ *COBIT 5, processus facilitants*

5.2.5 Catégorisation de l'information

La catégorisation des actifs informationnels en sécurité de l'information est un processus permettant à l'organisme public d'évaluer le degré de sensibilité de son information dans le but d'en déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité (DIC).

Les organismes publics peuvent ainsi tenir compte du degré de sensibilité déterminé pour mettre en place les mesures leur permettant de se conformer à leurs obligations légales, d'éviter des pertes financières, d'atteindre leurs objectifs en ce qui a trait aux niveaux de services et de rehausser la confiance des citoyennes et citoyens et des entreprises à l'égard des services publics.

Documents de référence :

- ✓ *Guide de catégorisation de l'information (PR-057)*
- ✓ *Guide et outil d'élaboration d'un registre d'autorité de la sécurité de l'information (PR-068)*
- ✓ *COBIT 5, processus facilitants*

5.2.6 Cryptographie

Les conséquences liées à la divulgation ou à la perte des clés sont telles qu'il convient de protéger celles-ci de façon adéquate. Les procédures doivent être correctement formalisées.

Les organismes publics sont invités à chiffrer les informations en fonction de leur sensibilité et à chiffrer les échanges lorsque les liaisons ne sont pas considérées comme sûres.

Documents de référence :

- ✓ *Analyse des risques associés à l'utilisation des équipements informatiques portables (mars 2014)*
- ✓ *ISO 27002 ch. 10, cryptographie : politique de chiffrement et gestion des clés*
- ✓ *NIST SP 800-133, Recommendation for Cryptographic Key Generation*
- ✓ *COBIT 5, processus facilitants*

5.2.7 Contrôle d'accès logique

Les contrôles d'accès logiques peuvent prescrire non seulement qui ou quoi (dans le cas d'un processus) doit avoir accès à une ressource système particulière, mais aussi quel type d'accès lui octroyer.

Ces contrôles peuvent être bâtis dans le système d'exploitation, incorporés dans les applications des programmes (comme les systèmes de gestion de base de données et les systèmes de communication) ou mis en oeuvre par des packs de sécurité.

Les organismes publics sont invités à limiter aux seuls utilisateurs autorisés l'accès aux systèmes, aux processus, aux transactions et aux fonctions.

Documents de référence :

- ✓ *Guide de gestion des accès logiques (PR-077)*
- ✓ *ISO 27002 ch. 9, contrôle d'accès*
- ✓ *COBIT 5, processus facilitants*

5.2.8 Identification et authentification

L'identification et l'authentification constituent une mesure technique qui prévient l'introduction, dans un système, d'individus et de processus non autorisés.

L'identification est le fait de vérifier l'identité d'un utilisateur, d'un processus ou d'un dispositif, typiquement comme un prérequis pour donner l'accès aux ressources à un système TI.

L'identification et l'authentification constituent un bloc critique de la sécurité de l'information, puisqu'elles sont la base de plusieurs types de contrôle d'accès et qu'elles établissent l'imputabilité de l'utilisateur.

Les organismes publics sont invités à identifier les utilisateurs des systèmes, les processus agissant pour le compte des utilisateurs ou les dispositifs. Ils doivent aussi authentifier ou vérifier les identités de ces utilisateurs, de ces processus ou de ces dispositifs, comme un prérequis à l'offre d'accès aux systèmes organisationnels.

Documents de référence :

- ✓ *NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Systems and Organizations*
- ✓ *COBIT 5, processus facilitants*

5.2.9 Audit des journaux

Un audit est une revue indépendante et un examen des registres et des activités pour évaluer l'adéquation des contrôles et s'assurer de la conformité avec les politiques établies et les procédures opérationnelles.

Une trace d'audit permet de savoir qui a accédé à un système et quelles opérations l'utilisateur a effectuées durant une période donnée. En conjonction avec les procédures et les outils appropriés, les traces d'audit peuvent aider dans la détection des violations de sécurité, des problèmes de performance et des défauts dans les applications.

Les organismes publics sont invités à créer, à protéger et à conserver les dossiers d'audit du système, dans la mesure nécessaire pour permettre le suivi, l'analyse, l'enquête et la communication d'activités illégales, non autorisées ou inappropriées du système. Ils vont veiller à ce que les actions de ces utilisateurs du système puissent être repérées.

Documents de référence :

- ✓ *ISO 27002 ch. 12, sécurité liée à l'exploitation*
- ✓ *COBIT 5, processus facilitants*

5.2.10 Sécurité opérationnelle

Pour garder les systèmes dans de bonnes conditions de fonctionnement et pour minimiser les risques reliés aux logiciels et au matériel, il est primordial que les organismes publics documentent des procédures d'exploitation, planifient les changements, garantissent la capacité de traitement de leur système d'information, séparent clairement les environnements de production de ceux de développement, déploient des antivirus, journalisent les évènements les plus pertinents et mettent en place une veille en vulnérabilités.

Documents de référence :

- ✓ *ISO 27002 ch. 12, sécurité liée à l'exploitation*

- ✓ *NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Systems and Organizations*
- ✓ *COBIT 5, processus facilitants*

5.2.11 Gestion des incidents

Les systèmes peuvent être l'objet de menaces qui vont des fichiers de données corrompus aux désastres naturels, en passant par les virus.

Les organismes publics sont invités à établir une capacité de traitement opérationnel des incidents incluant des étapes de préparation adéquate, de détection, d'analyse, de confinement et de reprise des activités. Ils doivent traquer, documenter et reporter les incidents aux autorités appropriées de l'organisme public. Si l'incident dépasse les frontières de l'organisme ou s'il porte atteinte à la vie des citoyennes et citoyens, ils doivent le déclarer comme incident à portée gouvernementale et s'en référer à l'autorité désignée à cet effet.

Documents de référence :

- ✓ *Guide sur la gestion des incidents de sécurité de l'information* (ex PR-060 – à produire par le CERTAQ)
- ✓ *ISO 27002 ch. 16, gestion des incidents liés à la sécurité de l'information*
- ✓ *ISO 27035, technologies de l'information – techniques de sécurité – gestion des incidents de sécurité de l'information*
- ✓ *NIST SP 800-61, Computer Security Incident Handling Guide*
- ✓ *COBIT 5, processus facilitants*

5.2.12 Contrôle d'accès physique

Le contrôle d'accès physique désigne les mesures prises pour protéger les systèmes, les bâtiments et les infrastructures de soutien connexes contre les menaces liées à leur environnement physique.

Les organismes publics sont invités à limiter aux seules personnes autorisées l'accès physique aux systèmes, aux équipements et aux environnements d'exploitation respectifs. Ils vont protéger l'infrastructure physique et les systèmes contre les risques environnementaux et fournir des services de soutien aux systèmes, en plus de protéger et de fournir des contrôles environnementaux appropriés dans les installations contenant des systèmes.

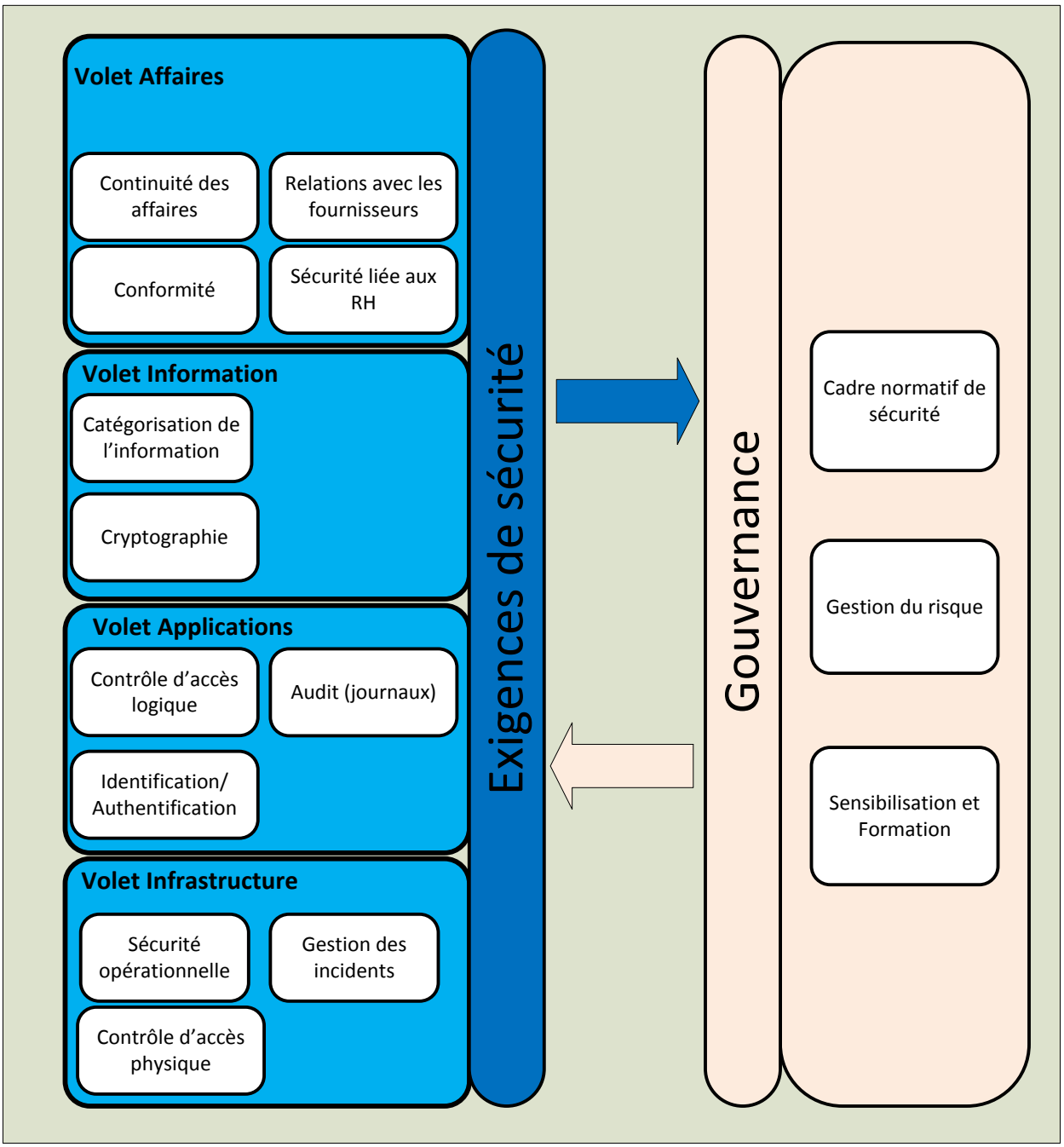
Documents de référence :

- ✓ *ISO 27002 ch. 11, sécurité physique et environnementale*
- ✓ *NIST SP 800-116, a Recommendation for the Use of PIV Credentials in Physical Access Control Systems*

5.3 Modèle de référence ASI de l'OP

Comme vu précédemment, et en référence au modèle d'architecture de sécurité de l'information gouvernementale (ASIG), l'ASI de l'organisme public est composée idéalement d'une partie « gouvernance » et d'une partie « exigences de sécurité ». En voici un modèle :

Figure 4 Composantes ASI de l'OP



Les volets Affaires, Information, Applications et Infrastructure sont ceux de l'architecture d'entreprise de l'organisme public.

- ✓ Le volet Affaires désigne la stratégie d'affaires, les modèles, les processus et les services. Il s'agit de la base sur laquelle reposent toutes les décisions relatives aux autres domaines de l'architecture d'entreprise.

- ✓ Le volet Information permet de cerner, de documenter et d'administrer les besoins en information de l'entreprise, d'attribuer la propriété et la responsabilité de l'information en question et de décrire la manière dont les parties intéressées entreposent les données et les échangent. Il s'agira de faire l'inventaire de l'information, de la classifier et de déterminer l'usage qui en sera fait.
- ✓ Le volet Applications représente le portefeuille des applications de l'organisme public et détermine les systèmes opérationnels qui permettent et soutiennent l'exécution des processus opérationnels pour illustrer les limites des applications.
- ✓ Le volet Infrastructures décrit l'infrastructure technique de l'organisme public et les technologies particulières de matériel et de logiciel qui soutiennent les systèmes d'information.

Références

COBIT 5 : un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise

COBIT 5 : Processus facilitants

COBIT 5 for Information Security

COBIT 5 for Information Risk

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Systems and Organizations

NIST SP 800-116, a Recommendation for the Use of PIV Credentials in Physical Access Control Systems

NIST SP 800-61, Computer Security Incident Handling Guide

NIST SP 800-133, Recommendation for Cryptographic Key Generation

NIST SP 800-30, Risk Management Guide

NIST SP 800-34, Contingency Planning Guide

ISO 27001, management de la sécurité de l'information

ISO 27002, technologies de l'information – techniques de sécurité – code de bonne pratique pour le management de la sécurité de l'information

ISO 27005, technologies de l'information – techniques de sécurité – gestion des risques liés à la sécurité de l'information

Guides de pratiques recommandées du Secrétariat du Conseil du trésor (PR 0xx)

Directive sur la sécurité de l'information gouvernementale

Approche stratégique gouvernementale 2014-2017

Cadre de référence de l'architecture de sécurité de l'information gouvernementale (ASIG)

Architecture d'entreprise gouvernementale (AEG 3.2)

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique