Pratique recommandée en sécurité de l'information

PR-065

Guide d'audit de la sécurité de l'information

ENSEMBLE on fait avancer le Québec

Québec

Guide d’audit de la 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
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 – Juillet 2016
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-76207-2 (en ligne)

Table des matières

Table des figures

Sigles et Acronymes

Acronymes :

CISA : *Certified Information System Auditor*

ISO : *International Organisation for Standardization* (Organisation internationale de normalisation)

OP : Organisme public

COBIT : *Control Objectives for Information and related Technology*

Remerciements

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

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Lyonel Vallès, chargé de projet
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Carmen Saint-Laurent
Bureau de décision et de révision

Daniel Guimont
Commission des lésions professionnelles

Claude Côté
Commission des transports du Québec

Daniel Carpentier
Contrôleur des finances

François Belleau
Ministère de l'Éducation, du Loisir et du Sport

Denis Shaink
Ministère des Finances

Gérard Tremblay
Ministère de la Justice

Marthe-Anaïs Kambou
Réseau de la santé et des services sociaux

Jacques Blouin
Régie de l'assurance maladie du Québec

Reynald Crépin
Régie des rentes du Québec

Pierre Bonhomme
Régie des rentes du Québec

Christian Marcotte
Société de l'assurance automobile du Québec

Farid Almahsani
Secrétariat du Conseil du trésor

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 » 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 et 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 ces derniers, de les adapter à leur organisation respective et aux risques qui leur sont propres.

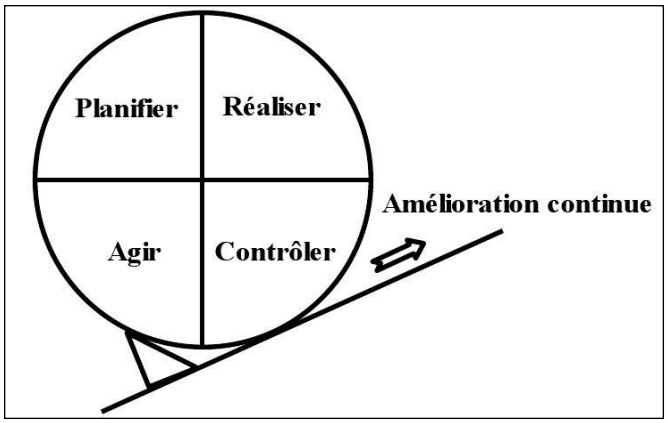
1. Introduction

Indépendamment de sa forme de stockage (électronique ou papier) ou de son mode de transmission (courrier postal ou courrier électronique), l'information gouvernementale est constamment exposée à des risques et sa sécurité doit être évaluée de façon régulière. Le présent guide sert de référence aux organismes publics lors de la mise en œuvre d'un audit de la sécurité de l'information. À cet effet, il propose une approche par étapes, qui peut être adaptée aux besoins particuliers de chaque organisme.

Afin de tirer parti de façon optimale de la pratique proposée, il convient de positionner celle-ci dans le cycle d'amélioration continue de la sécurité (cycle itératif) comme le préconise la norme ISO/CEI 27001 – norme portant sur la gestion de la sécurité de l'information.

La Figure 1 présente le cycle d'amélioration continue de la sécurité comme illustré par la roue de Deming.

Figure 1 : La roue de Deming



1.1 Contexte

Le présent guide est réalisé en application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) et de la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics; ces deux textes placent la sécurité de l'information au cœur de leurs priorités.

Ce guide prend appui sur quatre documents structurants ayant permis d'asseoir les fondements du nouveau cadre de gouvernance de la sécurité de l'information :

- ✓ La **Directive sur la sécurité de l'information** qui énonce, en son article 7.f, que les organismes publics doivent s'assurer de la réalisation d'un audit de la 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.
- ✓ Le **Cadre gouvernemental de gestion de la sécurité de l'information** qui complète les dispositions de la Directive sur la sécurité de l'information en précisant l'organisation

fonctionnelle de la sécurité de l'information ainsi que les rôles et responsabilités sur les plans gouvernemental et sectoriel. Il définit notamment le rôle de la vérification interne dans l'évaluation de l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

- ✓ L'**Approche stratégique gouvernementale en sécurité de l'information 2014-2017** qui fixe les cibles gouvernementales en matière de sécurité de l'information pour les trois prochaines années. Elle statue qu'en matière d'audit de la sécurité de l'information les travaux viseront à mettre à la disposition des organismes publics des procédés d'autoévaluation de l'adéquation des mesures de sécurité par rapport aux risques encourus.
- ✓ 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 sécurité de l'information gouvernementale et qui peuvent avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

1.2 Objectifs

Le présent guide est à l'usage des ministères, des organismes budgétaires et autres que budgétaires et des établissements du réseau de la santé et des services sociaux et du réseau de l'éducation[1]. Conformément au paragraphe f de l'article 7 de la Directive sur la sécurité de l'information gouvernementale, il vise à couvrir l'ensemble des étapes d'une mission d'audit de la sécurité de l'information. Il permet ainsi d'avoir une compréhension générale des activités réalisées aux différentes étapes de l'audit.

1.3 Clientèle cible

Le document s'adresse aux organismes publics appelés à effectuer des audits de la sécurité de l'information. Il concerne plus particulièrement les intervenants dont les responsabilités sont énoncées dans le Cadre gouvernemental de gestion de la sécurité de l'information. Il s'agit notamment :

- ✓ Des gestionnaires;
- ✓ Des détenteurs de l'information;
- ✓ Des responsables organisationnels de la sécurité de l'information (ROSI);
- ✓ Des conseillers organisationnels en sécurité de l'information (COSI);
- ✓ Des coordonnateurs organisationnels de gestion des incidents (COGI);

1. Au sens de la Loi sur la gouvernance et la gestion des ressources informationnelle des organismes publics et des entreprises du gouvernement, chapitre G-1.03, article 2.

- ✓ Des intervenants dans des domaines connexes à la sécurité de l'information : responsables de la sécurité physique, spécialistes en gestion des risques, auditeurs internes, responsables de l'accès et de la protection des renseignements personnels, responsables de la continuité des services, spécialistes en technologies de l'information, etc.

2. L'audit de la sécurité de l'information

L'audit de la sécurité de l'information vise à s'assurer de l'efficacité des mesures de sécurité en place dans l'organisme. Il permet de constater les écarts entre les mesures appliquées et celles normalement requises pour une bonne prise en charge des risques de l'organisation en matière de sécurité de l'information et de formuler, le cas échéant, des recommandations en vue de corriger les écarts repérés.

L'audit est réalisé par une personne ou une équipe compétente et indépendante des opérations et activités de l'entité auditée. Cette indépendance assure la conduite des travaux de façon professionnelle et objective. Pour s'assurer de la compétence des intervenants, il est toujours préférable d'engager des personnes détenant les certifications appropriées pour réaliser les travaux en audit. À ce sujet, se référer à la section 4 du présent document relativement aux compétences de l'auditeur.

Les référentiels d'audit

Pour réaliser son travail, l'auditeur s'appuie en général sur une démarche structurée. À cet égard, l'utilisation d'un référentiel d'audit est recommandée. Un référentiel d'audit est un ensemble codifié de règles, de procédures ou de bonnes pratiques reconnues internationalement que l'auditeur utilise pour mener à bien sa mission et pour formuler ses recommandations. Le référentiel permet ainsi à l'auditeur de mieux asseoir ses recommandations et d'en renforcer la pertinence.

Le référentiel tient compte des domaines dont les éléments sont susceptibles de faire l'objet, en partie ou en totalité, d'un audit de la sécurité. En matière de sécurité de l'information, plusieurs référentiels peuvent être utilisés. On peut citer notamment COBIT, les GTAG et ISO 27002.

COBIT

COBIT est un référentiel élaboré par l'ISACA, organisme à but non lucratif spécialisé dans la gouvernance et la sécurité de l'information[2]. Il propose l'application d'un cadre intégrant des connaissances en gouvernance de la sécurité de l'information et il permet à l'organisation de l'utiliser comme cadre unique et complet.

Dans sa version 5, COBIT rassemble les connaissances dispersées dans différents cadres et modèles de l'ISACA (COBIT 4.1, Risk IT, Val IT). Il prend aussi en considération les normes internationalement reconnues en sécurité de l'information comme la famille ISO/CEI 2700X, les standards de bonnes pratiques en sécurité de l'information de l'ISF(Information Security Forum) et les standards SP800-53A de l'US National Security Institute of Standards and Technology (NIST[3]).

GTAG

Les GTAG (*Global Technology Audit Guides*) font référence à une série de guides développés à l'Institut des auditeurs internes (IIA[4]) par des professionnels en provenance de divers milieux.

2. www.isaca.org
3. Ibid.
4. Guides pratiques d'audit des TI : www.theiia.org

Ces guides sont principalement destinés au personnel de gestion et aux auditeurs internes. Ce sont des outils qui peuvent les informer sur les différents risques liés à la technologie et sur les pratiques recommandées.

Chaque guide traite d'un thème qui a trait à la gestion, au contrôle et à la sécurité des systèmes d'information.

ISO 27002

La norme ISO 27002 fait partie des normes de la famille ISO 2700X qui promeuvent les meilleures pratiques de gestion de la sécurité de l'information[5]. Cette norme propose une série de contrôles permettant de tenir compte des risques de sécurité de l'information sur le plan organisationnel.

3. Les étapes de l'audit

Le présent chapitre décrit les différentes étapes d'un audit de la sécurité de l'information. L'audit peut être réalisé à l'interne par le personnel de l'organisme ou en ayant recours à des auditeurs externes.

Un audit de la sécurité de l'information comprend en général les étapes suivantes :

- ✓ Étape 1 : Planification;
- ✓ Étape 2 : Réalisation de l'audit;
- ✓ Étape 3 : Rapport;
- ✓ Étape 4 : Suivi des recommandations;

Étape 1 – Planification

L'étape de la planification consiste à élaborer une stratégie générale pour la réalisation de l'audit. Ses objectifs sont notamment les suivants :

- ✓ Obtenir une base pour formuler une opinion, laquelle devra se fonder sur des éléments probants, suffisants et pertinents pour s'assurer de l'absence d'écarts importants entre les pratiques appliquées dans l'organisme et ce que prévoient les lois, les directives, les règlements ou les meilleures pratiques.
- ✓ Fixer les rôles et responsabilités des parties prenantes à l'exercice.
- ✓ Prendre connaissance de la mission et des processus de l'organisme à auditer.
- ✓ S'informer des réglementations régissant l'organisation ou l'unité sur laquelle porte l'audit.

5. www.iso.org

- ✓ Acquérir une bonne connaissance des lieux visés par l'audit. L'auditeur documentera l'environnement informatique de l'organisme, si nécessaire, et les aspects de gouvernance qui s'y appliquent, c'est-à-dire la mission, les objectifs, la vision, etc;
- ✓ Acquérir une bonne connaissance de la structure organisationnelle de l'organisme. L'auditeur se renseignera également, le cas échéant, sur la formation et l'expérience du personnel exerçant les tâches associées à la sécurité;
- ✓ Déterminer une stratégie de coordination de la mission d'audit, des échanges de correspondance et de la prise de rendez-vous;
- ✓ Noter les contraintes liées à l'audit. Par exemple, prévoir la non-disponibilité de certaines personnes et tenir compte des ressources (humaines, matérielles, etc.) nécessaires au succès du mandat d'audit;
- ✓ Préparer le programme d'audit. Celui-ci est l'un des principaux documents réalisés au cours de la planification. Il présente les étapes clés de la réalisation de l'audit, notamment ses objectifs, les points de contrôle à considérer, les tests à réaliser et les ressources nécessaires. Un exemple de programme d'audit est présenté à l'annexe II du présent guide.

Une évaluation des risques peut être réalisée à l'étape de la planification. Elle a notamment pour but de prioriser les efforts à déployer afin d'assurer une bonne gestion du personnel disponible. Si une évaluation du risque a déjà été faite dans l'organisation, elle peut tout simplement servir pendant l'audit.

Le dossier d'audit

À l'étape de la planification, l'auditeur commence la mise en place du dossier d'audit. Celui-ci rassemble les documents de travail produits et mis à jour tout au long de l'exercice d'audit. Le dossier d'audit constitue l'un des principaux outils de travail de l'auditeur. Il comporte en général les sections suivantes :

- ✓ Section **Planification.** Cette section contient les points considérés à l'étape de la planification. On y trouve, notamment, les éléments suivants :
  - Énoncé des objectifs de l'audit;
  - Énoncé de l'étendue de l'audit;
  - Information sur la consultation des dossiers d'audits précédents et de leurs recommandations;
  - Budget de l'audit (Ressources humaines, matérielles et autres nécessaires à l'audit);
  - Correspondance avec l'audité;
  - Effort en heures de travail et durée estimée de l'audit;
  - Programme d'audit.
- ✓ Section **Points en suspens***.* Il s'agit de points pertinents qui ne sont pas pris en considération dans le présent exercice, mais qui seront traités lors d'un prochain audit, si nécessaire. Les éléments suivants y sont consignés :
  - Points soulevés dans les dossiers précédents, mais non traités;
  - Points à examiner dans de prochains audits, si nécessaire.

- ✓ Section **Exécution**. Cette section rassemble les documents créés pendant l'exécution du travail d'audit. Elle contient notamment les éléments suivants :
  - Comptes rendus des entrevues avec les personnes rencontrées;
  - Résultats des tests;
  - Réponses aux questionnaires;
  - Formulaires sur le constat des écarts, incluant les commentaires de l'audité;
  - Documents divers.
- ✓ Section **Rapports**. On trouve dans cette section toutes les versions du rapport d'audit. Elle contient principalement :
  - Le projet de rapport intermédiaire qui a été discuté avec l'audité lors de la réunion de clôture de l'audit (voir section suivante);
  - Le rapport final.

Le dossier d'audit contient une colonne Index. On y inscrit le numéro unique[6] de chacun des documents consignés dans le dossier pour permettre de le repérer facilement.

La bonne tenue du dossier d'audit renseigne sur le sérieux et le professionnalisme de l'auditeur. Ce dossier servira de base à toute évaluation de son travail.

Étape 2 – Réalisation de l'audit

L'étape de réalisation de l'audit est celle au cours de laquelle les travaux de terrain sont menés. Pendant cette étape, différents outils de collecte sont utilisés pour recueillir l'information en tenant compte de la portée de l'audit.

La rencontre de démarrage

Les travaux débutent, en général, par une rencontre de démarrage réunissant auditeurs et audités (gestionnaires, utilisateurs concernés, etc.). Cette rencontre sert à :

- ✓ Présenter les objectifs de l'audit;
- ✓ Identifier les parties prenantes à l'exercice;
- ✓ Expliquer la portée et les limites de l'exercice;
- ✓ Établir la liste de distribution du rapport préliminaire;
- ✓ Élaborer le calendrier des rencontres;
- ✓ Répondre aux interrogations des parties prenantes sur le déroulement de l'audit.

6. Ce numéro se trouve dans le champ indexé présent dans chaque document considéré. Voir un exemple de ce champ indexé dans les livrables présentés à l'annexe II du présent guide.

La réalisation de l'audit

En fonction du programme d'audit établi à l'étape de la planification (voir section 3.1), l'auditeur recueille des preuves qui lui permettront de relever les écarts entre les mesures appliquées et celles qui sont normalement requises et de formuler ses recommandations. Par exemple, dans un audit de la sécurité de l'information utilisant le référentiel COBIT, l'auditeur recueille des preuves concernant chacun des objectifs de contrôle sélectionnés de COBIT en appui aux domaines visés par l'audit. Cependant, un audit utilisant la norme ISO 27002 utiliserait une démarche semblable, mais requerrait des activités de vérification différentes.

Les techniques d'audit

Pour la réalisation de l'audit, différentes techniques sont utilisées. Les techniques d'audit sont les moyens appliqués pour évaluer les mesures de sécurité en place selon les domaines considérés. Ces techniques dépendent de la nature spécifique du cas pris en considération. Les différentes techniques auxquelles fait appel l'auditeur sont, notamment, les suivantes.

- ✓ L'observation – Technique qui permet à l'auditeur d'observer les actions, les façons d'accomplir un travail ou le comportement des employés en vue de s'assurer d'une information ou de relever certaines insuffisances. Par exemple, une visite des lieux de travail indiquera à l'auditeur si des mots de passe sont affichés à côté des écrans d'ordinateur ou si l'accès aux salles de serveurs est protégé.
- ✓ Le questionnaire – Technique qui permet de détecter des anomalies liées au dispositif de contrôle de la sécurité en place dans l'organisme. Les écarts constatés sont étudiés et appuyés par des preuves tangibles. Par exemple, à propos de la question concernant la participation du ROSI ou du COSI aux réunions sur la sécurité de l'information, l'auditeur pourra solliciter les procès-verbaux de ces rencontres comme preuve.
- ✓ L'entrevue – Technique de collecte de l'information qui permet à l'audité de fournir des explications sur un sujet donné. L'entrevue aide à mieux comprendre certains éléments qui ne peuvent être divulgués ou approfondis par un questionnaire. Les talents de communicateur de l'auditeur aideront à la réussite de l'entrevue.
- ✓ Les sondages par échantillon – Technique statistique qui permet, à partir d'un échantillon prélevé de façon aléatoire dans une population donnée, d'extrapoler à la population totale les observations faites sur l'échantillon. Par exemple, on peut se faire une opinion sur le respect d'une directive concernant les accès logiques en choisissant un échantillon de comptes d'anciens utilisateurs d'un système et en vérifiant si ces comptes ont été désactivés.

Pour s'assurer du bon déroulement de l'audit et conserver une communication correcte entre l'auditeur et l'audité, il est souhaitable de tenir régulièrement des rencontres pour discuter des principaux constats, pour formuler des recommandations ou pour soulever toute autre problématique. Les écarts sont communiqués à l'audité au fur et à mesure de leur constatation par l'auditeur. Une telle démarche réduit les situations conflictuelles et les effets de surprise lors de la remise du projet de rapport. Les procès-verbaux de ces réunions sont conservés dans le dossier d'audit.

Étape 3 – Rapport

Cette étape sert à la production du rapport d'audit. Les éléments de ce rapport doivent nécessairement être appuyés par des preuves consignées dans le dossier d'audit.

Le rapport d'audit constitue le produit fini de l'exercice. Il reprend les différentes étapes du mandat, indique les écarts et énonce des recommandations. Ce rapport doit être préparé avec la plus grande rigueur, puisque ses recommandations serviront de base à la prise de décisions en vue de corriger les écarts constatés. Le rapport est généralement préparé en deux phases.

Phase 1

L'auditeur transmet un projet de rapport à l'audité en vue de recueillir ses commentaires. Le projet de rapport est discuté au cours d'une rencontre de clôture regroupant l'auditeur et les responsables de l'entité auditée[7]. Pendant cette rencontre, le responsable de la mission présente le projet de rapport et demande à l'audité de formuler ses commentaires.

Phase 2

À la suite de la rencontre de discussion, le rapport final intégrant les commentaires de l'audité est produit pour être présenté à la haute direction. Le rapport d'audit contient au minimum les parties suivantes.

- ✓ Sommaire
- ✓ Objectifs et étendue de l'audit
- ✓ Résultats de l'audit
  - Constatations
  - Recommandations
  - Commentaires de l'audité
- ✓ Remarques générales
- ✓ Approbation par l'audité
- ✓ Signature des responsables de l'entité auditée

Étape 4 – Suivi des recommandations

L'étape de suivi des recommandations permet à l'organisation de s'assurer que les recommandations de l'auditeur ont été prises en considération. Il appartient à l'audité d'appliquer les recommandations formulées et d'assurer le suivi de leur mise en œuvre. Cette mise en œuvre du suivi des recommandations s'accompagne généralement d'un plan d'action

7. Il est possible que plus d'une rencontre soit prévue pour la discussion du rapport ou que des rencontres soient organisées pour chaque unité organisationnelle.

qui se traduit par un tableau comprenant les recommandations avec les dates arrêtées et les personnes responsables de leur mise en place.

4. Les compétences de l'auditeur

Cette section a pour objectif d'aider à la sélection d'un prestataire externe de service d'audit de la sécurité de l'information. Elle ne s'applique pas nécessairement à l'auditeur interne. Celui-ci fait déjà partie de l'organisme et normalement, il possède les compétences nécessaires à la réalisation de ses tâches.

4.1 Compétences

Les qualités professionnelles de l'auditeur de la sécurité de l'information sont une des conditions de succès de sa mission et une assurance quant à la valeur ajoutée que l'organisme audité tirera de l'exercice. Si l'auditeur ne fait pas déjà partie de l'organisme, son choix doit être fait de façon judicieuse. L'auditeur doit, en plus de sa formation générale, faire la preuve d'une solide expérience dans le domaine. La gouvernance de la sécurité de l'information couvrant des secteurs divers, l'auditeur doit avoir les connaissances requises, non seulement celles concernant la portée et les exigences relatives à la sécurité de l'information, mais aussi à la gouvernance des technologies de l'information, à l'architecture technologique et à la gestion des risques en matière de sécurité, etc. L'auditeur doit par ailleurs démontrer une complète indépendance, en fait et en apparence, concernant tous les sujets sur lesquels portera son travail et il ne doit pas être en position de conflit d'intérêts.

Il est aussi recommandé que le professionnel qui effectue l'audit de la sécurité de l'information possède de grandes qualités relationnelles, puisque ses tâches le mettront constamment en contact avec le personnel de l'organisme.

4.2 Certifications de soutien

Les certifications en audit de la sécurité permettent de présumer que l'auditeur possède les connaissances minimales des méthodologies, des techniques et des divers types d'outils disponibles dans ce domaine pour accomplir adéquatement son mandat. Ainsi, détenir une certification professionnelle sera un atout pour l'auditeur, bien que la certification ne soit pas obligatoire pour réaliser des travaux d'audit.

Actuellement, la certification la plus reconnue en matière d'audit de la sécurité de l'information est le CISA (*Certified Information System Auditor*[8]). Elle est en effet la seule certification admise qui soit exclusivement consacrée à l'audit, au contrôle et à la sécurité de l'information.

La certification CISA est délivrée par l'ISACA. Son but est de reconnaître la qualification des auditeurs en ce qui a trait à l'évaluation de la sécurité de l'information.

8. www.isaca.org/cisa

D'autres certifications en sécurité de l'information (CISSP[9], CEH[10], CRISC[11], CISM[12]), couplées à plusieurs années d'expérience ainsi qu'à une connaissance approfondie des techniques d'audit, pourraient indiquer à l'organisme public que le professionnel possède les qualifications nécessaires pour s'acquitter de sa mission d'audit de la sécurité de l'information de façon professionnelle. De plus, la certification CIA (délivrée par l'IIA[13]) permet à l'auditeur interne d'accomplir une mission d'audit selon les normes reconnues en matière d'audit interne.

4.3 Considérations supplémentaires

Dans la majorité des cas, le personnel qui accomplit des mandats d'audit de la sécurité de l'information est appelé à prendre connaissance de l'information sensible de l'organisme. Il doit donc faire preuve d'un haut niveau de professionnalisme et de discrétion. De son côté, l'organisme qui recrute un auditeur de la sécurité de l'information doit exercer sa vigilance en encadrant son choix par les mesures de sécurité adéquates liées à une telle embauche. À cet égard, la réalisation préalable d'une enquête d'habilitation ainsi que le filtrage de sécurité sont à considérer.

9. CISSP : *Certified Information Systems Security Professionnal*; https://www.isc2.org/CISSP
10. CEH : *Certified Ethical Hacker*; http://www.eccouncil.org/Certification/certified-ethical-hacker
11. CRISC : *Certified in Risk and Information Systems Control*; http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control
12. CISM : *Certified Information Security Manager*; http://www.isaca.org/certification/cism-certified-information-security-manager
13. CIA : *Certified Internal Auditor* : https://na.theiia.org/certification/CIA-Certification/Pages/CIA-Certification.aspx

ANNEXE I Définitions

Actif informationnel : Tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., chapitre C-1.1). Cette même loi, assimile au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Confidentialité : Propriété d'une information de n'être accessible et divulguée qu'aux personnes ou entités désignées et autorisées.

Disponibilité : Propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

Intégrité : Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

Politique de sécurité : Énoncé général émanant du conseil d'administration et indiquant la ligne de conduite adoptée relativement à la sécurité, à sa mise en œuvre et à sa gestion.

Prestataire : Entreprise ou personne ayant les compétences pour accomplir des mandats d'audit de la sécurité de l'information.

Risque : De manière générale, sans être nécessairement appliqué au domaine de la sécurité de l'information, un risque est une probabilité d'apparition d'une menace qui, dans le cas de l'exploitation d'une situation de vulnérabilité, peut potentiellement avoir un impact sur un actif informationnel (actif ou information). (Source : Norme ISO/CEI 27005)

Système d'information : Ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y compris, notamment, les technologies de l'information et les procédés utilisés pour exercer ces fonctions.

ANNEXE II Principaux livrables de l'audit

Cette annexe présente un exemple des principaux livrables de l'audit[14]. Il s'agit des documents suivants :

1. Le programme d'audit;
2. Le formulaire de constat des écarts;
3. Le rapport d'audit;
4. Le formulaire de suivi des recommandations.

14. Tous ces livrables ainsi que les autres documents produits pendant l'audit doivent nécessairement être joints au dossier d'audit.

A. Programme d'audit

Le programme d'audit est préparé à l'étape de la planification.

Cet exemple présente un programme d'audit dont l'objet est l'audit de la conformité d'un organisme public aux obligations de l'article 7 de la Directive sur la sécurité de l'information gouvernementale. Ce programme peut être modifié pour s'adapter aux besoins particuliers d'un organisme.

Programme d'audit de la conformité d'un organisme public aux dispositions de l'article 7 la Directive sur la sécurité de l'information gouvernementale[15]

Préparé par :	Vérifié par :
Date :	Date :

Index	Description des actions à accomplir	Date	Commentaires
	1. Objectifs et portée de l'audit		
	1.1. Définir les objectifs de l'audit Cette partie décrit les objectifs globaux de l'audit. Elle aide l'auditeur à préciser les objectifs de l'audit. Cet audit a pour but de vérifier la conformité de l'organisme aux obligations de l'article 7 de la Directive sur la sécurité de l'information gouvernementale.		
	1.2. Définir les limites de l'audit L'audit doit avoir un périmètre défini. L'auditeur doit comprendre l'organisation de la sécurité de l'information et définir un champ d'application pour l'audit. 1.2.1. Obtenir l'organigramme de l'organisme en vue de comprendre le fonctionnement de la fonction sécurité de l'information et la description des tâches associées. 1.2.2. Préciser le champ qui sera couvert par l'audit (p. ex. tout l'organisme, la fonction sécurité de l'information, etc.). 1.2.3. Déterminer les limites ou repérer les contraintes susceptibles d'avoir une incidence sur l'audit.		

15. Dans ce programme, qui peut être modifié selon les besoins particuliers de chaque organisme, l'auditeur passe en revue toutes les obligations faites par l'article 7 (7.a à 7.k) de la directive et il vérifie si l'organisme s'y conforme.

	2. Gouvernance et gestion de la sécurité de l'information		
	2.1. L'organisme a-t-il adopté et mis en œuvre une politique de sécurité de l'information (cf. 7.a)? Obtenir la documentation appropriée. 2.1.1. Si oui, la maintient-il à jour et assure-t-il son application? 2.1.2. Documenter.		
	2.2. L'organisme a-t-il adopté et mis en œuvre un cadre de gestion de la sécurité de l'information (cf. 7.a)? Obtenir la documentation appropriée. 2.2.1. Si oui, ce cadre est-il maintenu à jour et son application est-elle assurée? 2.2.2. Documenter. Pour les deux questions précédentes, demander la documentation appropriée.		
	2.3. Déterminer si l'organisme a déposé au dirigeant principal de l'information (cf. 7.b) : 2.3.1. Une planification des actions en matière de sécurité de l'information. Cette planification inclut-elle les priorités d'action et les échéanciers afférents découlant des exercices d'audit et de tests d'intrusion? 2.3.2. Un bilan de sécurité de l'information. Obtenir la documentation appropriée pour le dernier exercice. L'auditeur doit recevoir la documentation pour les points 2.3.i) et 2.3.ii) pour l'exercice, et vérifier que le plan d'action et le bilan de sécurité ont été présentés suivant une périodicité bisannuelle.		

	2.4. S'assurer que l'organisme a mis en œuvre des processus formels de sécurité de l'information[16]. 2.4.1. Vérifier si l'organisme assure la gestion des risques (cf. 7.c). 2.4.1.1. Obtenir le plan de gestion des risques. 2.4.1.2. Obtenir le document de classification des actifs informationnels. 2.4.1.3. L'organisme a-t-il réalisé une analyse de risques au cours de l'exercice précédent? Vérifier, le cas échéant, la cohérence des résultats de l'analyse de risques. 2.4.1.4. Vérifier que l'organisme a déclaré au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale (cf. 7.d). Obtenir la documentation pertinente.		
	2.4.2. Vérifier si l'organisme assure la gestion de l'accès à l'information (cf. 7.c). 2.4.2.1. Obtenir la directive sur les accès logiques de l'organisme. 2.4.2.2. Est-elle approuvée par les responsables? 2.4.2.3. Son application est-elle évaluée par l'organisme? Obtenir la documentation pertinente.		

16. D'autres aspects peuvent être pris en considération en plus de ceux indiqués aux points 2.4.1 à 2.4.3.

	2.4.3. Vérifier si l'organisme assure la gestion des incidents (cf. 7.c). 2.4.3.1. Obtenir la directive sur la gestion des incidents. 2.4.3.2. Est-elle approuvée par les responsables? 2.4.3.3. Son application est-elle évaluée par l'organisme? 2.4.3.4. Vérifier que l'organisme a déclaré au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale au cours de l'exercice précédent (cf. 7.e). Obtenir la documentation pertinente.		
	2.5. Vérifier que l'organisme a réalisé des audits de sécurité de l'information (cf. 7.f). Obtenir et examiner les rapports d'audit de l'exercice précédent. Repérer les questions en suspens et, suivant le cas, décider ou non de traiter ces questions. Pour ce point, l'auditeur doit vérifier que les audits sont réalisés suivant une périodicité bisannuelle.		
	2.6. Vérifier que l'organisme a réalisé des 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 et les échéanciers afférents (cf. 7.g). Obtenir et examiner les rapports de tests d'intrusion pour l'exercice précédent. Repérer les questions en suspens et, suivant le cas, décider ou non de traiter ces questions. Pour ce point, l'auditeur doit vérifier que les tests d'intrusion sont réalisés suivant une périodicité annuelle.		

	2.7. Vérifier que l'organisme a mis en place un registre d'autorité de la sécurité de l'information. Vérifier que sont consignés dans ce registre, notamment, 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 (cf. 7.h). Obtenir la documentation pertinente.		
	2.8. Vérifier que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comportent des clauses garantissant le respect des exigences en matière de sécurité de l'information (cf. 7.i). Vérifier si un processus existe pour intégrer les exigences de sécurité de l'information dans l'élaboration des ententes portant sur le niveau de service (SLA) avec les fournisseurs de services technologiques. 2.8.1. Obtenir un échantillon de SLA et déterminer si la fonction de sécurité de l'information avait été incluse dans ces ententes. 2.8.2. Déterminer si un processus existe pour intégrer les exigences de sécurité de l'information dans le cadre du développement des applications.		
	2.9. Vérifier si l'organisme favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor (cf. 7.j). Obtenir la documentation relative aux services communs déterminés par le Conseil du trésor et vérifier la conformité des pratiques de l'organisme à leur égard.		

	2.10. Vérifier si l'organisme a mis en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information (cf. 7.k). 2.10.1. Obtenir le plan de sensibilisation à la sécurité de l'information en usage dans l'organisme et évaluer sa pertinence. 2.10.2. Obtenir le plan de formation à la sécurité de l'information en usage dans l'organisme et évaluer sa pertinence.		

B. Formulaire de constatations

Pour chaque constat d'écart, un exemplaire de ce formulaire est rempli. Il contient :

- ✓ L'énoncé de la constatation;
- ✓ Les critères sur lesquels s'appuie la constatation;
- ✓ Le risque relatif à l'écart constaté;
- ✓ Les recommandations.

Le formulaire est transmis à l'audité pour communication du constat. De son côté, le responsable de l'entité auditée formule ses commentaires en remplissant la partie du formulaire réservée à cette fin. Par ses commentaires, l'audité peut notamment adopter les positions suivantes :

- ✓ D'accord avec les constatations et recommandations;
- ✓ D'accord seulement avec les constatations;
- ✓ En désaccord avec la ou les constatations;
- ✓ En désaccord avec les recommandations.

L'audité peut également choisir de ne pas formuler de commentaires.

Formulaire de constatations

Index _____

Préparé par :	*Vérifié Par:*
Date :	*Date :*

Constatation (ce qui est)

Critère (ce qui devrait être. Référence aux bonnes pratiques, par exemple)	Risque (conséquences éventuelles pour l'organisme)

Recommandations

Commentaires de l'audité (doit être rempli par l'audité)

Cocher l'une ou l'autre case, S.V.P

☐ D'accord avec les constatations et recommandations	☐ D'accord seulement avec les constatations	☐ En désaccord avec la ou les constatations; (si plusieurs constatations, préciser celles avec lesquelles vous êtes en désaccord)	☐ En désaccord avec la ou les recommandations (si plusieurs recommandations, préciser celles avec lesquelles vous êtes en désaccord)

Justification du choix ou autres commentaires

Signature :_____ Date :_____

	Oui	Non
Recommandation mise en œuvre durant la mission		
Recommandation en cours de mise en œuvre		

C. Rapport d’audit

Comme indiqué à la section 3.3, le rapport d’audit est préparé en deux phases à l’étape 3 de l’audit. Un rapport d’audit contient généralement, au minimum, les parties suivantes.

1. Sommaire

   Le sommaire expose d’une façon très brève les objectifs de l’audit, les principales constatations et les recommandations les plus importantes. Cette partie du rapport est destinée à la haute direction. Elle donne une idée générale de la réalisation de l’audit.

2. Objectifs et étendue de la mission

   Dans cette partie du rapport, on indique les objectifs de l’audit et les domaines touchés par l’exercice.

3. Résultats de la mission

   Cette partie recense les résultats de l’audit. On y trouve principalement les écarts constatés. Pour chaque écart, l'information suivante est indiquée :

   a. Constatation : l’énoncé du constat;
   b. Recommandations : les recommandations faites par l’auditeur pour corriger l’écart constaté;
   c. Commentaires de l’audité : l’audité peut être ou non d'accord avec l’auditeur à propos de l’écart constaté ou de la recommandation formulée. Il peut aussi choisir de ne pas formuler de commentaire sur l’écart constaté.

4. Remarques générales

   Dans cette partie, l’auditeur peut porter toutes les remarques générales concernant le mandat d’audit. Il y notera aussi la coopération, ou non, de l’entité auditée.

5. Approbation de l’audité

Cette partie est utilisée pour la signature du rapport par les responsables de l’entité auditée. En signant le rapport, ils confirment les commentaires qu’ils ont formulés sur le travail de l’auditeur.

D. Formulaire de suivi des recommandations

Index _____

Le formulaire de suivi des recommandations propose un plan d'action pour la mise en œuvre du suivi des recommandations formulées par l'auditeur. Il peut se présenter comme suit :

Référence	Constatation	Responsable du suivi	À réaliser le jj/mm/aaa	Réalisé le jj/mm/aaa	Remarque

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique