ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

THÈSE PRÉSENTÉE À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION DU
DOCTORAT EN GÉNIE
Ph. D.

PAR
Luc POULIN

LA SÉCURITÉ DES APPLICATIONS EN TECHNOLOGIE DE L'INFORMATION – UNE APPROCHE D'INTÉGRATION DES ÉLÉMENTS DE SÉCURITÉ DANS LE CYCLE DE VIE DES APPLICATIONS ET DES SYSTÈMES D'INFORMATION

MONTRÉAL, LE 15 SEPTEMBRE 2015

À mon père Raymond,
un être fondamentalement bon, doté d'un esprit curieux, déterminé et animé par des valeurs de partage et d'honnêteté,

À ma mère Suzanne,
qui m'a appris que toute grande réalisation commence par un rêve,

En remerciement pour leur legs, leurs enseignements et leur soutien indéfectible.

PRÉSENTATION DU JURY

CETTE THÈSE A ÉTÉ ÉVALUÉE

PAR UN JURY COMPOSÉ DE :

M. Michel Kadoch, Ph. D., président du jury
Département de génie électrique à l'École de technologie supérieure, Québec

M. Witold Suryn, Ph. D., membre du jury
Département de génie logiciel et des TI à l'École de technologie supérieure, Québec

M. Issa Traoré, Ph. D., membre externe du jury
Département de « Electrical and Computer Engineering » à l'université de Victoria, Colombie-Britanique

ELLE A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 22 AVRIL 2015

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

Tout au cours de la réalisation de cette thèse de doctorat, plusieurs personnes m'ont épaulé : je leur en suis très reconnaissant.

En tout premier lieu, je tiens à remercier mes directeurs de recherche, messieurs Alain Abran et Alain April, professeurs au département de génie logiciel et des technologies de l'information à l'École de technologie supérieure de l'Université du Québec. Leurs judicieux conseils et leurs remarques pertinentes m'ont aidé à bien orienter mon travail de recherche.

Merci aussi aux professeurs Michel Kadoch et Witold Suryn de l'École de technologie supérieure, ainsi qu'au professeur Issa Traoré de l'université de Victoria, pour leur participation au jury de cette thèse.

Ma gratitude s'adresse également à M. Bruno Guay. Son amitié et son esprit critique ont été un atout précieux. Les nombreuses discussions et les argumentations que nous avons eues tout au long de la rédaction de cette thèse ont permis de clarifier et de compléter les théories avancées. Merci également à M^{me} Nathalie Paré et M^{me} Sylvie Trudel pour leur soutien indéfectible et l'amitié qu'elles m'ont témoignés tout au long de ce processus laborieux.

De plus, je voudrais remercier M^{me} Jocelyne Breton pour son professionnalisme habituel dans la correction et la mise en page de cette thèse.

Enfin, ma famille et mes amis ont droit à toute ma reconnaissance pour m'avoir soutenu et encouragé. Votre présence, votre amitié et votre affection m'ont insufflé l'énergie nécessaire pour mener cette thèse à terme.

LA SÉCURITÉ DES APPLICATIONS EN TECHNOLOGIE DE L'INFORMATION – UNE APPROCHE D'INTÉGRATION DES ÉLÉMENTS DE SÉCURITÉ DANS LE CYCLE DE VIE DES APPLICATIONS ET DES SYSTÈMES D'INFORMATION

Luc POULIN

RÉSUMÉ

L'industrie des technologies de l'information (TI) et les organisations qui les utilisent ont à leur disposition beaucoup de moyens pour développer, acquérir et maintenir des applications sécuritaires. Toutefois, bien qu'il existe pour ce faire une panoplie de bonnes pratiques, de normes et d'outils, les organisations peinent à atteindre ce but.

Seize problématiques permettant d'expliquer cette situation ont été identifiées au cours de cette recherche dont le but est de concevoir, de faire approuver par une organisation internationale de normalisation, et de rendre accessible à ceux qui développent ou qui utilisent des applications, un nouveau modèle de sécurité des applications (modèle SA). L'utilisation de ce modèle permet la mise en place et la démonstration de la sécurité d'une application, assurant ainsi la protection des informations sensibles impliquées par son utilisation. Le modèle SA propose des concepts, des principes, des processus et des composants pour permettre à une organisation de se doter d'un cadre normatif répondant à ses besoins de sécurité, tout en respectant ses capacités.

Ce modèle SA permet de prendre en compte les contextes d'affaires, juridiques et technologiques spécifiques aux environnements où les applications sont développées et utilisées. Il permet aussi de gérer les risques de sécurité provenant des personnes, des processus et de la technologie qui pourraient menacer les informations sensibles impliquées par ces applications. Ce modèle SA permet d'identifier et de mettre en place un ensemble de contrôles et de mesures de sécurité afin d'assurer un niveau de confiance de la sécurité d'une application durant son cycle de vie. Finalement, le modèle SA permet à l'organisation qui l'utilise de fournir les preuves mesurables et répétables indiquant l'atteinte et le maintien du niveau de confiance ciblé, en fonction du contexte d'utilisation spécifique de ses applications.

Le modèle SA inclut les différents éléments d'une architecture de sécurité des applications pouvant être utilisés par les organisations et l'industrie des TI. Ces éléments sont définis, validés, testés et intégrés dans un cadre normatif qui sera utilisé comme une source autoritaire guidant la mise en œuvre de la sécurité pour les applications d'une organisation.

Mots clés : génie logiciel, informatique, modèle sécurité application, ISO 27034

APPLICATION SECURITY IN INFORMATION TECHNOLOGY – AN APPROACH FOR INTEGRATING SECURITY ELEMENTS IN THE LIFE CYCLE OF APPLICATIONS AND INFORMATION SYSTEMS

Luc POULIN

ABSTRACT

The information technology (IT) industry and organizations that use IT have at their disposal many resources to develop, acquire and maintain secure applications. However, although there is a variety of best practices, standards and tools that affect applications security, organizations are struggling to achieve that goal.

Sixteen issues to explain this situation were identified in this research, which goal is to design, to get approved by an international standards organization and to make available to those who develop or use applications, a new model of application security (AS model). Using this AS model will help to implement and demonstrate the security of an application, thus ensuring the protection of sensitive information involved in its use.

The AS model offers concepts, principles, processes and components to enable an organization to develop a normative framework that meets its security needs, while respecting its capabilities.

This AS model considers the business, legal and technological environments where specific applications are developed and used. It also helps to manage the security risks from the people, processes and technology that could threaten sensitive information involved in these applications. This AS model allows an organization to identify and implement a set of controls and security measures to ensure a level of confidence in the security of an application during its life cycle. Finally, the AS model allows the organization to provide measurable and repeatable evidence achieving and maintaining a target level of confidence, depending on the context of use of specific applications.

The AS model includes different elements of application security architecture that can be used by organizations and the IT industry. These elements are defined, validated, tested and integrated by organizations in a normative framework to be used as an authoritative source to guide the implementation of security for their applications.

Keywords: software engineering, computer science, application security model, ISO 27034

TABLE DES MATIÈRES

Page

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

Afin de faciliter la lecture, les abréviations, signes et acronymes utilisés dans cette thèse correspondent à ceux habituellement utilisés dans l'industrie du développement de logiciel, indépendamment de leur langue d'origine. Par exemple, l'abréviation ISO sera privilégiée à OIN pour présenter l'Organisation internationale de normalisation.

$(ISC)^2$	International Information Systems Security Certification Consortium
ACM	Association for Computing Machinery
ANSSI	Agence nationale de la sécurité des systèmes d'information
APIIQ	Association professionnelle des informaticiens et informaticiennes du Québec
ASIA	Application Security Issues Analysis
CISA	Certified Information System Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information System Security Professional
CLASP	Comprehensive, Lightweight Application Security Process
CLUSIF	Club de la Sécurité de l'Information Français
CMMI	Capability Maturity Model Integration
CNA	Cadre normatif de l'application
CNO	Cadre normatif de l'organisation
COBIT	Control Objectives for Information and related Technology
CSA	Contrôle de sécurité des applications
CSSLP	Certified Secure Software Lifecycle Professional
DGEQ	Directeur général des élections du Québec
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
FIPS	Federal Information Processing Standards
IEC	International Electronic Commission

IEEE	Institute of Electrical and Electronics Engineers
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organisation
ISSMP	Information System Security Management Professional
ITIL	Information Technology Infrastructure Library
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
MÉHARI	Méthode harmonisée d'analyse des risques
Modèle SA	Modèle de la sécurité des applications
MRCVSA	Modèle de référence du cycle de vie de la sécurité des applications
NdC	Niveau de confiance
NESSI	Networked European Software and Services Initiative
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCDE	Organisation for Economic Co-operation and Development
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OWASP	Open Web Application Security Project
SA	Sécurité des applications/Sécurité d'une application
SC27	Sous-comité 27 de l'organisation ISO
SDL	Security Developpment Lifecycle
SEI	Software Engineering Institute
SGSI	Système de gestion de la sécurité de l'information
SSE-CMM	System Security Engineering – Capability Maturity Model
SVÉ	Système de votation électronique
TI	Technologies de l'information

LISTE DES SYMBOLES

Un rectangle représente un ou plusieurs éléments utilisés, produits ou modifiés par un processus ou une activité.

Un rectangle à coins arrondis représente un processus.

Un rectangle pointillé représente un groupe d'éléments.

Un rectangle pointillé à coins arrondis représente un groupe de processus.

Ce symbole représente un acteur ayant un rôle et une implication dans un processus, une tâche ou une activité.

Ce symbole représente un contrôle de sécurité des applications (CSA).

Cette flèche représente une action lorsque l'étiquette de la flèche est un verbe, ou un transfert d'information lorsque l'étiquette est un nom.

INTRODUCTION

Les technologies de l'information (TI) font partie de notre quotidien : elles sont utilisées par tous, autant par des particuliers qui s'en servent pour réaliser des activités personnelles et professionnelles, que par des entreprises et des organisations[1] de toute taille et de tous les secteurs d'affaires. Chaque jour, une quantité d'information considérable et variée est transmise, traitée et conservée à l'aide des TI. L'usage généralisé des TI entraîne des conséquences sur la protection des renseignements sur les personnes et les organisations qui les utilisent.

Ce traitement de l'information est réalisé par des applications[2], composées de logiciels intégrés à des composants TI. Toute vulnérabilité dans ces logiciels et ces composants peut avoir un impact sur la sécurité des informations concernées par l'utilisation de l'application. Que faut-il faire pour mieux protéger les informations manipulées par une application ou inhérentes à l'utilisation de celle-ci?

C'est en 1997, lors d'un mandat de développement d'une application d'envergure, que nous avons pris conscience des problèmes de sécurité de l'information qui pouvaient provenir de l'utilisation d'une application TI stratégique dans l'entreprise. La réalisation de ce mandat, d'une durée de 3 ans, nécessitait le recours à une équipe de développement de plus de 100 personnes. Les problèmes de sécurité liés à ce projet provenaient principalement du processus de développement et de l'arrimage des besoins de cette application avec ses infrastructures technologiques soit, notamment, ses environnements de développement, de tests et opérationnel.

---

[1] Afin d'alléger le texte, le terme *organisation* sera utilisé pour représenter tout type de regroupements de personnes ayant un objectif commun, tels que : des entreprises, des compagnies, des corporations, des institutions gouvernementales, des organismes ou une de leurs divisions.

[2] Afin d'alléger le texte et lorsque le contexte le permet, l'expression *application* sera utilisée pour représenter tout type d'applications TI, d'applications informatiques ou de systèmes d'information.

L'industrie des TI n'est pourtant pas dépourvue d'outils pour développer des applications sécuritaires. Il existe une panoplie de bonnes pratiques, de normes et d'outils qui concernent la sécurité. Par exemple, Microsoft propose son *Security Developpment Lifecycle* (SDL) (Microsoft, 2010, p. 31) tandis que Le Projet public de sécurité des applications Web (OWASP) propose des guides de développement d'applications Web et de tests de sécurité (OWASP, 2005) (OWASP, 2008b). Pourquoi alors l'industrie des TI peine-t-elle à développer et à maintenir des applications sécuritaires?

Le Directeur général des élections du Québec (DGEQ) en a fourni un exemple, lorsqu'en 2006, il a décrété un moratoire pour suspendre l'utilisation des systèmes électroniques de votation : 140 municipalités québécoises avaient utilisé des systèmes de votation électroniques durant les élections municipales de 2005 et la majorité d'entre elles avaient rencontré des difficultés majeures provenant de l'utilisation des systèmes de votation électroniques dont, notamment, des problèmes de déploiement, d'utilisation, de fiabilité et d'intégrité (DGEQ, 2006). Ces problèmes avaient amené les citoyens concernés à douter de la validité des résultats de ces élections, ce qui a forcé le DGEQ à ouvrir une enquête.

L'enquête subséquente demandée par le DGEQ, que nous avons réalisée à l'étape de nos travaux prédoctoraux, a démontré qu'aucune des solutions TI proposées par les différentes entreprises n'a passé avec succès l'audit de sécurité demandé. Les résultats des vérifications mettent en doute la fiabilité de ces systèmes, car même si l'on ne peut affirmer hors de tout doute raisonnable que les résultats de ces élections obtenus avec ces systèmes sont faux, on ne peut pas non plus prouver qu'ils sont justes.

La problématique soulevée par la votation électronique n'est pas isolée. Les vulnérabilités de la sécurité des systèmes et des applications demeurent d'actualité (Savard et Poulin, 2008) (Neumann, 1996) (*Voir* l'appendice A – ANNEXE V). Les chercheurs et l'industrie œuvrant dans le domaine de la sécurité de l'information ont déjà produit une abondante littérature, des outils, des processus et des méthodes pour proposer des solutions à ce problème, mais les situations où la sécurité des applications (SA) est mise en cause sont encore légion.

Puisqu'il existe déjà une panoplie de bonnes pratiques, de normes et d'outils de toutes sortes en développement d'applications Web, en tests de sécurité, et en méthodologies de développement et de maintenance d'applications, pourquoi ne sommes-nous toujours pas en mesure de développer et de maintenir une application sécuritaire à un coût raisonnable pour l'organisation qui aurait à l'utiliser?

Malgré les recherches et tous les outils développés, un modèle de SA qui permettrait d'organiser tous ces éléments dans un ensemble cohérent semble encore inexistant.

La motivation première de ce projet de recherche doctorale est de développer une approche d'intégration des éléments de sécurité dans le cycle de vie des applications et des systèmes d'information. Cette approche se concrétisera par la conception d'un modèle qui aidera les organisations à développer, à utiliser et à maintenir des applications qu'elles pourront considérer comme sécuritaires.

En effet, le modèle devra permettre l'arrimage, ainsi que l'utilisation cohérente et complémentaire de l'ensemble des éléments concernant la sécurité de l'information, visant l'atteinte d'un objectif de sécurité d'une organisation en fonction de son contexte d'affaires et des moyens dont elle dispose. Il devra être conçu de manière à ce qu'il soit possible d'augmenter le niveau de SA en proposant l'intégration d'activités de sécurité vérifiables aux endroits requis dans son cycle de vie, et ce, dans une organisation ayant déjà des processus établis. Ce modèle devra aussi fournir, à l'organisation qui l'utilisera, les preuves nécessaires produites par des processus de vérification garantissant la répétabilité des résultats et soutenant l'affirmation qu'une application est sécuritaire.

Le but étant d'assister l'organisation dans l'atteinte d'un niveau de sécurité requis pour son application, sans lui demander de changer ses processus de développement ou de maintenance. Le modèle proposé préconisera plutôt une évolution progressive de la maturité de l'organisation en fonction de sa ligne d'affaires et de ses besoins de sécurité.

On dit d'un processus de mesure qu'il est répétable lorsqu'il produit le même résultat à chaque fois qu'il est utilisé pour mesurer la même valeur dans un même contexte (Abran, 2010, p. 124). Le résultat obtenu par ce processus doit être indépendant de la personne qui effectue la mesure.

Ayant conscience que ce travail de recherche couvre plusieurs domaines de connaissances et de secteurs d'interventions liés à la sécurité des applications, il est important d'intégrer à la stratégie de recherche une démarche de vérification qui favorise la participation d'un grand nombre d'experts de plusieurs pays. Dans la cadre de ce projet de recherche, des circonstances exceptionnelles ont permis la participation de plusieurs experts, provenant de différents domaines d'expertises en sécurité des TI, à des cycles de la validation Delphi du modèle SA.

Le contenu de cette thèse est présenté selon la structure suivante :

1) « Travaux préparatoires ». Ce chapitre 1 introduit le contexte de la SA et identifie ses problématiques majeures;
2) « Objectifs et méthodologie de recherche ». Ce chapitre 2 présente une synthèse des problématiques et des enjeux identifiés, afin de préciser le but et les objectifs de cette recherche, ainsi que les stratégies et la méthodologie de recherche proposée;
3) « Revue de littérature ». Ce chapitre 3 présente une analyse de la couverture des problématiques sous l'angle de la SA, permettant de dégager les principaux constats et les premières pistes de solution pouvant corriger les principales lacunes en SA;
4) « Conception du modèle de la sécurité des applications ». Ce chapitre 4 présente le développement et la vérification, à l'aide de la méthode Delphi, des éléments requis pour compléter un modèle de la sécurité des applications (modèle SA). Ceci inclut une vue chronologique de notre contribution au développement du modèle SA, permettant d'en obtenir une vision globale complète et d'introduire les principaux concepts et principes qui y sont intégrés. Ce chapitre présente également la deuxième phase des travaux de recherche qui a permis d'introduire le modèle à des organisations et d'utiliser certains de

ses éléments dans des projets de sécurité d'applications réels en industrie, afin d'avoir leurs commentaires sur la pertinence et l'utilité de ces éléments de sécurité pour l'industrie;

5) « Le modèle de la sécurité des applications ». Ce chapitre 5 présente, dans une vision globale de ce qu'implique la sécurité d'une application, les éléments suivants :

   - les enjeux de la mise en place du modèle SA pour une organisation, les besoins de l'audience ciblée, les caractéristiques du modèle, sa portée ainsi que les éléments clés qui composent le modèle. Il présente aussi les concepts, principes, termes et définitions amenés par le modèle et qui déterminent son positionnement par rapport aux normes, guides, méthodes et bonnes pratiques existants dans le domaine;

   - les principaux composants du modèle dont le comité de gestion du cadre normatif de l'organisation, les contextes d'affaires, juridiques et technologiques de l'application, la bibliothèque de contrôles CSA, le modèle de référence du cycle de vie de la sécurité d'une application (MRCVSA), la matrice de la traçabilité de la sécurité des applications de l'organisation et le cadre normatif de l'application (CNA); et

   - les processus clés permettant à une organisation de mettre en place et de gérer des éléments du modèle qu'elle a introduit dans son cadre normatif. Il présente ensuite les processus requis pour gérer et harmoniser la sécurité de ses applications dans l'ensemble de l'organisation;

6) « Validation du modèle SA ». Ce chapitre 6 présente la stratégie de validation du modèle ainsi que les événements clés qui se sont produits au cours des différents cycles Delphi de la validation, du déploiement et de la vérification empirique partielle du modèle SA;

7) « Contributions du chercheur et ATTEINTE DES OBJECTIFS DE RECHERCHE ». Ce chapitre 7 présente les résultats de ce travail de recherche, soit les éléments clés qui ont été amenés par le chercheur, démontrant l'atteinte des objectifs de recherche visés ainsi que les limites du modèle de la SA;

8) « Conclusion ». Ce dernier chapitre présente les premières évidences de l'impact du modèle SA dans l'industrie et suggère une liste de travaux futurs.

CHAPITRE 1

TRAVAUX PRÉPARATOIRES

Ce chapitre présente une vue d'ensemble des motivations du chercheur ainsi que des travaux préparatoires qu'il a réalisés pour bien cerner la problématique de la sécurité des applications (SA) en technologie de l'information. Ces travaux visent d'abord l'identification de tous les aspects à considérer pour déterminer l'approche de la question à privilégier. Ce faisant, les défaillances actuelles de la SA ont été mis en lumière et leurs sources ont été identifiées. Ces premiers constats ont permis d'entrevoir la gravité des impacts de la SA en fonction des contextes où elle doit jouer un rôle déterminant afin assurer le bon fonctionnement et l'intégrité des technologies de l'information. Voici donc l'ordre de déroulement de ces travaux préparatoires :

1) La motivation du chercheur (1.1);
2) La sécurité de l'information et la gestion du risque (1.2);
3) Les contextes de la sécurité de l'information (1.3);
4) L'analyse de l'impact de ces contextes sur la sécurité des applications (SA) (1.4);
5) La synthèse de la problématique de la SA (1.5).

1.1 Motivation du chercheur

Les différentes facettes de la problématique de la sécurité des applications nous sont apparues pour la première fois en 1997, alors que nous participions, à titre d'architecte principal et technologique, à un projet de développement d'une application multiserveur d'envergure de gestion d'inventaires. Malgré la disponibilité de bonnes pratiques de sécurité et de méthodes de développement en génie logiciel reconnues, le projet n'arrivait pas à produire une application qui pouvait être déployée en toute confiance, tel que commandé par le client. De plus, une partie du code source a été perdue, dû à des défaillances matérielles et à des processus inadéquats de gestion de l'environnement, de développement et de tests.

Dans ce projet qui impliquait une équipe de développement d'environ 150 personnes, notre rôle était de proposer des solutions pour améliorer des processus servant, notamment, à soutenir les analystes et les développeurs dans la gestion du code source, et à améliorer l'arrimage de l'ensemble à l'architecture technologique utilisée par l'application dans un environnement de développement et de production.

Même si on ne peut pas qualifier ce projet de développement d'application comme étant un grand succès, il constitue le point de départ de notre réflexion sur la sécurité des applications, et c'est ce qui nous a permis de débuter et d'orienter nos travaux de recherche universitaires en génie logiciel dans ce domaine de spécialisation.

Durant les dix années qui ont suivi cette expérience, un questionnement subsistait : connaissant la disponibilité de tous ces outils, méthodes et pratiques recommandés disponibles dans le domaine de la sécurité, que manque-t-il pour permettre le développement et l'utilisation d'applications sécuritaires?

1.2 Sécurité de l'information et gestion du risque

La « sécurité de l'information » se définit comme étant la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information (ISO/IEC, 2004a), (ISO/IEC, 2009d).

Par exemple, la norme internationale ISO 27000 définit :

- la confidentialité, comme étant la propriété d'une information à n'être disponible ou communiquée qu'à une entité[3] autorisée;
- l'intégrité, comme étant la propriété d'une information à ne pouvoir être modifiée ou supprimée que par une entité autorisée;

[3] Une entité peut être autant une personne ou un groupe de personnes, qu'un processus informatique.

- la disponibilité, comme étant la propriété d'une information à n'être accessible et utilisable sur demande que par une entité autorisée.

Selon ces définitions, toute perte de confidentialité, d'intégrité ou de disponibilité d'une information impliquée par une TI doit être considérée comme une violation de la sécurité de l'information, et ce, quelles qu'en soient les conséquences.

Par exemple, la perte de réputation d'une personne, provoquée par la divulgation d'une information confidentielle personnelle la concernant, et la perte monétaire d'une organisation, provoquée par la destruction d'une information financière lui appartenant, seront considérées comme des problèmes de sécurité de l'information autant que la perte de la vie d'une personne provoquée par la corruption d'une information contenue dans la mémoire d'un composant technologique. Toutefois, ces conséquences ont des niveaux très différents de gravité. Une perte de réputation peut généralement être indemnisée, mais la perte d'une vie peut avoir un impact beaucoup plus grand sur l'entourage de la personne décédée.

Cet exemple introduit un premier élément important du domaine de la gestion de la sécurité de l'information, soit : la gestion du risque.

La norme ISO 27000 définit le risque comme étant la combinaison de la probabilité d'un événement et de ses conséquences (ISO/IEC, 2009d, p. 4).

Afin de pouvoir gérer la sécurité d'une information, il faut être en mesure d'évaluer les risques (probabilité, événement et conséquences) qui pourraient menacer les informations à protéger. Cette même norme définit la gestion du risque comme étant « la coordination d'activités visant à diriger et à contrôler une organisation en fonction des risques »[4]. Cette

[4] Toutes les citations tirées de documents en anglais ont fait l'objet d'une traduction libre par l'auteur de cette thèse.

gestion comprend généralement l'évaluation, le traitement, l'acceptation, la communication, le suivi et la révision de l'évaluation des risques (ISO/IEC, 2009d, p. 5). La gestion des risques de sécurité permet d'identifier et d'évaluer les risques qui pourraient être associés à la perte, à la divulgation ou à la corruption d'une information, et de les ramener à un niveau acceptable à l'aide de mécanismes appelés : contrôles de sécurité. Plus les conséquences résultant de la violation de la sécurité d'une information seront graves, plus cette information devra être considérée comme étant sensible; il sera d'autant plus important de mettre en place des contrôles afin de ramener les risques de sécurité à un niveau acceptable.

Cet état de fait introduit un deuxième élément important du domaine de la gestion de la sécurité de l'information : pour pouvoir gérer la sécurité de l'information, tous les risques doivent être connus et acceptés.

1.3 Contextes de la sécurité de l'information

La sécurité de l'information concerne la gestion de la protection des informations, quel qu'en soit le support (ISO/IEC, 2009d), (SEI, 2001). L'approche de la gestion de la sécurité de l'information par la gestion des risques de sécurité requiert l'identification des informations sensibles de l'organisation pour lesquelles les conséquences découlant de la perte, de la corruption ou de la divulgation seront les plus graves. Cette approche a l'avantage de permettre aux organisations de mieux gérer leurs ressources en les canalisant sur la protection des informations qu'elle aura évaluées comme étant plus sensibles (SEI, 2001), (DCSSI, 2004), (ANSSI, 2004), (Alberts et al., 2005), (ISO/IEC, 2010d).

Andress apporte un nouvel élément aux contextes de la sécurité de l'information en expliquant qu'un des défis de la sécurité de l'information est d'intégrer les personnes, les processus et la technologie : ces risques de sécurité peuvent provenir, par ordre d'importance, de ces trois sources (Andress, 2003).

Il existe plusieurs outils pour aider les organisations à identifier correctement leurs informations sensibles et à gérer les risques qui les menacent, tels que :

- les guides *A Guide to Building Secure Web Applications and Web Services* (OWASP, 2005), *Code review guide* (OWASP, 2008a), *Testing guide* (OWASP, 2008b) de l'OWASP, *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) (Alberts et al., 2005) du *Software Engineering Institute* (SEI)/Carnegie Mellon, l'Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) (ANSSI, 2004) de l'Agence nationale de la sécurité des systèmes d'information (ANSSI),
- les méthodes d'analyse de risques de sécurité organisationnelle, telles que la Méthode harmonisée d'analyse des risques (MÉHARI) du Club de la sécurité de l'information Français (CLUSIF) (CLUSIF, 2005),
- le système de gestion de la sécurité de l'information (SGSI) de la série de normes ISO 27000 (ISO/IEC, 2005d), etc.

Viennent ensuite une panoplie de processus et d'outils de toutes provenances permettant la mise en place de contrôles visant à ramener les risques identifiés à un niveau acceptable pour une organisation. Sans en faire une liste exhaustive, il existe des processus tels que l'*Information Technology Infrastructure Library* (ITIL) (OGC, 2007) de l'Office du commerce du gouvernement du Royaume-Uni, et des outils qui ont pour objectif de contrer certaines problématiques technologiques, tels que les coupe-feux, les antivirus, les systèmes de sauvegarde des données et les systèmes de détection d'intrusions. Concernant le développement d'applications TI, les guides et les bonnes pratiques en sécurité d'OWASP (OWASP, 2005; 2008a; 2008b), le SDL de Microsoft (Microsoft, 2010), ainsi que plusieurs normes conjointes du *Federal Information Processing Standards* (FIPS) et du *National Institute of Standards and Technology* (NIST) (*Voir* l'appendice A – ANNEXE IX) sont disponibles pour mettre en place des contrôles.

Ayant à leur disposition toutes ces méthodes, ces bonnes pratiques et ces outils, les organisations réussissent-elles à protéger adéquatement les informations sensibles impliquées par les TI qu'elles utilisent? Les sections suivantes examinent cette problématique.

1.4 Analyse de l'impact de ces contextes sur la sécurité des applications (SA)

Nous avons identifié 16 problématiques de la SA suite à l'analyse des trois contextes suivants, soit : le contexte d'affaires, le contexte juridique et le contexte technologique (Poulin et Guay, 2006a, p. 10).

1.4.1 Problèmes de SA selon le contexte d'affaires

Cette section a pour but de déterminer quels sont les secteurs d'affaires touchés par des problèmes de sécurité de l'information (confidentialité, intégrité, disponibilité) amenés par l'utilisation d'applications TI, et d'en identifier sommairement les causes et les conséquences.

Les *Software Engineering Notes* de Neumann font mention de centaines d'accidents, dont certains mortels, impliquant l'informatique (Neumann, 1996). Au Québec, l'Association professionnelle des informaticiens et informaticiennes du Québec (APIIQ) a aussi dénombré, dans son mémoire « Encadrer la profession informatique, maintenant une nécessité! », des cas d'incidents dus à l'utilisation de systèmes d'information (Savard et Poulin, 2008).

Afin de procéder à l'identification des secteurs d'affaires qui peuvent être touchés par la sécurité des informations impliquées par l'utilisation d'applications TI, Neumann propose un regroupement des différents domaines d'applications reliés à l'utilisation de systèmes d'information : les communications, l'aérospatiale, la défense, le transport, le contrôle de sécurité critique (vie humaine), le secteur médical, la création et le transport d'électricité, le secteur financier, les élections, les établissements carcéraux, le secteur juridique, etc. Bien qu'incomplète (Neumann, 1996), car elle n'identifie pas les secteurs où peuvent être utilisées des applications TI telles que Google, Facebook et YouTube, cette classification est adéquate pour aider l'identification rapide de la majorité des secteurs d'affaires où sont utilisées les TI.

Cette classification sera utilisée ci-après pour faciliter la présentation de quelques exemples de situations qui ont été répertoriés et documentés, et dans lesquelles les risques reliés à l'utilisation de systèmes d'information n'ont pas été correctement gérés.

Les exemples mentionnés ci-après proviennent principalement de (Savard et Poulin, 2008). Voir l'appendice A – ANNEXE IV et ANNEXE V pour plus de renseignements sur les cas présentés en exemple dans le Tableau 1.1, qui indique, pour chacun des cas présentés, s'il a causé une perte de confidentialité (C), d'intégrité (I) ou de disponibilité (D) de données de l'application TI, ainsi que les principales conséquences résultant de ces situations.

Les TI sont présentes dans presque toutes les sphères de l'activité humaine, des systèmes de radiothérapie aux systèmes comptables, de la domotique aux centrales nucléaires, des cartes à puce aux stimulateurs cardiaques, en passant par les systèmes de gestion de médicaments et les guichets automatiques. Tous les secteurs touchés par la sécurité des informations impliqués par les TI seront de plus en plus nombreux.

Ces exemples démontrent que les dommages et inconvénients causés par la perte de la disponibilité, de la confidentialité ou de l'intégrité des informations reçues, traitées, conservées et communiquées par des applications peuvent parfois entraîner des conséquences très graves qui affectent tous les domaines d'affaires où des applications TI sont utilisées.

Tableau 1.1 Synthèse par secteur d'affaires, des cas et conséquences de bris de sécurité de l'information impliquant des applications

	Cas	A causé une perte de			Conséquences
		C	I	D	
Secteur des transports	a) 2006, dysfonctionnement du système de transport rapide BART		✓	✓	1. Données erronées acceptées par le système 2. Ouvertures des portes lorsque le train était en marche 3. Arrêt et retard du train
	b) 2010, dysfonctionnement du logiciel de la voiture Prius de Toyota			✓	1. Délai de traitement du signal de freinage trop long 2. Collisions et accidents de voiture 3. Rappels pour mises à jour du logiciel défectueux 4. Poursuites judiciaires
	c) 2000, panne dans un système de réservation de billets d'Air Canada			✓	1. Indisponibilité des systèmes durant la panne 2. Retards et annulations de plusieurs vols 3. Paiement de frais de séjour aux personnes ayant manqué leurs correspondances
Secteur financier	a) 2004, panne à la Banque Royale du Canada			✓	1. Indisponibilité des comptes de 2,5 millions de clients durant la panne 2. Frais causés par les retards de transactions
	b) 2007, panne à la Banque CIBC	✓		✓	1. Perte d'information de 470 000 Canadiens 2. Perte du fichier de sauvegarde 3. Investigation du vérificateur général du Canada
Secteur gouvernemental	a) 2005, arrêt d'applications liées à l'impôt sur le revenu des particuliers québécois			✓	1. Perte de revenu pour le gouvernement du Québec
	b) 2005, problèmes des systèmes de votation électronique	✓	✓	✓	1. Doutes sur le résultat des élections 2. Perte de la confidentialité d'une partie de la liste électorale 3. Enquête du DGEQ 4. Moratoire interdisant le vote électronique au Québec 5. Pertes de contrats de plusieurs millions
	c) 2004, panne du système d'approbation du paiement des prêts et bourses			✓	1. Des milliers d'étudiants sans prêts ni bourses pour la rentrée
Systèmes des communication	a) 2003, accès d'administration aux routeurs Cisco	✓	✓	✓	1. Modifications possibles des données d'administration du routeur 2. Accès possible aux données reçues et transmises par le routeur 2. Arrêt possible de service du routeur

Tableau 1.1 Synthèse par secteur d'affaires, des cas et conséquences de bris de sécurité de l'information impliquant des applications (suite)

	Cas	A causé une perte de			Conséquences
		C	I	D	
Secteur personnel	a) 2010, dysfonctionnement du composant de mise à jour du navigateur Web Firefox	✓		✓	1. Faille permettant le téléchargement et l'installation automatique de logiciels malicieux 2. Perte possible d'intégrité, de confidentialité et de disponibilité des informations accessibles par l'utilisateur
	b) 2010, divulgation d'information non autorisée, iPhone et Android	✓			1. Transmission de données personnelles sans autorisation 2. Perte possible de la confidentialité des informations de l'utilisateur

1.4.2 Problèmes de SA selon le contexte juridique

Le contexte juridique dans lequel un incident de sécurité survient a aussi un impact sur l'identification et l'évaluation des risques de sécurité. Par exemple, de nouvelles législations canadiennes[5] et québécoises[6] rendent maintenant les administrateurs personnellement responsables de la protection des informations sensibles gérées par leur organisation, par exemple les informations financières et les renseignements personnels qu'ils ont collectés. Ces lois stipulent qu'un manquement de leur part pourrait les amener en prison. L'importance de la sécurité de l'information prend donc, à leurs yeux, une toute nouvelle dimension.

De plus, on ne peut assumer qu'une application TI qui respectera la législation américaine, via les contrôles de sécurité qui y auront été appliqués, respectera automatiquement la

---

[5] *The federal Privacy Act*, *The Budget Measures Act* (Bill 198) aussi connu sous le nom : la Loi Sarbanes-Oxley canadienne, *The Personal Information Protection and Electronic Documents Act* (PIPEDA).

[6] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1), Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P-39.1).

législation canadienne. L'application Facebook est hébergée par des serveurs situés aux États-Unis, et elle contient notamment des informations personnelles de citoyens canadiens et américains. Immédiatement, des questions concernant la sécurité de l'information apparaissent. Comment ces informations doivent-elles être protégées? Selon les directives édictées dans la Loi américaine? Celles de la Loi canadienne?

C'est à cette deuxième conclusion qu'en est arrivée, le 16 juillet 2009, la commissaire à la protection de la vie privée du Canada dans son document intitulé *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection And Electronic Documents Act*. En effet, dans ce rapport, elle demande à l'organisation de modifier son application TI afin de s'ajuster à la règlementation canadienne sur la protection des renseignements personnels en regard des données des citoyens canadiens qui étaient conservées sur les serveurs de cette application TI (Denham, 2009). Ce rapport démontre clairement que le contexte juridique peut aussi influer sur les résultats d'une évaluation de la sécurité d'une application TI.

1.4.3 Problèmes de SA selon le contexte technologique

Avant l'arrivée de l'Internet, les risques de sécurité de l'information provenaient surtout de l'intérieur des organisations, de la qualité de leurs équipements technologiques ainsi que de la compétence et de l'intégrité des personnes qui pouvaient y avoir accès. Comme il s'agissait de problèmes principalement liés à la technologie, le premier réflexe de ces organisations a été, généralement, de déléguer la responsabilité de la protection des serveurs et de leurs informations au responsable de l'infrastructure des TI de l'entreprise; celui-ci devait prendre les mesures nécessaires pour acquérir et installer des contrôles de sécurité adéquats. Cela consistait principalement à la mise en place d'outils et de processus de relève et de sauvegarde de données, ainsi qu'à l'attribution et la gestion de droits d'accès aux utilisateurs des réseaux.

Dans les années 1990, les organisations y relient, une à une, leurs infrastructures TI à l'Internet. Il est aujourd'hui facile de comprendre que le risque de voir ces données compromises est beaucoup plus grand pour une application TI requérant un lien Internet que pour une application TI autonome.

Très vite, ces organisations ont réalisé que leurs informations sensibles étaient vulnérables à de nouvelles menaces : des pirates informatiques, des personnes et des logiciels malveillants pouvaient maintenant avoir accès à leurs informations de l'extérieur de l'organisation. Pour diminuer ces nouveaux risques, des coupe-feux, des antivirus, des systèmes de détection d'intrusion et plusieurs autres outils de sécurité ont alors été mis en place, tant sur les liens des réseaux que sur les serveurs et les postes de travail. L'amalgame et la coordination stratégiques d'un ensemble d'outils technologiques de sécurité constituent, depuis lors, le principal moyen de protection des informations contenues dans des infrastructures TI.

L'évolution et l'apparition de nouvelles menaces sur les informations qu'une organisation conserve sur ses systèmes illustrent que le contexte technologique peut aussi influencer le résultat d'une évaluation de la sécurité d'une application TI.

1.5 Synthèse de la problématique de la SA

L'utilisation d'applications induit la création ou le regroupement d'informations qui n'auraient peut-être pas existé dans l'organisation sans ces applications.

Le but de la sécurité des applications est de protéger l'information impliquée par l'utilisation des applications.

L'élaboration de la problématique de la sécurité des applications a pour but d'identifier les problèmes qui, s'ils ne sont pas tenus en compte, auront un impact négatif sur la protection de l'information d'une application. La démarche initiale de recherche a donc été de s'interroger sur le sujet pour permettre d'articuler, de hiérarchiser et d'identifier les

principaux obstacles auxquels il faudra apporter des solutions. C'est ainsi que l'on a pu identifier plusieurs problématiques, à l'étape des travaux préparatoires de cette recherche.

La version détaillée de cette analyse est présentée à l'appendice A – ANNEXE V.

Voici les 16 principales problématiques liées à la sécurité des applications :

P01 : Absence d'une vision globale de la sécurité des applications.

P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application.

P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations.

P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques.

P05 : Absence d'un vocabulaire et de références communes en sécurité des applications.

P06 : Absence d'une définition de la portée de la sécurité d'une application.

P07 : Absence d'une définition claire de ce qu'est une application sécuritaire.

P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application.

P09 : Absence de sources claires des exigences de sécurité d'une application.

P10 : Absence d'une méthode d'évaluation de la sécurité d'une application.

P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation.

P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications.

P13 : Absence de mécanismes permettant d'assigner aux principaux rôles, pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune des responsabilités qui leur sont assignées.

P14 : Les méthodes et outils existants de génie logiciel ne tiennent pas toujours compte de la sécurité de l'information TI.

P15 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur des processus impliqués dans la réalisation et l'opération de l'application.

P16 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur de l'application.

Telle que mise en évidence dans l'étude de cas de l'audit de sécurité des systèmes de votation électronique (DGEQ, 2006), l'atteinte du but de la SA ne se limite pas qu'à la sécurité de l'application logicielle elle-même (ISO/IEC, 2010g, p. 273), mais elle nécessite une vision plus globale de l'application, de façon à identifier les sources de l'ensemble des risques pouvant menacer les informations sensibles impliquées par l'utilisation d'une application, ainsi que le positionnement possible des contrôles de sécurité afin de diminuer à un niveau acceptable les risques identifiés.

CHAPITRE 2

OBJECTIFS ET MÉTHODOLOGIE DE RECHERCHE

Ce chapitre introduit la question de recherche (2.1) ainsi que les enjeux de la sécurité de l'information dans les applications qui ont été considérés (2.2). Ce sont ces éléments qui nous ont permis d'identifier le but de cette recherche (2.3), puis de préciser les objectifs de recherche (2.4) ainsi que les quatre axes de la stratégie de recherche pour les atteindre (2.5).

Les quatre phases de la méthodologie de recherche y sont également présentées (2.6). On y explique aussi la démarche d'identification et de sélection de la méthode Delphi comme technique à utiliser pour répondre aux exigences d'une recherche de niveau doctoral dans le domaine des TI, en appui à l'amélioration des pratiques du domaine de la sécurité des applications.

2.1 Question de recherche

Peut-on améliorer la sécurité d'une application, en développant un modèle permettant d'intégrer, de gérer et de vérifier des contrôles de sécurité tout au long de son cycle de vie? Et peut-on fournir à l'organisation qui l'utilise les preuves démontrant que le niveau de confiance qu'elle a ciblé pour son application a été atteint et maintenu?

2.2 Enjeux de la sécurité de l'information dans les applications

Les quatre principaux enjeux de la sécurité de l'information dans les applications sont :

1) D'assurer la protection adéquate des informations sensibles impliquées par l'application;
2) De rendre l'atteinte d'un niveau de sécurité démontrable et vérifiable pour ainsi justifier la confiance de l'organisation envers la protection de ses applications;
3) De favoriser l'intégration des activités de sécurité dans les processus existants de l'organisation afin de minimiser l'impact de la sécurité sur l'application;

4) De pouvoir soutenir l'implémentation du système de gestion de la sécurité de l'information (SGSI) dans une organisation (ISO/IEC, 2005d), telle qu'amené par l'intégration du modèle SA dans un projet du sous-comité 27 (SC27) de l'*International Standards Organisation* (ISO).

Les exigences et les procédés visés par ce modèle ne sont pas destinés à être mis en œuvre isolément, mais plutôt à être intégrés dans les processus existants de l'organisation. À cet effet, les organisations devraient identifier leurs processus et les éléments existants dans leurs cadres normatifs pour les comparer aux éléments proposés par ce modèle, réduisant ainsi l'impact de sa mise en œuvre.

À la fin de ce travail de recherche, le modèle SA qui sera développé devra :

1) Permettre d'affirmer qu'une application est sécuritaire, en fournissant les preuves que les contrôles de sécurité requis ont été identifiés, validés, mis en place, et qu'ils fonctionnent comme prévu, en fonction du niveau de confiance ciblé par l'organisation;
2) Fournir un modèle de sécurité des applications qui a été validé et approuvé par des experts, et qui permet d'implanter simultanément des contrôles de sécurité au niveau des personnes, des processus et de la technologie;
3) Soutenir l'implémentation de la norme ISO 27001 *Information security management systems – Requirements*.

2.3 But de la recherche

Le but de la présente recherche est de développer, faire vérifier et publier un modèle permettant à une organisation de mettre en place et de démontrer la sécurité d'une application, soit la protection des informations sensibles impliquées par son l'utilisation.

2.4 Objectifs de recherche

Les objectifs spécifiques de ce projet de recherche sont :

1) La mise au point d'un modèle SA qui propose un cadre normatif permettant :
   a) à une organisation d'identifier et d'intégrer des contrôles de sécurité durant tout le cycle de vie d'une application;
   b) de normaliser les activités et les contrôles de sécurité à l'intérieur de tous ses projets d'applications de l'organisation;
   c) d'identifier, de développer, de valider et de vérifier les contrôles de sécurité jugés prioritaires et de pouvoir les appliquer aux personnes, aux processus et à la technologie, dans l'application ou le produit développé;

2) La mise au point d'un modèle SA qui propose un cadre normatif disposant :
   a) des processus nécessaires à sa gestion et à son utilisation;
   b) des mécanismes permettant de fournir à l'organisation les preuves que son application a atteint et maintient le niveau de confiance ciblé, et ce, en fonction de son contexte d'utilisation spécifique;

3) L'atteinte des objectifs de validation et de vérification empirique partielle, soit :
   a) un modèle SA approuvé par une organisation internationale de normalisation;
   b) un modèle SA validé par des experts du domaine, reconnus et nommés par des instances nationales compétentes; et
   c) un modèle SA dont l'acceptabilité et l'applicabilité de certains éléments ont été vérifiés en industrie;

4) L'atteinte de l'objectif de diffusion consistant à rendre accessible le modèle SA à toute organisation désirant mettre en place ou vérifier la sécurité d'applications.

Il faut noter que ce travail de recherche ne vise pas à établir des directives pour la sécurité physique et de réseau, ni à fournir des contrôles ou des mesures, ni à mettre en place des spécifications de programmation sécuritaire.

Par contre, le modèle SA produit par ce travail de recherche ne définira pas :

1) Une nouvelle méthode de développement logiciel d'application TI,
2) Une norme de gestion de projets TI,
3) Un cycle de vie d'un logiciel.

2.5 Stratégies de recherche

La stratégie de réalisation de cette recherche s'articulera autour de quatre axes, soit :

1) La stratégie de conception, visant à déterminer les problématiques et les éléments de solutions pouvant être intégrés au modèle SA;
2) La stratégie de validation visant à faire valider les éléments du modèle SA par des experts du domaine, consistait à adapter et à utiliser la méthode de recherche Delphi à l'intérieur du processus de réalisation de projet d'une organisation crédible et reconnue internationalement;
3) La stratégie de vérification empirique partielle, visant à utiliser des éléments du modèle SA dans des projets d'applications réalisés par l'industrie; et
4) La stratégie de diffusion, visant à faciliter l'accessibilité et la distribution du modèle SA aux organisations intéressées;

Les quatre sous-sections qui suivent présentent les stratégies plus en détail.

2.5.1 Axe de la stratégie de conception du modèle SA

Notre stratégie de conception du modèle SA consiste à :

1) Déterminer si les problématiques présentées dans un ouvrage de la littérature concernent bien la sécurité des applications puis, lorsque c'est le cas, identifier les éléments de solutions de sécurité qui y sont présentés et les principes qui les sous-tendent;
2) Établir si ces éléments pourraient s'appliquer aux différents secteurs d'intervention en sécurité existants dans le contexte du développement ou de l'utilisation d'une application.

L'étude des ouvrages et des articles concernant la sécurité des applications TI, sous l'angle des 16 problématiques à résoudre, permettra de définir la portée du modèle SA et d'identifier les éléments à y être intégrés.

Cette démarche permettra également de limiter la portée de la revue de littérature en identifiant les types de problèmes pouvant concerner la sécurité des applications TI, selon les lignes d'affaires où ils sont utilisés, et qui pourraient avoir un impact sur la qualité de la vie de personnes.

2.5.2 Axe de la stratégie de validation

Notre stratégie de validation consiste à soumettre les résultats de ce travail de recherche à une organisation soutenue par des reconnaissances nationales officielles.

Cette stratégie se réalise en deux étapes consécutives, soit :

1) **La sélection d'une organisation internationale crédible et reconnue**

   Il s'agit de sélectionner et de soumettre les résultats de nos travaux de recherche à une organisation qui jouisse d'une crédibilité internationale et que soit reconnue par les experts œuvrant dans le domaine de la sécurité de l'information. La sélection de l'organisation tient aussi compte des éléments suivants :

   a) l'utilisation de processus de validation documentés et reconnus;

b) la reconnaissance de la compétence des experts impliqués ainsi que la pertinence de cette compétence dans le domaine de la sécurité;
c) la pluralité des lignes d'affaires représentées.

2) La validation du modèle SA

La stratégie élaborée pour réaliser la validation du modèle SA et de ses éléments est d'adapter la méthode Delphi au processus de validation d'une organisation crédible afin de proposer le modèle SA aux experts participants pour qu'ils puissent l'analyser et en commenter les différents éléments qui y sont proposés;[7]

2.5.3 Axe de la stratégie de vérification partielle

Notre stratégie de vérification partielle consiste à utiliser un processus de vérification empirique, intégré aux cycles Delphi, permettant d'avoir un aperçu de l'applicabilité et de l'acceptabilité des éléments du modèle SA par les organisations qui peuvent avoir à mettre en place ou à utiliser le modèle SA.

2.5.4 Axe de la stratégie de diffusion

Désirant aussi faciliter l'accessibilité et la distribution du modèle SA aux organisations intéressées, notre stratégie de R&D prévoit de tenir en compte les éléments favorisant une distribution efficace et rapide des résultats de nos travaux de recherche au plus grand nombre possible d'organisations.

---

[7] Idéalement, cette étape doit inclure une vérification périodique par les pairs, ainsi qu'un processus formel de résolution de commentaires et d'approbation.

2.6 Méthodologie de recherche

Afin de favoriser la réussite de ce projet de recherche, nous avons dû identifier une méthodologie de recherche permettant de :

1) Trouver une réponse à la question de recherche en utilisant une démarche systématique prédéfinie et reconnue pour la réalisation d'une recherche de doctorat dans le domaine des TI;
2) Trouver un ensemble de solutions permettant :
   a) d'identifier et de concevoir un modèle SA qui répondrait aux 16 problématiques liées à la sécurité des applications; et
   b) de permettre l'intégration d'éléments de sécurité dans le cycle de vie d'une application;
3) Faire valider les résultats de la recherche par un grand nombre d'experts du domaine de la sécurité;
4) Recueillir, d'analyser et de valider des preuves, qui appuient ou non nos résultats.

2.6.1 Description sommaire de la méthodologie de la recherche

Voici sommairement les caractéristiques, les processus et les critères balisant les quatre phases de la méthodologie de recherche. Une description détaillée de la méthodologie de recherche est présentée à l'appendice A – ANNEXE VII.

Le Tableau 2.1 présente les phases de la méthodologie de recherche qui a été adoptée pour atteindre les objectifs de ce projet.

Tableau 2.1 Les quatre phases de la méthodologie de recherche

Phase	Description sommaire
Phase 1 – Identification des principes, concepts, et éléments clés à être inclus dans le modèle SA *Principalement basée sur les articles scientifiques, les normes internationales et les principes généralement reconnus dans le domaine de la sécurité.*	Effectuer une revue de littérature afin d'identifier les modèles et les principaux concepts existants dans les domaines de la sécurité de l'information et de la sécurité des applications. Cet exercice ne se limitera pas seulement à la revue de littérature académique, mais inclura aussi une analyse extensive des normes et ouvrages pertinents reliés aux domaines identifiés.
Phase 2 – Conception et développement du modèle SA	Utilisation d'une méthodologie de réalisation de projets telle que celle utilisée par ISO (ISO/IEC, 2004b) en vue d'encadrer le développement d'un modèle SA.
Phase 3 – Validation et approbation formelle du modèle SA	Utilisation du cycle des processus formels de révision des projets tels qu'en usage dans les projets ISO (ISO/IEC, 2004b) englobant les mécanismes de communication de cette organisation afin de rendre accessible aux organisations un modèle SA approuvé par les instances nationales compétentes représentant les pays participants.
Phase 4 – Vérification empirique partielle des éléments du modèle SA *Supporté par la réalisation de projets en industrie.*	Utilisation des concepts et éléments du modèle SA pour en vérifier l'acceptabilité et l'applicabilité dans des projets en industrie. Vérification de la complémentarité des éléments de ce modèle aux normes, aux outils et aux pratiques existantes.

2.6.2 Sélection de la méthode Delphi

La méthode Delphi est la technique de recherche retenue pour les raisons suivantes :

1) Cette recherche pose une question visant à identifier les éléments d'un modèle SA qui pourraient être intégrés au cycle de vie d'une application pour en améliorer la sécurité. Cette question complexe visant, notamment, à répondre aux 16 problématiques liées à la SA, nécessite des connaissances de personnes qui comprennent les différents défis et contraintes liés à la gestion de la sécurité d'applications, au développement de logiciels sécuritaires, à la gestion des infrastructures TI utilisées par les applications, ainsi qu'à leur vérification et leurs audits de sécurité. La méthode Delphi est une technique de recherche

de type qualitatif permettant d'aborder et de proposer des solutions à ce type de questions (Nworie, 2011);

2) La méthode Delphi :
   a) peut être utilisée pour identifier les éléments qui peuvent être utiles à l'amélioration des pratiques d'un domaine (Nworie, 2011), ce qui répond à l'un des objectifs de cette recherche (*Voir* 2.4, objectifs 1 et 2);
   b) peut être adaptée au contexte d'une recherche universitaire tout en assurant une collecte de données via, notamment, les entrevues de suivis réalisées durant le projet de recherche. L'interprétation des données recueillies par le chercheur durant les cycles Delphi mène généralement à une meilleure compréhension des questions et problématiques de recherche (Okoli et Pawlowski, 2004);
   c) permettra de bonifier et d'entériner la pertinence de la réponse à notre question de recherche (Skulmoski, Hartman et Krahn, 2007). En effet, pour valider les solutions proposées, celle-ci requiert l'implication d'un groupe d'experts sur plusieurs cycles Delphi, plutôt que de s'appuyer sur la vision et les idées d'un seul chercheur;
   d) ne requiert pas que les experts aient à se rencontrer physiquement, ce qui favorise la participation d'experts internationaux dans nos travaux (Okoli et Pawlowski, 2004);

3) Un processus de révision et de validation des résultats de recherche en utilisant la méthode Delphi se compare avantageusement à la révision d'un article à l'aide d'un comité de réviseurs, étant donné que ces derniers ont une période de temps limitée pour réaliser leur travail (Skulmoski, Hartman et Krahn, 2007);

4) La méthode Delphi a été utilisée et validée de 1973 à 2005 par plusieurs groupes de chercheurs, issus de différentes universités, pour réaliser des projets de recherche dont une bonne proportion était de niveau doctoral dans le domaine des TI (Skulmoski, Hartman et Krahn, 2007).

2.6.2.1 Avantages de la méthode Delphi

La méthode Delphi est une technique qui peut être adaptée au contexte d'une recherche universitaire de type qualitatif afin de résoudre des problèmes complexes.

La méthode Delphi offre les avantages suivants. Elle :

1) Est fréquemment utilisée dans le développement de modèles théoriques complexes (Okoli et Pawlowski, 2004), (Skulmoski, Hartman et Krahn, 2007);
2) Emploie un processus de validation itératif par des experts (Okoli et Pawlowski, 2004);
3) Permet de structurer un processus de communication de groupe, généralement à l'aide des questionnaires avec commentaires contrôlés, pour permette à des d'experts de faire face à un problème complexe de manière efficace (Linstone et Turoff, 2002);
4) Est basée sur la prémisse que les opinions collectives d'un groupe d'experts sont de qualité plus riche que l'opinion qui s'appuie sur la vision limitée d'un seul individu (Skulmoski, Hartman et Krahn, 2007);
5) Est flexible et peut être adaptée aux contexte et contraintes spécifiques d'une recherche universitaire (Okoli et Pawlowski, 2004);
6) Repose sur l'anonymat des participants permettant ainsi de restreindre toute influence d'opinion entre les panélistes experts qui s'expriment et votent sur les mêmes questions (Nworie, 2011);
7) Permet de dégager un modèle de consensus après deux ou trois cycles de consultation des experts (Nworie, 2011);
8) Permet au chercheur et aux experts d'acquérir de nouvelles informations et connaissances pendant les cycles successifs du processus (Newman, Thompson et Roberts, 2006).

2.6.2.2 Faiblesses de la méthode Delphi

La méthode Delphi a aussi ses faiblesses et ne pas les gérer pourrait amener l'invalidation de l'ensemble des résultats et des conclusions découlant de ce travail de recherche.

Les faiblesses de la méthode Delphi sont, notamment :

1) Le temps requis pour résoudre une question de recherche ouverte ou complexe (Skulmoski, Hartman et Krahn, 2007);
2) Les libertés laissées au chercheur (Hsu et Sandford, 2007);
3) Le biais pouvant résulter de la sélection des experts (Skulmoski, Hartman et Krahn, 2007) :
    a) groupe généralement trop petit,
    b) nombre insuffisant de cycles de validation,
    c) temps limité pour la validation de la recherche (quelques heures par cycle),
    d) sélection sur la base des connaissances et de l'expérience des participants afin qu'ils soient en mesure de donner une évaluation compétente;
4) Le risque d'une baisse de participation après quelques cycles (Skulmoski, Hartman et Krahn, 2007).

2.6.3 Adaptation de la méthode Delphi au projet de recherche

La Figure 2.1, adaptée de la Figure 1 de *Helping practitioners understand the contribution of qualitative research to evidence-based practice* (Newman, Thompson et Roberts, 2006), présente les quatre phases et les activités qui ont été identifiées pour adapter la méthode Delphi à ce projet de recherche.

Les ajustements que nous avons apportés à ces activités pour contrer les faiblesses de la méthode Delphi, et qui sont aussi inclus dans la Figure 2.1, sont décrits ci-après.

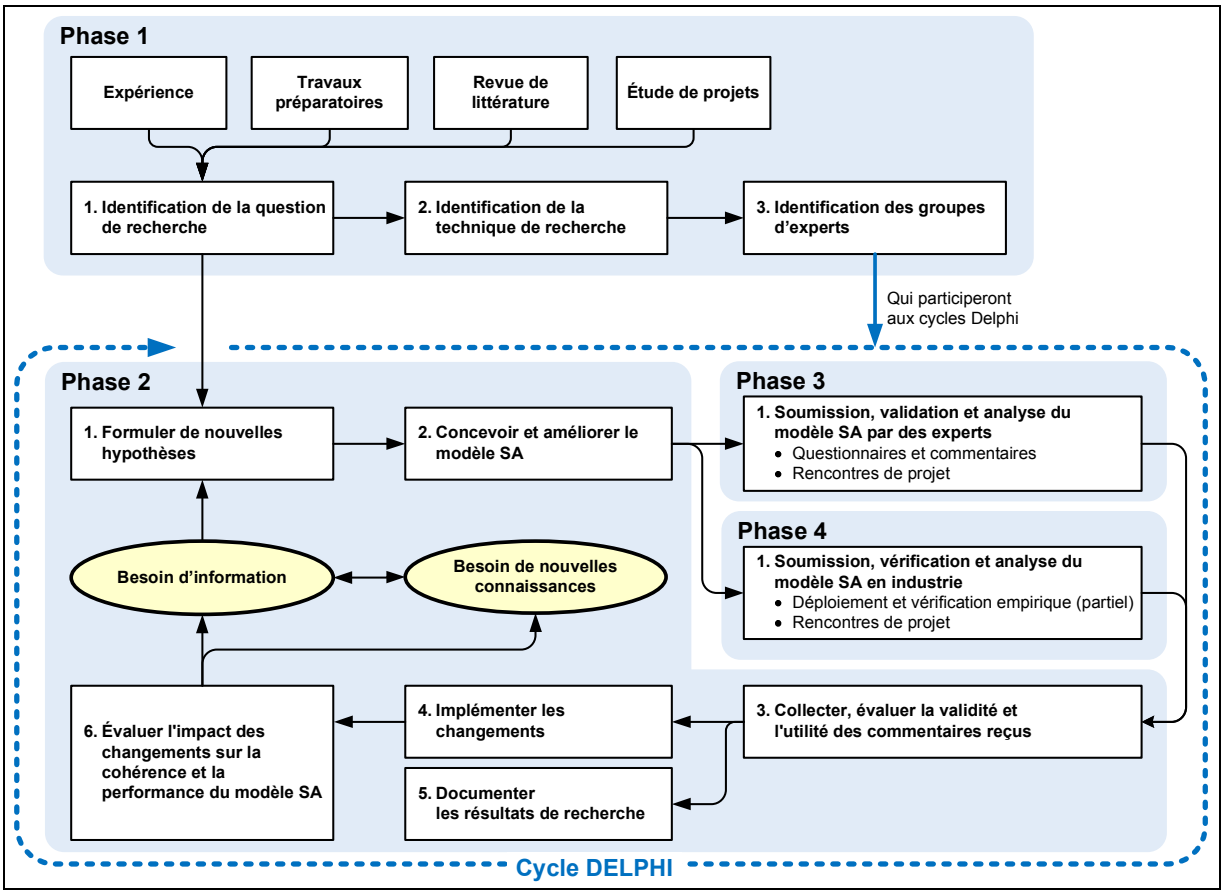


Figure 2.1 Adaptation de la méthode Delphi aux phases de conception et de validation de la méthodologie de recherche

Phase 1, activité 1 : Identification de la question de recherche – Activité réalisée à partir des travaux préparatoires, de la revue de littérature et des études de projet d'applications auxquelles le chercheur a participé.

Phase 1, activité 2 : Identification de la technique de recherche – Activité réalisée à partir de l'analyse de la synthèse de la problématique de la sécurité des applications, de la question ouverte de cette recherche, de la complexité des enjeux de la sécurité de l'information dans les applications identifiées, du but, des objectifs, de la stratégie et de la méthodologie de cette recherche.

Phase 1, activité 3 : Identification des groupes d'experts – Activité en trois étapes tout en tenant en compte les faiblesses de la méthode Delphi.

1) Le choix de l'organisation ISO a été fondé sur les critères suivants :
   a) L'organisation ISO utilise des processus rigoureux reconnus, répondant aux critères de la méthode Delphi (*Voir* l'appendice A – ANNEXE IX : Processus d'édition d'un projet ISO pour plus de détails.);
   b) La durée moyenne de la réalisation d'un projet d'ISO inclut l'utilisation de processus formels de communication et de distribution des documents à valider, via des questionnaires et des processus de collecte de réponses et de commentaires des experts qui, généralement, comprennent plus de huit cycles de validation;
   c) L'anonymat des opinions des experts participant aux travaux d'un projet ISO est assuré grâce au formulaire normalisé utilisé par l'organisation. Celui-ci demande uniquement l'identification du pays représenté par l'expert appelé à soumettre un commentaire ou une contribution. Aucun biais ne peut ainsi être apporté par le chercheur lors du traitement du contenu des formulaires reçus puisqu'il n'a pas la connaissance préalable de l'identité de leurs auteurs;
   d) L'organisation ISO regroupe la majorité des pays hautement industrialisés;
2) Le choix du sous-comité 27 d'ISO a été fondé sur les critères suivants :
   a) un comité d'experts internationaux travaillant sur la normalisation de techniques de sécurité en technologie de l'information (*Voir* l'appendice A – ANNEXE VIII : Sélection d'un sous-comité international d'ISO pour la validation du Modèle SA pour plus de détails.);
   b) un grand nombre d'experts délégués par plus de 36 pays y participent (ISO/IEC, 2007b);
   c) des experts reconnus par leur pays pour leur expertise dans la sécurité des TI, secteur directement lié au domaine ciblé par cette recherche.

Phase 2, activité 1 : Formulation de nouvelles hypothèses – Activité réalisée à partir des travaux préparatoires, de la revue de littérature et de l'étude de projets réalisés pour répondre

à la question de recherche et aux problématiques identifiées. Les hypothèses formulées par le chercheur orienteront la conception des différents éléments du modèle SA.

Phase 2, activité 2 : Concevoir et améliorer le modèle SA – Identification par le chercheur des principes, des concepts, des éléments clés à être intégrés dans le modèle SA selon les nouvelles hypothèses posées. Validation des interrelations entre les éléments du modèle SA afin de s'assurer du maintien de sa cohérence et de sa performance.

L'évaluation du modèle SA se produit lorsque toutes les informations recueillies, analysées et validées ont permis au chercheur de produire la nouvelle version du modèle SA et que celui-ci est transmis aux experts pour examen et validation (Linstone et Turoff, 2002, p. 5).

Phase 3, activité 1 : Soumission, validation et analyses du modèle par des experts – Selon la méthode Delphi (questionnaires et commentaires).

À chaque cycle Delphi de notre recherche, cette activité se réalise en deux étapes.

1) **Distribution du modèle SA avec un questionnaire et réception des commentaires**

   La première étape est caractérisée par l'exploration du sujet en discussion en fonction de la version du modèle SA proposée. Pour ce faire, le processus de communication aux experts d'ISO a été utilisé pour transmettre le modèle SA aux experts des pays participants ainsi que pour recueillir leurs commentaires et contributions à ce projet de recherche. La question ouverte associée à cette grille requiert de la part des experts une validation des éléments qui leur sont présentés, l'identification et l'explication de tout point de désaccord ou d'éléments manquants, et la proposition d'améliorations qui, selon eux, devraient être apportées.

   Avant leur transmission au chercheur, les commentaires et contributions reçus par le sous-comité d'ISO sont regroupés dans une grille identifiée seulement par le nom du pays d'origine des experts ayant participé à sa rédaction. L'utilisation de ce processus et de

cette grille de commentaires permet d'éviter tout biais pouvant être amené par le chercheur dans la construction du questionnaire ainsi que dans l'analyse des contributions reçues à chacun des cycles Delphi.

2) **Rencontre des experts**

   La deuxième étape de cette activité implique une rencontre de projet avec des experts délégués des pays participants, afin de parvenir à dégager un consensus sur le traitement de chacun des commentaires anonymes et l'adoption des dispositions proposées ou modifiées.

Phase 4, activité 1 : Soumission, vérification et analyse du modèle en industrie – Activité réalisée en utilisant une approche de vérification empirique partielle, soit l'utilisation de certains éléments du modèle SA à l'intérieur de projets d'applications en industrie. Cette activité de vérification est réalisée en deux étapes.

1) **Sélection des éléments du modèle SA pouvant s'appliquer au projet d'application**

   Présentation du modèle SA à l'équipe de projet (version du modèle SA proposée), puis sélection des éléments du modèle que les intervenants du projet (gestionnaires, architectes, équipe TI) désirent mettre en place.

2) **Déploiement des éléments sélectionnés et rencontres périodiques de vérification**

   Vérification empirique partielle pour vérifier l'acceptabilité et l'utilisabilité des éléments du modèle SA dans des projets réels à l'aide de rencontres de suivis périodiques du déploiement des éléments sélectionnés et de l'interprétation de la satisfaction des divers intervenants impliqués.

Phase 2, activité 3 : Collecter, évaluer la validité et l'utilité des commentaires reçus – Activité réalisée par le chercheur consistant à consolider et analyser l'ensemble des commentaires et des contributions reçus, et d'en évaluer l'utilité et l'implémentabilité. Lorsqu'un désaccord important survient opposant l'opinion des experts et celle du chercheur,

ce désaccord est alors étudié afin de comprendre et d'évaluer la pertinence des raisons sous-jacentes.

Phase 2, activité 4 : Implémenter les changements – Activité consistant à identifier, définir, concevoir et implémenter les ajustements ou les éléments manquants au modèle SA à partir des commentaires reçus.

Phase 2, activité 5 : Documenter les résultats de recherche – Activité consistant, notamment, à consolider l'ensemble des commentaires et contributions reçus, de documenter les décisions du chercheur et les rapports d'avancement du projet.

Phase 2, activité 6 : Évaluer l'impact des changements sur la cohérence et la performance du modèle SA – Activité consistant à valider que tous les objectifs sont atteints et toutes les problématiques résolues, et confirmant que le modèle répond toujours aux objectifs de la recherche. Cette étape adaptée du processus Delphi demande au chercheur une réévaluation des performances du modèle, suite à l'implémentation des changements (Figure 2.1, Phase 2, étape 4). Lorsqu'il y a doutes ou interrogations, l'information ou les connaissances à acquérir doivent être identifiées afin de permettre au chercheur de formuler de nouvelles hypothèses pour corriger le modèle.

2.6.4 Vision globale de la méthodologie de recherche

La Figure-A I-2 présente un schéma sommaire global des activités clés réalisées durant ce projet de recherche, ainsi que les intrants et les extrants de chaque phase de recherche.

Afin d'appliquer la stratégie de recherche pour la validation du modèle SA, le chercheur a conçu le contenu du modèle SA initial. À l'aide de la méthode Delphi, il a géré l'avancement de ce projet de recherche au sein du comité SC27 d'ISO à titre d'expert canadien, et proposé aux experts participants, des améliorations au contenu du modèle SA.

Le modèle SA ainsi que les éléments identifiés ont, par la suite, été validés et acceptés par les instances nationales compétentes des pays membres du comité SC27 d'ISO.

Cette activité de validation, présentée à la phase 3, a été effectuée itérativement, lors de chaque cycle Delphi. Il s'agit d'une activité périodique de 6 mois, réalisée dans chacun des pays, permettant une validation progressive des éléments du modèle par les instances concernées et qui a pu amener des travaux de recherche complémentaires, ainsi que certains ajustements du modèle SA proposé.

Afin de comprendre l'incidence de ce processus de validation sur l'évolution des éléments de ce travail de recherche, l'appendice A – ANNEXE IX présente sommairement le processus d'édition d'un projet ISO.

2.6.5 Critères à rencontrer durant la recherche

L'atteinte des objectifs de la recherche sera démontrée en utilisant les critères suivants :

1) Le modèle SA doit désigner les principaux groupes d'acteurs et cerner leurs besoins respectifs dans la mise en place de la sécurité d'une application;

2) Le modèle SA doit pouvoir offrir les éléments permettant :
   a) de définir et d'identifier le contexte et l'environnement de la sécurité d'une application;
   b) d'identifier et de catégoriser l'information sensible impliquée par une application;
   c) d'identifier le niveau de sécurité requis par une application;
   d) de gérer et d'assurer l'intégration et la réalisation des activités de sécurité et des activités de vérification tout le long du cycle de vie d'une application, en fonction du niveau de sécurité requis, quels que soient les processus en place dans l'organisation;
   e) de vérifier et de gérer la mise en place et le bon fonctionnement des contrôles de sécurité;

f) de mesurer, de vérifier et de valider l'atteinte du niveau de sécurité visé, à n'importe quel moment du cycle de vie de l'application;
g) de fournir les preuves démontrant que le niveau de sécurité visé pour une application a été atteint et est maintenu;
h) de rendre répétables l'implantation et la vérification du niveau de confiance mesuré;
i) de pouvoir soutenir le système de gestion de la sécurité de l'information d'ISO 27001 (ISO/IEC, 2005d);
j) de pouvoir soutenir les principes du modèle de maturité intégré du SEI (CMMI, 2006); et
k) de pouvoir soutenir les concepts d'assurances en génie logiciel d'ISO 15026 *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary* (ISO/IEC, 2009j).

CHAPITRE 3

REVUE DE LITTÉRATURE

Ce chapitre présente la démarche de la revue de littérature qui a permis de dégager les premiers constats concernant la SA, puis d'identifier des pistes de solutions qui ont directement influencé la conception du modèle SA. Cette démarche s'est déroulée en six étapes, soit :

1) L'identification des objectifs visés par cette revue de littérature (3.1),
2) La sélection et classement des ouvrages consultés sous l'angle de SA (3.2),
3) L'analyse des documents couverts par la revue de littérature (3.3),
4) L'identification des éléments de réponse aux problématiques en SA (3.4),
5) Les constats de la revue de littérature (3.5),
6) Une revue complémentaire (3.6).

Finalement, la section 3.7 présente les termes et définitions qui font consensus dans les ouvrages consultés et qui seront utilisés dans ce travail de recherche.

Seul un sommaire de la revue de littérature est présenté dans ce chapitre; le détail de la revue de littérature est présenté à l'appendice A – ANNEXE IX.

3.1 Objectifs de la revue de littérature

Les objectifs de la revue de littérature sont :

1) De préciser la question de cette recherche;
2) De déterminer les éléments sur lesquels ce travail de recherche pourrait s'appuyer en ce qui a trait au vocabulaire, aux principes, aux concepts, aux définitions et aux approches qui y sont présentés pour répondre aux 16 problématiques énoncées.

3.2 Sélection et classement des ouvrages consultés sous l'angle de la SA

En raison du grand nombre d'organisations et d'ouvrages dans le domaine de la sécurité de l'information, la présente revue de la littérature a été limitée à la revue et à l'analyse des travaux concernant ou pouvant être appliqués à la sécurité de l'information ou à la sécurité des applications. Des 299 documents initialement identifiés, dont 52 articles scientifiques, un ensemble de 75 documents, regroupant 13 livres, 35 normes et 27 articles (*Voir* l'appendice A – ANNEXE VI, Tableau-A VI-1) ont été retenus et classés selon les quatre groupes de critères suivants :

1) Les éléments du document pouvant s'appliquer directement ou partiellement à la SA ou à un modèle SA. En l'occurrence, le document :
   a) identifie des principes, une portée ou un modèle pertinent à la SA;
   b) définit du vocabulaire, un cadre de travail ou des processus présents dans le cycle de vie d'une application pouvant s'appliquer à la SA;
   c) intègre des principes de gestion de risques de sécurité pouvant s'appliquer à la SA;

2) Les contrôles de SA proposés par le document :
   a) s'appliquent à des personnes, des processus de réalisation de SA, des processus de gestion de SA ou sur de la technologie;
   b) comprennent des activités de sécurité ou des activités de vérification de leur bon fonctionnement;

3) Les phases du cycle de vie de l'application impactées par les éléments amenés par le document, soit durant :
   a) les phases de procuration, notamment, la phase de préparation et de définition des exigences, de conception, d'implémentation ou de transition et de déploiement;
   b) les phases d'opération, notamment, la phase d'utilisation, de maintenance, d'archivage ou de destruction;

4) Les éléments amenés par le document pouvant répondre ou servir de piste de solution aux 16 problématiques identifiées concernant la SA.

Les documents retenus proviennent des trois groupes suivants :

1) Articles scientifiques, publiés notamment par *l'Institute of Electrical and Electronics Engineers* (IEEE) et *l'Association for Computing Machinery* (ACM);
2) Normes et pratiques recommandées, provenant d'organisations nationales et internationales dont les suivantes : *Organisation for Economic Co-operation and Development* (OCDE), ISO, IEEE, NIST, ACM, ITIL, *Information Systems Audit and Control Association* (ISACA) et OWASP;
3) Livres et publications électroniques spécialisés proposant des modèles, des approches ou des outils pouvant s'appliquer à la SA, dont notamment : le SDL de Microsoft et le *Building Security In Maturity Model: BSIMM2* de McGraw, Chess et Migues.

3.3 Documents couverts par la revue de littérature

La littérature concernant la gouvernance de la sécurité de l'information, l'ingénierie des systèmes et des logiciels, la sécurité des infrastructures TI ou la vérification de la sécurité est très abondante. Parmi la documentation consultée, 75 documents, dont 27 articles scientifiques, ont été retenus parce qu'ils pouvaient apporter des éléments de solution aux problématiques de la sécurité des applications (*Voir* l'appendice A – ANNEXE VI, Tableau-A VI-1). Certains documents qui semblaient pertinents à première vue ont été rejetés par la suite, car ils n'apportaient pas d'élément nouveau ni à la réflexion ni aux pistes de solution pouvant répondre aux problématiques visées.

Pour faciliter la présentation, les documents retenus ont été classés de la façon suivante :

1) Les ouvrages liés à la gouvernance de la sécurité de l'information et des applications (*Voir* 3.3.1);
2) Les ouvrages liés au développement, à l'acquisition ou à la maintenance des applications (*Voir 3.3.2*);

3) Les ouvrages liés à l'environnement et à l'infrastructure technologique des applications (*Voir* 3.3.3); et
4) Les ouvrages liés à la vérification et aux audits de sécurité des applications (*Voir* 3.3.4).

3.3.1 Ouvrages liés à la gouvernance de la sécurité de l'information et des applications

La gouvernance de la sécurité de l'information et celle de la SA sont des secteurs d'intervention qui relèvent principalement de l'organisation. Elles permettent la définition, l'harmonisation, l'encadrement et la gestion de la vision, de la stratégie, des priorités et des éléments que l'organisation désire établir.

3.3.1.1 Ouvrage proposant une vision plus inclusive de la sécurité

En 2002, l'OCDE publie « Les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité » qui présente les buts et les principes que devrait soutenir la culture de la sécurité d'une organisation. Ce guide précise, notamment, que :

> « Seule une approche prenant dûment en compte les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes peut permettre d'assurer une sécurité efficace. L'instauration d'une culture de la sécurité … devrait se traduire par une priorité renforcée donnée à la planification et la gestion de la sécurité, ainsi que par une compréhension de l'exigence de sécurité par l'ensemble des participants. » (OCDE, 2002, p. 18).

De ces ouvrages présentant une vision plus inclusive de la sécurité, aucun guide ou méthode de réalisation d'applications n'offre une vision globale permettant d'identifier formellement « les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes » (OCDE, 2002, p. 18) à l'application afin de pouvoir gérer efficacement sa

sécurité. Cette problématique provient de l'absence d'une vision globale des principes et des éléments impliqués dans la sécurité des applications (P01)[8].

Finalement, l'OCDE présente dix principes, dont l'importance de gérer la sécurité en évaluant continuellement les risques (OCDE, 2002, pp. 19-23). C'est à cet effet qu'ISO a pris l'initiative du développement de la norme ISO 27001 *Information technology – Security techniques – Information security management systems – Requirements* (ISO/IEC, 2005d) pour la mise en place du SGSI dans l'organisation, et ce, afin de lui permettre de gérer de façon cohérente la sécurité de son information. L'objectif du développement de cette norme était de définir un cadre normatif contenant l'ensemble des exigences minimales à respecter pour la mise en place d'un système de gestion de la sécurité de l'information basé sur une approche de gestion du risque. Constatant que ce type de cadre normatif n'existait pas encore en SA, j'ai intégré ce premier élément au modèle SA initial, afin qu'il identifie les éléments qui devraient être utilisés pour protéger l'application d'une organisation et les éléments qui ne sont pas nécessaires (P03).

Andress propose une vision différente de la gestion de la sécurité de l'information qui intègre les personnes, les processus et la technologie comme sources de risques pour la sécurité de l'information (Andress, 2003, pp. 5, 453-468), (P15). Elle y introduit l'importance de gérer les risques de sécurité, de définir des exigences de sécurité (P09) et de mettre en place des processus de gestion de la sécurité (Andress, 2003, pp. 25-43), (P12). Andress présente aussi un ensemble de menaces et de solutions concernant autant la sécurité des postes de travail et la sécurité des serveurs, que la sécurité dans le développement d'applications, ainsi que la maintenance et la surveillance de l'infrastructure technologique de l'organisation (Andress, 2003, pp. 25-43). Cet ouvrage a innové puisqu'il est l'un des premiers à identifier les principaux éléments dont il faut tenir compte simultanément, tout en tentant de garder une vision plus globale (P01) en se concentrant sur les problématiques de sécurité des processus organisationnels ou sur les menaces pouvant compromettre des composants technologiques.

---

[8] *Voir* les descriptions des problématiques P01 à P16 à la section 3.4.

3.3.1.2 Ouvrages présentant des conflits dus à la convergence de plusieurs domaines d'intervention impliqués en sécurité

L'ISO encadre des travaux de plusieurs groupes d'expertises. Certains de ces groupes ont développé un document de vocabulaire afin de définir les termes en usage. Dans le contexte de cette recherche, notre attention s'est portée plus particulièrement sur deux de ces documents, soit :

- ISO/IEC 27000 *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO/IEC, 2009d), élaboré par le sous-comité 27 regroupant des experts internationaux du domaine de la sécurité de l'information; et
- ISO/IEC/IEEE 24765 *Systems and software engineering – Vocabulary* (ISO/IEC, 2010g) élaboré par le sous-comité 7 regroupant des experts internationaux du domaine de l'ingénierie des systèmes TI et de l'ingénierie des logiciels.

Cette duplication de définitions, parfois similaire parfois différente, amène la problématique du vocabulaire de la sécurité des applications. Par exemple, le terme « intégrité » est défini, dans ISO/IEC/IEEE 24765, comme étant « la mesure dans laquelle un système ou un composant empêche l'accès ou une modification non autorisée des programmes informatiques ou des données » (ISO/IEC, 2010g, p. 181), tandis que dans ISO 27000 ce même terme est défini comme étant « la propriété de protéger l'exactitude et l'intégralité des actifs » (ISO/IEC, 2009d, p. 4). Quoiqu'à première vue similaire, la première définition inclut le fait d'avoir un accès non autorisé à un programme ou à des données comme étant une problématique d'intégrité, tandis que ce concept est plutôt défini dans ISO 27000 par le terme « contrôle des accès » (ISO/IEC, 2009d, p. 1).

Cette situation se complique lorsqu'on y ajoute les termes définis dans les documents provenant d'autres domaines d'intervention, tels que :

- le document ITIL (OGC, 2007, pp. 177-225) élaboré par des experts du domaine de la gestion des services d'infrastructures TI;
- le document *Control Objectives for Information and related Technology* (COBIT) (ITGI, 2007, pp. 189-193) élaboré par des experts du domaine de la vérification et du contrôle de systèmes d'information; et
- le document *A guide to the project management body of Knowledge (PMBOK Guide*) (PMI, 2008, pp. 418-445) élaboré par des experts du domaine de la gestion de projets, pour n'en nommer que quelques-uns.

La confusion amenée par l'absence d'un vocabulaire et de références n'ayant pas nécessairement les mêmes valeurs selon le secteur d'intervention des personnes impliquées dans un projet de SA, crée une problématique qui peut avoir un impact important sur la SA (P05).

3.3.1.3 Ouvrages proposant la gestion des risques pour implémenter la sécurité

En publiant ISO 27002 *Information technology – Security techniques – Information security management systems – Code of practice for information security management* en 2002, puis en la rééditant en 2013, l'ISO a décrit un ensemble de contrôles de sécurité qui devrait être mis en place au sein d'une organisation, afin de lui permettre d'assurer la protection de son information (ISO/IEC, 2005c), (ISO/IEC, 2013b). Même si la majorité des contrôles qui y sont présentés concernent des risques de sécurité organisationnels, certains d'entre eux concernent spécifiquement la SA, notamment « le contrôle d'accès d'un système ou d'une application » et « le contrôle d'accès au code source ». Du fait de leurs descriptions générales, leur mise en œuvre dépend spécifiquement des connaissances et de l'interprétation des personnes qui sont responsables de cette mise en œuvre. De fait, après avoir identifié trois catégories de contrôles de sécurité, soit : les contrôles techniques, les contrôles opérationnels et les contrôles de gestion, Baker et Wallace ont mesuré la qualité de leur mise en œuvre dans diverses organisations. Il en résulte que même si ces dernières mettent en place des contrôles de sécurité, plusieurs d'entre elles gèrent la mise en œuvre de ces

contrôles et, par le fait même de leur sécurité, de manière inconsistante et superficielle (Baker et Wallace, 2007) (P03, P10 et P13).

Plusieurs méthodes d'analyse de risques de sécurité ont été développées, autant par des organisations nationales qu'internationales (SEI, 2001), (Alberts et al., 2005), (DCSSI, 2004), (CLUSIF, 2005). Elles ont toutes pour objectif d'aider les organisations à identifier et à gérer les risques de sécurité, à utiliser des systèmes TI en prenant en compte la sensibilité des informations présentes dans l'organisation, les applications et les manipulations, ainsi que les infrastructures TI qui soutiennent ces dernières. Par contre, elles s'utilisent toutes au niveau organisationnel, et elles n'offrent pas le niveau de granularité nécessaire à l'identification des risques et des contrôles de sécurité pouvant être intégrés à une application.

Ces méthodes d'analyse de risques de sécurité se réfèrent toutes à ISO 27005 *Information technology – Security techniques – Information security risk management* (ISO/IEC, 2010d) pour démontrer qu'elles sont conformes aux exigences minimales de gestion de risques qui y sont présentées.

Malheureusement, même si l'OCDE le recommande, peu de méthodes de développement et de processus de gestion de projets d'applications incluent des activités permettant d'identifier et de tenir en compte les risques provenant des contextes d'une application. Cette absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application est une des grandes problématiques de la SA (P02), car les risques de SA ne peuvent pas tous être identifiés par les intervenants d'un seul secteur d'intervention.

Une première tentative de développement d'une méthode d'analyse de risques de sécurité, qui offrirait un niveau de granularité adapté aux applications, a été réalisée par le NIST avec la publication, en 2002, de la norme SP 800-30 – *Risk Management Guide for Information Technology Systems* (Stoneburner, Goguen et Feringa, 2002). Ce document vise

principalement à aider les organisations qui développent des systèmes TI à identifier et à gérer des risques de sécurité pouvant se retrouver durant le cycle de vie de développement d'une application (Stoneburner, Goguen et Feringa, 2002, p. 4). Cette approche a récemment été étendue par le NIST au cycle de vie complet de l'application en publiant une révision du guide SP 800-37 Rev 1 – *Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach* et en l'orientant non plus sur la certification d'une application, mais sur la gestion des risques (NIST, 2010). La démarche proposée s'adresse principalement à une audience œuvrant soit au niveau de la gouvernance, soit au niveau du développement et de la maintenance d'applications. De plus, ne présentant que des contrôles de haut niveau, l'approche proposée par ce guide, tout comme les démarches proposées par les analyses de risques organisationnels, ne permet pas d'identifier précisément ni les besoins de sécurité, ni les activités de SA à mettre en œuvre pour estimer les coûts liés à ces activités, à leurs vérifications et à leur maintien (P04).

Plusieurs recherches ont été réalisées pour répondre à cette problématique, dont celle publiée par Caulkins et al. qui identifie notamment la difficulté d'estimer des montants quantitatifs justes et plausibles des coûts et des pertes potentielles d'adresser ou non une faille de sécurité (Caulkins et al., 2007). Ces auteurs proposent ensuite une méthode basée sur la résolution de « cas de mauvaise utilisation » qui offre une granularité permettant d'identifier ces coûts par cas analysé et de décider des actions à prendre (Caulkins et al., 2007). Quoique la portée de l'approche proposée se limite à la résolution des cas de mauvaise utilisation, et ne couvre pas tous les problèmes de sécurité qui peuvent provenir de l'utilisation d'une application, l'objectif d'évaluer des coûts de mise en œuvre de « petits » contrôles de sécurité afin d'améliorer la qualité des estimations obtenues est excellent.

De plus, Johnson et Goetz présentent les défis de gestion de la sécurité de l'information auxquels les organisations doivent faire face dont, notamment, le fait de gérer la sécurité au-delà des frontières de l'organisation et de tenir compte des lois, règlements et normes auxquelles elle devrait se conformer dans ces régions où elle voudrait faire des affaires. Ces auteurs identifient ensuite les éléments clés de sécurité qui, selon eux, devraient être intégrés

à l'organisation, et qui en transformeront la culture et les décisions de sécurité (Johnson et Goetz, 2007). Le fait de connaître les lois et règlements en vigueur où une application pourrait être utilisée est d'autant plus important que Jorshari, Mouratidis et Islam proposent un processus permettant d'identifier et de définir les exigences de sécurité qui en découleraient (Jorshari, Mouratidis et Islam, 2012), (P02).

Dans cette même volonté de définir les exigences de sécurité d'une application, Lamsweerde présente une approche d'identification d'antimodèles qui indique comment les spécifications des éléments d'un modèle peuvent être menacées, pourquoi et par qui (van Lamsweerde, 2004). Des approches similaires, visant la définition d'exigences de sécurité via l'utilisation de modèles permettant l'identification de menaces, puis proposant des stratégies pour les contrer, sont aussi présentées par plusieurs auteurs d'articles (Yi et al., 2003), (Evans et al., 2004), (Dianxiang et Nygard, 2006), (White, Wijesekera et Hatton, 2008), (Menzel et Meinel, 2009), (Sherief, Abdel-Hamid et Mahar, 2010), (Borek et al., 2012) *et* (Avramescu et al., 2013).

Les forces et les limitations de ces modèles ou antimodèles dépendent de leur portée. Un modèle s'appliquant aux cas d'utilisation d'une application permettra principalement de détecter des menaces fonctionnelles ainsi que celles provenant d'utilisateurs mal intentionnés (van Lamsweerde, 2004), (Evans et al., 2004), (Dianxiang et Nygard, 2006), (White, Wijesekera et Hatton, 2008), (Sherief, Abdel-Hamid et Mahar, 2010), tandis qu'un modèle s'appliquant soit à l'architecture de l'application (Yi et al., 2003), à l'architecture de services[9] utilisés par celle-ci (Menzel et Meinel, 2009), (Borek et al., 2012) ou encore aux composants de l'architecture technologique qui la soutient (Avramescu et al., 2013), permettra de détecter et, éventuellement, de contrer des menaces complètement différentes.

---

[9] SOA – Services Oriented Architecture

En résumé, aucun des articles et ouvrages révisés ne présentait une approche et un modèle offrant une portée suffisante pour lui permettre d'identifier l'ensemble des sources des risques pouvant menacer une application (P01 et P02).

De fait, Haley, Robin, Moffett et Nuseibeh précisent d'entrée de jeu qu'une application est plus que le logiciel qu'il contient; ils soulignent l'importance de définir des exigences de sécurité dans le développement d'une application, et présentent une méthode pour identifier les objectifs de sécurité qui guideront la rédaction des exigences désirées (Haley et al., 2008), (P04, P07 et P09).

Même si ISO/IEC/IEEE 29148 *Requirements engineering* définit les caractéristiques qu'une description d'exigences devrait posséder (ISO/IEC, 2009g, p. 8), elle ne précise pas les sources des exigences de sécurité. Trois articles proposent des approches différentes pour les identifier, le premier à partir des lois et règlements s'appliquant à la zone géographique où sera utilisée l'application (Jorshari, Mouratidis et Islam, 2012), le deuxième en utilisant une approche spécifiant des cas d'antimodèle (van Lamsweerde, 2004) et le troisième en identifiant préalablement les objectifs de sécurité visés pour l'application (Dianxiang et Nygard, 2006). Ces trois approches sont valables, mais elles sont limitées par leur portée respective. Sachant que si un élément de sécurité n'est pas exigé, on ne pourra pas vérifier s'il a été comblé. Le modèle SA doit proposer une vision qui permettra d'identifier l'ensemble des exigences de sécurité, soit les exigences de sécurité réglementaires, fonctionnelles et non fonctionnelles (P01, P02, P06 et P11).

La gestion des risques de sécurité est l'un des principes essentiels de la gouvernance de la sécurité de l'information (OCDE, 2002, p. 11). Mais quels sont les autres principes, éléments et problématiques que la gouvernance de la sécurité des applications doit tenir en compte?

3.3.2 Ouvrages liés à l'intégration d'éléments de sécurité dans les phases de développement, d'acquisition ou de maintenance d'applications

Un premier constat relié à l'analyse des ouvrages liés à l'intégration d'éléments de sécurité dans les phases de développement, d'acquisition ou de maintenance d'applications, c'est que le « cycle de vie du développement d'une application » n'est pas défini de manière uniforme dans tous les articles et documents revus et se rapproche parfois du « cycle de vie de l'application » elle-même. Afin d'éviter toute confusion, nous utiliserons ici la définition proposée par ISO 15288, *Systems and software engineering – System life cycle processes* (ISO/IEC, 2007g) pour définir la portée du « cycle de vie de l'application ».

3.3.2.1 Ouvrages proposant l'intégration d'activités de sécurité dans les processus de développement, pour sécuriser une application

Que l'on analyse les méthodes de développement *Waterfall*, de tests en V, de prototypages ou les méthodes de développement AGILE, il n'existe, à ce jour, aucune méthode de développement d'applications qui intègre des préoccupations de sécurité via un processus de gestion des risques de sécurité pour l'organisation qui utilisera l'application concernée. C'est pour pallier cette lacune qu'un nombre important de documents ont été rédigés et publiés afin d'aider les développeurs et les organisations à intégrer et à gérer les activités de sécurité dans le développement d'applications.

Force est de constater qu'il existe une panoplie de documents présentant de bonnes pratiques de programmation sécuritaire d'applications (SEI, 2007), (Seacord, 2013), (Long et al., 2011), ou encore (OWASP, 2010). Même si personne ne niera que la programmation est une des activités importantes à tenir en compte dans la sécurité des applications, une des faiblesses de ces documents est qu'ils ne guident pas le programmeur ni ne mettent en évidence les indicateurs qui lui permettraient de décider, dans le cas précis de son projet d'application, s'il est important d'implémenter ou non une technique de programmation particulière ou si ce travail supplémentaire est inutile ou trop couteux pour l'organisation.

Dans le même ordre d'idées, Howard, LeBlanc et Viega présentent les dix-neuf principales erreurs qu'une équipe de développement peut faire lors de la réalisation d'une application, et la façon de les éviter/corriger pour différents langages de programmation (Howard, LeBlanc et Viega, 2005), (P16).

Howard et LeBlanc présentent divers exemples sur divers thèmes de programmation sécuritaire en langage C. Ces thèmes présentent des approches de programmation sécuritaires soit pour corriger des faiblesses de sécurité du langage C, soit pour mettre en place des pratiques de programmation visant à améliorer la sécurité du code d'une application. Selon les auteurs, la sécurité est une fonctionnalité et, comme toute fonctionnalité, elle devrait être prise en compte et intégrée à l'application dès le début du cycle de vie de son développement (Howard et LeBlanc, 2002, pp. 37-40). Par contre, le propos des auteurs ne concerne que le cycle de vie de développement d'une application et ne présente pas de stratégie ou d'approche permettant de guider le développeur dans l'identification du contexte de leurs projets ni dans la pertinence de la mise en place de ces approches.

L'ensemble des documents produits par OWASP (OWASP, 2005), (OWASP, 2008a), (OWASP, 2008b), (OWASP, 2013) et (OWASP, 2014) regroupe des ouvrages qui s'adressent aux développeurs et qui se concentrent chacun sur un aspect spécifique ayant un impact sur la sécurité d'une application. En ciblant des activités précises, telles que la révision de code, ces documents ne présentent pas de vision globale permettant d'évaluer si, en appliquant toutes les recommandations proposées par ces guides, une application pourrait être considérée comme sécuritaire.

C'est notamment pour remédier à cette lacune que Zenah et Aziz indiquent que l'utilisation de ces pratiques de programmation sécuritaires devrait être abordée dans une perspective plus large, qui devrait inclure l'ensemble du cycle de vie du développement de l'application, afin d'en comprendre les tenants et aboutissants (Zenah et Aziz, 2011). De leur côté, Wyk et McGraw proposent l'intégration des experts en sécurité dans les équipes de développement

d'applications, puis recommandent un ensemble d'activités à intégrer dans certaines phases du cycle de vie du développement d'une application (van Wyk et McGraw, 2005).

Tous ces auteurs reconnaissent l'importance de l'introduction de la sécurité dans le développement de chacun des composants de l'application, ainsi que dans ses activités de réalisation, et ce, à toutes les étapes du processus.

Cette même vision d'intégration de la sécurité dans le cycle de vie d'un système et dans celui du logiciel a notamment été présentée par l'ISO notamment dans ISO 15288, *Systems and software engineering – System life cycle processes* l'ISO qui présente un ensemble de phases et la description générale des processus présents dans le cycle de vie d'un système TI (ISO/IEC, 2007g). D'autre part, ISO 12207, *Systems and software engineering – Software life cycle processes* (ISO/IEC, 2008e) et ISO 14764, *Software Engineering – Software Life Cycle Processes – Maintenance* (ISO/IEC, 2005g) présentent la description générale des processus présents dans les phases du cycle de vie du logiciel.

Définissant le terme « sécurité » à la section 4 de ces documents, ce terme est ensuite utilisé à l'intérieur de ceux-ci de manière générique, afin de mettre l'accent sur l'importance de tenir compte de la sécurité dans plusieurs processus du cycle de vie d'un système et du logiciel. La contrepartie de descriptions aussi générales, c'est que même si l'organisation comprend qu'elle doit tenir compte de la sécurité, aucun indice n'est présenté pour la guider dans le choix, la mise en œuvre ou l'évaluation de l'implémentation de la sécurité de ses applications en fonction des besoins de l'organisation.

Aucun des ouvrages précédents n'indique ni au programmeur, ni aux autres membres d'une équipe d'un projet d'application, une démarche ou un outil lui permettant de décider quand la réalisation d'une activité ou la mise en place d'une technique de sécurité spécifique est nécessaire, et quand elle ne l'est pas. Même si l'organisation ou le développeur est en accord avec tout ce qui lui est présenté, ce dernier ne saura pas nécessairement quoi mettre en œuvre et comment procéder, ni comment l'évaluer ou le justifier (P14). Par contre, Mouratidis et

Giorgini présentent l'ingénierie de logiciels sécuritaires comme étant les pratiques d'ingénierie de logiciel dans lesquelles ont été intégrées des préoccupations de sécurité. Ils présentent des problématiques et les défis d'intégrer la sécurité dans les pratiques d'ingénierie logicielle, et proposent des approches permettant d'y répondre telles que l'identification des objectifs de sécurité, de la définition et de la validation des exigences de sécurité, ainsi que l'utilisation de patrons de conception (de sécurité) dans les méthodes de développement (Mouratidis et Giorgini, 2007).

Dans le même ordre d'idées, le guide du NIST *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* propose une liste de principes de haut niveau à considérer dans la conception, le développement, l'opération et le retrait d'un système TI, afin de guider les organisations dans le développement des politiques de sécurité devant s'y appliquer. Selon ces auteurs, ces principes peuvent être utilisés autant lors du développent d'un nouveau système que pour vérifier s'ils ont été suivis lors de la révision d'un système existant (Stoneburner, Hayden et Feringa, 2004).

Dans l'intention d'appliquer le principe d'intégrer la sécurité aux méthodes de développement de logiciels existants, Beznosov et Kruchten présentent comment une approche d'assurance sécurité[10] pourrait s'adapter aux méthodes agiles pour permettre d'y intégrer la sécurité (Beznosov et Kruchten, 2005). C'est dans cette même optique que Nunes, Belchior et Albuquerque ont développé et proposent le processus *Process to Support Software Security* (PSSS) pour assurer l'intégration de la sécurité dans le développement de logiciels (Nunes, Belchior et Albuquerque, 2010), (P12, P14, et P15).

L'entreprise Microsoft présente, dans *Security Development Lifecycle – Simplified Implementation of the Microsoft SDL* (Microsoft, 2010), son « cycle de vie de

---

[10] « L'assurance sécurité est un mécanisme qui permet de donner confiance dans les propriétés et les fonctionnalités liées à la sécurité, ainsi que dans ses processus d'exploitation et d'administration d'une solution développée. » – traduction libre (Beznosov et Kruchten, 2005, p. 2).

développement sécuritaire » (SDL) comme un processus d'assurance qualité qui permet l'intégration d'activités de sécurité dans le processus de développement des logiciels de Microsoft. Précédé d'une phase de formation, le SDL propose six phases dont la phase de définition des d'exigences qui inclut, notamment, une pratique de gestion de risques de sécurité et une pratique de modélisation des menaces. Le SDL inclut aussi un processus de vérification permettant à une organisation de s'assurer que le SDL a bien été suivi par une équipe de développement. Fait intéressant, le SDL précise non seulement les responsabilités, mais aussi les qualifications requises par être assigné aux deux rôles en sécurité définis dans le document : le réviseur et l'équipe de champions (Microsoft, 2010).

Le document *Comprehensive, Lightweight Application Security Process* (CLASP) (OWASP, 2006) d'OWASP, présente un processus divisé en cinq vues, soit : la vue présentant les concepts, les vues basées sur les rôles, l'assignation d'activité, l'implémentation d'activité et la vue des vulnérabilités (OWASP, 2006, p. 3). Tout comme le SDL de Microsoft, ce processus permet notamment d'intégrer la sécurité dans le développement et la maintenance d'une application, et de comparer les coûts d'implémentation des activités de sécurité en fonction des impacts des risques présents si rien n'est fait.

Gregoire, J., Buyens, De Win, Scandariato et Joosen présentent une comparaison, phase par phase, des deux processus de développement sécuritaires : Microsoft SDL et CLASP. Quoique visant le même objectif de sécurité, leurs approches et les activités définies dans chacun de ces processus sont très différentes. Par exemple, au niveau organisationnel, CLASP focalise sur l'importance pour une organisation de se définir des politiques de sécurité qui serviront de guides au développement de logiciels, tandis que Microsoft focalise sur l'importance de soutenir le développement sécuritaire de logiciels par la définition des rôles (ou équipes) et indiquer comment ceux-ci interagissent dans un projet de développement d'une application. Chacun des deux processus comparés propose des activités et principes différents qui sont parfois complémentaires et qui pourraient avantageusement être intégrés en un seul processus, plus global. Par contre, les deux processus concernent seulement le développement du logiciel et ne couvrent pas les autres aspects de la SA

comme, notamment, son opération et son contexte technologique. De plus, les deux processus n'offrent qu'une focalisation limitée sur l'identification de critères servant à identifier les objectifs de sécurité d'une organisation pour son projet et d'en mesurer l'atteinte (Gregoire et al., 2007).

Cette conclusion peut s'appliquer à tous les ouvrages révisés dans cette section. Quoique visant le même objectif de sécurité, les approches et les activités définies dans chacun de ces ouvrages sont très différentes. Chacun des processus présentés :

1) propose des activités et principes différents qui pourraient avantageusement être intégrés en un seul processus, plus global (P01);
2) ne concerne que le développement du logiciel et ne couvre pas les autres aspects de la SA (P06);
3) n'offre qu'une focalisation limitée sur l'identification de critères servant à identifier les objectifs de sécurité d'une organisation et ne permet pas d'en mesurer l'atteinte de façon répétable (P10).

3.3.2.2 Ouvrages proposant l'utilisation d'une démarche de gestion du risque, pour identifier ce qui doit être protégé dans une application

Steel, Nagappan et Lai ont principalement orienté le contenu de leur livre afin de répondre aux défis de développement sécuritaire d'application Web en langage Java. La gestion du risque y est mentionnée, mais n'y est pas mise en œuvre (Steel, Nagappan et Lai, 2005, pp. 452-455). Cet ouvrage présente un ensemble de contrôles tels que des patrons de conception de sécurité (Security patterns) et autres fonctionnalités de sécurité telles que la journalisation sécuritaire (Steel, Nagappan et Lai, 2005, p. 577), (P01, P15 et P16).

De son côté, Jürjens présente une démarche de conception basée sur la notation UML qui permet d'identifier des risques et de placer des contrôles en fonction des scénarios d'utilisation identifiés (Jürjens, 2005). Cette approche permet d'intégrer la sécurité au niveau de l'architecture de l'application avant son développement, en identifiant les fonctionnalités

et les cas d'utilisation pouvant être à risque, puis d'y intégrer des éléments servant à les sécuriser.

Viega et McGraw introduisent des principes qui guident la sécurité dans le logiciel (Viega et McGraw, 2002, pp. 91-113), présentent des stratégies telles que la définition d'arbres d'attaques pour identifier des risques (Viega et McGraw, 2002, pp. 120-125), puis identifient un ensemble de contrôles pouvant être intégrés au logiciel, tels que différents algorithmes de chiffrement ou encore des stratégies pour renforcer les fonctions de mots de passe et de l'authentification (Viega et McGraw, 2002).

De leur coté, Whittaker et Thompson présentent des stratégies d'attaques sur le logiciel, telles qu'attaquer les dépendances logicielles et les interfaces utilisateurs, présenter une démarche pour concevoir, implémenter et appliquer des stratégies d'attaques, puis terminent par quelques conseils tels que de rechercher dans la base de données des corrections de bogues pour identifier des pistes d'attaques (Whittaker et Thompson, 2004).

La série de normes SP 800-64 – *Security Considerations in the Information System Development Life Cycle*, développée par le NIST, a été conçue pour aider les agences gouvernementales fédérales américaines à intégrer des activités de sécurité considérées essentielles, à l'intérieur du cycle de développement de leurs systèmes TI. Elle propose un ensemble de rôles et de responsabilités ainsi que des activités de sécurité qui devront être réalisées à chaque phase du cycle de vie du développement d'une application (NIST, 2008). Par contre, plusieurs concepts gagneraient à être précisés tels que, la gestion des risques de SA spécifiques par rapport à la réalisation et la vérification des activités recommandées afin de confirmer l'atténuation des risques ciblés (P01, P05, P06, P08 et P15).

3.3.2.3 Ouvrages proposant l'amélioration de la maturité des processus pour implémenter la sécurité dans le développement d'une application

En publiant *CMMi for development*, le SEI présente un modèle qui soutient une approche d'amélioration de la qualité d'un produit ou d'un service, par l'amélioration de la maturité de

ses processus (CMMI, 2006). Sachant que la sécurité ne peut être mise en place dans un produit qui n'est pas de qualité, ce modèle a été utilisé par plusieurs organisations pour améliorer la sécurité des applications qu'elles développent. Ce modèle a mené au développement de la norme ISO 21827 *Capability Maturity Model* (SSE CMM) visant la spécialisation du modèle afin d'y intégrer les éléments de sécurité (ISO/IEC, 2006a).

Le modèle de maturité de processus présenté dans le document *Systems Security Engineering Capability Maturity Model* (SSE-CMM), v3.0 (All, 2003) et la norme ISO *21827 System Security Engineering – Capability Maturity Model (SSE-CMM)* (ISO/IEC, 2006a) présentent une approche visant l'intégration de pratiques de sécurité spécifiques dans des processus de développement de système, tout en s'assurant l'amélioration de la maturité des processus concernés (All, 2003, pp. 65-114) (ISO/IEC, 2006a, pp. 108-123). Quoique le contexte de l'application ne soit pas pris en compte, cette approche d'amélioration de la maturité des processus est reconnue dans le domaine de l'ingénierie de système. Ces deux ouvrages présentent 11 pratiques de sécurité (All, 2003, pp. 115-202) (ISO/IEC, 2006a, pp. 21-58) ainsi que 22 pratiques organisationnelles de projets (All, 2003, pp. A203-301) (ISO/IEC, 2006a, pp. 60-101) qui devraient être intégrées aux processus d'une organisation afin de lui permettre de développer un système sécuritaire.

McGraw, Chess et Migues présentent un guide offrant une approche de sécurité similaire au *Capability Maturity Model Integration* (CMMI) en visant l'intégration de pratiques de sécurité spécifiques dans le processus de développement d'un système, tout en s'assurant l'amélioration de la maturité des processus de développement concernés. Quoique ne prenant pas en compte le contexte de l'application, ce guide propose des ensembles d'activités dont des pratiques stratégiques et de mesures (McGraw, Chess et Migues, 2010, pp. 15-16) ainsi que des pratiques de conformité et de politiques (McGraw, Chess et Migues, 2010, pp. 17-18) permettant d'intégrer des préoccupations de sécurité dans le cycle de vie du développement d'une application, soit de sa conception à son déploiement (McGraw, Chess et Migues, 2010, p. 13).

Le guide de développement de logiciel *Security in the software lifecycle – Making Software Development Processes – and Software Produced by Them – More Secure* présente une approche qui indique aux développeurs, architectes et formateurs comment améliorer la qualité, la fiabilité et la sécurité du logiciel qu'ils produisent (DHS, 2007, p. iii). Cet ouvrage ne recommande pas d'approche spécifique à des problèmes de sécurité génériques, mais présente plutôt des approches alternatives à des problèmes de sécurité spécifiques, affirmant « qu'il n'existe aucun processus, pratique ou méthode offrant une solution magique universelle à tous les problèmes de sécurité » (DHS, 2007, p. iii). L'accent est surtout placé sur les attaques possibles dirigées vers les vulnérabilités du logiciel, en précisant les sources d'insécurité du logiciel telles que la mise en place de principes et de pratiques de développement inadéquats. L'ouvrage recommande de réaliser une gestion de risques de sécurité continue durant tout le cycle de vie du logiciel, appuyée par une gestion serrée des exigences alignée sur la sécurité du logiciel. Sachant qu'ils ne peuvent énumérer et adresser tous les cas d'attaques, les auteurs s'appuient surtout sur leur approche d'amélioration de la maturité des processus similaire au CMMi (CMMI, 2006) pour améliorer la sécurité du logiciel. Par contre, ils ne définissent pas comment, de manière mesurable, affirmer qu'un logiciel peut être considéré comme sécuritaire (DHS, 2007).

Nunes, Belchior et Albuquerque présentent les résultats d'une étude de cas démontrant l'amélioration de l'efficacité de l'approche proposée par SSE-CMM en la combinant à certains processus proposés par les normes ISO 15408 et ISO 27002, le tout à l'intérieur d'une démarche de gestion de risques de sécurité telle que proposée par l'Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Nunes, Belchior et Albuquerque, 2010, p. 50).

Il est évident que le modèle SA à concevoir dans notre travail de recherche devra permettre d'appliquer les principes du CMMI et d'aider à l'amélioration de la maturité des processus par la mise en œuvre de contrôles de SA complets, définis, quantitativement gérés et optimisés (P15).

3.3.2.4 Ouvrages proposant l'utilisation d'une démarche de vérification de produit pour améliorer la sécurité d'une application

La norme ISO 15408 *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model* (ISO/IEC, 2009c) et l'ouvrage *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, présentent une introduction et une présentation du modèle général proposé par les critères communs (Group, 2009).

Pavlidis, Mouratidis, Islam et Kearney présentent un métamodèle qui comprend un ensemble de concepts de « base de confiance » qui soutiennent le développement de systèmes en lesquels on peut avoir confiance (Pavlidis et al., 2012). Par exemple, ils introduisent le concept de relation de confiance directe et indirecte qui, associé à un arbre de dépendance, permet d'obtenir une confiance acceptable qu'une vulnérabilité a été adéquatement corrigée, basée sur le fait que chacun des contrôles identifiés dans l'arbre a été implémenté avec succès et qu'ils ajoutent tous leurs éléments de confiance (Pavlidis et al., 2012).

3.3.2.5 Ouvrages proposant l'utilisation d'indicateurs mesurables pour évaluer la sécurité des applications

Dejun, Mu, Wei, Baolei et Bo présentent une approche différente pour sécuriser une application. La méthode proposée permet, à l'aide de portes booléennes, de surveiller et d'appliquer des contrôles stricts sur tous les flux d'information qui circulent dans l'application ainsi que dans le matériel sous-jacent. Elle offre, selon les auteurs, une base solide pour s'assurer d'une circulation sécuritaire de l'information et permet la possibilité de démontrer l'atteinte des propriétés de sécurité, et ce, à tous les niveaux d'abstraction de l'application (Dejun et al., 2014). L'élément à considérer, tel que proposé par ces auteurs, est de suivre les flux d'information à l'intérieur de l'application.

Walton, Longstaff et Linger présentent une nouvelle approche permettant de définir des « Attributs de Sécurité Calculés » rendant possible l'analyse de la sécurité d'un logiciel en

termes de données et de transformation de données par l'application. Cette approche fournit des exigences de comportement pour certains attributs de sécurité, et discute de l'application possible de cette approche pour réaliser l'analyse d'attributs de sécurité calculés au cours des phases de développement, d'acquisition, de vérification et d'exploitation d'une application (Walton, Longstaff et Linger, 2009). Il faut noter que, dans leurs définitions, une propriété de sécurité est une fonctionnalité de sécurité devant être offerte par l'application telle que l'authentification ou la non-répudiation. Cette approche est un bon exemple de situation où l'on tente d'utiliser une approche mathématique pour calculer un résultat qui est le comportement attendu d'une fonction de sécurité, soit un comportement qui est, finalement, un résultat qualitatif qui sera interprété comme acceptable ou non. L'« Attribut de Sécurité Calculé » est en fait un contrôle de sécurité de haut niveau qui devra être mis en place et produire un résultat attendu pour pouvoir considérer que le risque ciblé a été diminué à un niveau acceptable.

Abran présente les principes et les qualités que doivent respecter les unités et les mécanismes de mesures du logiciel (Abran, 2010). Identifier des méthodes de mesures significatives permettant de bonifier un modèle est rarement un exercice trivial, et l'évaluation de l'atteinte d'exigences non fonctionnelles reste l'un des défis de ce domaine. Les mêmes défis d'identifier des éléments et des mécanismes de mesures significatives et répétables existent aussi en sécurité des applications. L'utilisation d'un modèle SA intégrant des éléments de métrologie pourrait aider à présenter des résultats de mesures significatifs et répétables aux demandes d'une organisation comme, à titre d'exemple, de pouvoir définir ce que devrait être une application qui serait considérée comme sécuritaire et de pouvoir le mesurer (P10).

3.3.3 Ouvrages liés à l'environnement et l'infrastructure technologiques des applications

Plusieurs ouvrages ont été réalisés concernant l'environnement et l'infrastructure technologiques utilisés par les applications.

Chen, Chriqi, Otrok et Robert présentent dans leur article différents risques amenés via l'infrastructure réseau utilisée par l'application, ainsi que des stratégies pour les détecter ou les atténuer (Chen et Robert, 2004), (Chriqi, Otrok et Robert, 2009).

Schumacher et al. présentent une approche par patron de conception en sécurité qui concerne principalement des cas d'infrastructures TI, tels que des patrons d'identification et d'authentification de modèles de contrôle d'accès, d'architectures de contrôle d'accès aux systèmes, d'architectures de pare-feu, de patrons permettant d'identifier des critères aidant à identifier des applications Internet sécuritaires, puis termine par une étude de cas sur la téléphonie IP avec certains des patrons présentés (Schumacher et al., 2006).

Paquet et Saxe présentent l'architecture réseau comme un des pivots de la sécurité des TI d'une organisation. La sécurité est une question de gouvernance qui doit être amenée au niveau du conseil d'administration (Paquet et Saxe, 2005, p. 169): c'est de là que devraient être prises les décisions de mise en place de politiques et de processus menant à la sécurisation de l'infrastructure réseau où seront déployées les applications de l'organisation. La sécurité est un processus vivant; la roue de la sécurité sécurise, surveille, teste et améliore, ce qui reprend globalement la roue de Deming avec son « *plan, do, check, act* » (Paquet et Saxe, 2005, p. 295).

L'*ITIL v3* (OGC, 2007), (ITIMF, 2013) présente des pratiques de bonne gestion des services pouvant être offerts par l'infrastructure TI d'une organisation. Sachant que cette infrastructure TI est requise pour soutenir les applications hébergées par une organisation, ITIL v3 tient aussi compte de la sécurité en définissant la « garantie d'un service » (ITIMF, 2013, p. 14). Sans descendre au niveau de l'application, ITIL demande la mise en place d'un processus de gestion de la sécurité de l'information (ISM) tel que requis par ISO 27001, dont l'objectif est d'aligner la sécurité TI avec les besoins de sécurité de l'organisation. Il permet de s'assurer que la sécurité de l'information de l'organisation est présente et adéquatement gérée dans l'opération de tous les services ainsi que dans leurs processus de gestion de

l'organisation (ITIMF, 2013, p. 22), et ce, en proposant un ensemble de contrôles de sécurité intégrés au système de gestion de la sécurité de l'information (ISMS).

Ben-Natan présente des activités pour renforcer les environnements et appliquer les rustines aux systèmes de gestion des basses de données. Puis, il présente des principes et des solutions concernant l'impact des bases de données sur la sécurité d'une application, tels que l'audit des catégories d'information et d'architecture, la conformité aux lois, le chiffrement, la granularité du contrôle d'accès, etc. (Ben-Natan, 2005).

Le NIST propose, dans SP 800-53 Rev 4 – *Security and Privacy Controls for Federal Information Systems and Organizations,* une démarche de sécurité ainsi qu'un catalogue de 256 contrôles de sécurité, regroupés en 18 familles pouvant être mis en place afin de répondre aux principales exigences de sécurité d'un système TI requises par une organisation. Quoique de haut niveau, la description de chacun de ces contrôles propose souvent trois degrés d'implémentation : bas, moyen et haut, permettant ainsi d'en ajuster le niveau de sécurité en fonction des besoins de sécurité spécifiques de l'organisation (NIST, 2013). La démarche et les contrôles présentés dans ce document s'alignent principalement sur la norme ISO 15408 (Critère commun) (ISO/IEC, 2009c).

(Qun et Edwards, 1998), (Chen et Robert, 2004), (Garcia et Robert, 2009), (Peterson, 2010) et (Chriqi, Otrok et Robert, 2009) présentent des problématiques de sécurité d'infrastructure TI qui auraient des impacts sur la sécurité des applications qu'elles soutiennent. La question qui se pose est : est-ce que les éléments d'une infrastructure TI, qui soutiennent une application sensible, devraient être inclus dans la définition de la portée de la sécurité de cette application, peu importe que cette infrastructure soit installée dans l'établissement, dans un établissement situé dans une autre ville ou chez un fournisseur de services d'hébergement? Afin d'alimenter cette réflexion, élaborons un cas précis. Un établissement hospitalier a fait l'acquisition d'une application lui permettant de gérer les dossiers de ses patients. Toutes les informations personnelles et confidentielles des patients qui ont été traités dans cet hôpital sont conservées par l'application et, de ce fait, sont transmises ou stockées quelque part dans

l'un des serveurs de l'infrastructure TI qui soutient cette application. Si une personne ou une application malicieuse parvient à contourner les contrôles de sécurité de l'application, et réussit à se connecter directement au serveur de la base de données que cette dernière utilise, peut-on considérer que la sécurité de l'application a été compromise, sachant que les informations accédées sont conservées dans cette infrastructure TI seulement parce que l'établissement utilise l'application concernée? Dans l'affirmative, il faut alors considérer le contexte technologique nécessaire au fonctionnement d'une application comme faisant partie des sources de risques devant être incluses dans la portée de sa sécurité, que ce contexte implique notamment l'utilisation de serveurs internes, son système d'exploitation, ou encore la capacité de stockage et de traitement de serveurs virtuels déployés sur le nuage d'une entreprise externe (P02 et P06).

3.3.4 Ouvrages liés à la vérification et aux audits de SA

L'ISACA propose dans COBIT 4.1 (ITGI, 2007), et plus récemment COBIT 5.0 (ISACA, 2012) des référentiels destinés à la gouvernance des TI permettant à un gestionnaire de définir les objectifs de contrôle, soit préciser pourquoi la gestion des TI est requise dans son organisation, et déterminer les acteurs impliqués par cette gestion ainsi que les besoins à combler. Ces référentiels contiennent notamment des processus d'audits et de contrôles de sécurité permettant la vérification et l'audit de systèmes d'information impliquant l'utilisation des TI. Même s'il est principalement utilisé pour auditer des applications qui sont déjà déployées dans l'environnement opérationnel d'une organisation, COBIT fait autorité dans le domaine de la gestion, de la vérification et du contrôle des systèmes d'information.

Il faut noter que l'utilisation de ces cadres présuppose une compréhension réelle des risques de sécurité amenés par l'utilisation des TI.

L'approche et la certification de systèmes TI selon les critères communs (ISO/IEC, 2009c) sont considérées par bien des experts comme étant les références en sécurité des systèmes TI. L'ISO présente aussi, dans la deuxième partie de la norme ISO 15408 *Information*

technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements, un ensemble d'exigences de sécurité fonctionnelle pouvant être mis en place dans un système TI (ISO/IEC, 2005a). Bien que reconnue dans l'industrie des TI, cette norme de certification est considérée trop dispendieuse, par bien des organisations, par rapport aux impacts liés aux risques de sécurité amenés par l'utilisation de leurs applications.

Même si le NIST a, depuis, révisé cette norme pour l'aligner sur une approche de gestion du risque, la première version du document SP 800-37 – *Guide for the Security Certification and Accreditation of Federal Information Systems* présente des lignes directrices pour la certification et l'accréditation de la sécurité de systèmes d'information utilisés par des organismes fédéraux Américains. Elle permet notamment des évaluations cohérentes, comparables et répétables de contrôles de sécurité (Ross et al., 2003).

3.4 Identification des éléments de réponses aux problématiques en SA

Cette section présente dans un premier temps, le constat de cette revue de littérature pour chacune des 16 problématiques identifiées (P01 à P16) puis, dans un deuxième temps, identifie le ou les éléments nécessaires pour la conception du modèle SA.

P01 : Absence d'une vision globale de la sécurité des applications

Bien que l'OCDE recommande d'intégrer tous les intervenants dans la gestion de la sécurité, aucun des documents revus ne présente de vision de la SA qui inclut simultanément : les personnes, les processus et la technologie, les trois contextes dont proviennent les risques de SA, ainsi que les besoins des acteurs œuvrant dans les quatre domaines d'interventions liés à la SA. De plus, aucun document ne fait état d'un cycle de vie de la sécurité des applications qui présenterait clairement les phases, les activités et les acteurs des quatre domaines d'interventions de la SA, et dans lequel peuvent être intégrés des contrôles de sécurité contenant leurs propres processus de vérification.

Le modèle à développer dans cette recherche devra être en mesure de présenter cette vision globale de la SA.

P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application

Aucun ouvrage revu n'offre de processus ou d'indication que les risques de SA à tenir en compte dans le processus de sécurisation d'une application proviennent simultanément des trois contextes de l'application, soit : le contexte d'affaires, le contexte juridique et le contexte technologique.

Tout comme la sécurité de l'information, le modèle SA développé dans cette recherche devra intégrer une approche basée sur la gestion du risque et proposer une vision permettant d'identifier et de tenir en compte les risques provenant des contextes spécifiques d'utilisation d'une application.

P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations

Il existe présentement des modèles de sécurité comme CLASP et COBIT qui offrent une bonne flexibilité d'adaptation aux besoins de sécurité d'une organisation. Cependant, étant donné qu'aucun des modèles revus ne couvre les quatre domaines d'intervention ni l'ensemble des phases et des activités du cycle de vie de la SA, il est presque certain qu'en les utilisant, certains besoins de sécurité d'une organisation ne pourront n'être ni identifiés ni répondus.

Le modèle développé dans cette recherche devra être en mesure de s'adapter aux besoins de sécurité d'une organisation pour ses applications.

P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques

Bien que plusieurs ouvrages proposent une approche appliquant le principe de gestion des risques pour identifier les activités et les contrôles de sécurité à mettre en place pour une application, aucun d'entre eux ne propose de mesures permettant d'évaluer quantitativement les coûts affectés à la diminution de ces risques, ni des mesures permettant de vérifier l'atteinte des objectifs de sécurité visés.

Le modèle à concevoir dans cette recherche devra être en mesure de fournir les mesures et les activités permettant à une organisation d'évaluer les coûts de la diminution d'un risque de sécurité et la vérification de l'atteinte du niveau de sécurité ciblé pour une application.

P05 : **Absence d'un vocabulaire et de références communes en sécurité des applications**

Comme le domaine de la sécurité des applications implique la collaboration d'intervenants provenant de quatre domaines d'intervention, des risques de confusion peuvent apparaître de par l'utilisation de certains termes.

Le modèle à développer dans cette recherche devra minimalement être en mesure de proposer des définitions des termes clés.

P06 : **Absence d'une définition de la portée de la sécurité d'une application**

Haley, Laney, Moffett et Nuseibeh définissent une application « comme étant plus que le logiciel », mais ne précisent pas clairement les frontières et la portée de leur définition (Haley et al., 2008, p. 134).

Le modèle à développer dans cette recherche devra proposer une définition claire de la portée de la sécurité d'une application.

P07 : Absence d'une définition claire de ce qu'est une application sécuritaire

Le modèle à développer dans cette recherche devra proposer une définition claire d'une application sécuritaire.

P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application

Plusieurs modèles de cycles de vie différents sont utilisés par les auteurs des divers ouvrages analysés. Certains modèles ne couvrent que la phase de développement, d'autres couvrent un cycle de vie plus long qui se termine à la disposition du système TI.

Le modèle à développer dans cette recherche devra proposer un modèle de référence du cycle de vie de la sécurité d'une application.

P09 : Absence de sources claires des exigences de sécurité d'une application

Lorsque les auteurs abordent le sujet, l'origine des exigences de sécurité diffère d'un ouvrage à l'autre. Pour certains, ils proviennent des lois et règlements, pour d'autres, ils proviennent notamment des objectifs de sécurité de l'organisation.

Le modèle à développer dans cette recherche devra proposer une démarche unique et inclusive qui permettra d'identifier toutes les exigences de sécurité qu'une organisation pourrait désirer pour une application.

P10 : Absence d'une méthode d'évaluation de la sécurité d'une application

Évaluer la SA présente trois défis majeurs. L'obtention de la mesure, la qualité de la mesure et l'interprétation de la mesure obtenue. Certains ouvrages proposent l'utilisation de mesures pour évaluer les cibles de sécurité, mais aucun ne définit ces mesures clairement. Par exemple, aucun ouvrage ne propose de suggestions sur ce que pourrait être une unité de mesure de la sécurité.

Sachant qu'il existe trois façons d'obtenir une mesure (elle résulte d'une équation mathématique, d'une activité de mesure ou d'un modèle de décision quantitative (Abran, 2010)), et sachant aussi qu'un mécanisme de mesure doit pouvoir produire un résultat répétable et indépendant du mesureur, le modèle SA à développer dans cette recherche devra proposer des mesures pour évaluer la cible de sécurité ainsi qu'une démarche permettant de vérifier l'atteinte de cette cible.

P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation

Les critères communs constituent l'une des approches qui propose un processus reconnu permettant la vérification des éléments de sécurité d'une application. Par contre, ce processus implique des investissements monétaires non négligeables qui ne sont pas disponibles à tous les types d'organisations.

Le modèle SA à développer dans cette recherche devra proposer une démarche crédible, flexible et répétable permettant la vérification des éléments de sécurité d'une application, en fonction des besoins et des moyens de l'organisation.

P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications

Aucun des ouvrages analysés ne propose d'approches ni d'éléments complètement erronés. Personne ne peut être contre la gestion du risque pour minimiser les coûts de la sécurité, ni contre l'introduction d'éléments de sécurité dans les processus existants au sein d'une organisation pour diminuer la résistance aux changements, ni contre des bonnes pratiques de programmation sécuritaire. Mais aucun ouvrage ne propose d'approches pour relier adéquatement toutes ces bonnes pratiques, selon les besoins et les attentes de sécurité d'une organisation pour ses applications.

Le modèle SA à développer dans cette recherche devra proposer un modèle qui permet l'arrimage entre les approches, méthodes, bonnes pratiques, contrôles, acteurs et outils

existants afin de permettre à une organisation de les utiliser selon ses besoins de sécurité, pour chacune de ses applications.

P13 : Absence de mécanismes permettant d'assigner aux principaux rôles, pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune des responsabilités qui leur sont assignées

Sur l'ensemble des ouvrages analysés, un seul identifie les qualifications d'un rôle comme un élément essentiel à définir afin de s'assurer de la compétence de cet acteur à bien assumer ses responsabilités, et cet ouvrage ne définit que deux rôles.

Le modèle SA à développer dans cette recherche devra proposer un outil permettant d'assigner, aux principaux rôles pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune des responsabilités qui leur sont assignées.

P14 : Les méthodes et outils existants de génie logiciel ne tiennent pas toujours compte de la sécurité de l'information TI

Les méthodes et outils existants de génie logiciel tiennent rarement compte explicitement de la sécurité de l'information TI. Cette préoccupation se retrouve généralement au niveau de l'organisation.

Le modèle SA à développer dans cette recherche devra permettre de faire le lien entre les besoins de sécurité de l'information exprimés par l'organisation avec les activités et les contrôles qui seront mis en place par les ingénieurs logiciels et les équipes de développement afin de s'assurer d'une réponse adéquate et homogène de ces derniers aux attentes de sécurité requises par l'organisation.

P15 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur des processus impliqués dans la réalisation et l'opération de l'application

Aucun des documents revus durant cette recherche ne propose d'activités ou de contrôles de sécurité précis, couvrant le développement d'une application ainsi que son opération. La

majorité des ouvrages qui proposent ce type d'éléments se concentrent sur le cycle de vie du développement du logiciel. Pour ceux qui adressent le cycle de vie d'un système dans son ensemble, ils soulignent que la sécurité doit être prise en compte dans les processus présents à tous les stages du cycle de vie, sans réellement en préciser la teneur et les résultats attendus.

Le modèle SA à développer dans cette recherche devra permettre d'identifier formellement, et d'intégrer de manière vérifiable, des contrôles de sécurité à l'intérieur des processus impliqués dans tout le cycle de vie de la sécurité d'une application.

P16 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur de l'application

Aucun des documents revus durant cette recherche ne propose d'approches permettant de définir un mécanisme ou un contrôle de sécurité qui s'intégrerait directement à l'intérieur de l'application. Cette approche est généralement laissée à la discrétion des ingénieurs et des développeurs qui identifieront des fonctionnalités de sécurité à intégrer à l'application.

Tout comme pour les processus du cycle de vie de la SA, le modèle SA à développer dans cette recherche devra permettre d'identifier formellement, et d'intégrer de manière homogène et vérifiable, des contrôles de sécurité à l'intérieur même d'une l'application.

3.5 Constats de la revue de littérature

La SA est un domaine qui ne concerne pas seulement les développeurs et le logiciel, mais qui embrasse l'ensemble des domaines d'expertises des divers intervenants œuvrant à réaliser, à déployer, à opérer, à maintenir et à disposer une application de manière sécuritaire. Ce travail de recherche a identifié une quantité impressionnante d'ouvrages et d'articles traitant de l'une ou l'autre des facettes de la sécurité pouvant s'appliquer à la SA. Tous ces ouvrages abordent une ou plusieurs problématiques de sécurité selon la perspective du domaine d'expertise des auteurs. Par exemple, les développeurs et ingénieurs logiciels présentent des problématiques de sécurité survenant lors de la conception et de la maintenance d'une

application, et proposent des solutions, par exemple une méthode de développement incluant la sécurité, une pratique de programmation sécuritaire, le développement de composants de sécurité à intégrer à l'application, etc. Les ouvrages rédigés par des intervenants en gouvernance présentent les problématiques de gestion du risque et de contrôles rarement mesurables, qui sont répondus à l'aide de directives, de règles et de politiques organisationnelles. Tandis que les ouvrages rédigés par des intervenants en génie logiciel présentent les problématiques de méthodes de développement qui intègrent des éléments de sécurité tels que la programmation sécuritaire, l'identification des menaces ou l'amélioration de la maturité des processus.

En résumé, même si cette revue de littérature a permis de démontrer qu'aucun d'entre eux ne propose de solution répondant de manière satisfaisante à la totalité des 16 problématiques identifiées, cette revue de littérature nous a tout de même permis de bénéficier d'un apport considérable de concepts et d'approches pouvant être appliqués à la SA (*Voir* l'appendice A – ANNEXE VI, Tableau-A VI-1).

3.5.1 Synthèse des éléments provenant d'articles scientifiques

Plusieurs éléments, présentés dans les ouvrages répertoriés, ont directement influencé la portée et la conception du modèle SA. Voici quelques exemples d'approches et de pistes de solutions provenant de ces articles scientifiques revus qui ont directement influencé les travaux de cette recherche.

1) Articles scientifiques proposant diverses approches prônant, notamment :
   a) l'utilisation de patrons de conception (de sécurité) dans les méthodes de développement (Mouratidis et Giorgini, 2007);
   b) l'inclusion de la sécurité des infrastructures TI à la sécurité des applications qu'elles soutiennent (Qun et Edwards, 1998), (Chen et Robert, 2004), (Garcia et Robert, 2009), (Peterson, 2010), et (Chriqi, Otrok et Robert, 2009);

c) l'intégration de la gestion du risque à SA confirmant l'une des orientations de cette recherche (Baker et Wallace, 2007), (Yi et al., 2003), (Evans et al., 2004), (Dianxiang et Nygard, 2006), (White, Wijesekera et Hatton, 2008), (Menzel et Meinel, 2009), (Sherief, Abdel-Hamid et Mahar, 2010), (Borek et al., 2012), et (Avramescu et al., 2013);
d) la vérifiabilité de la SA (Baker et Wallace, 2007) et (Peterson, 2010);

2) Articles scientifiques proposant diverses pistes de solutions pour, notamment :
   a) aider à l'estimation des coûts de la sécurité (Caulkins et al., 2007);
   b) intégrer la sécurité des applications au niveau organisationnel (Johnson et Goetz, 2007);
   c) définir des exigences de sécurité des applications en précisant qu'une application est plus que le logiciel qu'il contient (Haley et al., 2008);
   d) permettre l'arrimage de la sécurité des applications au contexte juridique (Jorshari, Mouratidis et Islam, 2012);
   e) identifier un ensemble d'activités de sécurité comme, par exemple, la programmation sécuritaire à intégrer dans les processus de développement d'une application (Zenah et Aziz, 2011) et (van Wyk et McGraw, 2005);
   f) suivre les flux d'information qui circulent dans une application, ainsi que dans le matériel sous-jacent, pour démontrer l'atteinte des propriétés de sécurité dans la circulation sécuritaire de l'information à tous les niveaux d'abstraction d'une application (Dejun et al., 2014). Dans cet article scientifique, les auteurs proposent une approche différente pour sécuriser une application.

3.5.2 Synthèse des pistes de solutions proposées par les ouvrages consultés

Le Tableau 3.1 présente une synthèse des ouvrages qui proposent des éléments de solution en réponse aux 16 problématiques énoncées et détermine la couverture des solutions proposées.

Tableau 3.1 Nombre d'ouvrages proposant des pistes de solution à chacune des 16 problématiques en SA

Nombre d'ouvrages	proposant au moins une piste de solution, complète ou partielle, à la problématique
49	P01 : Absence d'une vision globale de la sécurité des applications
38	P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application
18	P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations
12	P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques
42	P05 : Absence d'un vocabulaire et de références communes en sécurité des applications
54	P06 : Absence d'une définition de la portée de la sécurité d'une application
3	P07 : Absence d'une définition claire de ce qu'est une application sécuritaire
2	P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application
24	P09 : Absence de sources claires des exigences de sécurité d'une application
19	P10 : Absence d'une méthode d'évaluation de la sécurité d'une application
8	P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation
5	P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des **applications**
9	P13 : Absence de mécanismes permettant d'assigner aux principaux rôles, pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune des responsabilités qui leur sont **assignées**
15	P14 : Les méthodes et outils existants de génie logiciel ne tiennent pas toujours compte de la sécurité de l'information TI
30	P15 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur des processus impliqués dans la réalisation et l'opération de l'application
5	P16 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur de l'application

3.6 Revue complémentaire

Ayant l'intuition que des concepts et des éléments importants n'avaient pas été identifiés et n'étant pas complètement satisfait des éléments de réponses aux problématiques en SA contenus dans les ouvrages consultés, nous avons ajouté une étape supplémentaire à la revue de littérature. Cette nouvelle étape consiste à identifier et à analyser un nouveau type

d'information, soit des rapports et documents issus de projets liés à la SA qui pourraient apporter de nouvelles pistes de réflexion.

Parmi les projets auxquels l'auteur a contribué durant les 15 dernières années, nous en avons sélectionné quatre qui sont liés au sujet de cette recherche. Ces projets, réalisés en milieux universitaires et industriels, ont fait l'objet d'une analyse rétroactive visant à découvrir de nouveaux éléments de réponses aux 16 problématiques déjà évoquées dans ce document. Il s'agit des projets suivants :

1) Les travaux de maîtrise du chercheur en sécurité informatique (3.6.1);
2) Le cours universitaire de premier cycle en sécurité appliquée développé par le chercheur (3.6.2);
3) Les certifications professionnelles liées à la sécurité de l'information et des applications obtenues par le chercheur (3.6.3);
4) La démarche et des résultats de l'audit de sécurité des applications dirigé par le chercheur en industrie et dans des organisations (3.6.4).

Les sections 3.6.1 à 3.6.4 présentent les résultats de cette analyse rétroactive qui a permis de dégager des concepts et des éléments absents, ou complémentaires aux éléments de réponses déjà répertoriés dans la revue de littérature, et qui ont été intégrés au modèle SA préliminaire ou, encore, qui en ont influencé la conception.

3.6.1 Analyse rétroactive des travaux de maîtrise du chercheur en sécurité informatique

En 2002, notre mémoire de maîtrise « Méthodologie et politique de sécurité – *Security Policy Markup Language* » a permis de dégager des pistes de solutions pratiques pouvant s'appliquer aux lacunes de sécurité qui se trouvaient au niveau des applications et des systèmes d'information. Ce mémoire proposait une réflexion pratique à la problématique : les organisations « … se demandent comment s'assurer que ces composantes commerciales, insérées dans leur système informatique, ne contiennent pas de codes malicieux, de portes dérobées ou de fonctionnalités indésirables susceptibles de violer leurs politiques de

sécurité. » (Poulin, 2002, p. 1) C'est à la fin de ce travail de recherche que les premiers concepts et éléments du modèle SA ont été définis (P01, P03, P14, et P15).

Le Tableau 3.2 présente les concepts et éléments provenant du mémoire de maîtrise du chercheur qui ont été intégrés dans ce projet doctoral au modèle SA.

Tableau 3.2 Concepts et éléments du mémoire de maîtrise intégrés au modèle SA

Concepts et éléments amenés par la réalisation du mémoire	Concepts et éléments intégrés au modèle
• « Le milieu de la sécurité informatique utilise l'expression «base informatique de confiance », … pour désigner l'ensemble des mécanismes de protection d'un système informatique. » (Poulin, 2002, pp. 8-10) • « Base informatique de confiance (Trusted Computing Base) » (Pfleeger, 1989)	1) Niveau de confiance : ensemble des mécanismes de protection d'une application, incluant les mécanismes de protection matérielle, logicielle et organisationnelle, qui ensemble mettent en œuvre la politique de sécurité de l'organisation
• « Vision d'un système d'information et de l'architecture de sa sécurité » (Poulin, 2002, pp. 44-46)	2) Posséder une vision globale de la cible de sécurité, identifier et évaluer les mesures à mettre en place afin d'éviter toute improvisation des divers intervenants, optimisant ainsi le rapport coûts versus pertinence des solutions apportées 3) La confiance que l'on peut accorder à une application est liée au résultat de l'évaluation de sa sécurité : niveau de confiance mesuré

3.6.2 Analyse rétroactive du cours universitaire de premier cycle en sécurité appliquée développé par le chercheur

Suite à l'obtention de ce diplôme, le département d'informatique et de génie logiciel de l'Université Laval nous a demandé de préparer et donner un cours de premier cycle sur les aspects pratiques de la sécurité informatique. Le développement de ce cours, basé sur 5 ouvrages (Poulin et Guay, 2006a, p. 3), a permis de préciser les éléments du modèle et d'en identifier les points faibles qui méritaient d'être retravaillés.

Ces auteurs, qui présentaient chacun un regard différent de la sécurité, sont :

1) Andress, qui présente une vision de haut niveau de la sécurité et qui identifie notamment les personnes, les processus et la technologie comme étant les principales sources de risques de sécurité de l'information (Andress, 2003), (P01, P09, P12 et P15);
2) Barman, qui présente les préoccupations de sécurité des informations utilisées par une organisation, d'où l'importance de la rédaction de politiques adaptées ou appliquées comme étant un des outils essentiels pour la gestion des risques de sécurité dans une organisation (Barman, 2002), (P09);
3) Viega et McGraw, qui présentent les préoccupations de génie logiciel concernant l'introduction de la sécurité dans le développement de logiciels (Viega et McGraw, 2002), (P04, P10, P14 et P15);
4) Des auteurs anonymes, qui présentent, dans l'ouvrage *Maximum Security*, les préoccupations de sécurité concernant la protection de l'infrastructure technologique d'une organisation ainsi que des exemples des différentes stratégies et outils variés pour y répondre (Anonymous, 2003), (P04 et P15);
5) Schneier, qui présente les préoccupations de sécurité concernant la protection de l'information, dont notamment la mise en place de mécanismes de cryptographie (Schneier, 1996), (P16).

Le cours ift-22514 – Aspects pratiques de la sécurité informatique, présente la sécurité des applications selon une nouvelle vision. Cette vision explique notamment comment les activités de développement et de maintenance d'une application, réalisées par les ingénieurs logiciels, sont liées aux activités de gouvernance, de gestion de l'infrastructure TI et d'audit de cette même application. Ce cours identifie des activités de sécurité à intégrer tout au long du cycle de vie de l'application, telles que dans les processus de développement et les processus de support de l'infrastructure TI (P01, P02, P03, P04, P07, P09, P10, P12, P14, P15 et P16).

Le Tableau 3.3 présente les concepts et éléments provenant du cours ift-22514 qui ont été développés et intégrés au modèle SA par le chercheur.

Tableau 3.3 Concepts et éléments du cours intégrés au modèle SA

Concepts et éléments amenés par la conception du cours	Concepts et éléments intégrés au modèle
• « Une vision globale des domaines de connaissances » (Poulin et Guay, 2006a, pp. 4-5)	1) Les quatre domaines d'intervention liés à la sécurité de l'information et des applications
• Le « cadre de gestion de la sécurité de l'information » (Poulin et Guay, 2006a, p. 10)	2) Représentation sommaire et préliminaire de l'environnement de la sécurité d'une application
• La sécurité est tributaire du cumul des interactions des personnes, des processus et de la technologie. (Andress, 2003, p. 5)	3) La source d'un risque de sécurité peut être une personne, un processus ou une technologie
• « Un projet de développement de système doit s'assurer de couvrir adéquatement les besoins de sécurité provenant des quatre domaines de connaissances, selon le niveau de confiance désiré, en tenant compte du type de données et du contexte d'exécution cible. Il faut aussi être en mesure de prouver l'atteinte du niveau de confiance visé. » (Poulin et Guay, 2006b, p. 14)	4) Les exigences de sécurité 5) Le niveau de confiance ciblé 6) La classification des informations liées à l'utilisation de l'application 7) Les trois contextes d'exécution de l'application (affaires, juridiques et technologiques) aident à déterminer certains risques de sécurité 8) L'exigence de preuves vérifiables permet de démontrer l'atteinte du niveau de confiance ciblé
• « Le développement d'un système d'information a un impact sur les quatre secteurs de la sécurité d'une organisation. » (Poulin et Guay, 2006b, p. 14)	9) La prise en compte simultanée des quatre domaines d'intervention liés à la sécurité d'une application
• Les « principaux acteurs de l'équipe de réalisation » (Poulin et Guay, 2006b, p. 21).	10) Identification des rôles impliqués dans la SA lors de la réalisation d'une application
• Le « cadre normatif : ensemble des normes, politiques et procédures de l'organisation concernant le développement, la maintenance et l'évolution des systèmes d'information. » (Poulin et Guay, 2006b, p. 25)	11) Le cadre normatif de l'organisation
• « Méthodologie de développement sécuritaire » (Poulin et Guay, 2006b, p. 39)	12) La portée du cycle de vie d'une application sécuritaire commence au stade de la préparation et se termine au stade de l'élimination 13) Deux des quatre couches du cycle de vie d'une application sécuritaire, soit : la réalisation de l'application et la gestion des infrastructures technologiques de l'application
• « Gestion du risque logiciel en pratique : l'équilibre entre les buts de sécurité et de gestion de projets est difficile à trouver » (Poulin et Guay, 2006c, p. 6)	14) Appuyer la démarche de sécurité sur la gestion du risque de manière à s'assurer que les décisions seront prises au niveau décisionnel approprié

3.6.3 Analyse rétroactive des certifications professionnelles obtenues par le chercheur en sécurité de l'information et des applications

Désirant comprendre et pouvoir utiliser les concepts, le vocabulaire, les processus, les outils, les normes et les pratiques recommandés qui sont utilisés dans les différents secteurs de la sécurité de l'information et des applications, nous avons obtenu les certifications professionnelles suivantes :

1) *Certified Information Security Manager* (CISM) de l'ISACA qui porte aussi sur la gouvernance de la sécurité de l'information, par le biais de la gestion d'entreprise;
2) *Information System Security Management Professional* (ISSMP) de l'*International Information Systems Security Certification Consortium* $(ISC)^2$ qui porte principalement sur la gouvernance de la sécurité de l'information, par le biais de la gestion des TI;
3) *Certified Secure Software Lifecycle Professional* (CSSLP) du $(ISC)^2$ qui porte principalement sur la gestion de la sécurité durant tout le cycle de vie du logiciel;
4) *Certified Information System Security Professional* (CISSP) du $(ISC)^2$ qui porte principalement sur la sécurité des infrastructures; et
5) *Certified Information System Auditor* (CISA) de l'ISACA qui porte sur les audits de sécurité des systèmes d'information.

Ces certifications ont permis de nous familiariser et de comparer les différents vocabulaires utilisés par les experts de ces domaines (P05), puis d'identifier les éléments qui pourraient aider à améliorer le modèle SA (P01). C'est à cette période que l'hypothèse d'étendre le modèle de cycle de vie de la SA sur plusieurs niveaux (gouvernance de la SA, fournir l'application, infrastructure TI, vérification et contrôle de la SA) a été énoncée (P08).

Le Tableau 3.4 présente les concepts et éléments provenant de six certifications professionnelles en sécurité des TI qui ont été définis puis intégrés au modèle SA par le chercheur.

Tableau 3.4 Concepts et éléments liés aux certifications professionnelles intégrés au modèle SA

Concepts et éléments amenés par ces certifications professionnelles en sécurité de l'information	**Concepts et éléments intégrés au modèle**
• CISM – Responsable de la gestion de la sécurité de l'information. Soit d'assurer la gouvernance, la gestion des risques, le développement et la gestion de programmes de sécurité de l'information ainsi que la gestion et la réponse aux incidents (ISACA®, 2013b) • ISSMP – Responsable de la construction du cadre de la sécurité de l'information et de définir les moyens de soutenir l'organisation ((ISC)², 2013a)	1) Principes de sécurité – La gestion du risque et des ressources doit être réalisée par le propriétaire de l'application 2) Tout ce qui impliqué dans la gouvernance de la sécurité et des opérations sécuritaires d'une application, ainsi que des informations impliquées par l'utilisation de cette application, doit être vérifié pour s'assurer que tous les risques de sécurité, pouvant survenir dans ce secteur d'intervention, ont été ramenés à un niveau acceptable 3) Un cadre normatif doit être mis en place et approuvé afin d'améliorer la maturité de la SA dans l'organisation
• CSSLP – Réaliser des activités de sécurité tout au long du cycle de vie du logiciel afin de protéger les informations qui y sont manipulées ((ISC)², 2013c)	4) Principe de sécurité – Des contrôles de sécurité peuvent être mis en place tout au long du cycle de vie de l'application 5) Tout ce qui est impliqué dans la réalisation, le déploiement et la maintenance, la retraite ou la destruction d'une application sécuritaire, ainsi que l'application elle-même, doit être vérifié pour s'assurer que tous les risques de sécurité, pouvant survenir dans ce secteur d'intervention, ont été ramenés à un niveau acceptable
• Certified Information System Security Professional (CISSP) – Fournir l'assurance de la protection de l'information de l'organisation dans l'architecture par la conception, la gestion et la mise en place de contrôles qui assurent la sécurité de l'environnement des affaires. ((ISC)², 2013b)	6) Principe de sécurité – Des contrôles de sécurité peuvent être mis en place dans l'infrastructure TI, tout au long du cycle de vie de l'application 7) Tout ce qui est impliqué dans l'acquisition, le déploiement, la maintenance, la retraite ou la réutilisation de composants technologiques requis par l'utilisation de l'application, ainsi que les composants eux-mêmes, doit être vérifié pour s'assurer que tous les risques de sécurité, pouvant survenir dans ce secteur d'intervention, ont été ramenés à un niveau acceptable
• ITIL – Fournit un cadre de guide des meilleures pratiques pour la gestion des services TI (ITIMF, 2013)	8) La gestion des services TI est plus large que la gestion des TI, la gestion de la SA est plus large que l'application elle-même
• CISA – Programme de certification consacré exclusivement à l'audit, au contrôle et à la sécurité afin de veiller à ce que les technologies et systèmes de l'entreprise soient convenablement contrôlés, suivis et évalués. (ISACA®, 2013a) • Vérifier que les contrôles requis pour protéger les informations sensibles d'une organisation ont été mis en place et qu'ils fonctionnent comme prévu. Principe de vérification : les résultats produits par la vérification d'un processus doivent être répétables et indépendants de l'auditeur. (ITGI, 2007, p. 14)	9) Principe de sécurité – La SA doit être vérifiable 10) Tout ce qui est impliqué dans la vérification et les audits de la gouvernance, de la réalisation, de la gestion des infrastructures TI, ainsi que dans les processus de vérification et d'audit eux-mêmes, doit être vérifié pour confirmer que tous les risques de sécurité, pouvant survenir dans ces secteurs d'intervention, ont été ramenés à un niveau acceptable

3.6.4 Analyse rétroactive de la démarche et des résultats de l'audit de sécurité des applications dirigée par le chercheur

Notre fonction de conseiller en sécurité spécialisé dans la SA nous a permis d'accomplir plusieurs réalisations en industrie et dans des organisations. Les mandats touchaient principalement la conception, le développement, la vérification et l'audit de SA.

Un de ces mandats professionnels nous a permis de faire une avancée importante dans nos travaux de recherche. Il s'agit de notre nomination à la position d'auditeur principal lors de l'audit de sécurité des systèmes de votation électroniques (SVÉ) commandé par le Directeur général des élections du Québec, suite aux problèmes rencontrés avec l'utilisation des SVÉ durant des élections municipales de 2005. Avec ce mandat, nous avons pu établir une stratégie, identifier les éléments et définir une démarche d'audit visant à vérifier la SA logicielle s'exécutant sur un SVÉ en fonction d'une approche globale.

Un des défis posés par la portée de ce mandat consistait à réaliser un audit de sécurité de chacun des cinq SVÉ utilisés avec les mêmes critères de vérification. Pour être crédible, cet audit devait s'appuyer sur des méthodes et des normes reconnues, et devait couvrir tout le cycle de vie de l'application.

Le développement de la démarche se fit en se basant sur trois documents (Poulin, 2006c, p. 3), soit :

1) La méthode COBIT 4.0 qui propose des pratiques reconnues en audit des systèmes d'information;
2) La bibliothèque de l'infrastructure des technologies de l'information (ITIL) qui propose des pratiques reconnues de gestion des services TI;

3) Les pratiques organisationnelles de sécurité de l'information proposées par la norme ISO 17799 : 2005[11].

Dans ce cas de figure, la vérification d'un SVÉ ne devait pas se limiter qu'à la vérification du logiciel, mais devait aussi inclure la vérification des personnes (rôles, responsabilités et qualifications), des processus et des technologies impliqués dans le fonctionnement sécuritaire de ces applications tout au long de leur cycle de vie. De plus, afin de limiter la portée de l'audit, il fallait pouvoir identifier l'information à être protégée, ainsi que les acteurs (personnes ou éléments du système) pouvant avoir accès à cette information (P01, P02, P03, P06, P10, P11. P13, P15 et P16).

Pour ce faire, nous avons développé un modèle générique de SA sur lequel nous avons basé notre démarche d'audit. Le Tableau 3.5 présente quelques étapes de la démarche, des concepts et des éléments provenant de la méthode d'audit de sécurité des SVÉ qui ont été développés et intégrés au modèle SA par le chercheur.

C'est à la suite de ces travaux prédoctoraux que le modèle initial de la sécurité des applications fut élaboré. C'est ce modèle qui a servi de fondation à ce travail de recherche et qui fut présenté à une équipe de projet lors de notre première rencontre du SC27, démarrant ainsi la phase 2, soit celle de la conception du modèle SA.

[11] La norme ISO/IEC 17799 a maintenant été renommée ISO/IEC 27002 par l'organisation ISO.

Tableau 3.5 Concepts et éléments de la méthode de l'audit de sécurité intégrés au modèle SA

Concepts et éléments amenés par la création de la méthode de l'audit de sécurité	**Concepts et éléments intégrés au modèle**
• « L'identification de l'information sensible impliquée dans un système de votation électronique, ainsi que les caractéristiques de sécurité essentielles au bon fonctionnement d'un système de votation électronique; » (DGEQ, 2006, p. 174)	1) Les informations classifiées impliquées par l'utilisation de l'application 2) Exigences de sécurité désirées
• « Figure 1 – Schéma des principaux éléments vérifiés dans un système de votation électronique » (Poulin, 2006a, p. 8), (DGEQ, 2006, p. 177)	3) Identification de groupes d'informations liés à l'utilisation d'une application
• « L'identification des principaux intervenants, composantes et processus impliqués dans un système de votation électronique générique ; » (DGEQ, 2006, p. 174)	4) Contexte d'affaires
• « … la définition des rôles, des responsabilités et les qualifications des divers intervenants (équipe de projet, équipe technique et personnel électoral). » (DGEQ, 2006, p. 182) • « Validation des rôles, des responsabilités et des qualifications requises de tous les intervenants (incluant le fournisseur) devant interagir avec le système. » (Poulin, 2006c, p. 10)	5) Identification de rôles impliqués dans la SA lors de son utilisation
• Un modèle d'application de SVÉ générique (Poulin, 2006c, pp. 6-9), incluant notamment le choix des infrastructures technologiques, les appareils de votation, les logiciels, les codes source, les paramètres des systèmes et les bulletins de vote	6) Le contexte technologique d'une application, incluant notamment l'architecture technologique et l'aménagement des lieux
• Le regroupement des éléments à vérifier en cinq sections et la définition de la portée des audits (Poulin, 2006c, p. 113)	7) La bibliothèque de CSA : la liste des contrôles de sécurité des applications qui devrait exister et avoir été vérifiée
• « Démarche sommaire de la vérification » (Poulin, 2006a, p. 9)	8) Éléments du processus de l'audit de la sécurité d'une application

3.7 Termes et définitions retenus pour ce travail de recherche

La revue de littérature a permis d'identifier plusieurs des termes dont les définitions faisaient consensus. Cette section présente ceux qui seront utilisés dans cette thèse, ainsi que les références correspondantes.

application logicielle

Logiciel conçu pour aider les utilisateurs à exécuter des tâches particulières ou à gérer des types particuliers de problèmes, par opposition à un logiciel qui contrôle l'ordinateur lui-même (ISO/IEC, 2010g, p. 18).

cycle de vie

Évolution d'un système, produit, service, projet ou de toute autre entité fabriquée par une personne, de sa conception à sa retraite (ISO/IEC, 2008e, p. 4).

modèle de cycle de vie

Un cadre de processus et d'activités concernés par le cycle de vie qui peut être organisé en étapes, agissant comme une référence commune pour la communication et la compréhension (ISO/IEC, 2008e, p. 4).

projet d'application

Entreprise d'acquisition d'une application, en conformité avec les ressources et les exigences spécifiées, qui comprend des critères de démarrage et de fin de projet définis (ISO/IEC, 2008e, p. 5)[12].

[12] Spécialisation de la définition 4.29 de la norme ISO/IEC 12207:2007 pour champ d'application.

CHAPITRE 4

CONCEPTION DU MODÈLE DE LA SÉCURITÉ DES APPLICATIONS

La revue de littérature a permis de constater que, dans l'état actuel de la pratique, la sécurité des applications est généralement mise en place et évaluée de façon subjective (Walton, Longstaff et Linger, 2009), habituellement avec la participation de professionnels et d'experts en sécurité des TI. Cet exercice nous a également confirmé qu'une grande partie des articles scientifiques et des ouvrages sur les méthodes et processus d'évaluation de la SA, propose en fait des solutions approximatives ou basées sur des modèles et des portées qui ne garantissent pas forcément la fidélité des résultats (ISO/IEC, 2009c), (Walton, Longstaff et Linger, 2009), (Pavlidis et al., 2012) et (Dejun et al., 2014).

Pour atteindre les objectifs de recherche, il semble nécessaire de développer une nouvelle approche et un nouveau modèle SA permettant l'analyse, l'évaluation et la vérification des éléments et des attributs de sécurité, en fonction des besoins de sécurité d'une organisation.

Le modèle SA devra notamment permettre :

1) d'appliquer des principes et d'intégrer des contrôles de sécurité durant tout le cycle de vie d'une application;
2) de fournir à l'organisation les preuves que son application a atteint et maintient le niveau de confiance préalablement ciblé, en fonction de son contexte d'utilisation spécifique.

Ce chapitre présente les étapes et activités clés de conception et de développement du modèle SA qui ont été réalisées durant la deuxième phase de ce projet de recherche.

Les éléments de réponses aux 16 problématiques, les enjeux et les critères à rencontrer par le modèle SA résultant de la revue de littérature et des travaux d'analyse complémentaires ont

permis d'identifier les concepts et les composants qui serviront de fondation au modèle SA, dont, notamment :

1) La vision globale servant à relier les éléments du modèle SA en un ensemble structuré;
2) Le concept d'un cycle de vie de la sécurité d'une application, qui tient compte des activités des acteurs des quatre secteurs d'intervention en SA;
3) Le concept de cadre normatif, servant de source autoritaire pour identifier et distribuer les éléments de SA approuvés par l'organisation; ainsi que
4) Le concept de contrôle de sécurité d'une application (CSA) intégrant son propre processus de vérification.

La Figure 4.1 illustre les phases 2, 3 et 4 impliquées dans la conception, le développement, la validation et l'évolution des éléments du modèle SA. Elle met en évidence deux groupes d'activités de validation et de vérification distinctes, soit :

1) La validation périodique des experts délégués par les pays participants (phase 3), ainsi que la rétroaction générée par la réception de leurs commentaires qui sont réintroduits dans la phase 2 de conception et d'amélioration du modèle SA;
2) Le déploiement et la vérification empirique de certains éléments du modèle (phase 4), lors de la réalisation de projets de sécurité des applications en industrie. Cette dernière phase sert à déployer et à vérifier certains éléments du modèle en projets pilotes, afin de permettre d'identifier en situation réelle ceux qui pourraient être améliorés pour en faciliter l'adoption, l'implémentation ou l'utilisation par les gestionnaires, les ingénieurs, les techniciens ou les auditeurs impliqués dans ces projets.

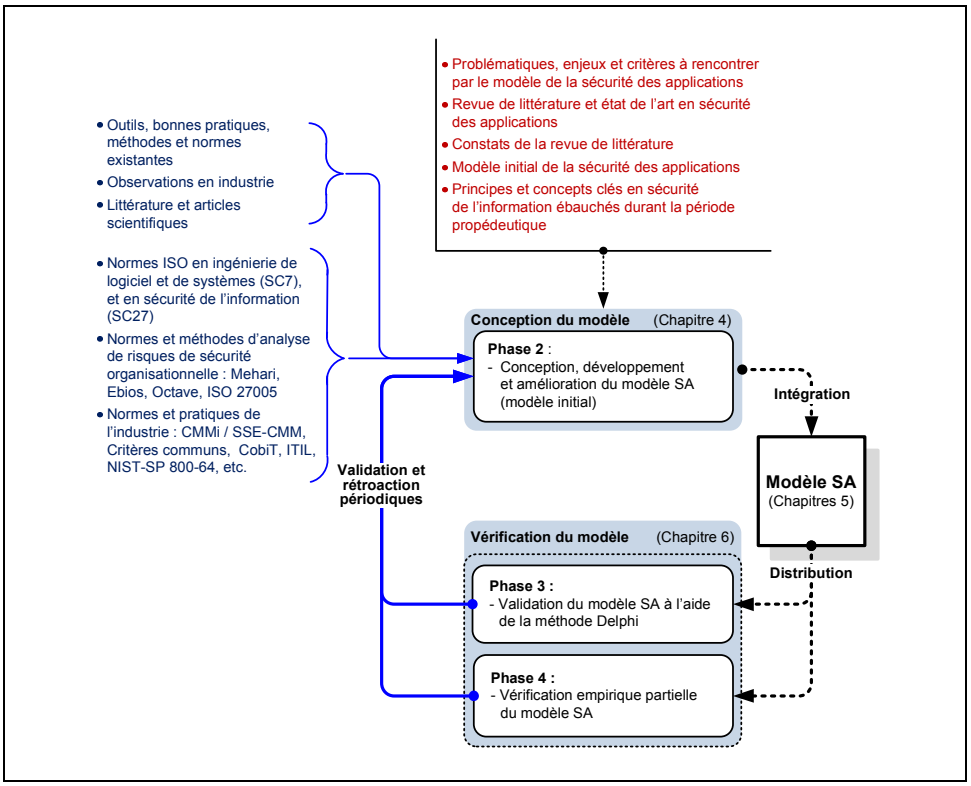


Figure 4.1 Processus de conception, de développement et de validation des éléments du modèle

Afin de pouvoir bénéficier simultanément de commentaires provenant des pays participants à ce projet de recherche, ainsi que des observations provenant d'organisations utilisant le modèle, les phases 3 et 4 de validation et de vérification des éléments du modèle étaient réalisées en parallèle, et leurs résultats ont été utilisés simultanément pour améliorer le modèle SA ou en corriger les lacunes.

Ces trois phases (Figure 4.1), incluent les activités suivantes :

- Le processus, qui englobe les phases 2 et 3, concerne la construction et la validation du modèle SA, à l'aide de la méthode Delphi adaptée à la méthodologie de réalisation de projet ISO. Ce premier processus a permis d'obtenir un consensus sur la portée, les principes et les éléments contenus dans le modèle SA ainsi que le support de la majorité des pays participants à sa diffusion à l'intérieur d'un projet ISO.

- Le processus regroupant les activités réalisées durant les phases 2 et 4, concerne la vérification empirique partielle des éléments du modèle SA par des organisations intéressées à connaître le modèle ou désirant utiliser les éléments qu'il propose pour sécuriser leurs applications.

4.1 Synthèse des travaux de recherche

Le modèle SA a pu évoluer vers sa version finale grâce à la progression des travaux de recherche du chercheur, aux 11 cycles Delphi du projet de recherche qu'il a supervisé, et aux actions qui ont été prises en fonction des commentaires consolidés reçus des experts, des chercheurs universitaires et des professionnels de l'industrie des pays où a été présenté le modèle.

Cette section présente une synthèse des actions clés qui ont permis de concrétiser l'évolution du modèle SA. Afin de faciliter la comparaison entre les éléments du modèle initial et ceux du modèle final, les tableaux suivants présentent ces actions par catégorie d'éléments.

4.1.1 Besoins de l'audience visée

Nous avons identifié et cerné des besoins de l'audience visée du modèle SA initial, que nous avons ensuite fait évoluer à la fin de chaque cycle Delphi.

Le Tableau 4.1 présente la progression de l'évolution des besoins de l'audience visée par le modèle SA, telle que réalisée par le chercheur durant ce travail de recherche.

Tableau 4.1 Évolution des besoins de l'audience visée par le modèle SA

Modèle initial Besoins de l'audience visée	**Évolution du modèle**	**Modèle final** Besoins de l'audience visée
1) Gestionnaire 2) Équipe TI - infrastructure TI - développement 3) Auditeur 4) Utilisateur	→ Amélioration de la description de l'audience visée → Ajout des rôles *acheteur* et *fournisseur*, parmi l'audience visée par le modèle à la demande du Japon	1) Gestionnaire 2) Équipe TI - infrastructure TI - réalisation 3) Vérificateur, auditeur 4) Acheteur 5) Fournisseur 6) Utilisateur

4.1.2 Évolution de la portée du modèle SA

Le chercheur a identifié et précisé la portée du modèle SA initial. Ces travaux ont fait l'objet de discussions entre les experts présents aux premières rencontres Delphi jusqu'à ce qu'un consensus soit établi, validant ainsi la portée du modèle SA présentée par le chercheur.

Le Tableau 4.2 présente l'évolution de la portée du modèle SA réalisée par le chercheur durant ce travail de recherche.

Tableau 4.2 Évolution de la portée du modèle SA

Éléments du modèle initial Portée	**Évolution du modèle**	**Modèle final** Portée
1) Intégration des contrôles de sécurité dans toutes les phases du cycle de vie d'une application 2) L'environnement de l'application 3) Les groupes d'informations impliqués par l'existence de l'application 4) S'applique autant à l'application elle-même qu'à ses facteurs environnants qui ont un impact sur sa sécurité, tel que l'information, les personnes, les processus et ses trois contextes	→ Aucun changement n'a affecté la portée du modèle	1) Le cycle de vie de la sécurité d'une application 2) L'environnement de l'application[13] 3) Les groupes d'informations impliqués par l'existence de l'application 4) La SA s'applique autant à l'application elle-même qu'à ses facteurs environnants qui ont un impact sur sa sécurité, tel que l'information, les personnes, les processus et ses trois contextes

4.1.3 Principes identifiés par le modèle SA

Nous avons identifié et précisé dans le modèle SA initial, les principes sur lesquels il s'appuie. Lors de l'analyse et de la disposition des commentaires reçus dans les questionnaires Delphi, certains des principes présentés ont été remis en question puis adaptés par le chercheur afin de les clarifier. Ces modifications ont par la suite été soumises au comité d'expert pour validation.

Le Tableau 4.3 présente l'évolution des principes identifiés par le modèle SA réalisée par le chercheur durant ce travail de recherche.

[13] L'environnement d'une application inclut son contexte d'affaires, son contexte technologique, son contexte juridique, ainsi que les fonctionnalités et les spécifications de l'application en vigueur durant tout son cycle de vie de sécurité.

Tableau 4.3 Évolution des principes soutenant le modèle SA

Éléments du modèle initial Principes	**Évolution du modèle**	**Modèle final** Principes
1) La confiance que l'on peut accorder à une application est liée au résultat de l'évaluation de sa sécurité 2) La SA dépend de son contexte d'utilisation	→ Fusion de ces deux principes	1) La sécurité est dépendante du contexte
	→ Ajout du principe - la sécurité est une exigence	2) La sécurité est une exigence
3) La SA doit pouvoir être démontrée 4) Investir le montant approprié pour la SA	→ Amélioration des énoncés et des descriptions des principes de la sécurité des applications	3) La SA doit pouvoir être démontrée 4) Investir le montant approprié pour la SA
5) La confidentialité d'une application 6) L'intégrité d'une application 7) La disponibilité d'une application 8) L'authentification à une application 9) La non-répudiation face à une application	→ Retrait des attributs de sécurité de l'information des principes de la sécurité des applications : confidentialité, intégrité, disponibilité, authentification et non-répudiation	

4.1.4 Termes définis dans le modèle SA

Le chercheur à identifié et défini les termes intégrés au modèle SA initial, qu'il a ensuite fait évolué en tenant compte des commentaires et contributions reçus des experts à la fin de chaque cycle Delphi.

Le Tableau 4.4 présente l'évolution des termes définis dans le modèle SA réalisée par le chercheur durant ce travail de recherche.

Tableau 4.4 Évolution du vocabulaire du modèle SA

Éléments du modèle initial Termes	**Évolution du modèle**	**Modèle final** Termes
1) Application 2) Application sécuritaire 3) Niveau de confiance - cible et mesuré 4) Mesure de sécurité 5) Cadre normatif de l'organisation 6) Cadre normatif de l'application	→ Évolution de la définition du terme : application. → L'expression « mesure de sécurité des applications », a été changée pour « contrôle de sécurité des applications »	1) Application 2) Application sécuritaire 3) Niveau de confiance - cible (ciblé) et actuel (mesuré) 4) Contrôle de sécurité des applications (CSA) 5) Cadre normatif de l'organisation 6) Cadre normatif de l'application

4.1.5 Concepts intégrés au modèle SA

C'est principalement pour répondre aux problématiques P01 et P02 que nous avons identifié et précisé les concepts sur lesquels le modèle SA initial devait s'appuyer (*Voir* 5.8).

Le Tableau 4.5 présente l'évolution des concepts intégrés au modèle SA qui a été réalisée par le chercheur durant ce travail de recherche.

Tableau 4.5 Évolution des concepts du modèle SA

Éléments du modèle initial Concepts	**Évolution du modèle**	**Modèle final** Concepts
1) Vision globale et les quatre domaines d'interventions liés à la sécurité de l'application - gouvernance - infrastructure TI - réalisation de l'application - vérification et contrôle	→ Aucun changement n'a été apporté aux concepts amenés par le modèle	1) Quatre domaines d'intervention liés à la sécurité de l'application - gouvernance - infrastructure TI - réalisation de l'application - vérification et contrôle
2) La prise en compte simultanée des quatre domaines d'interventions pour protéger l'information liée à l'utilisation d'une application		2) La prise en compte simultanée des quatre domaines d'interventions pour protéger l'information liée à l'utilisation d'une application

Tableau 4.5 Évolution des concepts amenés par le modèle SA (suite)

Éléments du modèle initial Concepts	**Évolution du modèle**	**Modèle final** Concepts
3) Les contextes d'utilisation d'une application incluent : - le contexte d'affaires, - le contexte juridique, - le contexte technologique, - les spécifications de l'application, en vigueur durant tout le cycle de vie.	→ Changements de nom de certains composants	3) L'environnement de l'application inclut : - le contexte d'affaires,[14] - le contexte juridique, - le contexte technologique, - les fonctionnalités et les spécifications de l'application, en vigueur durant tout le cycle de vie.
4) La source d'un risque de sécurité peut être une personne, un processus ou une technologie		4) La source d'un risque de sécurité peut être une personne, un processus ou une technologie appartenant à l'un des trois contextes de l'application
5) Pouvoir intégrer des contrôles de sécurité dans toutes les phases du cycle de vie de la sécurité d'une application		5) Pouvoir intégrer des contrôles de sécurité dans toutes les activités présentes dans les phases du cycle de vie de la sécurité d'une application
6) Niveau de confiance de l'application - niveau de confiance cible - niveau de confiance mesuré		6) Niveau de confiance de l'application - niveau de confiance cible (ciblé) - niveau de confiance actuel (mesuré)
7) L'exigence de preuves démontrant l'atteinte du niveau de confiance ciblé		7) L'exigence de preuves démontrant l'atteinte du niveau de confiance ciblé
8) Application sécuritaire		8) Application sécuritaire
9) Cadre normatif de l'organisation		9) Cadre normatif de l'organisation
10) Cadre normatif de l'application		10) Cadre normatif de l'application
11) Pour tous les acteurs ayant accès aux informations sensibles, la nécessité d'identifier les qualifications requises pour pouvoir assumer les responsabilités associées à leur rôle respectif		11) Pour tous les acteurs ayant accès aux informations sensibles, la nécessité d'identifier les qualifications requises pour pouvoir assumer les responsabilités associées à leur rôle respectif
12) Pouvoir démontrer qu'une application a atteint et maintient le niveau de confiance ciblé		12) Pouvoir démontrer qu'une application a atteint et maintient le niveau de confiance ciblé

[14] Qui inclut les personnes, les processus et l'information.

4.1.6 Composants du modèle SA

Afin de garantir une vision globale complète du modèle SA, nous avons défini et conçu le composant « modèle de référence du cycle de vie de la sécurité des applications » qui comprend les phases de réalisation et d'opération de l'application (*Voir* 5.9.12). De nombreux ouvrages et articles proposent des démarches pour intégrer les activités de sécurité dans les processus de développement pour sécuriser une application. L'idée semble simple, mais nous savons déjà que la SA doit couvrir, non seulement les processus de développement d'une application, mais un champ bien plus vaste.

Le Tableau 4.6 présente l'évolution des composants du modèle SA réalisée par le chercheur durant ce travail de recherche.

Tableau 4.6 Évolution des composants du modèle SA

Éléments du modèle initial Composants	**Évolution du modèle**	**Modèle final** Composants
1) Le cadre normatif de l'organisation (CNO) 2) Le CNA 3) Le cycle de vie générique de la sécurité d'une application	→ Alignement du cycle de vie de la sécurité d'une application aux quatre domaines de connaissances	1) Le CNO 2) Le CNA 3) Le modèle de référence du cycle de vie de la sécurité d'une application, incluant la liste des activités et des rôles impliqués 4) Le répertoire des rôles, responsabilités et qualifications
4) Les exigences de sécurité 5) L'information classifiée liée à l'utilisation de l'application 6) La liste des CSA	→ Changements de nom de certains composants	5) Les exigences de sécurité 6) L'information classifiée liée à l'utilisation de l'application 7) La bibliothèque de CSA
	→ Ajout de la matrice de traçabilité à la suite d'une rencontre de projet (*Voir* 6.2.4, ÉC, juin 2010).	8) La matrice de traçabilité

Tableau 4.6 Évolution des composants du modèle SA (suite)

Éléments du modèle initial Composants	**Évolution du modèle**	**Modèle final** Composants
7) Le CSA - niveau de confiance - exigence de sécurité - activité de sécurité : qui, quand, quoi et combien - activité de vérification : qui, quand, quoi et combien	→ Précision amenée dans la description des activités contenues dans un CSA - ajout du « où » et du « comment »	9) Le CSA - niveau de confiance - exigence de sécurité - activité de sécurité : qui, quoi, où, quand, comment et combien - activité de vérification **:** qui, quoi, où, quand, comment et combien
8) Vision globale des éléments clés du modèle SA 9) Schémas XML décrivant - le CSA - le cycle de vie générique de la sécurité d'une application, incluant les stages, les activités et les rôles	→ Développement de la structure du modèle et des divers schémas XML[15]	10) Vision globale des éléments clés du modèle SA 11) Schémas XML décrivant - le CSA - le cycle de vie générique de la sécurité d'une application, incluant les stages, les activités et les rôles

4.1.7 Groupes et rôles d'acteurs identifiés dans le modèle SA

Dans le modèle SA initial, nous avons identifié et précisé les groupes et les rôles d'acteurs qui y évoluent. Lors de l'analyse et de la disposition des commentaires reçus dans les questionnaires Delphi, certains des rôles présentés ont été retirés ou intégrés dans un rôle existant afin de simplifier les deux listes.

Le Tableau 4.7 présente l'évolution des groupes et des rôles d'acteurs identifiés dans le modèle SA réalisée par le chercheur durant ce travail de recherche.

[15] Bien que faisant partie des résultats des travaux de cette recherche, les schémas XML n'ont été présentés aux experts vérificateurs des pays participants que lors de l'édition de la cinquième partie de la norme. Le diagramme conceptuel du modèle est un document de travail intermédiaire qui n'a pas été présenté aux experts vérificateurs, mais qui a servi à vérifier la cohérence du modèle produit par ce travail de recherche.

Tableau 4.7 Évolution des groupes et rôles du modèle SA

Éléments du modèle initial Groupes et rôles	**Évolution du modèle**	**Modèle final** Groupes et rôles
Groupes 1) Comité du CNO 2) Équipe d'architecture 3) Équipe d'exécution 4) Équipe de compilation et d'intégration 5) Équipe de développement 6) Équipe de sécurité 7) Équipe de tests 8) Équipe de vérification 9) Équipe technologique	→ Simplification de la liste des rôles impliqués dans la SA lors de sa réalisation[16]	Groupes 1) Comité du CNO 2) Direction de l'organisation 3) Équipe de projet 4) Équipe de vérification 5) Équipe des opérations
Rôles 1) Auditeur 2) Détenteur, propriétaire de l'application 3) Expert d'un domaine 4) Gestionnaire 5) Gestionnaire de projet 6) Le représentant des utilisateurs 7) Officier de sécurité 8) Opérateur 9) Technicien 10) Utilisateur final	→ Ajustement de la dénomination de certains rôles[17]	Rôles 1) Acheteur 2) Architecte d'application 3) Architecte de sécurité 4) Architecte technologique 5) Vérificateur / Auditeur 6) Chef de la sécurité 7) Chef de projet 8) Détenteur / Propriétaire de l'application 9) Développeur 10) Équipe de l'infrastructure TI 11) Expert des lois et règlements 12) Expert du domaine 13) Formateur 14) Fournisseur 15) Gestionnaire 16) Opérateur d'application 17) Testeur 18) Utilisateur

[16] Bien que faisant partie des résultats des travaux de cette recherche, la liste des rôles n'a été présentée aux experts vérificateurs des pays participants que lors de l'édition de la deuxième partie de la norme.

[17] Idem.

4.1.8 Processus identifiés par le modèle SA

Nous avons identifié et précisé, dans le modèle SA initial, les processus qui devaient y être intégrés afin de permettre la conception, la maintenance et l'intégration d'éléments de sécurité à l'intérieur des processus impliqués par une application. Plusieurs discussions ont été tenues lors des rencontres Delphi. Elles ont permis aux experts de débattre et de proposer des améliorations des différents processus du modèle SA, qui ont par la suite été intégrées par le chercheur.

Le Tableau 4.8 présente l'évolution des processus du modèle SA réalisée par le chercheur durant ce travail de recherche.

Tableau 4.8 Évolution des processus du modèle SA

Éléments du modèle initial Processus	**Évolution du modèle**	**Modèle final** Processus
1) Gestion du CNO 2) Gestion de la sécurité d'une application 3) Identification et classification des groupes d'informations liés à l'utilisation d'une application 4) Gestion des risques de sécurité d'une application 5) Vérification de la sécurité d'une application	→ Bonification régulière de la description des processus	1) Gestion du CNO a) gérer le comité du CNO b) élaborer la sécurité des applications dans le CNO c) implémenter la sécurité des applications dans le CNO d) surveiller et réviser la sécurité des applications dans l'organisation e) améliorer de façon continue la SA dans l'organisation f) auditer la sécurité des applications dans le CNO 2) Gestion des risques de la SA 3) Gestion de la SA a) identifier les besoins et l'environnement de l'application b) évaluer les risques de sécurité amenés par l'application c) créer et maintenir le CNA d) réaliser et opérer l'application e) vérifier la sécurité de l'application 4) Identification et classification des groupes d'informations liés à l'utilisation d'une application 5) Audit et certification de la mise en œuvre du modèle SA a) auditer et certifier la SA dans le CNO b) auditer et certifier une application c) auditer et certifier un expert en sécurité des applications

Le chapitre suivant présente les résultats de nos travaux de recherche, soit le modèle SA. Dans un premier temps, il présente ce qu'implique la SA, puis il présente les éléments du modèle, les enjeux de sa mise en place, ses caractéristiques, les besoins de son audience, sa portée, les principes clés qu'il soutient, ainsi que les termes et définitions. Ce chapitre présente finalement les divers composants et processus contenus dans le modèle SA.

CHAPITRE 5

LE MODÈLE DE LA SÉCURITÉ DES APPLICATIONS

Ce chapitre présente sommairement les divers éléments du modèle SA que nous avons conçus afin de proposer une vision plus globale et inclusive de la SA, et ce, de manière à mieux répondre aux 16 problématiques identifiées au début de ce projet de recherche. Ainsi, dans chacune des sections suivantes, nous verrons sur quelles assises se basent les éléments qui ont été développés et systématiquement validés :

1) Ce qu'implique la SA (5.1);
2) Éléments du modèle SA (5.2);
3) Enjeux de la mise en place du modèle SA (5.3);
4) Caractéristiques du modèle SA et réponses aux problématiques identifiées (5.4);
5) Besoins de l'audience ciblée par le modèle SA (5.5);
6) Portée du modèle SA (5.6);
7) Principes clés de la SA (5.7);
8) Concepts, termes et définitions introduits par le modèle SA (5.8);
9) Composants du modèle SA (5.9); et
10) Processus du modèle SA (5.10).

5.1 Ce qu'implique la SA

La SA concerne la protection des groupes d'informations sensibles impliqués par sa réalisation ou son opération (*Voir* l'appendice A – ANNEXE XII.2.7). Cette protection est assurée par la réalisation d'un ensemble de processus permettant à une organisation :

1) D'identifier et de catégoriser les informations impliquées par l'utilisation de l'application ou provenant de ses environnements de réalisation et d'opération;
2) D'évaluer des risques de sécurité amenés par la réalisation et l'opération d'une application;
3) De définir ses exigences de sécurité pour diminuer à un niveau acceptable les risques de sécurité; et

4) De mettre en place des CSA afin de présenter des preuves vérifiables de l'atteinte et du maintien d'un niveau de confiance ciblé, et ce, à n'importe quel moment du cycle de vie de l'application concernée.

5.2 Éléments du modèle SA

Dans un souci de synthèse, les sections 5.3 à 5.10 de ce chapitre présentent sommairement les éléments du modèle SA qui ont été conçus par le chercheur durant ce projet de recherche. Une description plus détaillée des éléments introduits se trouve aux annexes de l'appendice I suivantes :

- ANNEXE XI : Le modèle SA : Enjeux, besoins, portée et principes supportés
- ANNEXE XII : Le modèle SA : Concepts, termes et définitions
- ANNEXE XIII : Le modèle SA : Composants
- ANNEXE XIV : Le modèle SA : Processus

La Figure 5.1 présente un schéma global des éléments contenus dans le modèle SA.

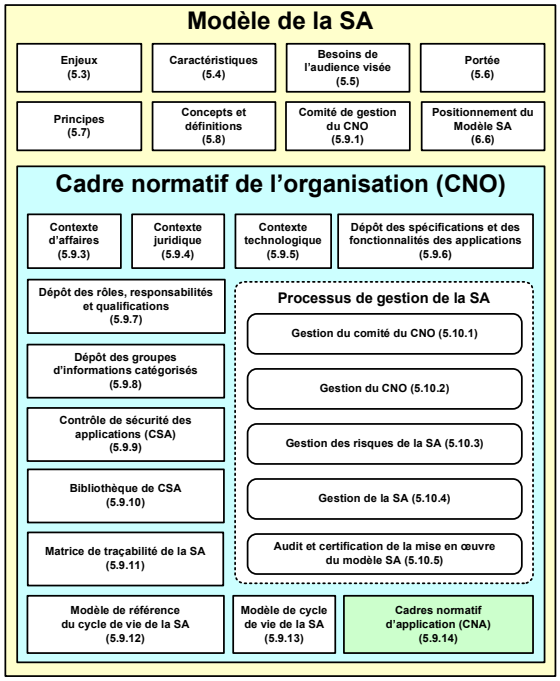


Figure 5.1 Les éléments du modèle de la SA

5.3 Enjeux de la mise en place du modèle SA

Afin de pouvoir être en mesure de fournir toutes les preuves requises, permettant à une organisation d'affirmer et de démontrer qu'une application est sécuritaire, il est important de bien comprendre les enjeux associés à la mise en place du modèle SA dans une organisation.

Quatre enjeux sont à prendre en compte lors de la mise en place du modèle SA dans une organisation :

1) Priorisation des éléments du modèle à mettre en place (5.3.1);
2) Formalisation du CNO (5.3.2);
3) Engagement d'investissement des ressources appropriées (5.3.3); et
4) Participation des intervenants liés aux quatre domaines d'intervention couverts par le modèle SA (5.3.4).

5.3.1 Priorisation des éléments du modèle à mettre en place

Dans un souci de flexibilité et d'adaptabilité aux besoins, priorités et ressources limitées des organisations, le modèle SA n'impose pas de préséance dans la mise en place des divers éléments du modèle. Il exige de l'organisation une compréhension des conséquences de ses choix, en fonction du contexte d'affaires, du contexte juridique et du contexte technologique dans lesquels ce modèle sera mis en place. (*Voir* l'appendice A – ANNEXE XI.1.1 pour plus de détails.)

Contribution originale : nous avons conçu le modèle SA de manière à ce que son implémentation demeure valide, efficiente et vérifiable, quels que soient les éléments que l'organisation aura décidé de mettre en place, et ce, sans qu'aucune démarche de mise en œuvre ne soit imposée.

5.3.2 Formalisation du CNO

Le modèle exige de l'organisation la conservation des éléments du modèle à l'intérieur d'un CNO qui sera utilisé comme source autoritaire, ceci afin d'assurer la gestion et la communication des éléments du modèle à l'échelle de l'organisation. Tout élément défini dans le CNO doit avoir été approuvé par l'organisation et le CNO doit être vérifiable. (*Voir* l'appendice A – ANNEXE XI.1.2 pour plus de détails.)

Contribution originale : nous avons conçu le modèle SA de manière à ce qu'il favorise la création d'un dépôt central géré, soit le CNO, où seront conservés les dernières versions approuvées de tous les processus et informations concernant les divers éléments de SA que l'organisation aura décidé de mettre en place (*Voir* l'appendice A – ANNEXE XIII.2).

5.3.3 Engagement d'investissement des ressources appropriées

Le modèle SA permet de prendre en compte et de respecter les ressources et priorités d'une organisation, dans le choix de la mise en place des éléments que celle-ci décidera de mettre en place pour atteindre ses objectifs de sécurité. Cet enjeu est critique, car quel que soit l'élément du modèle que l'organisation aura décidé de mettre en place, il viendra un temps où celui-ci ne répondra plus à ses besoins de sécurité et où il devra être éliminé, remplacé ou mis à jour. (*Voir* l'appendice A – ANNEXE XI.1.3 pour plus de détails.)

5.3.4 Participation des intervenants liés aux quatre domaines d'intervention couverts par le modèle SA

Les personnes qui interviennent dans les différents secteurs des quatre domaines d'intervention en sécurité de l'information (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-1), interviennent aussi en SA. Seule la portée de leurs interventions diffère, car elle ne consiste plus à assurer la protection de l'ensemble des ressources informationnelles de l'organisation, mais bien à assurer la protection des applications sensibles de l'organisation,

soit des applications qui impliquent de l'information qui doit être protégée. (*Voir* l'appendice A – ANNEXE XI.1.4 pour plus de détails.)

Contribution originale : nous avons conçu le modèle SA de manière à ce qu'il tienne compte simultanément des personnes, des processus et des technologies provenant des quatre domaines d'intervention liés à la SA. Ceci afin de donner à l'organisation, qui l'utilisera, une vision globale des sources de risques de SA liées à une application ainsi qu'à ses contextes de réalisation et d'opération. Cela lui permettra aussi d'identifier les moments et les endroits où il est le plus efficace et efficient d'intégrer les contrôles de SA qu'elle aura conçus pour gérer les risques de sécurité (*Voir* l'appendice A – ANNEXE XII.2.2 et le Tableau-A XII-1).

5.4 Caractéristiques du modèle SA et réponses aux problématiques identifiées

Le Tableau 5.1 présente les caractéristiques du modèle SA et démontre clairement qu'elles résolvent adéquatement les problématiques identifiées aux sections 3.5.2 et 3.4.

Tableau 5.1 Synthèse des caractéristiques du modèle et des problématiques résolues par chacune d'elles

Caractéristique	Problématiques résolues
1) Regroupe, en une vision globale, les principaux éléments à considérer pour la sécurité des applications	P01 : Absence d'une vision globale de la sécurité des applications
2) Peut être adapté aux réalités de l'organisation soit, notamment, à sa taille, son contexte d'affaires, ses contraintes et ses ressources disponibles	P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques

Tableau 5.1 Synthèse des caractéristiques du modèle et des problématiques résolues par chacune d'elles (suite)

Caractéristique	Problématiques résolues
3) Identifie les principes clés, termes et concepts associés à la sécurité d'une application, tels que : a) la définition d'une application; b) la portée de la sécurité d'une application; c) la définition d'une application sécuritaire; d) le modèle de référence du cycle de vie de la sécurité d'une application	P05 : Absence d'un vocabulaire et de références communes en sécurité des applications P06 : Absence d'une définition de la portée de la sécurité d'une application P07 : Absence d'une définition claire de ce qu'est une application sécuritaire P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application
4) Identifie les principaux groupes d'acteurs (rôles) qui peuvent être impliqués dans le processus de sécurisation d'une application, afin : a) d'identifier et de répondre à leurs besoins; b) d'être accepté et appliqué par ses principaux acteurs	P13 : Absence de mécanismes permettant d'assigner aux principaux rôles, pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune des responsabilités qui leur sont assignées
5) Permets la création, la gestion et la réutilisation de contrôles de sécurité vérifiables, devant être intégrés dans le cycle de vie d'une application, en fonction des risques de sécurité amenés par son utilisation	P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation P16 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur de l'application
6) Facilite l'arrimage entre les éléments du modèle et les approches, normes, méthodes, processus et outils existants pour mettre en place la sécurité des applications	P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications
7) Aide l'organisation qui l'utilise à identifier et à évaluer les risques de sécurité liés à l'utilisation d'une application, et à tenir compte des contextes pouvant avoir des conséquences sur les besoins de sécurité de son application	P09 : Absence de sources claires des exigences de sécurité d'une application P10 : Absence d'une méthode d'évaluation de la sécurité d'une application
8) Permets de fournir des mécanismes axés sur le processus pour établir des exigences de sécurité à partir des risques de sécurité, assignant un niveau de confiance ciblé, et de sélectionner des contrôles de sécurité et les mesures de vérification correspondantes	P09 : Absence de sources claires des exigences de sécurité d'une application P10 : Absence d'une méthode d'évaluation de la sécurité d'une application P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation
9) Aide l'organisation qui l'utilise à évaluer et à gérer les coûts de la sécurité d'une application	P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques

Tableau 5.1 Synthèse des caractéristiques du modèle et des problématiques résolues par chacune d'elles (suite)

Caractéristique	Problématiques résolues
10) Fournis des mécanismes axés sur les processus permettant la détermination, la production et la collecte des preuves nécessaires pour démontrer qu'une application peut être utilisée en toute sécurité dans un environnement défini	P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation
11) Permets d'identifier et de démontrer l'atteinte d'un niveau de confiance pour une application, en fonction de son contexte d'utilisation spécifique	P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques P09 : Absence de sources claires des exigences de sécurité d'une application P10 : Absence d'une méthode d'évaluation de la sécurité d'une application P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation
12) Permets de fournir des directives pour l'établissement de critères d'acceptation aux organisations qui confient en sous-traitance le développement ou l'exploitation des applications, et pour les organisations qui acquièrent des applications tierces de fournisseurs	P07 : Absence d'une définition claire de ce qu'est une application sécuritaire P09 : Absence de sources claires des exigences de sécurité d'une application P14 : Les méthodes et outils existants de génie logiciel ne tiennent pas toujours compte de la sécurité de l'information TI
13) Associe certains éléments du modèle à un cadre normatif de sécurité des applications pouvant s'adapter aux besoins de sécurité de l'organisation qui l'utilisera. Ces éléments sont : a) un processus de gestion du cadre normatif de la sécurité des applications de l'organisation; b) un modèle de référence de sécurité du cycle de vie des applications, servant de contenant pour les composants et les processus de sécurité d'une application; c) un processus de gestion de la sécurité d'une application; d) les sources et une démarche d'identification des exigences de sécurité d'une application; e) un processus d'évaluation et de vérification de la SA en fonction des besoins de sécurité de	P01 : Absence d'une vision globale de la sécurité des applications P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application P09 : Absence de sources claires des exigences de sécurité d'une application P10 : Absence d'une méthode d'évaluation de la sécurité d'une application

Tableau 5.1 Synthèse des caractéristiques du modèle et des problématiques résolues par chacune d'elles (suite)

Caractéristique	Problématiques résolues
l'organisation; f) une structure normalisée des contrôles de sécurité d'une application; g) un processus de gestion (conception, développement, validation, maturation, communication et réutilisation) des contrôles de sécurité d'une application	P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications P15 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur des processus impliqués dans la réalisation et l'opération de l'application P16 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur de l'application
14) Soutenir les concepts généraux spécifiés dans la norme ISO 27001 et aider à la mise en œuvre satisfaisante de la sécurité de l'information basée sur une approche de gestion des risques	P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications
15) Fournir un cadre qui aide à mettre en œuvre les contrôles de sécurité spécifiés dans la norme ISO 27002 et autres normes	P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications

Contribution originale : tout au long de la conception et de la validation du modèle SA, nous nous sommes assurés que le modèle SA permette de répondre simultanément aux 16 problématiques identifiées par cette recherche (*Voir* 6.5).

5.5 Besoins de l'audience ciblée par le modèle SA

Les audiences suivantes sont ciblées par ce modèle SA dans l'exercice de leurs fonctions :

1) Les gestionnaires (5.5.1);
2) Les équipes d'approvisionnement et d'opération (5.5.2);
3) Les vérificateurs et les auditeurs (5.5.3);
4) Les acheteurs (5.5.4);

5) Les fournisseurs (5.5.5); et
6) Les utilisateurs (5.5.6).

Contribution originale : dès le début de ce projet de recherche, nous avons identifié les besoins de l'audience cible et nous nous sommes assurés que le modèle SA sera en mesure de fournir les éléments permettant d'y répondre (*Voir* 7.2.1).

5.5.1 Besoins des gestionnaires

Les gestionnaires sont les personnes impliquées dans la gestion d'activités de développement, d'acquisition, d'utilisation, de la maintenance, ou de toute autre activité pouvant survenir au cours du cycle de vie d'une application (*Voir* l'appendice A – ANNEXE XIII, Figure-A XIII-6, couche : gestion de l'application). (*Voir* l'appendice A – ANNEXE XI.2.1 pour plus de détails.)

Les besoins de ces personnes sont notamment :

1) De gérer les coûts d'implémentation et de maintenance de la SA en fonction des risques et de la valeur qu'elle représente pour l'organisation;
2) D'assurer la conformité avec les normes, les lois et les règlements en fonction du contexte juridique d'une application *(Voir* l'appendice A – ANNEXE XII, Figure-A XII-3);
3) D'autoriser le niveau de confiance ciblé en fonction des contextes spécifiques de l'organisation;
4) De déterminer quelles activités de sécurité et de vérification correspondantes doivent être mises en œuvre et testées.

5.5.2 Besoins des équipes d'approvisionnement et d'opération

Les membres des équipes de projet d'approvisionnement et d'opération sont responsables de l'approvisionnement et de l'exploitation qui sont, notamment, impliqués dans des activités de

conception, de développement, d'acquisition, de maintenance ou de mise à la retraite pouvant survenir durant le cycle de vie d'une application (*Voir* l'appendice A – ANNEXE XIII, Figure-A XIII-6, couches : fournir une application et gestion de l'infrastructure). (*Voir* l'appendice A – ANNEXE XI.2.3 pour plus de détails.)

Les besoins de ces personnes sont, notamment :

1) De comprendre quels contrôles doivent être appliqués à chaque étape du cycle de vie d'une application, et pourquoi;
2) De veiller à ce que les contrôles introduits répondent aux exigences de sécurité qui leur sont associées.

5.5.3 Besoins des vérificateurs et des auditeurs

Les vérificateurs et les auditeurs sont responsables de la vérification et des audits de sécurité des activités et composants reliés à l'application durant son cycle de vie (*Voir* l'appendice A – ANNEXE XIII, Figure-A XIII-6, couche : audit de l'application). (*Voir* l'appendice A – ANNEXE XI.2.4 pour plus de détails.)

Les besoins de ces personnes sont notamment :

1) De comprendre la portée et les activités de mesure impliquées dans les processus de vérification des contrôles correspondants;
2) D'établir une liste d'activités de vérification de mesures qui généreront les preuves requises pour démontrer que le niveau de confiance ciblé par le propriétaire de l'application a été atteint.

5.5.4 Besoins des acheteurs

Les acheteurs sont les personnes impliquées dans l'acquisition d'un produit ou service.

Les besoins de ces personnes sont notamment de s'assurer de sélectionner des fournisseurs et des applications en fonction des exigences de sécurité de l'organisation. (*Voir* l'appendice A – ANNEXE XI.2.4 pour plus de détails.)

5.5.5 Besoins des fournisseurs

Les fournisseurs sont les personnes impliquées dans la livraison d'un produit ou d'un service.

Les besoins de ces personnes sont notamment de répondre aux exigences de sécurité qui sont incluses dans les demandes de propositions de services ou de biens. (*Voir* l'appendice A – ANNEXE XI.2.5 pour plus de détails.)

5.5.6 Besoins des utilisateurs

Les utilisateurs sont les personnes qui interagiront directement avec au moins une interface de l'application, lorsque cette dernière sera en phase de test ou en opération (*Voir* l'appendice A – ANNEXE XIII, Figure-A XIII-6, couche : fournir une application, groupe d'activités : utilisation).

Les besoins de ces personnes sont, notamment, d'être confiants que l'application est sécuritaire et qu'elle produit des résultats fiables, de manière cohérente et en temps opportun. (*Voir* l'appendice A – ANNEXE XI.2.6 pour plus de détails.)

5.6 Portée du modèle SA

Le modèle SA vise à s'appliquer à tous les types d'applications, autant à leurs composants logiciels qu'à leurs éléments TI, et ce, quels que soient la taille et le type d'organisation qui le développe ou l'utilise. Ce modèle SA ne fournit aucun contrôle ou activité de sécurité, ni spécification de programmation sécuritaire. (*Voir* l'appendice A – ANNEXE XI.3 pour plus de détails.)

5.7 Principes clés de la SA

Afin de délimiter l'objet du présent travail, il est important ici de présenter les principaux principes de sécurité de l'information, adaptés à la SA, et sur lesquels ce travail s'appuie. La section 5.7 présente les 5 principes clés du modèle SA, soit :

1) La SA doit être gérée (5.7.1);
2) La SA est une exigence (5.7.2);
3) La SA est dépendante de l'environnement de l'application (5.7.3);
4) La SA nécessite les ressources appropriées (5.7.4);
5) La SA doit pouvoir être démontrée (5.7.5).

Contribution originale : dès le début de ce projet de recherche, nous avons identifié les principes clés que le modèle SA devrait soutenir pour permettre aux organisations de sécuriser leurs applications. Tous les éléments du modèle SA ont été conçus afin d'aider une organisation à respecter ces principes, lors de leur mise en place.

5.7.1 La SA doit être gérée

Selon l'OCDE « La gestion de la sécurité doit être fondée sur l'évaluation des risques et être dynamique et globale afin de couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations. » (OCDE, 2002, p. 22). De la même façon, la SA est liée à la gestion des différents risques de sécurité amenés par l'utilisation d'une application dans un environnement spécifique. (*Voir* l'appendice A – ANNEXE XI.4.1 pour plus de détails.)

5.7.2 La SA est une exigence

L'utilité de l'exigence de sécurité est de spécifier un besoin de sécurité afin de diminuer un ou plusieurs risques spécifiques à un niveau acceptable. Des exigences[18] de sécurité devraient donc être énoncées, analysées et fixées pour tous les risques de sécurité existants à chaque étape du cycle de vie de la sécurité d'une application. (*Voir* l'appendice A – ANNEXE XI.4.2 pour plus de détails.)

5.7.3 La SA est dépendante de l'environnement de l'application

La SA doit être évaluée en fonction de l'évolution de son environnement qui est, notamment, défini par trois contextes, soit : le contexte d'affaires, (*Voir* l'appendice A – ANNEXE XII.2.3), le contexte juridique (*Voir* l'appendice A – ANNEXE XII.2.4) et le contexte technologique (*Voir* l'appendice A – ANNEXE XII.2.5). Cette évaluation doit aussi prendre en compte les spécifications et les fonctionnalités de l'application (*Voir* l'appendice A – ANNEXE XII.2.6). Pour minimiser ces risques, des exigences de sécurité devront être fixées par l'organisation.

L'identification de l'environnement d'une application servira à reconnaître les événements qui peuvent être à l'origine des risques de sécurité d'une application. Ces événements pourraient provenir autant de l'extérieur que de l'intérieur de l'organisation.

Une organisation peut affirmer qu'une application est sécuritaire lorsque la vérification des contrôles de sécurité des applications mis en place répond adéquatement aux exigences de sécurité requises par cette organisation. Mais, cette affirmation n'est valide que pour l'environnement spécifique dans lequel les risques et les exigences de sécurité ont été évalués et satisfaits. (*Voir* l'appendice A – ANNEXE XI.4.3 pour plus de détails.)

---

[18] Selon ISO/IEC 26702:2006, une exigence est un énoncé qui cerne une caractéristique ou une contrainte d'un produit ou d'un processus qui est non ambiguë, testable ou mesurable, et nécessaire pour l'acceptation du produit ou du processus. *(Traduction libre)*

5.7.4 La SA nécessite les ressources appropriées

Afin d'assurer la SA, il est nécessaire d'investir et de justifier l'affectation des ressources appropriées permettant la mise en place de contrôles de sécurité adéquats, fiables et vérifiables. Ce principe est dérivé du processus de sélection des traitements d'un risque présenté par la norme ISO 31000 : *Risk management – Principles and guidelines* (ISO/IEC, 2009f, p. 19). Dans le contexte de la SA, les coûts et les ressources requises pour appliquer et vérifier un contrôle de sécurité, afin de diminuer le risque ciblé à un niveau acceptable, doivent être proportionnels à l'évaluation de ce risque (menace, impact, probabilité) et au niveau de confiance requis par le propriétaire de l'application ou par la direction de l'organisation. (*Voir* l'appendice A – ANNEXE XI.4.4 pour plus de détails.)

5.7.5 La SA doit pouvoir être démontrée

Une application ne peut être déclarée sécuritaire pour un contexte spécifique, à un moment précis, que si le propriétaire de l'application accepte que les preuves générées par les activités de vérification des contrôles de sécurité, telles qu'identifiées par le niveau de confiance ciblé, démontrent que ce niveau a bien été atteint. Pour ce faire, ce niveau doit être mesurable (Abran, 2010, pp. 69-97). Ce principe est une spécialisation du concept d'assurance (ISO/IEC, 2005b). (*Voir* l'appendice A – ANNEXE XI.4.5 pour plus de détails.)

Contribution originale : tout au long de ce projet de recherche, nous nous sommes assuré d'intégrer au modèle SA les concepts, attributs et autres éléments de métrologie de manière à permettre à une organisation de définir et d'accumuler des résultats attendus vérifiables afin de rendre la SA mesurable (Abran, 2010, pp. 69-95).

5.8 Concepts et définitions introduits par le modèle SA

La section 5.8 présente les principaux concepts utilisés dans cette thèse ainsi que les définitions des expressions clés qui y figurent.

5.8.1 Application

Une application est un système TI qui a été construit pour soutenir un ou plusieurs processus ou exigences d'affaires. (*Voir* l'appendice A – ANNEXE XII.2.1 pour plus de détails.)

5.8.2 Environnement d'une application

L'environnement d'une application, qu'il s'agisse de l'environnement actuel ou de l'environnement cible, décrit et spécifie les caractéristiques des contextes dans lesquels l'application se réalise ou s'utilise, incluant ses spécifications ainsi que l'ensemble des acteurs et des informations impliqués dans sa réalisation et son opération. (*Voir* l'appendice A – ANNEXE XII.2.2 pour plus de détails.)

Contribution originale : même si l'IEEE définit l'environnement d'une application comme étant « tout ce qui affecte un système ou est affecté par un système lors des interactions avec lui, ou n'importe quoi qui partage une interprétation d'interactions avec le système concerné » (ISO/IEC/IEEE, 2010, pp. 127, 3.1018.1), cette expression est généralement interprétée dans le monde des TI et du génie logiciel comme étant « la configuration du matériel et du logiciel dans lequel un logiciel opère » (ISO/IEC/IEEE, 2010, pp. 127, 3.1018.2), (Goldberg et al., 1996), (Kacsuk et al., 2004), (MacIntyre et al., 2011). Afin de faciliter l'identification de l'ensemble des risques de SA, nous avons précisé la première définition de l'environnement d'une application au-delà de son contexte technologique afin d'y inclure le contexte d'affaires et le contexte juridique, et de pouvoir faciliter l'identification des sources de risques SA qui pourraient se situer à l'extérieur de la portée initiale de la définition de cette expression (*Voir* l'appendice A – ANNEXE XII.2.2 pour plus de détails.)

5.8.3 Contexte d'affaires de l'application

Il s'agit des normes, pratiques, vocabulaire, directives, politiques, règlements, contraintes et façons de faire provenant de la ligne d'affaires de l'organisation s'appliquant à l'utilisation

d'une application (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-3). Ce contexte comprend aussi les descriptions et l'inventaire catégorisés des rôles et des informations impliquées par l'opération et l'utilisation de cette application. (*Voir* l'appendice A – ANNEXE XII.2.3 pour plus de détails.)

5.8.4 Contexte juridique de l'application

Il s'agit de l'inventaire des différents règlements, directives, règles et lois nationaux inhérents à la juridiction, et au territoire où sera utilisée l'application, et qui s'appliquent à l'organisation (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-3) pour l'utilisation d'une de ses fonctionnalités ou de ses données. *(Voir* l'appendice A – ANNEXE XII.2.4 pour plus de détails.)

5.8.5 Contexte technologique de l'application

Il s'agit de l'inventaire des divers éléments TI utilisés ou nécessaires au fonctionnement de l'application (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-3) ainsi que les paramètres et processus qui leur sont associés. (*Voir* l'appendice A – ANNEXE XII.2.5 pour plus de détails.)

5.8.6 Spécifications et fonctionnalités de l'application

Il s'agit de l'inventaire et des descriptions des diverses spécifications fonctionnelles et non fonctionnelles de l'application (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-3). *(Voir* l'appendice A – ANNEXE XII.2.6 pour plus de détails.)

5.8.7 Groupes d'informations liées à la SA

Il s'agit de la liste et de la description des groupes d'informations liées à une application qui peuvent devoir être protégées. *(Voir* l'appendice A – ANNEXE XII.2.7 pour plus de détails.)

Contribution originale : il n'est pas évident d'identifier l'ensemble des informations sensibles liées à une application qui devraient être protégées. Afin de faciliter cette démarche, nous avons précisé les 9 types de groupes d'informations qui étaient inclus dans la portée de la SA (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-4).

5.8.8 Risques de la SA

Le risque de la SA se définit par la probabilité qu'un événement, qui menace une information sensible de l'application, survienne et génère un impact non désiré. La gestion des risques de sécurité d'une application nécessite l'identification et l'analyse préalable des risques de sécurité menant à la rédaction des exigences de sécurité de l'organisation pour cette application. (*Voir* l'appendice A – ANNEXE XII.2.8 pour plus de détails.)

5.8.9 Exigences de la SA

Description de ce qui est demandé pour diminuer un ou plusieurs risques de SA et les ramener à un niveau acceptable. Le but de l'exigence de sécurité est de définir clairement ce que l'on attend du contrôle qui devra être mis en place pour atténuer un risque. Une exigence de sécurité devrait minimalement contenir les cinq éléments suivants, soit : le rôle de l'acteur qui désire cette exigence (qui?), l'action désirée pour diminuer le risque (comment?), le moment où cette action doit se produire (quand?), l'endroit où cette action sera réalisée (où?) et l'information concernée par cette exigence (quoi?) et, si besoin est, le risque ou la source du risque concerné (pourquoi?). L'atteinte d'une exigence de sécurité doit être vérifiable. (*Voir* l'appendice A – ANNEXE XII.2.9 pour plus de détails.)

Contribution originale : nous avons déterminé que l'exigence de sécurité n'est pas un type d'exigence spécifique, comme l'est une exigence d'affaires ou une exigence fonctionnelle. La différence entre une exigence de sécurité et les autres exigences liées à une application réside dans le fait que cette dernière a été rédigée pour préciser un besoin à combler, tandis que l'exigence de sécurité a été rédigée pour préciser un risque de sécurité à atténuer. Afin de

faciliter cette étape, nous avons précisé une démarche permettant de définir les 12 types d'exigences de SA qui sont inclus dans la portée de la SA.

5.8.10 Contrôles de SA

Description normalisée d'un ensemble d'éléments, dont des opérations vérifiables, humaines ou automatiques destinées à ramener, à un niveau acceptable, un ou plusieurs risques de sécurité liés à la réalisation ou à l'opération d'une application. (*Voir* l'appendice A – ANNEXE XII.2.10 pour plus de détails.)

5.8.11 Vulnérabilités d'une application

Les vulnérabilités de l'application se définissent par l'ensemble des risques de sécurité inacceptables qui sont toujours présents dans l'environnement de l'application. (*Voir* l'appendice A – ANNEXE XII.2.11 pour plus de détails.)

5.8.12 Niveau de confiance d'une application

Nom de l'étiquette associée à un ensemble de CSA spécifiques, approuvés par l'organisation, permettant de rencontrer, ou même, de dépasser les exigences de sécurité identifiées.

Le niveau de confiance d'une application se décline de deux façons :

1) **Le niveau de confiance ciblé,** qui permet d'identifier et de communiquer l'ensemble des CSA qui doivent être mis en place et être vérifiés à différents moments du cycle de vie de la sécurité de l'application;

2) **Le niveau de confiance actuel,** qui est la conclusion du processus permettant de déterminer que tous les CSA d'une application ont été correctement implémentés et qu'ils ont tous produit les résultats attendus. Ce niveau de confiance permet de démontrer la conformité d'une application aux exigences de sécurité requises.

Un des objectifs visés par une organisation qui utilise le modèle SA est d'assurer, lorsque deux applications de sensibilités semblables sont évaluées, de l'atteinte du même niveau de confiance par la mise en place des mêmes CSA. (*Voir* l'appendice A – ANNEXE XII.2.12 pour plus de détails.)

5.8.13 Application sécuritaire

Application pour laquelle le niveau de confiance actuel est égal ou supérieur au niveau de confiance ciblé. (*Voir* l'appendice A – ANNEXE XII.2.13 pour plus de détails.)

5.9 Composants du modèle SA

Le modèle SA propose l'ajout de plusieurs composants, non seulement pour assurer la sécurité d'une application, mais aussi pour s'assurer que les éléments de sécurité en vigueur dans l'organisation auront été mis en place et vérifiés de manière uniforme pour toutes les applications sensibles de l'organisation. La section 5.9 présente les 14 composants clés du modèle SA.

5.9.1 Comité de gestion du CNO

Le comité de gestion du CNO est un rôle organisationnel chargé d'identifier les objectifs de sécurité et la stratégie de réalisation de la SA dans l'organisation. Ce groupe est responsable de la définition et de la mise en œuvre du plan d'action de la SA de l'organisation ainsi que de la gestion, de la maintenance et de l'approbation des divers éléments de la SA qui seront intégrés au CNO. (*Voir* l'appendice A – ANNEXE XIII.1 pour plus de détails.)

5.9.2 Cadre normatif de l'organisation (CNO)

Le CNO est le dépôt de données officiel de l'organisation; il contient l'ensemble des éléments normatifs requis à la mise en place de la SA de l'organisation (*Voir* Figure 5.1). On y trouve, notamment, les meilleures pratiques reconnues par l'organisation, les politiques de

l'organisation, ses règlements, ses pratiques, les rôles et responsabilités des postes clés, ainsi que ses processus et façons de faire. Le CNO est la source autoritaire des éléments qui normalisera le cadre des actions et des décisions prises par l'organisation. (*Voir* l'appendice A – ANNEXE XIII.2 pour plus de détails.)

5.9.3 Contexte d'affaires

Le contexte d'affaires du CNO est un dépôt qui contient la documentation décrivant tous les processus d'affaires, les normes et les meilleures pratiques adoptés par l'organisation, pouvant générer des risques de sécurité lors de la réalisation de projets portant, notamment, sur le développement, l'utilisation ou la maintenance des applications de l'organisation (*Voir* l'appendice A – ANNEXES XII.2.3 et XIII.3 pour plus de détails.)

5.9.4 Contexte juridique

Le contexte juridique du CNO est un dépôt qui contient la documentation décrivant toutes les lois et réglementations qui peuvent générer des risques de sécurité concernant les projets portant, notamment, sur le développement, l'utilisation ou la maintenance des applications de l'organisation en fonction des lieux où cette application sera utilisée (*Voir* l'appendice A – ANNEXES XII.2.4 et XIII.4 pour plus de détails.)

5.9.5 Contexte technologique

Le contexte technologique du CNO est un dépôt qui contient la documentation décrivant tous les composants TI, tels que : les composants physiques, les serveurs, les câbles, les routeurs, les services, les infrastructures réseau ou infonuagiques, etc., incluant les paramètres, les règles et les pratiques recommandés pour leur mise en place dans l'organisation (*Voir* l'appendice A – ANNEXES XII.2.5 et XIII.5 pour plus de détails.)

5.9.6 Dépôt des spécifications et des fonctionnalités des applications

Le dépôt des spécifications des applications du CNO constitue un ensemble de documents et de renseignements décrivant les éléments et les processus associés aux diverses spécifications fonctionnelles et non fonctionnelles, telles que les fonctionnalités et services TI préapprouvés, intégrés ou offerts par les applications de l'organisation, incluant la description de leurs spécifications (*Voir* l'appendice A – ANNEXES XII.2.6 et XIII.6 pour plus de détails.)

5.9.7 Dépôt des rôles, responsabilités et qualifications

Le dépôt des rôles, responsabilités et qualifications du CNO est un inventaire catégorisé des rôles des acteurs impliqués dans au moins une des activités amenées par les applications de l'organisation. (*Voir* l'appendice A – ANNEXE XIII.7 pour plus de détails.)

Contribution originale : ce projet de recherche nous a amené à constater que lors de l'assignation d'une responsabilité à un rôle, les qualifications requises par ce dernier pour exécuter adéquatement une fonction spécifique n'étaient que très rarement formellement spécifiées. Nous avons donc conçu le modèle SA de manière à ce que le critère de la qualification requise d'un rôle pour pouvoir recevoir une responsabilité précise ne soit, non seulement inclus dans le processus de définition d'une activité de sécurité (*Voir* l'appendice A – ANNEXE XIII, Figure-A XIII-2, élément d'information « Qui »), mais aussi que cette définition soit formalisée dans le dépôt contenu dans le CNO (*Voir* l'appendice A – ANNEXE XIII.7) et que la rédaction d'un type d'exigence spécifique puisse être effectuée (*Voir* l'appendice A – ANNEXE XII, Figure-A XII-6, type d'exigence #5).

5.9.8 Dépôt des groupes d'informations catégorisés

Le dépôt des groupes d'informations catégorisés du CNO contient la liste et la description des groupes d'informations catégorisés, liées aux applications de l'organisation qui peuvent devoir être protégées. (*Voir* l'appendice A – ANNEXE XIII.8 pour plus de détails.)

5.9.9 Contrôle de sécurité des applications (CSA)

Le CSA est un composant normalisé et vérifiable qui permet notamment de décrire des activités de sécurité et de vérification ainsi que de préciser les résultats attendus par leur réalisation. Une fois approuvé par le comité du CNO, il est utilisé pour répondre de manière homogène à des exigences de sécurité visant la diminution, à des niveaux acceptables, des risques de sécurité pouvant menacer l'information impliquée liée à la réalisation ou à l'opération d'une l'application. (*Voir* l'appendice A – ANNEXES XII.2.10 et XIII.9 pour plus de détails.)

Contribution originale : dans notre préoccupation de faciliter la gestion des risques de SA et de rendre la SA mesurable, nous avons formellement défini le composant CSA qui doit obligatoirement inclure deux types d'activités. La première est une activité de sécurité conçue pour répondre à une exigence de SA spécifique, tandis que la deuxième est une activité de vérification de la mesure conçue pour vérifier que l'activité de sécurité a bien été implémentée, qu'elle fonctionne correctement et qu'elle produit les résultats vérifiables attendus. De fait, chacune de ces deux activités du CSA doit préciser les « qui, quoi, où, quand, comment et combien » intégrant ainsi un état mesurable « réussi » ou « échec » à chacun d'eux. Le modèle SA recommande aussi que l'attribut « combien » soit évalué de façon monétaire, afin d'en faciliter la comparaison avec le coût monétaire de l'impact d'un risque de SA, facilitant ainsi la gestion de ce risque par le détenteur de l'application et par l'organisation. Finalement, afin d'en faciliter l'adoption et l'implémentation, nous avons conçu et fait valider, lors de nos cycles Delphi, une version préliminaire du schéma XML permettant de définir formellement le CSA.

5.9.10 Bibliothèque de CSA

La bibliothèque de CSA est un dépôt qui est utilisé pour répertorier, documenter, regrouper et classer tous les CSA approuvés par l'organisation. (*Voir* l'appendice A – ANNEXE XIII.10 pour plus de détails.)

Contribution originale : même s'ils sont tirés de normes ou de pratiques recommandées, telles que de COBIT (ISACA, 2012), d'ISO 27002 (ISO/IEC, 2013b), du « Top 10 d'OWASP » (OWASP, 2013) ou de Microsoft SDL (Microsoft, 2010), la sélection, la conception et la mise en place des contrôles de sécurité pour démontrer qu'une application se conforme à une loi ou à une directive n'est pas toujours aisée (Huang, Zavarsky et Ruhl, 2009). Un des objectifs de cette recherche étant de rendre la SA mesurable, et son implémentation répétable, nous avons conçu et intégré au modèle SA une bibliothèque de CSA qui identifie des listes spécifiques de CSA approuvés, chacune d'elles identifiées à l'aide d'un niveau de confiance. La bibliothèque de CSA permet donc de s'assurer qu'une exigence de SA, liée à un niveau de confiance, sera toujours répondue à l'aide du même CSA, que ce CSA diminuera adéquatement les risques de SA pour lesquels il a été conçu, car il devra avoir été préalablement validé, vérifié et approuvé par l'organisation avant d'être intégré à la bibliothèque. Finalement, il devient possible de mesurer la sécurité d'une application en vérifiant simplement que tous les CSA identifiés par un niveau de confiance affichent un état « réussi ». Si une exigence de conformité est associée à un niveau de confiance, il devient alors facile de démontrer qu'une application la respecte.

5.9.11 Matrice de traçabilité de la SA

La matrice de traçabilité de la sécurité des applications de l'organisation est un composant du CNO qui contient l'information nécessaire permettant d'assurer la traçabilité du changement d'un risque de sécurité jusqu'à la réimplémentation d'une nouvelle version d'un CSA dans une application de l'organisation. (*Voir* l'appendice A – ANNEXE XIII.11 pour plus de détails.)

Contribution originale : une matrice de traçabilité n'est pas un nouveau concept. En 1990, l'IEEE a défini cette expression, comme étant l'enregistrement de relations, entre deux ou plusieurs produits, d'un processus de développement. Un exemple serait une matrice qui conserve la relation entre une exigence fonctionnelle et le design d'un composant logiciel

(IEEE, 1990). Une fois mis en place, il devient facile pour l'organisation de démontrer que son logiciel répond à toutes les exigences qu'on lui a indiquées.

Nous avons repris et adapté ce concept au domaine de la sécurité des applications afin que le modèle SA puisse proposer un composant permettant de conserver les relations allant de la source d'un risque de SA : (1) au risque de SA qui a été évalué, (2) à l'exigence de SA qui a été définie pour atténuer ce risque, (3) au CSA qui répond à cette exigence, (4) au niveau de confiance qui contient ce CSA, et ce, jusqu'aux applications assignées à ce niveau de confiance où ce CSA a été implémenté.

Une fois la matrice de traçabilité de la SA mise en place, non seulement il devient facile pour une organisation de démontrer que les risques de SA liés à l'opération d'une application ont tous été ramenés à un niveau acceptable. Mais, cette matrice soutient aussi l'organisation dans la gestion de la sécurité de ses applications en lui permettant, à la suite de la détection d'un changement dans la source d'un risque de SA, d'identifier rapidement les risques concernés par ce changement, d'en réévaluer les impacts et de suivre les relations stockées dans la matrice afin d'identifier les applications qui seront touchées par ces changements.

Connaissant les coûts d'implémentation et de vérification du nouveau CSA développé, le nombre d'applications dont le niveau de confiance contient ce CSA, ainsi que le niveau de sensibilité des applications concernées, il devient facile pour l'organisation d'estimer les coûts et de définir une stratégie de mise à jour de ce CSA, dans le respect de ses priorités et de la disponibilité de ses ressources.

5.9.12 Modèle de référence du cycle de vie de la SA (MRCVSA)

Le modèle de référence du cycle de vie de la SA (MRCVSA), est un composant décrivant les quatre couches (une couche par domaine d'intervention), les phases (réalisation et opérations) et des groupes d'activités. Tel que présenté à l'appendice A – ANNEXE XIII.9.2, le MRCVSA permet de normaliser l'identification des attributs « qui » et « quand » qui

indiquent les acteurs et les moments ou devraient être réalisées les activités de sécurité et de vérification des CSA. Le MRCVSA contient, notamment, les noms des activités et des rôles des acteurs impliqués dans le développement, l'opération, la maintenance et le retrait d'une application afin d'assurer la sécurité des informations sensibles qu'elle contient pendant toute sa durée de vie, de la définition de ses exigences à la fin de son utilisation, sa désinstallation ainsi que la destruction de ses données. (*Voir* l'appendice A – ANNEXE XIII.12 pour plus de détails.)

Contribution originale : sachant qu'un des objectifs de cette recherche est de communiquer et d'intégrer des activités de sécurité aux processus existants dans les organisations, il devient très difficile, voire impossible, de définir un CSA qui pointerait sans ambigüité sur une activité (quand), dans un modèle de cycle de vie particulier, et d'espérer qu'il sera assigné aux bonnes activités des autres modèles de cycle de vie. Ne voulant pas imposer ni recommander des changements dans les modèles de cycle de vie des applications actuellement en place dans les organisations, nous avons défini un modèle de MRCVSA qui permettra aux organisations de valider les activités et les rôles absents de leurs façons de faire et, autant aux organisations qui développeront des CSA qu'à celles qui en feront l'acquisition, d'en faciliter la communication et l'implémentation à l'intérieur des processus présents dans les modèles du cycle de vie de la sécurité des projets d'applications. Finalement, afin d'en faciliter l'adoption, nous avons conçu et fait valider lors de nos cycles Delphi, une version préliminaire du schéma XML permettant de définir formellement le MRCVSA.

5.9.13 Modèle du cycle de vie de la sécurité d'une application

Différents modèles de cycle de vie sont parfois utilisés par différentes équipes de développement, dans différents projets ou dans différentes parties d'une même organisation. Le modèle du cycle de vie de la sécurité d'une application permet aux organisations qui le désirent d'aligner et d'arrimer les méthodes qu'elles utilisent au MRCVSA, afin de les aider à compléter les modèles en place, de faciliter la communication des CSA aux équipes de

projets d'applications et de faciliter l'intégration de CSA aux activités existantes dans les processus des modèles utilisés par les équipes de projets d'applications. (*Voir* l'appendice A – ANNEXE XIII.13 pour plus de détails.)

5.9.14 Cadre normatif de l'application (CNA)

Le CNA est la source autoritaire des éléments et informations concernant la sécurité d'une application spécifique. Ses composants représentent un sous-ensemble du CNO qui ne contient que des composants, des processus et des informations concernant spécifiquement cette application. Il permet ainsi d'éviter les imbroglios, les recherches inutiles et les improvisations dans les prises de décision, la réalisation d'activités ou dans la mise en place de CSA requis pour assurer l'atteinte du niveau de confiance ciblé. (*Voir* l'appendice A – ANNEXE XIII.14 pour plus de détails.)

5.10 Processus du modèle SA

Le modèle SA place quatre processus dans le CNO pour aider les organisations à :

1) Acquérir, déployer, utiliser et vérifier des applications dans lesquelles elles peuvent avoir confiance;
2) Définir, déployer, utiliser et vérifier un CNO qui soit en mesure de soutenir les objectifs de SA contenant l'information appartenant à l'organisation; et
3) Encadrer les travaux de vérification, d'audit et de certification de SA des personnes, des applications et des CNO.

La section 5.10.1 introduit le processus Gérer le comité du CNO permettant de mettre en place le comité responsable de la SA au sein de l'organisation, puis présente les quatre processus clés du modèle SA dont il a la charge. (*Voir* l'appendice A – ANNEXE XIV pour plus de détails.)

Contribution originale : nous avons intégré au modèle SA des processus permettant de répondre aux besoins de SA des intervenants oeuvrant au niveau organisationnel, et d'autres processus pour répondre aux besoins de SA des intervenants oeuvrant au niveau opérationnel, soit ceux qui participent aux projets d'applications. Ces processus intègrent aussi des mécanismes de communication visant à faciliter la gestion et l'arrimage des activités et des décisions de SA prises à chacun de ces niveaux. Non seulement le modèle SA permet d'encadrer la gestion des éléments du CNO que l'organisation aura décidé de mettre en place, soit l'identification des priorités et des stratégies en SA ainsi que la spécification, la validation, la conception, la mise en place, la maintenance et la vérification harmonisée, mais il encadre aussi leurs transferts et leurs réutilisations dans les CNA des divers projets d'applications où celui-ci aura requis l'atteinte d'un niveau de confiance cible. Finalement, le modèle SA propose un processus d'audit et de vérification de la mise en œuvre de la SA, permettant à une autorité de vérifier si une organisation, un intervenant ou une application a atteint la cible de vérification qui lui a été assignée (*Voir* l'appendice A – ANNEXE XIV, Figure-A XIV-1 pour plus de détails).

Ensemble, ces quatre processus permettent d'arrimer l'intégration et la vérification des activités de SA à n'importe quelle personne, composant TI ou processus du cycle de vie de la sécurité d'une application présents dans l'organisation, tant au niveau organisationnel qu'au niveau opérationnel, selon une démarche basée sur la gestion de risques.

5.10.1 Gérer le comité du CNO

La mise en place du comité de gestion du CNO par l'organisation vise à assurer une gestion homogène de la SA dans toute l'organisation, en respect avec les priorités et les capacités de cette dernière. (*Voir* l'appendice A – ANNEXE XIV.1.2 pour plus de détails.)

Contribution originale : le modèle SA nécessite la mise en place d'un comité permanent responsable de la SA regroupant, autour d'une même table, des représentants de la direction de l'organisation avec des responsables des quatre secteurs d'interventions en SA, tous

pouvant provenir des trois contextes dans lesquels opère l'organisation. Le rôle principal de ce comité est d'agir en tant qu'autorité de la SA pour l'ensemble de l'organisation. Sa responsabilité principale est d'identifier les cibles de SA à atteindre dans le respect des priorités, de la maturité et des capacités de l'organisation, et de s'assurer de la gestion et de la vérification de l'atteinte de ses objectifs.

5.10.2 Gestion du CNO

Le comité de gestion du CNO applique le processus de gestion du CNO pour mettre en place les éléments et les processus du modèle SA, afin qu'il puisse développer et gérer son CNO en fonction de ses besoins, de ses priorités et de ses ressources. (*Voir* l'appendice A – ANNEXE XIV.1 pour plus de détails.)

Ce processus contient les six sous-processus suivants :

1) Création et gestion du comité du CNO;
2) Élaboration de la SA dans le CNO;
3) Implémentation de la SA dans le CNO;
4) Surveillance et révision de la SA dans l'organisation;
5) Amélioration continue de la sécurité des applications dans l'organisation; et
6) Audit de la SA dans le CNO.

Contribution originale : ce processus propose une approche selon la roue de Deming (Deming, 2000), soit du modèle « Prévoir, Faire, Vérifier, Réagir »[19] qui permet de s'assurer de la sélection, du maintien et de l'approbation de tous les éléments du modèle SA dont l'implémentation aura été décidée par le comité du CNO.

[19] Plan, Do, Check, Act.

5.10.3 Gestion des risques de la SA

Mise en place et approuvée par le comité de gestion du CNO, elle est utilisée par les équipes de projets d'application afin de les guider dans la gestion des risques de sécurité amenés à l'organisation par l'approvisionnement et l'utilisation d'une application. (*Voir* l'appendice A – ANNEXE XIV.2 pour plus de détails.)

Contribution originale : durant la réalisation de ce projet de recherche, nous n'avons trouvé aucune méthode d'analyse de risques de sécurité qui a spécifiquement été conçue pour identifier, évaluer et gérer les risques de SA provenant autant des personnes, des processus et des technologies impliqués dans la réalisation et l'opération d'une application en tenant compte de son environnement. Plus encore, aucune des normes et méthodes existantes liées à la gestion de la sécurité de l'information, qui ont été identifiées durant cette recherche, n'offre une démarche ni un niveau de granularité qui permettraient d'identifier, d'évaluer ou de gérer des risques de sécurité provenant de l'intérieur même d'une application, soit de l'implémentation de ses spécifications fonctionnelles et non fonctionnelles. Sans ces informations, l'implémentation et la vérification des contrôles de sécurité directement à l'intérieur de cette dernière deviennent difficiles à justifier. Sachant que la gestion des risques de la sécurité d'une application ne pouvait être implémentée sans cet élément, nous avons conçu, validé et développé une première version de la méthode d'analyse de risques de la sécurité d'une application : *Application Security Issues Analysis* (ASIA) (*Voir* l'appendice A – ANNEXE XIV.2.3).

5.10.4 Gestion de la SA

La gestion de la SA est utilisée par l'équipe de projet d'une application, pour les guider dans l'intégration des éléments de la SA dans leurs projets. (*Voir* l'appendice A – ANNEXE XIV.3 pour plus de détails.)

Ce processus contient les six sous-processus suivants :

1) Processus de gestion de la sécurité d'une application;

2) Identification des besoins et de l'environnement de l'application;
3) Évaluation des risques de sécurité amenés par l'application;
4) Création et maintien du CNA;
5) Réalisation et opération de l'application; et
6) Vérification de la sécurité de l'application.

5.10.5 Audit et certification de la mise en œuvre du modèle SA

Cette démarche est utilisée par les équipes de vérification internes et externes à l'organisation, pour encadrer leurs travaux de vérifications, d'audits et de certifications de personnes, d'applications et des CNO. (*Voir* l'appendice A – ANNEXE XIV.4 pour plus de détails.)

Ce processus contient les trois sous-processus suivants :
1) Audit et certification de la SA dans le CNO;
2) Audit et certification d'une application; et
3) Audit et certification d'un expert en SA.

Contribution originale : pouvoir rendre la sécurité des applications mesurable et s'assurer que les résultats produits par un processus de mesure soient répétables et vérifiables sont l'un des défis que nous avions relevés au début de nos travaux de recherche. Cet objectif nous a amenés à intégrer au modèle SA un ensemble d'éléments et de caractéristiques visant spécifiquement ce but. Le processus d'audit et de certification de la mise en œuvre du modèle SA est l'élément final qui permet l'atteinte de ces deux objectifs.

CHAPITRE 6

VALIDATION DU MODÈLE SA

Ce chapitre présente une vue d'ensemble des événements clés qui se sont produits lors des cycles de validation Delphi et des cycles de vérification empirique partielle en entreprise du modèle SA. Ces événements ont été initiés par le traitement de commentaires reçus qui ont eu un impact, soit sur l'orientation du modèle SA, soit sur un des éléments (*Voir* Figure 2.1 et Figure 4.1).

6.1 Validation du modèle SA à l'aide de la méthode Delphi

La méthodologie suivie, pour concevoir et développer le présent projet, a été présentée à la section 2.6. Nos activités de recherche, en tant que concepteur des éléments intégrés au modèle SA, sont présentées au CHAPITRE 4.

La conception, le développement, la validation et la vérification des concepts, des principes, du vocabulaire et des autres éléments de cette recherche reposent principalement sur les cycles de validation Delphi, qui ont été effectués lors de la réalisation du projet de norme ISO 27034.

Bien que nos travaux aient été communiqués aux membres du SG17 de l'*International Telecommunication Union – Telecommunication Standardization Sector* (ITU-T) ainsi qu'aux membres des sous-comités 7, 22 et 27 d'ISO, nous avons principalement reçu des commentaires des chercheurs et experts des sous-comités 7 et 27 d'ISO.

Il est à noter que les efforts fournis par les experts participant à l'analyse et à la validation du modèle SA représentent une moyenne de cinq jours par cycle, et ce, durant les 11 cycles Delphi qu'a duré ce projet de norme ISO. Les phases de conception, de développement et de

validation du modèle SA résultant de ce projet de recherche ont donc été réalisées sur une période de 5 ½ ans.

Le Tableau-A I-1 présente une synthèse du nombre des commentaires reçus par cycle Delphi, de la façon dont ces commentaires ont été traités, du nombre de pays inscrits au SC27 à la fin de chaque cycle, ainsi que du résultat de leur vote approuvant ou non la progression du document. (*Voir* l'appendice A – ANNEXE X et ANNEXE XIX pour plus de détails.)

6.2 Vérification empirique partielle du modèle SA

Cette section présente la phase de vérification empirique des éléments du modèle à l'aide d'études de cas en projets réels, par leur présentation, leur déploiement et leur utilisation en milieu universitaire et en industrie (*Voir* Figure 2.1 et Figure 4.1). Cette vérification empirique vise à mesurer le niveau d'intérêt et de satisfaction de gestionnaires, d'architectes et d'équipes TI désirant vérifier l'acceptabilité et l'utilisabilité des éléments du modèle SA employés par leurs organisations ou dans leurs projets.

6.2.1 Processus de vérification empirique partielle de l'applicabilité et de l'acceptabilité des éléments du modèle SA par les organisations

Cette section présente les cinq étapes du processus de vérification empirique partielle des éléments du modèle SA qui ont été réalisées durant ce projet de recherche (Runeson et Höst, 2009, p. 137), soit :

1) Conception de l'étude de cas;
2) Préparation de la collecte des données;
3) Collecte des données;
4) Analyse des données; et
5) Rapport.

6.2.2 Conception de l'étude de cas

L'objectif de cette vérification empirique, même si elle n'est que partielle, est de déterminer si le modèle SA semble un moyen acceptable et utilisable par les professionnels oeuvrant au sein des organisations qui désirent intégrer la sécurité dans leurs applications et, si oui, de vérifier s'ils considèrent que les éléments du modèle qui ont été utilisés s'appliquaient à la réalité de leurs projets.

Ces activités de vérification empirique du modèle SA, réalisées concurremment aux cycles de validation Delphi, suivent la méthode de collecte de donnée appelée : l'observation participante. Cette méthode fait référence à une recherche qui implique l'interaction sociale entre le chercheur et les informateurs dans le milieu de celui-ci, au cours de laquelle les données sont systématiquement et discrètement collectées (Seaman, 1999). Une vérification empirique partielle des éléments du modèle SA, en utilisant l'observation participante à l'intérieur d'études de cas, a donc été privilégiée, car cette approche permet d'intégrer les activités de vérification aux activités d'un projet d'application, de s'ajuster au contexte d'un projet réel et de déterminer si les résultats attendus s'appliquent toujours dans les circonstances spécifiques du projet (Kitchenham, 1996, p. 13).

6.2.3 Préparation de la collecte des données

Définition des procédures et protocoles pour la collecte de données.

6.2.3.1 Identification des énoncés de base

Pour réaliser cette vérification empirique partielle, quatre énoncés de base permettant de constater des faits sur un événement particulier ont préalablement été décrits afin de pouvoir mesurer de façon objective le niveau d'intérêt et de satisfaction des professionnels des organisations face au modèle SA. La colonne « A » du Tableau 6.1 présente les quatre énoncés de base pour permettre de prendre la mesure du degré d'intérêt et de satisfaction des

professionnels des organisations concernant l'acceptabilité et l'applicabilité des éléments du modèle SA, suite aux présentations et aux projets qui ont été réalisés par le chercheur.

6.2.3.2 Scénario d'évaluation qualitative de la mesure

Pour chacun des énoncés de base décrits dans la première colonne du Tableau 6.1 sont spécifiés, dans les colonnes « B » et « C », un certain nombre de faits qualitatifs objectifs permettant de mesurer ou non l'atteinte de l'énoncé concerné. Par exemple, si lors d'une présentation du modèle SA en industrie, où il y a eu 50 participants, la majorité des professionnels présents sont intervenus d'une manière ou d'une autre pour confirmer nos dires ou demander des éclaircissements sur les éléments présentés, nous pouvons objectivement constater que pour l'énoncé « L'intérêt des organisations, à recevoir ou à faire connaître de l'information sur le modèle SA, peut être mesuré lorsque l'on constate que : »

- ✓ Des organisations ont libéré au moins un professionnel pour qu'il puisse assister à une rencontre ou une conférence durant ses heures de travail, en tenant compte que certaines d'entre-elles investissent aussi le coût du transport, de l'hébergement ainsi que la perte due à une non-facturation du temps du professionnel libéré.
- ✓ La majorité des professionnels, qui ont assisté à la rencontre, ont manifesté de l'intérêt pour le sujet.

Nous pouvons raisonnablement interpréter la valeur de cette mesure, sans trop nous avancer, comme étant : « L'organisation qui ont libéré leurs professionnels pour assister à la rencontre veulent savoir si le modèle SA les aidera à combler leurs besoins de sécurité des applications dans de futurs projets. », car, sauf pour des cas d'exception, rares sont les professionnels TI qui peuvent être libérés pour pouvoir assister à un événement qui n'offre aucun intérêt ni pour l'organisation ni pour le professionnel.

6.2.3.3 Analyse des données

Présentation de la démarche utilisée pour l'analyse et l'interprétation des données qualitatives collectées durant les diverses études de cas.

6.2.3.4 Analyse de la mesure effectuée

À chaque énoncé sont associées deux valeurs permettant leur évaluation, ainsi que l'interprétation de la mesure effectuée. Ces interprétations s'appuient sur l'évaluation objective de ce que l'on peut déduire de la valeur de la mesure constatée.

Par exemple, si l'on constate qu'une organisation, qui avait décidé d'intégrer des éléments du modèle SA dans un de ses projets d'application, est déçue des résultats obtenus, on peut facilement conclure que cette dernière n'est pas satisfaite du progrès apporté par le modèle SA.

6.2.3.5 Raisonnement soutenant l'interprétation du résultat de la variable mesurée

Chaque énoncé défini pour la vérification empirique partielle a été sélectionné afin d'obtenir une progression sur quatre niveaux dans l'évaluation de l'intérêt et de la satisfaction mesurée (Tableau 6.1, rangées 1 à 4).

Le niveau d'intérêt et de satisfaction identifié dans la première colonne se définit par l'évaluation qualitative simultanée de la facilité d'intégration et de l'acceptation générale des éléments du modèle par les personnes qui ont participé à une présentation ou à la réalisation d'un projet.

Par exemple, lorsque les participants d'une présentation sont satisfaits des éléments présentés, et qu'ils considèrent que le modèle pourra peut-être les aider à atteindre leur objectif de sécurité (niveau 2), on peut considérer que ces personnes acceptent bien le modèle

et ses éléments. De la même manière, lorsque les participants d'un projet sont satisfaits des résultats de sécurité obtenus par l'utilisation des éléments du modèle, on peut considérer que ces éléments ont pu s'intégrer adéquatement à leur projet d'application, et ce, sans trop de complications (niveau 3). Simultanément, on peut considérer que, dans ce deuxième exemple, l'équipe de projet a sommairement analysé et accepté le modèle SA avant de décider d'investir des efforts pour le comprendre et l'utiliser.

Trois variables supplémentaires ont été identifiées pour aider à préciser le contexte dans lequel ont été vérifiées l'acceptabilité et l'applicabilité des éléments du modèle, soit :

1) La date ou la période, et l'endroit où a eu lieu l'événement;
2) L'approximation du nombre de participants à l'événement ou au projet de l'organisation; puis, lorsqu'applicable;
3) L'envergure du projet de sécurité de l'application en jours/personnes.

6.2.3.6 Contraintes et limitations de la vérification empirique partielle

Malgré l'avantage de pouvoir directement confronter le modèle SA avec des projets d'applications de l'industrie, la vérification empirique a certaines limites.

1) La fiabilité de l'évaluation et de l'interprétation des mesures est limitée, car les quatre énoncés de base posés :
   a) n'ont pas été testés intersubjectivement dans un assez grand nombre de situations;
   b) n'offraient pas un niveau de granularité suffisant pour identifier quels éléments du modèle étaient les plus efficients dans l'intégration de la sécurité dans des projets d'applications;
2) La couverture de la vérification des éléments du modèle SA dépend directement des besoins de sécurité des projets sélectionnés, ainsi que des ressources qui ont été allouées au volet sécurité de ces projets;

3) La vérification empirique du modèle SA doit être considérée comme partielle, car elle n'a pas permis de couvrir tous les éléments du modèle qui ont été conçus lors de ces travaux de recherche.

Tableau 6.1 Variables et mesures empiriques utilisées pour l'évaluation du niveau d'intérêt et de satisfaction de l'acceptabilité et de l'applicabilité du modèle SA

		A **Énoncé à mesurer**	B **Mesure de l'atteinte du niveau d'intérêt et de satisfaction**	C **Mesure de la perte du niveau d'intérêt et de satisfaction**	D **Interprétation de la mesure**
Niveaux d'intérêt et de satisfaction (Élevé ↑ / ↓ Faible)	**4**	- La satisfaction de l'organisation par rapport aux résultats de sécurité obtenus grâce à l'utilisation du modèle SA peut être mesuré lorsque l'on constate que :	✓ L'organisation considère qu'elle a atteint ses objectifs de sécurité ✓ L'organisation reconnaît le progrès réalisé en matière de SA dans son projet ✓ L'organisation est prête à exprimer sa satisfaction de manière concrète	✓ L'application du modèle n'a pas répondu aux attentes de sécurité de l'organisation ✓ L'organisation n'a pu identifier de changements positifs apportés par le modèle ✓ L'organisation est déçue des résultats obtenus	- L'organisation **est / n'est pas** satisfaite du progrès apporté par le modèle dans la sécurité de ses applications
	3	- La satisfaction de la facilité avec laquelle l'organisation a pu intégrer les éléments du modèle SA dans un projet spécifique peut être mesuré lorsque l'on constate que :	✓ L'organisation n'a pas eu à modifier sa méthodologie de développement ✓ Elle a pu choisir et intégrer les éléments qui lui convenaient pour atteindre ses objectifs de sécurité dans un projet d'application	✓ L'organisation a essayé d'intégrer le modèle dans un de ses projets d'application, et elle a fini par l'abandonner	- L'organisation a identifié des éléments de sécurité du modèle qui **ont pu/n'ont pas pu** s'intégrer à l'environnement d'un projet d'application
	2	- L'intérêt de l'organisation à utiliser des éléments du modèle SA dans l'un de ses projets d'application peut être mesuré lorsque l'on constate que :	✓ L'organisation investit des ressources ou de l'accompagnement afin de lui permettre d'utiliser le modèle pour pouvoir intégrer la sécurité dans un de ses projets d'application	✓ L'organisation ne fera aucune démarche particulière	- L'organisation a des besoins de sécurité à combler pour au moins un de ses projets d'application et **pense / ne pense pas** que le modèle l'aidera à atteindre cet objectif
	1	- L'intérêt d'une organisation à recevoir ou à faire connaître de l'information sur le modèle SA peut être mesuré lorsque l'on constate que :	✓ L'organisation souhaite investir pour connaître ou faire connaître une nouvelle approche lui permettant d'intégrer la sécurité dans un de ses projets d'application ✓ Le professionnel manifestera de l'intérêt pour le sujet	✓ L'organisation n'invitera aucun professionnel à venir présenter une conférence sur ce sujet ✓ L'organisation n'enverra personne assister à une présentation sur ce sujet ✓ Le professionnel ira assister à une autre conférence	- L'organisation **croit / ne croit pas** que le modèle l'aidera à combler ses besoins de sécurité d'application dans de futurs projets

6.2.4 Collecte des données : présentation et utilisation du modèle en industrie

L'industrie regroupe des professionnels qui peuvent avoir à utiliser et à mettre en place les principes et éléments proposés par le modèle à l'intérieur de projets d'applications réels. Ce groupe offre l'avantage de pouvoir vérifier le modèle proposé sous l'angle de l'applicabilité et de l'atteinte des résultats de sécurité visés.

La majorité des professionnels œuvrant dans l'industrie de la sécurité de l'information connaissent les principes et les pratiques recommandées, exigées par leur travail. Une majorité a déjà vécu des insatisfactions face aux méthodes et outils disponibles pour les aider à améliorer la sécurité de leurs applications. Toutes les entreprises, qui ont déjà réalisé au moins un projet d'application où elles devaient y intégrer de la sécurité, ont rencontré des défis et des questionnements. Riches de cette expérience, elles sont en mesure d'exprimer clairement leurs exigences et leurs satisfactions face à toute nouvelle approche de SA.

On peut donc s'attendre à ce que les professionnels œuvrant au sein de ces entreprises soient en mesure, en voyant le modèle lors d'une conférence ou en le déployant durant un projet d'application, de se faire une opinion claire sur la possibilité d'utiliser les éléments du modèle dans leur organisation et d'exprimer clairement leur satisfaction des résultats prévus ou obtenus en matière de sécurité.

Les présentations du modèle SA ont été réalisées pour des professionnels en gestion, en sécurité, en développement et en audit d'applications lors de plusieurs événements. Les projets d'application ont été réalisés au sein d'organisations qui développent, impartissent ou gèrent la réalisation d'applications. Il faut noter qu'aucun projet n'a implémenté tous les éléments du modèle. Cette situation était prévisible, car le modèle a été conçu de manière à ce que les organisations puissent ne choisir que les éléments qu'ils désirent déployer en fonction des besoins de sécurité de leur projet d'application et des ressources disponibles dans l'organisation.

Plusieurs événements de présentation du modèle SA ont eu lieu durant la réalisation du projet de recherche. La liste suivante regroupe ceux qui ont permis de mesurer l'intérêt des professionnels des entreprises à obtenir de l'information sur le modèle SA.

Afin d'alléger ce chapitre, nous ne mentionnerons ici que quatre projets qui ont eu un impact ou qui ont mené à l'intégration d'éléments du modèle dans un projet d'application. Une description complète des cinq projets et des huit présentations qui ont été évalués lors de cette vérification empirique partielle du modèle SA est présentée à l'appendice I – annexe XX.1.

Projet DGÉQ, janvier 2006

Présentation, développement et utilisation d'un processus d'audit technique de sécurité, basé sur le modèle SA préliminaire[20], par l'équipe de vérification des systèmes de votation électronique (SVÉ) qui ont été utilisés lors des élections municipales du 6 novembre 2005 au Québec. Ce projet d'audit de sécurité s'est conclu par la publication d'un rapport des nouveaux mécanismes de votation (DGEQ, 2006) et la mise en place d'un moratoire interdisant l'utilisation des SVÉ au Québec pour toute élection municipale et provinciale à venir.

- Dates et lieu : du 10 janvier au 24 octobre 2006, Québec
- Nombre de participants : 4 à 7 personnes, selon la période
- Envergure du projet : 960 jours/personne
- Interprétation de la mesure : (1) intérêt de l'organisation à avoir de l'information sur le modèle; (2) intérêt à appliquer certains éléments du modèle dans le projet d'audit de sécurité technique des SVÉ; (3) utilisation des éléments qui convenaient à l'atteinte des objectifs d'audit de sécurité; (4) l'organisation a exprimé sa satisfaction de manière concrète en recommandant le chercheur à Élections Canada pour

[20] Ce projet a été réalisé durant les travaux propédeutiques du chercheur.

prendre en charge le volet de la SA dans la première phase du projet pilote de réalisation du système de votation canadien par Internet.

Projet ÉC, juin 2010

Projet pilote d'Élections Canada (ÉC) concernant la réalisation, la certification et l'utilisation éventuelle d'un système de votation par Internet (SVI) sécuritaire, lors de futures élections fédérales. L'utilisation et l'adaptation de certains éléments du modèle ont permis à l'organisation de bien comprendre le défi sur la portée de la sécurité qu'elle devait relever pour pouvoir garantir et fournir les preuves que les résultats d'élections réalisées avec les SVI seraient aussi justes et fiables que ceux obtenus avec le système de votation actuel (Poulin, 2013b, pp. 13-45). C'est lors d'une des rencontres de ce projet que le composant « Matrice de traçabilité de la sécurité des applications » a été conçu et intégré dans le modèle par le chercheur, afin de répondre à un besoin de gestion du suivi de l'impact d'un changement d'un risque de sécurité jusqu'à l'application utilisant le CSA concerné.

- Dates et lieu du projet : de mai 2010 à décembre 2010, et de juin 2011 à septembre 2012, Ottawa
- Nombre de participants : 7 à 10 personnes selon la période
- Envergure du projet : 2 960 jours/personne, en deux phases
- Interprétation de la mesure : (1) intérêt de l'organisation à avoir de l'information sur le modèle; (2) intérêt à appliquer certains éléments du modèle dans le projet pilote afin de bien identifier les risques et les exigences de sécurité; (3) adaptation et utilisation des éléments qui convenaient à l'atteinte des objectifs de sécurité de l'organisation; (4) l'organisation a exprimé sa satisfaction de manière concrète en renouvelant le mandat du chercheur et en l'autorisant à présenter les résultats du travail réalisé dans le projet au DGÉQ.

Projet Desjardins, novembre 2011

Le projet « Sécurité des applications Desjardins » consistait à assister l'organisation dans la mise en place d'une première partie du modèle SA afin notamment d'intégrer des CSA dans le cycle de vie des applications critiques utilisées par l'organisation (Poulin, 2011b).

- Dates et lieu : du 11 novembre au 22 décembre 2011, Montréal
- Nombre de participants : 3 à 5 selon la période
- Envergure du projet : 125 jours/personne
- Interprétation de la mesure : (1) intérêt de l'organisation à avoir de l'information sur le modèle; (2) intérêt à appliquer certains éléments du modèle dans le projet de sécurisation des applications critiques de l'organisation; (3) utilisation des éléments qui convenaient à l'atteinte des objectifs de sécurité de l'organisation; (4) soutien de l'organisation à la délégation canadienne au SC27, dans le but de faire participer un de ses professionnels au projet de la norme ISO 27034.

Projet OWASP Novembre 2013

Présentation et démarrage du projet « Conversion des Top 10 d'OWASP en CSA de la norme ISO 27034 – Application Security » qui consistait à créer des CSA à partir des dix principaux risques de sécurité identifiés par l'organisation internationale *Open Web Application Security Project* (Poulin, 2013a).

- Dates et lieu : 15 novembre 2013 – projet toujours actif, Montréal
- Nombre de participants : 10 à 20 selon le nombre de sous-projets actifs
- Envergure du projet : 500 jours/personne
- Interprétation de la mesure : (1) intérêt de l'organisation à avoir de l'information sur le modèle; (2) intérêt à appliquer certains éléments du modèle dans le projet; (3) utilisation des éléments qui conviennent à l'atteinte des objectifs de sécurité du projet.

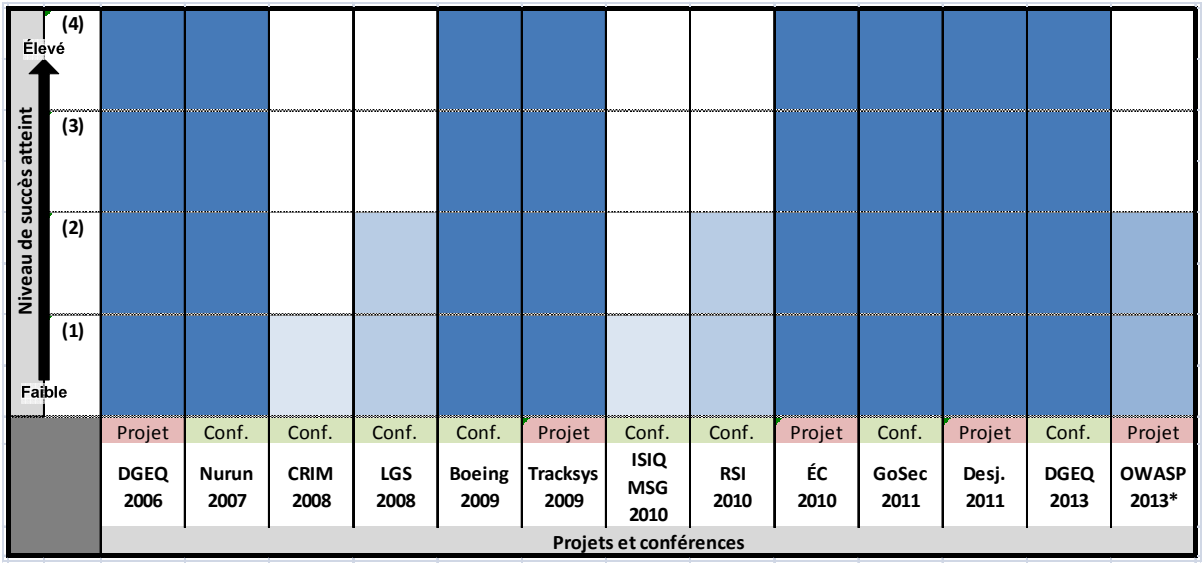
6.2.5 Rapport : interprétation des mesures empiriques et de l'impact du modèle dans l'industrie

L'objectif visé par l'interprétation des mesures empiriques partielles est d'avoir une évaluation préliminaire qualitative, tenant compte des limites de l'échantillon de conférences et de projets réalisés, de l'acceptation et de l'applicabilité de certains éléments du modèle.

Les mesures d'intérêt et de satisfaction ont été réalisées à partir des quatre variables présentées à la colonne « D » du Tableau 6.1.

Le Tableau 6.2 présente le niveau d'intérêt et de satisfaction mesuré à partir de l'appréciation générale des organisations qui ont participé à au moins un des projets ou une des conférences concernant le modèle SA.

Tableau 6.2 Niveaux d'intérêt et de satisfaction atteints par conférence et par projet



Des cinq projets qui ont utilisé le modèle SA, quatre organisations ont été satisfaites des résultats au point d'autoriser un de leurs professionnels à s'impliquer activement dans le projet SC27 d'ISO, à témoigner de leur expérience ou à recommander l'utilisation du modèle

à une autre organisation (niveau 4). En ce qui concerne le 5e projet, OWASP 2013, il n'est qu'en phase de démarrage, aucune mesure d'intérêt et de satisfaction de l'intégration des éléments du modèle dans les processus d'OWASP n'a pu encore être effectuée. On ne peut que constater que, comme l'organisation démarre un projet d'arrimage avec certains éléments du modèle, elle pense que celui-ci l'aidera à atteindre ses objectifs.

Des huit conférences où le modèle a été présenté, quatre d'entre elles ont chacune amené au moins une organisation intéressée par le modèle à faire participer l'un de ses professionnels au projet de la norme ISO 27034 ou à planifier le démarrage d'un projet qui utilisera le modèle.

Sachant que cette vérification n'a été réalisée que sur 13 études de cas, dont 5 projets réels, et que même s'il n'y a aucune certitude que des résultats similaires seront obtenus dans d'autres projets d'application (Kitchenham, 1996, p. 13), nous sommes confiants que les résultats obtenus nous donnent un bon indice de l'acceptabilité et de l'utilisabilité du modèle SA. De fait, dans l'ensemble des cas, tous les projets et conférences réalisés ont suscité un intérêt certain de la part des organisations qui y ont participé. Cette évaluation qualitative est basée sur l'interprétation de l'intérêt de leurs professionnels à partager de l'information, soit par la pertinence des questions posées, par leur désir d'implication à prendre part aux développements futurs de la norme ou par les témoignages de leurs expériences dans des cas de projets de sécurité des applications. Il est à noter que les conférences Nurun 2007 et LGS 2007 étaient des rencontres de travail servant à identifier des pistes d'amélioration de l'offre de service de l'entreprise ou servant à identifier des stratégies pour intégrer la sécurité dans des projets d'applications.

Finalement, aucune des prestations n'a déclenché de discussions houleuses ou des réactions de rejet de la part des participants ou des organisations.

6.3 Évaluation de la qualité des mesures de la méthode ASIA

L'analyse de risques de sécurité est un processus qui permet de comprendre l'origine et la nature des risques, et de déterminer leurs niveaux d'acceptabilité. Elle constitue la base de l'évaluation des risques et des décisions concernant leur traitement.

Plusieurs méthodes d'analyse des risques de sécurité telles que MÉHARI, OCTAVE ou EBIOS ont été conçues pour évaluer des risques de sécurité organisationnelle. Cependant, sans ajustements majeurs, ces méthodes ne permettent pas d'identifier et d'évaluer les risques de sécurité qu'une organisation devra affronter si elle décide d'acquérir et d'utiliser une application; elles pourront encore moins proposer des contrôles à mettre en place pour atténuer ces risques. En conséquence, le modèle SA propose la méthode d'analyse de risques de la sécurité d'une application « ASIA » qui ne présente pas ces lacunes.

La méthode ASIA est un processus permettant d'identifier et d'évaluer les risques amenés par l'acquisition et l'utilisation d'une application par l'organisation. Ce processus a été développé en respectant les concepts et processus proposés par la norme ISO 27005, et en utilisant les concepts et les composants du modèle SA.

La méthode ASIA permet de couvrir les cinq étapes du processus amené par la norme ISO 27005 (*Voir* ANNEXE XVII, Figure-A XVII-1) :

1) Établir le contexte;
2) Évaluer les risques de sécurité de l'information;
3) Traiter les risques de sécurité de l'information et accepter les risques résiduels;
4) Communiquer les risques;
5) Surveiller et réviser les risques.

Aussi, la méthode ASIA propose un ensemble d'éléments, de mesures et d'activités de mesure permettant d'identifier et d'évaluer des risques de sécurité amenés par une application à l'intérieur d'un contexte d'affaires, juridique et technologique précis.

Lors de son développement, une évaluation de la qualité des mesures de la méthode a été réalisée afin de déterminer sa conformité aux concepts de métrologie (vraies mesures : répétables, qualités, etc.).

6.3.1 Objectif

L'objectif est d'évaluer la qualité des mesures et des activités de mesure proposées par la méthode ASIA version 1.0 en identifiant et en validant la qualité des mesures impliquées dans la méthode d'analyse, et en déterminant les actions à prendre pour les améliorer.

6.3.2 Démarche

Les étapes et la démarche d'analyse proposées pour réaliser la validation et l'évaluation des éléments proposés par la méthode ASIA s'appuient, notamment, sur les quatre activités du modèle des processus de mesure de la norme ISO 15939:2006 – *Software and Systems Engineering – Measurement Process* (Figure 6.1).

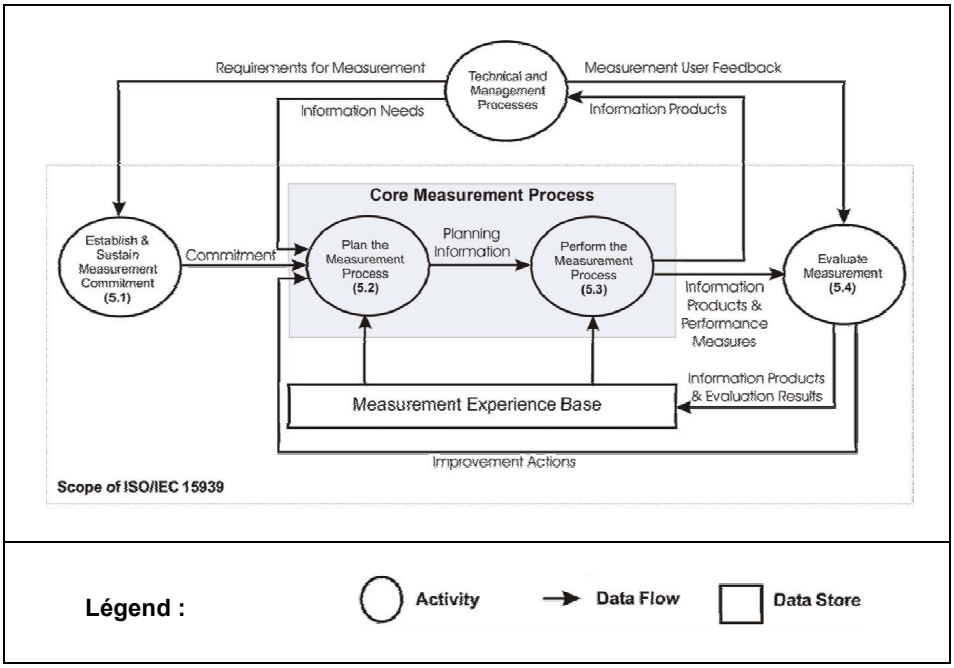


Figure 6.1 Modèle des processus de mesure selon ISO 15939
Tirée de (ISO/IEC, 2006b, p. 9)

La Figure 6.1 montre que le processus de mesure de base est dirigé par les besoins d'information de l'organisation.

Pour chaque besoin d'information identifié, le processus de mesure de base produit un élément d'information qui répond à ce besoin. Le produit d'information est ensuite transmis à l'organisation comme une base à la prise de décision. Le lien entre les mesures et les besoins d'information est décrit comme l'information sur la mesure de modèle, tel que présenté à la Figure 6.2.

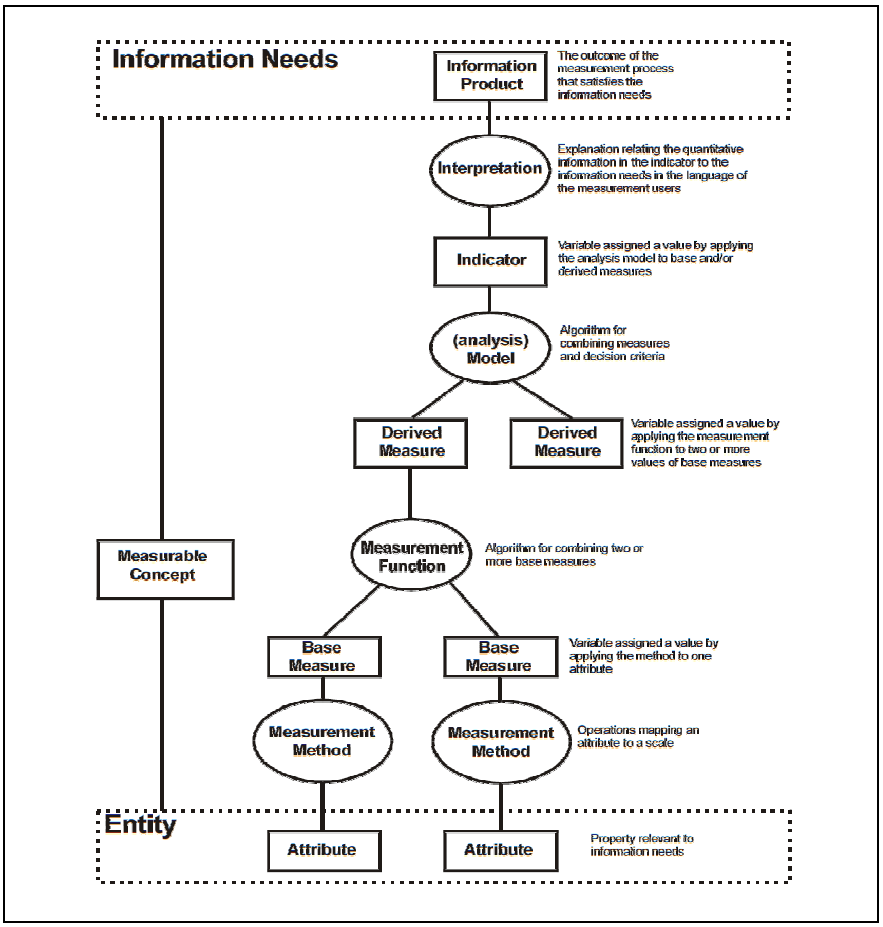


Figure 6.2 Relations clés du modèle de mesure de l'information selon ISO 15939
Tirée de (ISO/IEC, 2006b, p. 20)

Le besoin d'information (*Information Needs*) est l'objectif auquel doit répondre ce processus de mesure. Dans le cas de la méthode ASIA, l'information requise par l'organisation est le niveau de confiance ciblé ou mesuré pour une de ses applications. Les attributs (*Entity*) sont les éléments d'information qui seront mesurés ou évalués pour combler le besoin d'information de l'organisation.

Les critères et la démarche utilisés pour réaliser la validation et l'évaluation des mesures et des activités de mesure proposées par la méthode ASIA se basent principalement sur les éléments de la section 5 de cette norme.

Présentée dans l'ouvrage « *Software Metrics and software Metrology* » (Abran, 2010, p. 78), la Figure 6.3 offre une représentation détaillée de ce modèle, incluant le modèle standard (*Standard Model*) et le contexte de référence organisationnel (*Organizational Reference Context*), qui ont été utilisés afin de présenter les relations entre les mesures de l'information proposées par la norme ISO 15939 et le contexte organisationnel dans lequel les activités de mesure sont réalisées.

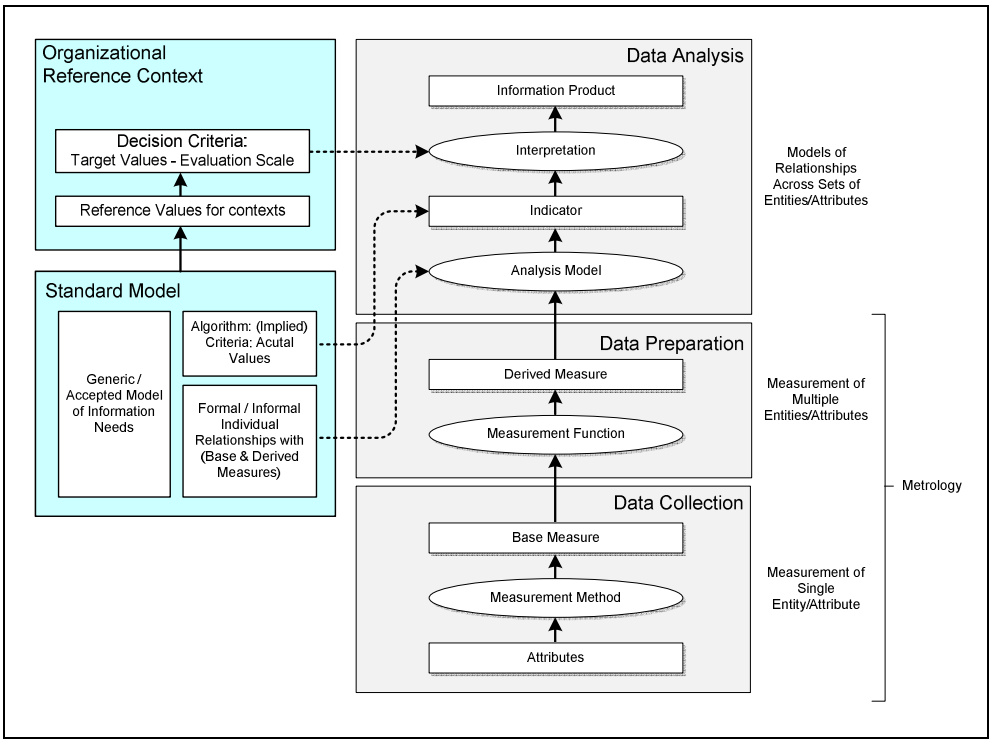


Figure 6.3 Représentation détaillée du modèle de mesure de l'information
Tirée de (Abran, 2010, p. 78).

Ce modèle standard contient un ensemble d'éléments, notamment, le contexte d'évaluation des mesures, les algorithmes et les tables d'interprétation des différentes mesures et un modèle des relations entre les différents types d'objets d'intérêt pouvant provenir de normes internes, internationales ou de pratiques recommandées par l'industrie. Il est utilisé comme référence pour l'ensemble des activités de mesure qui seront réalisées lors des projets d'analyse de risques de SA de l'organisation.

Le contexte de référence organisationnel, qui est aligné avec le modèle standard, comporte un ensemble de critères et de valeurs spécifiques propres à l'organisation. Le modèle SA inclut déjà dans le CNO l'ensemble des éléments de références approuvés, tels que le modèle standard et le contexte de référence organisationnel. Il contient, notamment, les valeurs de référence approuvées par l'organisation dans ses contextes d'affaires, juridiques et technologiques, ainsi que les critères d'évaluation, de décision et les domaines de valeurs correspondantes.

La démarche et la couverture de ce rapport ont permis d'identifier les forces et les opportunités d'améliorations qui pourront être apportées à la méthode ASIA.

La Figure-A I-3 a été produite pour présenter les principaux éléments spécifiques de la méthode ASIA dans un diagramme permettant d'identifier et de mettre en relation les mesures, les activités de mesure et le contexte organisationnel. Pour ce faire, elle utilise la structure de la représentation détaillée du modèle de mesure de l'information (Abran, 2010, p. 78), pour présenter une vision synthèse du résultat de cette démarche d'analyse de la qualité des mesures et activités de mesure de la méthode (Figure 6.3). (*Voir* l'appendice A – ANNEXE XVII pour plus de détails.)

6.3.3 Évaluation des critères et activités de mesure

Cette section présente les 39 critères d'évaluation de mesures dans un projet global, ou de la structure organisationnelle des mesures, selon la norme ISO 15939, qui ont été utilisés lors de travaux d'analyse. Ces critères sont regroupés en 4 sections, soit :

1) Établir et maintenir l'engagement de mesure;
2) Planifier les processus de mesure;
3) Effectuer les processus de mesure;
4) Évaluer les activités de mesure.

Cette section présente aussi les résultats de l'évaluation de chacun de ces critères, en fonction des mesures et activités de mesure proposées par la méthode d'analyse de risques de la sécurité des applications ASIA.

1) Établir et maintenir l'engagement de l'organisation des activités de mesure

Les cinq critères présentés dans cette section servent à évaluer les deux tâches suivantes :

a) accepter les exigences pour la mesure;

b) affecter les ressources.

Note : Voir la section 5.1 de la norme ISO 15939 *Systems and software engineering – Measurement process* (ISO/IEC, 2002) pour plus de détails sur le contenu et la portée des différents critères présentés dans cette section.

Le Tableau 6.3 présente l'analyse des résultats des trois critères concernant l'acceptation des exigences pour la mesure.

Tableau 6.3 Accepter les exigences pour la mesure

Critères	**Résultats**
Cr 1. La portée de la mesure doit être déterminée.	Les objectifs de la méthode ASIA sont de mesurer et de permettre l'analyse de risques de sécurité amenés par l'utilisation d'une application par une organisation (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (D) et (E)). 1) La portée de la mesure est l'environnement d'utilisation d'une application par une organisation, tel que défini dans le modèle SA. 2) La méthode précise que les mesures des risques doivent être réalisées à partir de l'analyse des contextes d'affaires, juridiques et technologiques de l'organisation ainsi qu'à partir des spécifications de l'application. Les définitions de ces contextes sont aussi décrites dans le modèle SA. 3) La méthode précise aussi les sept couches d'informations qui doivent être prises en compte durant l'identification des risques de sécurité. Les définitions de ces couches d'informations sont décrites dans le modèle SA. 4) Les intervenants impliqués dans la réalisation des activités de mesure et d'analyse des risques ne sont pas tous identifiés par la méthode. Cette section de la méthode gagnerait à être bonifiée.

Tableau 6.3 Accepter les exigences pour la mesure (suite)

Critères	Résultats
Cr 2. L'engagement de la direction et du personnel à réaliser une mesure doit être établi	La méthode identifie les éléments devant être mis en place afin de réaliser la mesure des risques de sécurité d'une application, tels que le budget, le responsable de l'analyse et une communication officielle de la réalisation de ce projet.
Cr 3. L'engagement à réaliser une mesure doit être communiqué aux unités concernées	La méthode demande, en début de projet, l'identification des unités concernées par l'analyse sommaire de risques de sécurité d'une application.

Le Tableau 6.4 présente l'analyse des résultats des deux critères concernant l'affectation des ressources.

Tableau 6.4 Affecter les ressources

Critères	Résultats
Cr 4. La responsabilité de la réalisation des activités de mesure doit être assignée aux personnes de chaque unité concernée de l'organisation	La méthode désigne un responsable de la mesure des risques de sécurité, ainsi que les profils des connaissances nécessaires pour réaliser les différentes activités de mesure.
Cr 5. Les personnes assignées doivent avoir les ressources nécessaires pour pouvoir planifier la réalisation des activités de mesure	La méthode fournit les exigences requises pour pouvoir réaliser une analyse, ainsi que des processus de mesure et d'analyse. Elle fournit aussi une liste de questions (banque de connaissances) et des guides pour faciliter la réalisation des activités de mesure (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (F) et (A5)). Par contre : 1) Les exigences gagneraient à être précisées; 2) Le questionnaire permettant l'identification des menaces est incomplet; 3) Le processus d'évaluation des mesures gagnerait à être précisé, et 4) La méthode n'identifie pas toutes les ressources nécessaires à la planification et la réalisation des activités de mesure. Elle identifie les utilisateurs de la mesure, l'analyste, mais pas le bibliothécaire des mesures. Une bonification des quatre éléments identifiés ci-dessus devrait être réalisée.

2) Planifier les processus de mesure

Les dix-sept critères présentés dans cette section servent à évaluer les sept tâches suivantes :

a) caractériser l'unité d'organisation (Tableau 6.5);
b) identifier les besoins en information (Tableau 6.6);
c) choisir les mesures (Tableau 6.7);
d) définir la collecte de données, l'analyse et les procédures de déclaration (Tableau 6.8);
e) définir les critères pour évaluer les produits d'informations et les processus de la mesure (Tableau 6.9);
f) examiner, approuver et fournir les ressources pour des tâches de la mesure (Tableau 6.10);
g) acquérir et déployer les technologies requises à la réalisation de la mesure (Tableau 6.11).

Le Tableau 6.5 présente l'analyse des résultats du critère concernant la caractérisation de l'unité d'organisation.

Tableau 6.5 Caractériser l'unité d'organisation

Critère	Résultat
Cr 6. Les caractéristiques de l'unité d'organisation qui sont pertinentes pour le choix des mesures et l'interprétation des produits d'information doivent être explicitement décrites	La méthodologie propose une démarche permettant à l'organisation l'identification de ses contextes d'affaires, juridiques et technologiques, spécifiques à son application (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (A), (A1), (A2), (A3) et (A4)). En se référant au modèle SA, la méthode ASIA propose à l'organisation de conserver le résultat de cette démarche à l'intérieur de son cadre normatif. L'utilité de ce cadre normatif est similaire au « Organisationnal Reference Context » proposé dans le livre « Software Metric and Software Metrology » (Abran, 2010, pp. 77-78).

Le Tableau 6.6 présente l'analyse des résultats des quatre critères concernant l'identification les besoins en information.

Tableau 6.6 Identifier les besoins en information

Critères	Résultats
Cr 7. Les besoins d'information pour la mesure doivent être identifiés	L'objectif de la réalisation d'une méthode d'analyse de risques de sécurité est d'identifier les contrôles de sécurité à mettre en place pour diminuer les risques d'utiliser une application à un niveau acceptable pour l'organisation (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, l'élément : (Reference Values for contexts)). Afin d'atteindre cet objectif, les groupes d'informations suivants ont été identifiés par la méthode ASIA : 1) L'information impliquée par l'utilisation de l'application; 2) Les groupes et les rôles des acteurs impactés par l'utilisation de l'application; 3) La liste des spécifications de l'application; 4) Les contextes d'affaires, juridiques et technologiques à l'intérieur desquels l'application sera utilisée.
Cr 8. Les besoins d'information doivent être priorisés	La méthode ASIA propose une démarche de catégorisation permettant de sélectionner les éléments d'information qui seront évalués, parmi l'ensemble des informations préalablement identifiées ((*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments (B), (B1) à (B5)).
Cr 9. Les besoins d'information concernés doivent être sélectionnés	La démarche de catégorisation inclut un mécanisme de sélection des besoins d'information qui lui permette d'identifier l'information qui est critique pour l'organisation dans le contexte de cette application.
Cr 10. Les besoins d'information sélectionnés doivent être documentés et communiqués	La démarche de catégorisation des informations impliquées par une application permet de produire un rapport de catégorisation qui devra être distribué aux personnes concernées.

Le Tableau 6.7 présente l'analyse des résultats des trois critères concernant le choix des mesures.

Tableau 6.7 Choisir les mesures

Critères	Résultats
Cr 11. Les mesures candidates qui pourraient répondre aux besoins des informations sélectionnées doivent être identifiées	Lors du développement de la méthode ASIA ont été réalisées l'identification et la sélection, parmi les mesures candidates, des mesures qui devront être évaluées (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2les éléments (Entity)). Ceci afin d'assurer l'harmonisation des concepts et résultats produits par la méthode, celle-ci utilise les définitions officielles provenant de la norme ISO 27005 – *Information security risk management* (ISO/IEC, 2010d). a) Risque Potentialité qu'une menace donnée exploite la vulnérabilité d'un actif ou d'un groupe d'actifs, nuisant ainsi à l'organisation. Cette définition place en corrélation les mesures suivantes : potentialité, menace et impact. Le risque est donc une mesure dérivée, exprimée par une valeur numérique entière comprise entre 1 et 4. b) Impact Changement défavorable des objectifs d'affaires réalisés. Cet impact se mesure via la perte de disponibilité, d'intégrité, de confidentialité d'une information sensible. Il peut être estimé en pertes financières comme, notamment : une perte de revenu, une perte de confiance (baisse des ventes), une perte de vie, ou une perte d'actifs à la suite de poursuites judiciaires. L'impact est une mesure estimée, exprimée en monnaie, notamment, en dollars ou en Euros. c) Menace Il existe deux types de menaces, soit : i) la menace intentionnelle – action d'une personne mal intentionnée. Cette action se mesure par la motivation de l'attaquant, la complexité et le coût de l'attaque, comparés au risque pour l'attaquant d'être identifié et puni, etc. ii) la menace accidentelle – panne ou bris d'équipement, situation climatique, erreur humaine, etc. La menace est une mesure dérivée, exprimée par une valeur numérique entière comprise entre 1 et 4.
Cr 12. Des mesures doivent être choisies parmi les mesures candidates	Les mesures identifiées par la méthode ASIA sont : 1) le niveau de sensibilité, tel que celui d'une information, d'un acteur, d'une spécification de l'application, d'un processus et d'un article de loi (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2 les éléments : (Base Measure) et (Base/Derived Measure)).

Tableau 6.7 Choisir les mesures (suite)

Critères	Résultats
Cr 13. Certaines mesures doivent être documentées par leur nom, l'unité de mesure, leur définition formelle, la méthode de collecte de données, et leur lien avec les besoins d'information	Les mesures proposées par la méthode ASIA sont documentées et clairement définies. Le niveau de sensibilité de toutes les entités est actuellement défini par une valeur numérique entière comprise entre 1 et 4. Cette décision stratégique est en cours de validation par l'équipe méthodologie de la méthode.

Le Tableau 6.8 présente l'analyse des résultats des trois critères concernant la définition de la collecte de données, de l'analyse et les procédures de déclaration.

Tableau 6.8 Définir la collecte de données, l'analyse et les procédures de déclaration

Critères	**Résultats**
Cr 14. Les procédures de collecte, de stockage et de vérification des données doivent être définies	Des procédures de collecte de données ont été définies, mais elles ne sont pas complètes et gagneraient à être bonifiées (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (A), (A1) à (A4)). 1) Identification du risque – processus permettant d'identifier, de lister et de caractériser les éléments d'un risque. L'identification des risques se fait à l'aide d'un questionnaire, dont les questions permettent l'identification, sur une échelle de 1 à 4, de la potentialité des menaces présentes dans la portée de la méthode et d'en estimer les impacts respectifs. Les procédures de stockage et de vérification des données sont inexistantes. Ces procédures devraient être développées.
Cr 15. Les procédures d'analyse des données et la déclaration des produits d'information doivent être définies	Des procédures d'analyse de données ont été définies, mais ne permettent pas nécessairement l'obtention répétitive des mêmes résultats lors de l'analyse des mêmes données par des personnes différentes. Il est à noter qu'en dépit du fait que la mesure de base soit la même pour toutes les entités mesurées, l'activité de mesure et le mécanisme d'héritage du résultat d'une mesure peuvent différer d'une entité à l'autre. Ces spécificités devront être clairement spécifiées dans les descriptions des processus correspondants.
Cr 16. Les procédures de gestion de configuration doivent être définies	Un outil Web, permettant la gestion de la configuration et des données traitées lors de la réalisation d'une analyse de risques de la sécurité, est prévu pour la version 2.0 de la méthode.

Le Tableau 6.9 présente l'analyse des résultats des deux critères concernant la définition des critères pour évaluer les produits d'information et le processus de mesures

Tableau 6.9 Définir les critères pour évaluer les produits d'information et le processus de mesure

Critères	Résultats
Cr 17. Les critères d'évaluation des produits d'information doivent être définis	Les critères d'évaluation de certains éléments d'information ont été clairement définis. Un mécanisme d'héritage de niveau de sensibilité a aussi été défini (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (B) et (C)). 1) Estimation du risque Activité de mesure qui assigne une valeur entière de 1 à 4 à la potentialité, et une valeur monétaire à la conséquence d'un risque. La conséquence étant ici une estimation de l'impact potentiel maximum d'un risque qui s'est produit.
Cr 18. Les critères d'évaluation des processus de mesure doivent être définis	Aucun critère d'évaluation des processus de mesure n'a été défini par la méthode ASIA. Cet élément devra être corrigé lors de futurs travaux de recherche.

Le Tableau 6.10 présente l'analyse des résultats des deux critères concernant l'examen, l'approbation et la disponibilité des ressources pour des tâches de mesure.

Tableau 6.10 Examiner, approuver et fournir des ressources pour des tâches de mesure

Critères	Résultats
Cr 19. Les résultats de la planification de la mesure doivent être vérifiés et approuvés	La méthode ASIA prévoit le dépôt de la planification de l'analyse de risques à la direction de l'organisation, aux fins d'approbation. Par contre, aucun mécanisme de vérification formel n'a été défini. Cet élément devra être précisé dans la version 2.0 de la méthode.
Cr 20. Les ressources nécessaires doivent être mises à la disposition des intervenants pour l'exécution des tâches de mesure prévues	La méthode permet l'identification des ressources requises à l'exécution des tâches de mesure prévues pour une analyse de risques spécifiques (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, l'élément : (D)).

Le Tableau 6.11 présente l'analyse des résultats des deux critères concernant l'acquisition et le déploiement des technologies requises à la réalisation de la mesure.

Tableau 6.11 Acquérir et déployer les technologies requises à la réalisation de la mesure

Critères	Résultats
Cr 21. Les technologies de soutien disponibles doivent être identifiées, évaluées et sélectionnées	La version 1.0 de la méthode ne nécessite l'utilisation d'aucun outil de soutien autre que des applications bureautiques usuelles. Le processus d'identification et d'évaluation de technologies pour soutenir la réalisation, la conservation et la réutilisation des informations recueillies, les mesures et les résultats de leur évaluation, est en marche pour la réalisation de la version 2.0 de la méthode.
Cr 22. Les technologies retenues à l'appui sont acquises et déployées	Aucun outil de soutien n'est requis pour l'utilisation de la version actuelle de la méthode.

3) Effectuer les processus de mesure

Les onze critères présentés dans cette section servent à évaluer les quatre tâches suivantes :

a) intégrer les procédures (Tableau 6.12);
b) recueillir les données (Tableau 6.13);
c) analyser les données et développer les produits d'information (Tableau 6.14);
d) communiquer les résultats (Tableau 6.15).

Le Tableau 6.12 présente l'analyse des résultats des trois critères concernant l'intégration des procédures.

Tableau 6.12 Intégrer les procédures

Critères	Résultats
Cr 23. La production et la collecte des données doivent être intégrées dans les processus pertinents	Ces activités sont définies et intégrées dans le processus d'inventaire des actifs informationnels de l'application, dans le processus de catégorisation et dans le processus de réalisation du rapport. Il s'agit notamment des processus permettant l'identification des contextes, de leurs valeurs de référence et de l'identification des entités concernant l'application (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (References Values for contexts), (A), (B),(C) et (D)).
Cr 24. Les procédures de collecte de données intégrées doivent être communiquées aux fournisseurs de données	Un processus utilisant la matrice de traçabilité a été prévu pour communiquer l'ensemble des données collectées aux fournisseurs de données.
Cr 25. L'analyse de données et les rapports doivent être intégrés dans les processus pertinents	Les processus d'analyse des données dont, notamment, celui permettant l'identification des risques de la sécurité de l'application sont bien intégrés à la méthode.

Le Tableau 6.13 présente l'analyse des résultats des trois critères concernant la cueillette des données

Tableau 6.13 Recueillir les données

Critères	Résultats
Cr 26. Les données doivent être collectées	La méthode ASIA fournit les processus et gabarits facilitant les collectes des données requises à la réalisation de l'analyse (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, l'élément : (D)).
Cr 27. Les données recueillies doivent être entreposées, y compris les informations de contextes nécessaires à la vérification, la compréhension ou à l'évaluation des données	Les informations recueillies peuvent être consolidées et conservées dans les gabarits fournis par la méthode et dans la matrice de traçabilité de l'organisation. L'ensemble des informations de contexte nécessaires à la vérification, la compréhension ou à l'évaluation des données est aussi conservé dans les rapports produits lors de la réalisation de la méthode.
Cr 28. Les données recueillies doivent être vérifiées	Aucun processus de vérification formelle des données n'est défini par la méthode. Par contre, le processus de collecte et de dépôt des informations à analyser, lors du processus d'approbation de la portée de l'analyse de risques, pourrait contenir une vérification informelle des données. Le processus permettant la vérification formelle des données recueillies sera intégré à la version 2.0 de la méthode.

Le Tableau 6.14 présente l'analyse des résultats des trois critères concernant l'analyse des données et le développement des produits d'information.

Tableau 6.14 Analyser les données et développer les produits d'information

Critères	Résultats
Cr 29. Les données recueillies doivent être analysées	La méthode offre un processus formel d'analyse des données recueillies. Celui-ci inclut, notamment, des tables de correspondances ainsi que des exemples de cas facilitant l'analyse homogène des différentes données (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (G) et (I)).
Cr 30. Les résultats d'analyse des données doivent être interprétés	La méthode offre des tables d'analyse et d'interprétation des résultats, mais celles-ci ne sont pas complètes et gagneraient à être bonifiées (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, les éléments : (J) et (K)).
Cr 31. Les produits d'information doivent être réexaminés	Aucun processus d'examen des données ou des résultats produits n'est offert par la méthode. Ce processus sera intégré à la version 2.0 de la méthode.

Le Tableau 6.15 présente l'analyse des résultats des deux critères concernant la communication des résultats produits par l'analyse de risques de sécurité ASIA.

Tableau 6.15 Communiquer les résultats

Critères	Résultats
Cr 32. Les produits d'information doivent être documentés	Les informations recueillies sont consolidées et conservées dans les gabarits fournis par la méthode. Ces rapports d'analyse contiennent les informations nécessaires à la documentation du contexte de mesure et des résultats obtenus (*Voir* l'appendice A – ANNEXE XVII, Figure-A XVII-2, l'élément : (D)).
Cr 33. Les produits d'information doivent être communiqués aux utilisateurs de mesures	À la fin de l'exercice, une copie du rapport d'analyse de risques est transmise aux personnes concernées.

4) Évaluer les activités de mesure

Les six critères présentés dans cette section servent à évaluer les deux tâches suivantes :

a) évaluer les produits d'information et les processus de mesure (Tableau 6.16);

b) identifier les améliorations potentielles (Tableau 6.17).

Le Tableau 6.16 présente l'analyse des résultats des trois critères concernant l'évaluation des produits d'information et des processus de mesure offerts par l'analyse de risques de sécurité ASIA.

Tableau 6.16 Évaluer les produits d'information et les processus de mesure

Critères	Résultats
Cr 34. Les produits d'information mesurés doivent être évalués en fonction des critères d'évaluation spécifiés et des conclusions sur leurs forces et faiblesses	Un processus d'évaluation des produits d'information mesuré par des experts externes du domaine de l'évaluation des risques de sécurité est en cours de développement. Les comités méthode du CLUSIF et du CLUSIQ ont accepté de réviser la méthode ASIA. Ces travaux sont à venir.
Cr 35. Les processus de mesure utilisés doivent être évalués selon les critères d'évaluation spécifiés et des conclusions sur leurs forces et faiblesses	Selon la même entente avec les comités méthode du CLUSIF et du CLUSIQ, un processus d'évaluation des processus de mesure utilisés par la méthode ASIA sera mis en place par des experts externes du domaine de l'évaluation des risques de sécurité.
Cr 36. Les leçons tirées de l'évaluation doivent être stockées dans l'expérience de mesure de base	Ce processus n'existe pas et devrait être implémenté dans la version 2.0 de la méthode.

Le Tableau 6.17 présente l'analyse des résultats des trois critères concernant l'identification des améliorations potentielles de l'analyse de risques de sécurité ASIA.

Tableau 6.17 Identifier les améliorations potentielles

Critères	Résultats
Cr 37. Les améliorations potentielles aux produits d'information doivent être identifiées	Une des étapes de cette recherche cible la publication prochaine d'une deuxième version de la méthode qui amènera notamment une bonification des questionnaires et des groupes d'informations utilisés par les lignes d'affaires pour améliorer la couverture de l'identification les risques de sécurité de chacun des contextes.
Cr 38. Les améliorations potentielles au processus de mesure doivent être identifiées	Idem.
Cr 39. Les améliorations potentielles doivent être communiquées	La méthode d'analyse de risques de sécurité des applications ASIA sera publiée sur un site Web. Des liens RSS ainsi qu'une liste de distribution sera mise en place pour tenir informées les personnes et les organisations intéressées.

6.3.4 Résultats

L'analyse des éléments de la méthode d'analyse de risques de sécurité ASIA développée dans cette recherche soit, notamment, par la validation et la vérification de la qualité des mesures et processus de mesure qu'elle contient, a permis de conclure :

1) Que la méthode propose une portée et des mesures adéquates pour identifier les besoins de sécurité amenés par une application dans le contexte d'affaires d'une organisation;

2) Que les critères du modèle d'analyse de risques sont compréhensibles et correctement définis (ISO/IEC, 2002, p. 20);

3) Qu'en général, la méthode identifie, précise et documente bien des mesures et processus de mesure crédibles et vérifiables pour soutenir les résultats apportés par l'analyse de risques de sécurité, et les prises de décisions qui en découlent;

   Par contre, les actions suivantes devraient être réalisées afin d'améliorer la performance :

   a) la banque de questions permettant l'identification des menaces, ainsi que la documentation de plusieurs des processus gagneraient à être bonifiées (*Voir* le critère : Cr 5);

   b) les procédures de stockage et de vérification des données sont inexistantes et devraient être développées (*Voir* le critère : Cr 14);

   c) les procédures d'analyse de données, qui ont été définies, devraient être bonifiées afin de permettre l'obtention répétitive des résultats des mesures (*Voir* le critère : Cr 15);

   d) un processus de communication aux fournisseurs des données collectées devrait être défini (*Voir* le critère : Cr 24).

4) Les tables d'analyse et d'interprétation des résultats gagneraient à être bonifiées (*Voir* le critère : Cr 30);

5) On ne peut assumer que la définition des processus de mesure est vérifiable.

   Pour corriger cette situation, les actions suivantes devraient être réalisées :

   a) tous les intervenants impliqués dans la réalisation des activités de mesure, ainsi que toutes les ressources nécessaires à la planification et à la réalisation des activités devraient être identifiés (*Voir* les critères : Cr 1 et Cr 4);

b) une méthode de vérification formelle des données, ainsi qu'un processus d'examen des données et des résultats produits devraient être définis (*Voir* le critère : Cr 28 et Cr 31);

c) le processus d'amélioration de la méthode ASIA gagnerait à être formalisé (*Voir* Tableau 6.17);

6) Le concepteur de l'analyse gagnerait à bonifier la documentation des processus de mesure proposés par la méthode, ainsi que les critères de vérification.

   De fait, aucun critère d'évaluation des processus de mesure n'a été défini (*Voir* le critère : Cr 18) ni aucun mécanisme de vérification formelle des résultats de la planification (*Voir* le critère : Cr 20). Des actions rapides devraient être réalisées pour corriger cette situation.

6.4 Comparaison de l'impact du modèle sur la sécurité des systèmes de votation des projets DGÉQ 2006 et ÉC 2010

Afin de pouvoir vérifier l'impact du modèle sur le développement et la vérification de la sécurité des applications, une comparaison des critères de sécurité a été réalisée entre des applications de même type, provenant de deux projets différents.

Voici un résumé des deux projets sélectionnés :

DGÉQ 2006 Audit de sécurité du Directeur général des élections du Québec (DGÉQ) basé sur le modèle, pour vérifier des systèmes de votation électroniques (SVÉ) qui n'avaient pas été développés en utilisant le modèle SA;

ÉC 2010 Projet pilote d'Élection Canada (ÉC), utilisant le modèle, concernant la réalisation, la certification et l'utilisation éventuelle d'un système de votation par Internet (SVI) sécuritaire.

Ces deux projets ont été sélectionnés pour effectuer la comparaison de l'impact du modèle, car ils impliquent tous deux le même type d'applications, soit des SVÉ constitués, notamment, de systèmes tels que : des terminaux et des tabulateurs de votes, des applications de gestion de listes électorales et des applications de services de données. Sachant que ces

applications doivent s'échanger des données via des canaux de communication, tels un réseau, une ligne téléphonique, l'Internet, une carte de mémoire ou du papier, un SVI n'est qu'un type de système de votation qui appartient à la grande famille des SVÉ.

Étant donné que l'audit a été réalisé à l'aide d'une version préliminaire du modèle SA et que, même s'il a évolué depuis, les principes, la portée et les éléments qui le constituaient sont toujours présents dans la version actuelle du modèle SA, nous pouvons réutiliser les points d'évaluation de l'audit du DGÉQ et comparer l'atténuation des risques identifiés entre les différents SVÉ.

L'objectif de notre comparaison est de voir s'il y aura ou non une amélioration de la sécurité entre le SVÉ d'ÉC qui a été développé en utilisant le modèle versus ceux qui ont été développés selon une autre démarche de sécurité.

La comparaison des systèmes de votation a été réalisée en utilisant :

1) la démarche et les éléments vérifiés qui ont mené à l'identification des 18 constats généraux de l'audit de sécurité du DGÉQ des SVÉ (Poulin, 2006c, pp. 10-25, 113-114) (*Voir* l'appendice A – ANNEXE XXII); et
2) des documents du projet pilote du SVI d'ÉC.

Le rapport détaillé d'audit de sécurité des SVÉ concerne, notamment, la vérification de cinq applications produites et déployées par différentes entreprises. Le projet pilote SVI d'ÉC ne concerne qu'une seule application.

Le Tableau 6.18 présente un résultat sommaire de la comparaison de l'atténuation des risques de sécurité, entre les différents SVÉ, selon les constats généraux de sécurité identifiés lors de l'audit de sécurité du projet DGÉQ 2006. Une version plus détaillée de cette comparaison est présentée à l'appendice A – ANNEXE XXIII.

En utilisant la même démarche d'audit, la comparaison des résultats de vérification des mêmes éléments, qui ont été audités en 2006 par l'équipe du DGÉQ, présente clairement une nette amélioration de l'atténuation des risques de sécurité qui ont mené à l'identification des 18 constats généraux du DGÉQ.

En intégrant des éléments du modèle SA dans ses processus de réalisation, ÉC a, dès le début de son projet pilote, identifié les principes de sécurité auxquels elle voulait se conformer, tel que : la SA doit pouvoir être démontrée (Morin, 2012, p. 9). L'organisation a aussi identifié le niveau de confiance cible qu'elle voulait atteindre, soit de réaliser, déployer et utiliser un SVÉ qui donnera aux Canadiens le même niveau de confiance aux résultats des élections que celui obtenu avec le système de votation actuel.

Tableau 6.18 Sommaire du comparatif de l'atténuation des risques de sécurité entre les différents SVÉ

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice	Tabulatrice	Tabulatrice	Terminal de votation	Terminal de votation	Terminal de votation	Inclus dans le
#	Section du rapport	Constats généraux #	Environnements	Accu-Vote ES 2000	Perfas-Tab	Perfas-Tab 2 (DVS)	Perfas-MV	Votex	SVI d'ÉC	Modèle de la SA
3.1.1	**Les processus**									
3.1.1.1	Les rôles, les responsabilités et les qualifications requises	CG1, CG2, CG3	Réalisation & opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.1.2	Les processus touchés par l'introduction d'un système de votation électronique	CG4, CG5, CG6, CG7	Opération	Partielle	Partielle	Partielle	Partielle	Partielle	Oui	Oui
3.1.2	**La protection du système et l'aménagement des lieux de votation**									
3.1.2.1	Les spécifications physiques		Opération	Partielle	Partielle	Partielle	Partielle	Partielle	Oui	Oui
3.1.2.2	Les spécifications techniques et électriques		Opération	Partielle	Partielle	Partielle	Partielle	Partielle	Oui	Oui
3.1.3	**La protection du système de votation**									
3.1.3.1	L'infrastructure technologique : réseau, appareils de votation et autre matériel	CG8	Réalisation & opération	Partielle	Non	Non	Non	Partielle	Oui	Oui
3.1.3.2	Le logiciel utilisé par le système de votation	CG9, CG10	Réalisation & opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.3.3	Le bulletin de vote (papier ou électronique)	CG11	Opération	Non	Non	Non	Non	Oui	Oui	Oui
3.1.4	**La protection du dépôt des votes**									
3.1.4.1	L'identification et la protection du dépôt des votes	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.4.2	L'intégrité du résultat du dépouillement des votes	CG13	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.5	**La protection du vote**									
3.1.5.1	Les mesures d'identification des types de vote	CG14	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.5.2	Le choix de l'électeur	CG15	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.5.3	La protection d'un vote	CG16, CG17	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.6	**Conclusion des constats généraux**									
	Évaluaton du niveau de confiance envers le SVÉ	CG18	Réalisation & opération	Plus faible que l'actuel	Plus faible que l'actuel	Plus faible que l'actuel	Plus faible que l'actuel	Plus faible que l'actuel	Équivalent à l'actuel	

L'organisation a ensuite commencé à identifier ses contextes d'affaires, technologiques et juridiques dans lesquels la nouvelle application de votation devra être utilisée. ÉC a réalisé

l'inventaire des processus actuels qui sont impliqués dans une élection, et a identifié ceux qui pourraient être impactés par l'arrivée de cette nouvelle application. C'est ainsi que l'organisation a identifié les groupes d'informations sensibles qu'elle devait protéger ainsi que les acteurs impliqués, et qu'elle a pu commencer à identifier les risques de sécurité qui seraient apportés par le déploiement et l'utilisation de ce nouveau système.

Ayant analysé le système de votation actuel afin de constituer des listes de risques, de processus et de contrôles de sécurité actuellement en place, elle est en mesure de les compléter avec les nouveaux risques de sécurité amenés par le SVÉ. C'est à partir de l'identification de ces risques qu'ÉC a été en mesure de commencer l'identification des exigences de sécurité qui devront être rencontrées, ainsi que les CSA qui devront être adaptés ou développés, puis intégrés dans le nouveau système.

Finalement, ÉC a commencé à mettre en place et à gérer son CNO où sont conservés tous les documents et éléments organisationnels qui ont été produits durant ce projet pilote. Ce CNO est considéré comme la source autoritaire des documents de l'organisation concernant la SA et est accessible par les professionnels de tous les départements et directions de l'organisation.

La portée, les principes, la démarche, les composants et les processus amenés par le modèle SA ont aidé ÉC à identifier le niveau de confiance ciblé pour son SVÉ, puis à développer et mettre en place les CSA requis pour vérifier et démontrer l'atteinte de ce niveau de confiance.

6.5 Compilation des réponses apportées par le modèle SA aux problématiques de la sécurité des applications

Afin de démontrer que le modèle SA, produit par ce travail de recherche répond aux problématiques soulevées, le Tableau 6.19 présente pour chacune d'elles les éléments du modèle qui les concernent.

Tableau 6.19 Réponses du modèle SA aux 16 problématiques de SA

	Réponses du modèle SA	
Problématiques	**Types d'élément**	**Éléments du modèle**
P01 : Absence d'une vision globale de la sécurité des applications	Audience :	1) Liste des besoins des groupes de personnes suivantes : le gestionnaire, l'équipe TI, le vérificateur, l'auditeur, l'acheteur, le fournisseur et l'utilisateur
	Portée :	2) Intégrer des contrôles de sécurité dans toutes les phases du cycle de vie d'une application 3) L'application dans son environnement 4) La SA s'applique autant à l'application elle-même qu'aux facteurs environnants qui ont un impact sur la SA, tel que l'information, les personnes, les processus, ses trois contextes
	Principes :	5) La sécurité est dépendante du contexte 6) La sécurité est une exigence 7) La SA doit pouvoir être démontrée 8) Investir le montant approprié pour la SA
	Termes :	9) La définition d'une application 10) La définition d'une application sécuritaire
	Concepts :	11) La prise en compte simultanée des quatre domaines de connaissances pour protéger l'information liée à l'utilisation d'une application 12) La portée du cycle de vie de la SA 13) L'environnement de l'application
	Processus :	14) Le processus de gestion du CNO 15) Le processus de la gestion de la SA
	Groupes / rôles :	16) Les 15 groupes et rôles définis par le modèle
	Composants :	17) Le modèle de référence du cycle de vie de la SA
P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application	Portée :	1) Le cycle de vie de la SA 2) L'environnement de l'application 3) Les groupes d'informations impliqués par l'existence de l'application
	Principes :	4) La sécurité est une exigence[21]
	Concepts :	5) Niveau de confiance de l'application
	Processus :	6) Gestion de la SA 7) Identification et classification des groupes d'informations liés à l'utilisation d'une application 8) Gestion des risques de SA

[21] Les exigences de sécurité sont définies pour répondre aux risques de sécurité et s'assurer que le CSA qui sera développé selon ces spécifications, atténuera le risque concerné à un niveau acceptable.

Tableau 6.19 Réponses du modèle SA aux 16 problématiques de SA (suite)

	Réponses du modèle SA	
Problématiques	**Types d'élément**	**Éléments du modèle**
	Groupes / rôles :	9) Direction de l'organisation 10) Équipe de projet 11) Détenteur / propriétaire de l'application
P02 : Absence d'une vision permettant d'identifier et de tenir en compte les risques et les contextes d'utilisation d'une application	Portée :	1) Le cycle de vie de la SA 2) L'environnement de l'application 3) Les groupes d'informations impliqués par l'existence de l'application
	Principes :	4) La sécurité est une exigence[22]
	Concepts :	5) Niveau de confiance de l'application
	Processus :	6) Gestion de la SA 7) Identification et classification des groupes d'informations liés à l'utilisation d'une application 8) Gestion des risques de SA
	Groupes / rôles :	9) Direction de l'organisation 10) Équipe de projet 11) Détenteur / propriétaire de l'application
P03 : Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations	Modèle :	1) Le modèle de la SA
P04 : Absence d'une approche permettant de sélectionner les solutions de sécurité requises par une organisation, en fonction de ses besoins de sécurité et de ses ressources économiques	Principes :	1) La sécurité est dépendante du contexte 2) Investir le montant approprié pour la sécurité de la SA
	Concepts :	3) Le cycle de vie de la SA 4) L'environnement de l'application 5) Les groupes d'informations impliqués par l'existence de l'application 6) Niveau de confiance de l'application
	Processus :	7) Gestion de la SA 8) Gestion des risques de SA
	Groupes / rôles :	9) Direction de l'organisation 10) Détenteur / propriétaire de l'application 11) Équipe de projet
	Composants :	12) Le CNO 13) La bibliothèque de CSA

[22] Les exigences de sécurité sont définies pour répondre aux risques de sécurité et s'assurer que le CSA qui sera développé selon ces spécifications, atténuera le risque concerné à un niveau acceptable.

Tableau 6.19 Réponses du modèle SA aux 16 problématiques de SA (suite)

	Réponses du modèle SA	
Problématiques	**Types d'élément**	**Éléments du modèle**
P05 : Absence d'un vocabulaire et de références communes en sécurité des applications	Portée :	1) Le cycle de vie de la SA 2) L'environnement de l'application 3) Les groupes d'informations impliqués par l'existence de l'application 4) La SA s'applique autant à l'application elle-même qu'aux facteurs environnants qui ont un impact sur sa sécurité, tel que l'information, les personnes, les processus, ses trois contextes
	Principes :	5) La sécurité est dépendante du contexte 6) La sécurité est une exigence 7) La SA doit pouvoir être démontrée 8) Investir le montant approprié pour la SA
	Termes :	9) Application 10) Application sécuritaire 11) Niveau de confiance cible et mesuré 12) Contrôle de SA 13) CNO 14) CNA
	Concepts :	15) La prise en compte simultanée des quatre domaines de connaissances pour protéger l'information liés à l'utilisation d'une application
P06 : Absence d'une définition de la portée de la sécurité d'une application	Portée :	1) Le cycle de vie de la SA 2) L'environnement de l'application 3) Les groupes d'informations impliqués par l'existence de l'application 4) La SA s'applique autant à l'application elle-même qu'aux facteurs environnants qui ont un impact sur sa sécurité, tel que l'information, les personnes, les processus, ses trois contextes
	Composants :	5) Le CNO
P07 : Absence d'une définition claire de ce qu'est une application sécuritaire	Portée :	1) La sécurité est dépendante du contexte
	Termes :	2) Application 3) Application sécuritaire 4) Niveau de confiance
P08 : Absence d'un modèle de référence du cycle de vie de la sécurité d'une application	Portée :	1) Le cycle de vie de la SA
	Composants :	2) Le modèle de référence du cycle de vie de la SA
P09 : Absence de sources claires des exigences de sécurité d'une application	Principes :	1) La sécurité est une exigence 2) La sécurité est dépendante du contexte 3) Investir le montant approprié pour la SA

Tableau 6.19 Réponses du modèle SA aux 16 problématiques de SA (suite)

	Réponses du modèle SA	
Problématiques	**Types d'élément**	**Éléments du modèle**
	Concepts :	4) La prise en compte simultanée des quatre domaines de connaissances pour protéger l'information liés à l'utilisation d'une application
	Processus :	5) Gestion des risques de SA
	Groupes / rôles :	6) Équipe de projet 7) Détenteur / propriétaire de l'application
P10 : Absence d'une méthode d'évaluation de la sécurité d'une application	Principes :	1) La SA doit pouvoir être démontrée
	Termes :	2) Application sécuritaire 3) Niveau de confiance actuel (mesuré)
	Concepts :	4) Niveau de confiance cible et actuel de l'application
	Processus :	5) Processus de gestion de la SA 6) Vérification de la SA
	Groupes / rôles :	7) Équipe TI, vérificateur / auditeur
	Composants :	8) La bibliothèque de CSA 9) Le CSA
P11 : Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de l'organisation	Concepts :	1) Processus de gestion de la SA
	Processus :	2) Vérification de la SA
	Composants :	3) CNO 4) CNA 5) Bibliothèque des CSA 6) CSA
	Groupes / rôles :	7) Vérificateur / auditeur
P12 : Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications	Portée :	1) La SA s'applique autant à l'application elle-même qu'aux facteurs environnants qui ont un impact sur sa sécurité, tels que l'information, les personnes, les processus, ses trois contextes
	Concepts :	2) Pouvoir intégrer des contrôles de sécurité dans toutes les activités présentes dans les phases du cycle de vie de la SA
	Processus :	3) Processus de gestion du CNO 4) Processus de gestion de la SA
	Groupes / rôles :	5) Comité du CNO
	Composants :	6) CNO

Tableau 6.19 Réponses du modèle SA aux 16 problématiques de SA (suite)

	Réponses du modèle SA	
Problématiques	**Types d'élément**	**Éléments du modèle**
P13 : Absence de mécanismes permettant d'assigner aux principaux rôles, pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune des responsabilités qui leur sont assignées	Portée :	1) L'environnement de l'application 2) Les groupes d'informations impliqués par l'existence de l'application 3) La SA s'applique autant à l'application elle-même qu'aux facteurs environnants qui ont un impact sur sa sécurité, tel que l'information, les personnes, les processus, ses trois contextes
	Principes :	4) La sécurité est une exigence
	Concepts :	5) Quatre domaines de connaissances liés à la SA
	Processus :	6) Processus de gestion du CNO 7) Processus de la SA
		8) Les 5 groupes et 18 rôles
	Composants :	9) CNO 10) Le répertoire des rôles, responsabilités et qualifications 11) CSA 12) CNA
P14 : Les méthodes et outils existants de génie logiciel ne tiennent pas toujours compte de la sécurité de l'information TI	Portée :	1) Le cycle de vie de la SA
	Concepts :	2) Pouvoir intégrer des contrôles de sécurité dans toutes les activités présentes dans les phases du cycle de vie de la SA
	Processus :	3) Gestion de la SA
	Composants :	4) CNA
	Groupes / rôles :	5) Équipe TI
P15 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur des processus impliqués dans la réalisation et l'opération de l'application	Portée :	1) Le cycle de vie de la SA
	Principes :	2) La sécurité est une exigence
P16 : La sécurité n'a pas été implémentée en intégrant des contrôles de sécurité à l'intérieur de l'application	Concepts :	1) Pouvoir intégrer des contrôles de sécurité dans toutes les activités présentes dans les phases du cycle de vie de la SA
	Processus :	2) Gestion de la SA
	Groupes / rôles :	3) Équipe TI
	Composants :	4) CSA

6.6 Positionnement du modèle SA avec les pratiques et normes existantes

Certaines normes ainsi que de bonnes pratiques reconnues sont en lien direct avec le modèle SA. Elles peuvent être utilisées :

1) Comme sources de contrôles de sécurité des applications, qui serviront à définir des CSA requis par l'organisation pour ses applications (*Voir* l'appendice A – ANNEXE XXI.1);
2) Pour identifier des principes et des processus à prendre en compte lors de la mise en place du modèle, en fonction des besoins de l'organisation (*Voir* l'appendice A – ANNEXE XXI.2);
3) Pour fournir des méthodes d'analyse de risques de sécurité de l'organisation servant à l'identification des applications les plus à risque pour une organisation (*Voir* l'appendice A – ANNEXE XXI.3); et
4) Pour identifier les processus présents dans le cycle de vie d'une application, afin de pouvoir y intégrer les CSA de l'organisation en fonction de ses besoins (*Voir* l'appendice A – ANNEXE XXI.4).

La Figure-A I-1 positionne le modèle SA avec une sélection des principaux documents qui présentent des principes, des normes, des processus, des méthodes et de bonnes pratiques pouvant être utilisés dans les domaines des TI, durant le cycle de vie d'une application. (*Voir* l'appendice A – ANNEXE XXI pour plus de détails.)

CHAPITRE 7

CONTRIBUTIONS DU CHERCHEUR ET ATTEINTE DES OBJECTIFS DE RECHERCHE

Ce chapitre ferme la démarche de recherche en mettant en lumière les contributions du chercheur dans le développement du modèle SA issu de l'approche d'intégration des éléments de sécurité dans le cycle de vie des applications et des systèmes d'information (7.1). Il précise comment les six objectifs visés par cette thèse ont été atteints (7.2).

7.1 Éléments clés du modèle SA et contributions du chercheur

L'approche d'intégration des éléments de sécurité dans le cycle de vie des applications et des systèmes d'information a mené le chercheur à concevoir le modèle SA, présenté dans ce document. Ce modèle définit les bases d'un vocabulaire et de références communes en sécurité des applications ainsi que les principes de la SA. Il intègre à l'intérieur de ses éléments les principes de niveau d'assurance, de vérifiabilité, de gestion du risque, et permet ainsi de tenir compte des risques et des contextes d'utilisation d'une application. Il s'adapte aux besoins d'affaires et demeure économiquement accessible à la majorité des organisations qui désirent le mettre en place. Il offre à ces dernières de mettre en place les éléments requis afin d'estimer, de mesurer et d'évaluer les coûts de la SA.

Le modèle SA permet donc d'intégrer, de gérer et de vérifier des contrôles de sécurité (CSA) tout au long du cycle de vie d'une application, et de fournir à l'organisation qui l'utilise les preuves démontrant que le niveau de confiance qu'elle a ciblé pour son application a été atteint et maintenu. Il permet, notamment, à l'aide des CSA et de l'alignement des processus et activités en place dans une organisation avec le MRCVSA, d'intégrer des activités de sécurité dans ses processus existants de réalisation et d'utilisation, minimisant ainsi l'impact de la SA dans l'organisation.

Les contributions que le chercheur a proposées à chacun des cycles Delphi, réalisés durant ce travail de recherche (phases 2 et 3) et qui ont mené à la conception, au développement, à la validation et à l'amélioration des éléments du modèle SA sont présentées à l''APPENCIDE I – ANNEXE X.

Les principaux éléments du modèle SA, les références aux contributions du chercheur ainsi que les problématiques auxquelles ces groupes d'éléments répondent sont présentés aux tableaux 7.1 à 7.8.

Le Tableau 7.1 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les besoins de l'audience visée par le modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

Tableau 7.1 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Besoins de l'audience visée

Modèle final Besoins de l'audience visée	**Références aux contributions du chercheur**
Soit : les gestionnaires, les équipes d'approvisionnement et d'opération, les vérificateurs, les auditeurs, les acheteurs, les fournisseurs et les utilisateurs (*Voir* 5.5)	Annexe X.1.2, source : (Poulin, 2006b, pp. 29-31) Annexe X.2.2, source : (Poulin, 2007b, pp. 9-11) Annexe X.3.2, source : (Poulin, 2009e, p. 35) Annexe X.4.2, source : (ISO/IEC, 2011e, p. 7)
❖ Problématiques répondues par l'identification des besoins de l'audience visée par le modèle SA	Section 3.4, problématiques : P01 et P02

Le Tableau 7.2 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer la portée du modèle SA, ainsi que les problématiques de sécurité répondue par celle-ci.

Tableau 7.2 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Portée du modèle

Modèle final Portée	**Références aux contributions du chercheur**
1) Le cycle de vie de la sécurité d'une application	Section 3.6.1, Tableau 3.2, source : (Poulin, 2002, pp. 44-46) Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 39) Section 0, Tableau 3.4, source : ((ISC)², 2013c) Annexe X.2.2, source : (Poulin, 2007b, p. 22) Annexe X.3.2, source : (Poulin, 2009e, p. 18)
2) L'environnement de l'application[23]	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006a, p. 10) Annexe X.2.2, source : (Poulin, 2007b, p. 5)
3) Les groupes d'informations impliqués par l'existence de l'application	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 3.6.4, Tableau 3.5, source : (DGEQ, 2006, p. 174) Annexe X.3.2, source : (ISO/IEC, 2009a, p. 9), (ISO/IEC, 2009i, p. 14)
4) La SA s'applique autant à l'application elle-même qu'à ses facteurs environnants qui ont un impact sur sa sécurité, tels que l'information, les personnes, les processus et ses trois contextes	Section 3.6.1, Tableau 3.2, source : (Poulin, 2002, pp. 44-46) Annexe X.1.2, source : (Poulin, 2006b, p. 8) Annexe X.2.2, source : (Poulin, 2007b, p. 5) Annexe X.3.2, source : (Poulin et Guay, 2008, p. 2)
❖ Problématiques répondues par la portée du modèle SA	Section 3.4, problématiques : P01, P02 et P12

Le Tableau 7.3 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les principes du modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

[23] L'environnement d'une application inclut son contexte d'affaires, son contexte technologique, son contexte juridique, ainsi que les fonctionnalités et les spécifications de l'application en vigueur durant tout son cycle de vie de sécurité.

Tableau 7.3 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Principes

Modèle final Principes	**Références aux contributions du chercheur**
1) La sécurité est dépendante du contexte	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006a, p. 10) Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 3.6.4, Tableau 3.5, source : (DGEQ, 2006, p. 174) Section 3.6.4, Tableau 3.5, source : (Poulin, 2006c, pp. 6-9) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9) Annexe X.3.2, source : (Poulin, 2009e, p. 10)
2) La sécurité est une exigence	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 3.6.4, Tableau 3.5, source : (DGEQ, 2006, p. 174)
3) La SA doit pouvoir être démontrée	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 0, Tableau 3.4, source : (ISACA®, 2013a) et (ITGI, 2007, p. 14)
4) Investir le montant approprié pour la SA	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006c, p. 6) Annexe X.3.2, source : (Poulin, 2009e, p. 10)
❖ Problématiques répondues par les principes proposés dans le modèle SA	Section 3.4, problématiques : P02, P03 et P12

Le Tableau 7.4 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les définitions des termes du modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

Tableau 7.4 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Termes

Modèle final Termes	**Références aux contributions du chercheur**
1) Application	Annexe X.3.2, source : (Poulin et Guay, 2008, p. 2), (Poulin, 2009e, p. 3)
2) Application sécuritaire	Annexe X.1.2, source : (Poulin, 2006b, p. 7) Annexe X.2.2, source : (Poulin, 2007b, p. 8). Annexe X.3.2, source : (Poulin et Guay, 2008, p. 10), (Poulin, 2009e, p. 15)
3) Niveau de confiance - cible (ciblé), et - actuel (mesuré)	Section 3.6.1, Tableau 3.2, source : (Poulin, 2002, pp. 8-10) Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Annexe X.1.2, source : (Poulin, 2006b, p. 5) Annexe X.2.2, source : (Poulin, 2007b, p. 5)

Tableau 7.4 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Termes (suite)

Modèle final Termes	**Références aux contributions du chercheur**
4) CSA	Section 0, Tableau 3.4, source : ((ISC)², 2013c) Annexe X.3.2, source : (Poulin et Guay, 2008, pp. 14-15), (ISO/IEC, 2008a, p. 28), (ISO/IEC, 2009a, p. 24), (Poulin, 2009e, p. 17)
5) CNO	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 25) Section 0, Tableau 3.4, source : ((ISC)², 2013a)
6) CNA	Annexe X.2.2, source : (Poulin, 2007b, pp. 38-42)
❖ Problématiques répondues par les termes proposés dans le modèle SA	Section 3.4, problématiques : P05, P07 et P06

Le Tableau 7.5 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les concepts amenés par le modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

Tableau 7.5 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Concepts

Éléments du modèle initial Concepts	**Références à la contribution du chercheur**
1) Vision globale et les quatre domaines d'interventions liés à la sécurité de l'application - Gouvernance, - infrastructure TI, - réalisation de l'application, - vérification et contrôle,	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006a, pp. 4-5) Annexe X.1.2, source : (Poulin, 2006b, p. 6) Annexe X.3.2, source : (Poulin et Guay, 2008, p. 3)
2) La prise en compte simultanée des quatre domaines d'interventions pour protéger l'information liée à l'utilisation d'une application	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Annexe X.1.2, source : (Poulin, 2006b, p. 8) Annexe X.3.2, source : (Poulin et Guay, 2008, p. 2)

Tableau 7.5 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Concepts (suite)

Éléments du modèle initial Concepts	**Références à la contribution du chercheur**
3) L'environnement de l'application inclut : - le contexte d'affaires,[24] - le contexte juridique, - le contexte technologique, - les fonctionnalités et les spécifications de l'application en vigueur durant tout le cycle de vie.	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006a, p. 10) Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 3.6.4, Tableau 3.5, source : (DGEQ, 2006, p. 174) Section 3.6.4, Tableau 3.5, source : (Poulin, 2006c, pp. 6-9) Annexe X.1.2, source : (Poulin, 2006b, p. 5) Annexe X.2.2, source : (Poulin, 2007b, pp. 5-6)
4) La source d'un risque de sécurité peut être une personne, un processus ou une technologie appartenant à l'un des trois contextes de l'application	Section 3.6.2, Tableau 3.3, source : (Andress, 2003, p. 5) Annexe X.2.2, source : (Poulin, 2007b, p. 6)
5) Pouvoir intégrer des contrôles de sécurité dans toutes les activités présentes dans les phases du cycle de vie de la SA	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 39) Annexe X.2.2, source : (Poulin, 2007b, pp. 26 - 36) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9)
6) Niveau de confiance de l'application - cible (ciblé) - actuel (mesuré)	Section 3.6.1, Tableau 3.2, source : (Poulin, 2002, pp. 8-10) Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Annexe X.1.2, source : (Poulin, 2006b, p. 5)
7) L'exigence de preuves démontrant l'atteinte du niveau de confiance ciblé	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 0, Tableau 3.4, source : (ISACA®, 2013a) et (ITGI, 2007, p. 14) Annexe X.1.2, source : (Poulin, 2006b, p. 7)
8) Application sécuritaire	Section 0, Tableau 3.4, source : (ISACA®, 2013b) Section 0, Tableau 3.4, source : ((ISC)², 2013c) Annexe X.1.2, source : (Poulin, 2006b, p. 7) Annexe X.2.2, source : (Poulin, 2007b, pp. 7-8)
9) CNO	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 25) Section 0, Tableau 3.4, source : ((ISC)², 2013a) Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9) Annexe X.4.2, source : (ISO/IEC, 2009b, p. 13)
10) CNA	Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9)

[24] Qui inclut les personnes, les processus et l'information.

Tableau 7.5 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Concepts (suite)

Éléments du modèle initial Concepts	**Références à la contribution du chercheur**
11) CNA	Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9)
12) Pour tous les acteurs ayant accès aux informations sensibles, la nécessité d'identifier les qualifications requises pour pouvoir assumer les responsabilités associées à leur rôle respectif	Section 3.6.2, Tableau 3.3, source : (Andress, 2003, p. 5) Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 21) Section 3.6.4, Tableau 3.5, source : (DGEQ, 2006, p. 182) et (Poulin, 2006c, p. 10)
13) Pouvoir démontrer qu'une application a atteint et maintient le niveau de confiance ciblé	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14)
❖ Problématiques répondues par les concepts proposés dans le modèle SA	Section 3.4, problématiques : P01, P02, P03, P12, P15 et P16

Le Tableau 7.6 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les composants du modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

Tableau 7.6 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Composants

Modèle final Composants	**Références à la contribution du chercheur**
1) Le CNO	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 25) Annexe X.1.2, source : (Poulin, 2006b, p. 12) Annexe X.2.2, source : (Poulin, 2007b, pp. 38-42) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9), (Poulin et Guay, 2008, p. 19)
2) Le CNA	Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9)

Tableau 7.6 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Composants (suite)

Modèle final Composants	**Références à la contribution du chercheur**
3) Le modèle de référence du cycle de vie de la sécurité d'une application, incluant la liste des activités et rôles impliqués	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 39) Section 0, Tableau 3.4, source : ((ISC)², 2013c), ((ISC)², 2013b) Annexe X.1.2, source : (Poulin, 2006b, pp. 16-27) Annexe X.2.2, source : (Poulin, 2007b, p. 22) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9), (Poulin et Guay, 2008, pp. 11-12)
4) Le répertoire des rôles, responsabilités et qualifications	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 21)
5) Les exigences de sécurité	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 3.6.4, Tableau 3.5, source : (DGEQ, 2006, p. 174)
6) L'information classifiée liée à l'utilisation de l'application	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14)
7) La bibliothèque de CSA	Section 3.6.4, Tableau 3.5, source : (Poulin, 2006c, p. 113) Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9), (Poulin et Guay, 2008, p. 18)
8) La matrice de traçabilité	Section 6.2.4, source : ÉC, juin 2011.
9) Le CSA - niveau de confiance, - exigence de sécurité, - activité de sécurité : qui, quoi, où, quand, comment et combien, - activité de vérification : qui, quoi, où, quand, comment et combien	Annexe X.2.2, source : (Poulin, 2007b, pp. 23 - 25) Annexe X.3.2, source : (ISO/IEC, 2007c, p. 9)
10) Vision globale des éléments clés du modèle SA	Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42)
11) Schémas XML décrivant - le CSA, - le cycle de vie générique de la SA, incluant les stages, les activités et les rôles	Annexe X.3.2, source : (ISO/IEC, 2009a, pp. 6-7) Annexe XIII.12.3, source : (ISO/IEC, 2013a; 2015), en cours de développement
❖ Problématiques répondues par les composants proposés dans le modèle SA	Section 3.4, problématiques : P01, P02, P03, P04, P08, P09, P13, P14, P15 et P16

Le Tableau 7.7 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les groupes et les rôles des acteurs définis dans le modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

Tableau 7.7 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Groupes et rôles

Modèle final Groupes et rôles	**Références à la contribution du chercheur**
1) Groupes : comité du CNO, direction de l'organisation, équipe de projet, équipe de vérification, équipe des opérations	Annexe X.3.2, source : (Poulin et Guay, 2008, p. 13)
2) Rôles : acheteur, architecte d'application, architecte de sécurité, architecte technologique, vérificateur / auditeur, chef de la sécurité, chef de projet, détenteur / propriétaire de l'application, développeur, équipe de l'infrastructure TI, expert des lois et règlements, expert du domaine, formateur, fournisseur, gestionnaire, opérateur d'application, testeur, utilisateur	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 21) Annexe X.1.2, source : (Poulin, 2006b) Annexe X.3.2, source : (Poulin et Guay, 2008, p. 13)
❖ Problématiques répondues par les groupes et rôles proposés dans le modèle SA	Section 3.4, problématiques : P02 et P13

Le Tableau 7.8 présente les références aux documents contenant les contributions du chercheur qui ont servi à faire évoluer les processus du modèle SA, ainsi que les problématiques de sécurité répondues par ces derniers.

Tableau 7.8 Synthèse du modèle SA, des contributions du chercheur et des problématiques répondues – Processus

Modèle final Processus	**Références à la contribution du chercheur**
1) Gestion du CNO	Annexe X.3.2, source : (Poulin, 2009e, p. 24) Annexe X.4.2, source : (ISO/IEC, 2010b, p. 36)
a) Gérer le comité du CNO	Annexe X.3.2, source : (Poulin et Guay, 2008, pp. 16-17), (Poulin, 2009e, p. 16) Annexe X.4.2, source : (ISO/IEC, 2010b, p. 36)
b) Élaborer la SA dans le CNO c) Implémenter la SA dans le CNO d) Surveiller et réviser la SA dans l'organisation e) Améliorer de façon continue la SA dans l'organisation f) Auditer la SA dans le CNO	
2) Gestion des risques de la SA	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006c, p. 6) Section 0, Tableau 3.4, source : (ISACA®, 2013b) Section 0, Tableau 3.4, source : (ITIMF, 2013) Annexe X.3.2, source : (Poulin et Guay, 2008, p. 21)
3) Gestion de la SA	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006c, p. 6) Section 0, Tableau 3.4, source : (ISACA®, 2013b), ((ISC)², 2013c) Annexe X.3.2, source : (Poulin et Guay, 2008, pp. 20, 27), (ISO/IEC, 2008b, p. 6), (Poulin, 2009e, p. 16)
a) Identifier les besoins et l'environnement de l'application a) Évaluer les risques de sécurité amenés par l'application b) Créer et maintenir le CNA c) Réaliser et opérer l'application	
d) Vérifier la SA	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 0, Tableau 3.4, source : ((ISC)², 2013c), ((ISC)², 2013b) Annexe X.2.2, source : (Poulin, 2007b, pp. 38 - 42) Annexe X.3.2, source : (Poulin et Guay, 2008, p. 20)
4) Identification et classification des groupes d'information liés à l'utilisation d'une application	Section 3.6.2, Tableau 3.3, source : (Poulin et Guay, 2006b, p. 14) Section 3.6.4, Tableau 3.5, source : (Poulin, 2006a, p. 8) et (DGEQ, 2006, p. 177)
5) Audit et certification de la mise en œuvre du modèle SA	Section 3.6.4, Tableau 3.5, source : (Poulin, 2006a, p. 9)
a) Auditer et certifier une application	Annexe X.3.2, source : (Poulin, 2009e, p. 32)
b) Auditer et certifier un expert en SA	
❖ Problématiques répondues par les processus proposés dans le modèle SA	Section 3.4, problématiques : P01, P02, P04, P09, P10, P11, P12, P13, P14, P15 et P16

7.2 Atteintes des objectifs de recherche

Les sections 7.2.1 à 7.2.6 précisent la manière dont ont été atteints les six objectifs de recherche de cette thèse.

Rappelons ici que le terme « niveau de confiance » a été défini dans le modèle SA pour formaliser le concept de « niveau de sécurité ».

7.2.1 Premier objectif : développer un modèle SA qui répond aux critères du but de la recherche

Le but de cette recherche est de développer, de faire vérifier et de publier un modèle permettant à une organisation de mettre en place et de démontrer la sécurité d'une application, soit la protection des informations sensibles impliquées par son l'utilisation.

Ce but implique que :

1) Le modèle SA doit désigner les principaux groupes d'acteurs et cerner leurs besoins respectifs dans la mise en place de la sécurité d'une application.

   Ce critère a été atteint par l'identification des audiences visées ainsi que de leurs principaux besoins respectifs (*Voir* 5.5);

2) Le modèle SA doit pouvoir offrir les éléments permettant :
   a) de définir et d'identifier le contexte et l'environnement de la sécurité d'une application.
      Ce critère a été atteint par l'introduction dans le modèle :
      i) de l'énoncé des principes qui soutiennent la SA (*Voir* 5.7);
      ii) des concepts et des définitions d'application, d'environnement et d'application sécuritaires (*Voir* l'appendice A – ANNEXE XII.2);
      iii) des composants définissant les contextes de l'application (*Voir* l'appendice A – ANNEXES XIII.3 à XIII.5); et

iv) du processus Identifier les besoins et l'environnement de l'application (*Voir* l'appendice A – ANNEXE XIV.3.3);

b) d'identifier et de catégoriser l'information sensible impliquée par une application.
Ce critère a été atteint par l'introduction dans le modèle :
   i) des groupes d'informations liées à la sécurité d'une application (*Voir* l'appendice A – ANNEXE XII.2.7); et
   ii) de l'activité d'identification et de catégorisation de l'information concernant l'application (*Voir* l'appendice A – ANNEXE XIV.2.2, 2a);

c) d'identifier le niveau de sécurité requis par une application.
Ce critère a été atteint par l'introduction dans le modèle :
   i) du concept de niveau de confiance, qui formalise le niveau de SA en lui donnant une valeur mesurable, permettant d'évaluer, de mesurer et de vérifier l'atteinte d'un niveau de confiance envers une application (*Voir* l'appendice A – ANNEXE XII.2.12); et
   ii) du processus d'analyse de risques de SA (*Voir* l'appendice A – ANNEXE XIV.2.2);

d) de gérer et d'assurer l'intégration et la réalisation des activités de sécurité et des activités de vérification tout le long du cycle de vie d'une application, en fonction du niveau de sécurité requis, quels que soient les processus en place dans l'organisation.
Ce critère a été atteint par l'introduction dans le modèle :
   i) de la définition du concept de niveau de confiance (*Voir* l'appendice A – ANNEXE XII.2.12);
   ii) de l'assignation du niveau de confiance cible à l'application (*Voir* l'appendice A – ANNEXE XIV.2.2.2);
   iii) du MRCVSA (*Voir* l'appendice A – ANNEXE XIII.12);
   iv) de l'attribut « quand » des activités du CSA (*Voir* l'appendice A – ANNEXE XIII.9.2); et
   v) du processus d'arrimage des activités des processus des modèles utilisés dans l'organisation avec le MRCVSA (*Voir* l'appendice A – ANNEXE XIV.1.4.2);

e) de vérifier et de gérer la mise en place et le bon fonctionnement des contrôles de sécurité.

   Ce critère a été atteint par l'introduction dans le modèle :

   i) de la définition de la bibliothèque de CSA de l'organisation (*Voir* l'appendice A – ANNEXE XIII.10);
   ii) de l'introduction de l'activité de vérification de la mesure dans le CSA (*Voir* l'appendice A – ANNEXE XIII.9.2);
   iii) du processus Vérifier la sécurité de l'application (*Voir* l'appendice A – ANNEXE XIV.3.7);
   iv) du processus Auditer et certifier la sécurité d'une application (*Voir* l'appendice A – ANNEXE XIV.4.2);

f) de mesurer, de vérifier et de valider l'atteinte du niveau de sécurité visé, à n'importe quel moment du cycle de vie de l'application.

   Ce critère a été atteint par l'introduction dans le modèle :

   i) du processus Vérifier la sécurité de l'application (*Voir* l'appendice A – ANNEXE XIV.3.7); et
   ii) du processus Auditer et certifier la sécurité d'une application (*Voir* l'appendice A – ANNEXE XIV.4.2);

g) de fournir les preuves démontrant que le niveau de sécurité visé pour une application a été atteint et est maintenu.

   Ce critère a été atteint par l'introduction dans le modèle :

   i) de la définition du concept de niveau de confiance (*Voir* l'appendice A – ANNEXE XII.2.12);
   ii) de l'attribut « quoi » des activités du CSA (*Voir* l'appendice A – ANNEXE XIII.9.2);
   iii) du processus Vérifier la sécurité de l'application (*Voir* l'appendice A – ANNEXE XIV.3.7); et
   iv) du processus Auditer et certifier la sécurité d'une application (*Voir* l'appendice A – ANNEXE XIV.4.2);

h) de rendre répétables l'implantation et la vérification du niveau de confiance mesuré.
   Ce critère a été atteint par l'introduction dans le modèle :
   i) des attributs « qui », « quoi », « où », « quand » et « comment » dans les activités du CSA (*Voir* l'appendice A – ANNEXE XIII.9.2);
   ii) du processus Vérifier la sécurité de l'application (*Voir* l'appendice A – ANNEXE XIV.3.7); et
   iii) du processus Auditer et certifier la sécurité d'une application (*Voir* l'appendice A – ANNEXE XIV.4.2);

i) de pouvoir soutenir le système de gestion de la sécurité de l'information d'ISO/IEC 27001 (ISO/IEC, 2005d).
   Ce critère a été atteint par l'introduction dans le modèle :
   i) de l'étape d'identification des sources des principes et des processus devant être pris en compte et intégrés au présent modèle (*Voir* l'appendice A – ANNEXE *XXI.1*);
   ii) du comité de gestion du CNO, dont l'un des objectifs est d'assurer le soutien du SGSI (*Voir* l'appendice A – ANNEXE XIII.1.1); et
   iii) du CNO, dont l'un des objectifs est d'opérationnaliser le soutien de l'architecture d'entreprise et du SGSI (*Voir* l'appendice A – ANNEXE XIII.2.1);

j) de pouvoir soutenir les principes du modèle de maturité intégré du SEI (CMMI, 2006).
   Ce critère a été atteint par l'introduction dans le modèle :
   i) de l'encadrement de la conception, du développement, de la vérification et de la validation d'un CSA par le processus de Gestion du CNO (*Voir* l'appendice A – ANNEXE XIV.1);
   ii) de l'encadrement de l'implémentation et de la vérification d'un CSA par le processus de Gestion de la SA (*Voir* l'appendice A – ANNEXE XIV.3); et
   iii) de la définition formelle du CSA (*Voir* l'appendice A – ANNEXE XIII.9.1);

k) de pouvoir soutenir les principes d'assurances en génie logiciel d'ISO/IEC 15026 (ISO/IEC, 2009j).

   Ce critère a été atteint par l'introduction dans le modèle :

   i) de l'étape d'identification des sources des principes et processus devant être pris en compte et intégrés au présent modèle (*Voir* l'appendice A – ANNEXE *XXI.2*); et

   ii) de l'encadrement de la conception, du développement, de la vérification et de la validation d'un CSA par le processus de Gestion du CNO afin de s'assurer que les résultats produits par les CSA auront préalablement été approuvés par l'organisation comme des preuves valides soutenant l'affirmation de diminution du risque de sécurité à un niveau considéré acceptable (*Voir* l'appendice A – ANNEXE XIV.1).

Finalement, le Tableau 7.1 regroupe les principaux éléments du modèle SA et associe à chacun de ces groupes les problématiques auxquelles ils répondent.

Satisfaire à tous les critères permet de valider et d'affirmer l'atteinte de ce premier objectif de recherche.

7.2.2 Deuxième objectif : s'assurer que le modèle permette d'intégrer des contrôles de sécurité durant tout le cycle de vie d'une application

Cet objectif a été réalisé dès l'atteinte du critère 2)d) du premier objectif présenté ci-dessus (*Voir* 7.2.1).

7.2.3 Troisième objectif : munir le modèle SA de mécanismes permettant de fournir à l'organisation les preuves que son application a atteint et maintient le niveau de confiance préalablement ciblé, et ce, en fonction de son contexte d'utilisation spécifique

Cet objectif a été atteint par l'introduction dans le modèle :

1) Des principes : « La SA doit être gérée », « La SA est dépendante de l'environnement » et « La SA doit pouvoir être démontrée » (*Voir* 5.7.1, 5.7.3 et 5.7.5);
2) De la définition de la bibliothèque de CSA de l'organisation (*Voir* l'appendice A – ANNEXE XIII.10);
3) De l'introduction de l'activité de vérification de la mesure dans le CSA (*Voir* l'appendice A – ANNEXE XIII.9.2);
4) Du processus Gestion des risques de la sécurité d'une application (*Voir* l'appendice A – ANNEXE XIV.2);
5) Du processus Vérifier la sécurité de l'application (*Voir* l'appendice A – ANNEXE XIV.3.7); et
6) Du processus Auditer et certifier la sécurité d'une application (*Voir* l'appendice A – ANNEXE XIV.4.2).

Utilisés ensemble, ces éléments permettent de fournir les preuves attendues, nécessaires et vérifiables pour affirmer et démontrer qu'une application a atteint et maintient un niveau de confiance.

7.2.4 Quatrième objectif : faire vérifier le modèle SA par plusieurs vérificateurs experts, délégués par différentes instances nationales compétentes

Cet objectif a été atteint via l'utilisation du processus d'édition d'ISO dans le projet 27034 du SC27, sous-comité regroupant des experts mondiaux en sécurité de l'information. À la publication de la première partie de la norme, ce projet a regroupé des vérificateurs experts de plus de 46 pays (*Voir* l'ANNEXE I, Tableau-A I-1) dont 18 ont fourni plus de 1 140 commentaires et contributions (*Voir* l'appendice A – ANNEXE XIX, Tableau-A XIX-1).

7.2.5 Cinquième objectif : faire approuver le modèle par une organisation internationale de normalisation

Cet objectif a été atteint par la soumission du modèle SA aux processus d'édition et de distribution d'un projet de norme ISO qui a mené à la publication de la norme ISO 27034 – *Application Security, part 1 : Overview and concepts*. Cette publication a été approuvée par 96 % des pays participants (*Voir* l'ANNEXE I, Tableau-A I-1).

7.2.6 Sixième objectif : rendre le modèle SA accessible à toute organisation désirant mettre en place ou vérifier la sécurité d'applications

Cet objectif a été atteint par l'approbation finale et la publication de la norme ISO 27034 – *Application Security* par ISO. Le modèle SA est maintenant accessible à tous, via le site d'ISO[25], ainsi que sur les sites des organisations normatives nationales de certains pays dont celui du Canada[26], de l'Allemagne[27] de la France[28] et des États-Unis[29], permettant ainsi l'atteinte de cet objectif.

---

[25] Site web d'ISO : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378

[26] Site web du *Canadian Standards Association (CSA)* : http://shop.csa.ca/en/canada/information-technology/cancsa-isoiec-27034-112/invt/27034692012/

[27] Site web du *DIN Standards Committee on Information Technology and Applications (NIA)* : http://www.nia.din.de/cmd?artid=148454745&subcommitteeid=146321440&bcrumblevel=1&contextid=nia&level=tpl-art-detailansicht&committeeid=54738935&languageid=en

[28] Site web de l'Association française de Normalisation (AFNOR) : http://www.boutique.afnor.org/norme/iso-cei-27034-12011/technologies-de-l-information-techniques-de-securite-securite-des-applications-partie-1-apercu-general-et-concepts/article/765719/xs117588

[29] Site web de l'American National Standard Institute (ANSI) : http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC+27034-1%3A2011

CHAPITRE 8

CONCLUSION

Ce dernier chapitre met en lumière les résultats de cette recherche (8.1), les trois éléments soutenant la crédibilité de l'approche d'intégration des éléments de sécurité dans le modèle SA (8.2), ainsi que les limites du modèle SA 8.3. On y aura aussi un aperçu des impacts qui ont déjà été constatés par l'industrie et les utilisateurs du modèle SA (8.4). Finalement, nous présentons un aperçu de nos travaux futurs (8.5) dont les objectifs seront, entre autres, de réaliser une certification de SA reconnue, créer des outils d'implantation et favoriser l'intégration de ce modèle dans les organisations à l'échelle internationale.

8.1 Résultats de la recherche

Ce travail de recherche visait à développer une approche globale d'intégration des éléments de sécurité dans le cycle de vie des applications et des systèmes d'information. C'est cette approche qui a permis de concevoir le modèle SA et de le faire valider par des experts en sécurité de l'information de plus de 46 pays. Ce nouveau modèle SA fournit, à l'organisation qui l'utilise, les preuves nécessaires garantissant la répétabilité des résultats et soutenant l'affirmation que ses applications sont sécuritaires. En outre, il propose l'intégration d'activités de sécurité vérifiables tout au long du cycle de vie des applications, et ce, même si les organisations qui l'adopteront ont déjà des processus établis qu'ils n'auront pas à modifier, que ce soit pour les activités de développement ou de maintenance. Le modèle SA préconise une évolution progressive de la maturité de l'organisation en fonction de sa ligne d'affaires et de ses besoins de sécurité.

En résumé, le modèle SA propose :

1) Une vision globale de la SA;

2) Une définition de la portée de la SA et une définition claire de ce qu'est une application sécuritaire;
3) Un modèle de référence du cycle de vie de la SA, afin d'offrir une compréhension globale et commune de l'ensemble des activités, des acteurs et des interdépendances qui s'y rapportent;
4) Les sources et une démarche permettant l'identification des exigences de SA;
5) Une démarche d'évaluation de la SA;
6) Un processus permettant la vérification des éléments de SA, en fonction des besoins de sécurité de l'organisation;
7) Des mécanismes permettant d'assigner aux principaux rôles requis pour définir, gérer, réaliser et vérifier les activités de SA, les qualifications requises par chacune de ces responsabilités;
8) Une méthode et un cadre normatif de SA qui permet d'évaluer, de développer, de valider et de vérifier les activités et contrôles de sécurité jugés prioritaires et de les intégrer directement dans les processus existants de l'organisation. Ce cadre normatif pourra aussi être utilisé pour aider l'organisation à identifier les nouveaux processus qui devraient être ajoutés à ceux déjà en place. Ce cadre normatif peut aussi servir à normaliser les activités et les contrôles de sécurité à l'intérieur de tous les projets d'applications de l'organisation;
9) Une méthode et un cadre normatif de SA qui permet de développer, valider et vérifier les activités de sécurité jugées prioritaires et de les intégrer directement dans l'application ou le produit développé. Ce cadre normatif pourra aussi être utilisé pour aider l'organisation à identifier les nouveaux contrôles de sécurité devant être intégrés à l'intérieur des applications et qui devraient être ajoutés à ceux existants. Finalement, il pourra servir à normaliser ses activités et contrôles de sécurité à l'intérieur de tous ses projets d'applications.

Le modèle SA facilite :

1) L'arrimage entre les approches, méthodes et outils existants pour mettre en place la SA;

2) L'intégration des contrôles de SA à l'intérieur des méthodes et de bonnes pratiques existantes reconnues de génie logiciel, afin de favoriser l'utilisation de ces pratiques recommandées et de minimiser la résistance aux changements des membres des équipes de développement d'applications, entre les approches, méthodes et outils existants pour mettre en place la SA.

8.2 Éléments soutenant la crédibilité du modèle SA

Trois éléments permettent de soutenir la crédibilité du modèle SA, soit :

1) La méthode Delphi qui a été adaptée au processus de gestion de projet ISO et a rigoureusement été suivie pour valider le modèle SA. Cette validation a été effectuée durant les 11 cycles Delphi qu'a duré ce projet de recherche, par des experts en sécurité de l'information provenant de plus de 46[30] pays et de 4 organisations[31] (*Voir* 6.1 et l'appendice A – ANNEXE X);
2) Cette recherche a bénéficié d'un apport considérable de concepts et d'approches provenant de plusieurs ouvrages et articles scientifiques, pouvant être appliqués à la SA (*Voir* 3.3 et l'appendice A – ANNEXE VI);
3) Les processus de validation, de vérification et d'approbation intégrés au modèle SA (*Voir* l'appendice A – ANNEXE XIV.1, Figure-A XIV-3);
4) L'arrimage du modèle SA à la norme ISO 27001 *Information security management systems – Requirements* (*Voir* l'appendice A – ANNEXE XIV.1, Figure-A XIV-4).

---

[30] Selon les rapports de résultats de votes inclus dans certaines versions du document de travail du projet ISO *27034 – Application Security*, le nombre de pays participant aux travaux du SC27 de l'organisation ISO est passé de 35 pays en 2006, à 46 pays en 2011.

[31] Les quatre organisations contactées pour participer à la vérification du modèle de la SA sont : ISO/JTC1/SC7, ISO/JTC1/SC22, ITU-T/SG17 et Networked European Software and Services Initiative (NESSI).

8.2.1.1 Crédibilité amenée par le processus de validation du modèle

L'ISO possède un processus d'édition et de révision de contenu de normes qui est utilisé par tous les sous-comités de l'organisation. Ce processus, auquel participent des vérificateurs experts provenant de plus de 46 pays, produit des normes qui sont reconnues internationalement.

La première version des concepts, des principes et des éléments du modèle SA a été introduite dans le projet ISO 27034 – *Application Security*, par le chercheur en octobre 2006, lors d'une rencontre du SC27 qui est responsable de la publication des normes ISO dans le domaine de la SA.

Tout au long de la recherche doctorale, le modèle a été vérifié par les délégués des pays participants à tous les six mois, et durant six années consécutives. Durant cette période, l'énoncé de chaque principe, le contenu de chaque définition, de chaque processus, et de chaque composant a été abordé, vérifié, discuté, révisé puis approuvé. Ces rencontres regroupaient des intervenants délégués par, notamment : le Canada, les États-Unis, le Japon, l'Afrique du Sud, le Royaume-Uni, et la France. Plus de 1 140 commentaires ont été produits et résolus et six processus de vote ont été réalisés avec les pays participants qui pouvaient signifier leurs insatisfactions en votant contre la continuation du projet. Le vote final autorisant la publication de la norme ISO 27034 qui présente les résultats des travaux de cette recherche a reçu un appui de 96 % des pays participants (*Voir* 6.1 et l'appendice A – ANNEXE XIX.2).

8.2.1.2 Crédibilité amenée par les processus de validation, de vérification et d'approbation intégrés au modèle

Parce que tous les éléments du modèle ont été validés, vérifiés et approuvés par l'organisation, que cette dernière s'est dotée d'une bibliothèque de CSA classée par niveaux de confiance, et que chacun d'eux contient son propre processus de vérification de ses mesures, la mise en place du modèle SA permet de fournir des résultats attendus mesurables

et répétables provenant des CSA requis pour confirmer l'atteinte du niveau de sécurité ciblé, justifiant ainsi la confiance d'une organisation dans la protection adéquate de ses applications.

8.2.1.3 Crédibilité amenée par l'arrimage du modèle à la norme ISO 27001

Finalement, ayant été développé pour répondre autant aux besoins techniques qu'organisationnels, le modèle SA peut soutenir le SGSI d'une organisation (ISO/IEC, 2013b) en apportant à ses gestionnaires les preuves démontrant que les applications, qui ont été identifiées par le SGSI comme étant des actifs informationnels sensibles, possèdent toutes un CNA qui définit les CSA requis à l'atteinte du niveau de confiance ciblé. Ces CSA sont en mesure de fournir les preuves, requises par l'organisation, démontrant que les applications devant être sécurisées ont été adéquatement protégées et que les risques de sécurité les concernant ont tous été ramenés à un niveau acceptable approuvé (*Voir* l'appendice A – ANNEXE XIV.1.1).

8.3 Limites du modèle SA

Le modèle SA que nous avons développé peut être adapté et s'appliquer à tout type d'application, quel que soit son contexte technologique, son contexte d'affaires ou son contexte juridique, et être utilisable autant par de très petites que de grandes organisations.

Par contre, le modèle SA ne fournit aucun contrôle de sécurité des applications (CSA) et n'identifie pas d'éléments obligatoires à mettre en place. Il ne fournit que les structures du CSA et du CNO ainsi que les processus nécessaires à leur développement, à leur mise en place et à leur maintenance. Une organisation qui voudra utiliser ce modèle devra identifier et définir elle-même les éléments qu'elle désire implémenter dans son CNO, ainsi que ses niveaux de confiances et les contrôles qui seront conservés dans sa bibliothèque de CSA.

8.4 Impacts sur l'industrie

L'impact de ces travaux de recherche peut être perçu dans l'évaluation de la SA de deux grands groupes d'organisations : celles qui développent des applications et celles qui les utilisent. Tandis que les organisations du premier groupe désirent développer et produire des applications sécuritaires, les organisations du deuxième groupe désirent s'assurer que leurs applications sont capables de protéger adéquatement les informations impliquées par leurs utilisations.

Sachant que cet impact se fera de manière graduelle, on peut classer les événements qui aideront à les détecter en trois niveaux progressifs d'impacts, soit :

1) La prise de connaissance du modèle SA
   Les événements seront liés à ce niveau lorsqu'une organisation aura acquis la norme ISO 27034, dans l'intention d'en prendre connaissance.

2) L'adoption du modèle SA
   Une organisation qui juge que le modèle SA apporte une vision et une approche globales nouvelles qui n'étaient pas disponibles avant la publication du modèle et qui vont l'aider à protéger ses applications. Ces organisations sont communément identifiées comme étant des « adopteurs précoces » d'idées novatrices. Les événements liés à ce niveau sont :
   a) l'acquisition de la norme ISO 27034;
   b) l'ajustement de processus existants en fonction du modèle SA;
   c) la mise en place de processus du modèle;
   d) le développement d'un service en utilisant des éléments du modèle; ou
   e) l'annonce de leur nouvelle orientation en SA, selon la norme ISO 27034.

3) L'utilisation du modèle pour soutenir l'affirmation d'amélioration de la sécurité.
   Les événements seront liés à ce niveau lorsqu'une organisation aura acquis la norme ISO 27034, qu'elle aura décidé d'adapter certains de ses processus, et qu'elle affirmera offrir

un service ou une application sécuritaire, en utilisant les éléments du modèle pour soutenir son affirmation.

La norme ISO 27034 – *Application security – Part 1: Overview and concepts*, qui est basée sur le modèle SA, a été publiée par ISO, le 15 novembre 2011 (ISO/IEC, 2011d).

La section suivante présente les principaux éléments qui ont été portés à notre connaissance.

8.4.1 Événements et constats d'adoption du modèle SA par l'industrie

Cette section présente, par ordre chronologique, les principaux événements qui sont survenus depuis la publication du modèle SA par ISO. La visibilité et la crédibilité donnée au modèle par la publication de la première partie de la norme ISO 27034 a tout de suite attiré l'attention de l'industrie. Son adoption rapide, illustrée dans les prochaines sous-sections, dès la première année de sa publication, semble démontrer que le modèle répond à des besoins en SA qui n'étaient pas nécessairement comblés par les modèles et outils disponibles pour l'industrie, et laisse présager les impacts positifs que ce modèle SA pourra avoir pour cette dernière.

Nov. 2001 Utilisation du modèle SA : acquisition et utilisation de la norme ISO 27034-1 par l'institution financière Mouvement Desjardins, et réalisation d'un projet de SA sensible de l'organisation basé sur le modèle. La phase 1 de ce projet consistait à développer une base de connaissance de contrôles (Sinning, 2011, pp. 4, 9) et à intégrer les éléments du modèle SA aux processus et outils utilisés lors du développement et de la maintenance de l'organisation (Sinning, 2011, pp. 6, 8), afin d'harmoniser l'intégration et la vérification d'éléments de sécurité à travers l'organisation.

Déc. 2011 Utilisation du modèle SA : acquisition de la norme 27034-1 et annonce par l'entreprise de consultation de Québec nurun inc., d'une nouvelle offre de

service en SA dans le développement d'applications. L'organisation affirme sur leur site corporatif : « … nous proposons une approche de gestion intégrée de la sécurité applicative en nous basant sur la norme ISO/CÉI 27034. » (nurun, 2011).

Déc. 2011 Utilisation du modèle SA : acquisition de la norme ISO 27034-1 et annonce par l'entreprise de consultation en sécurité des TI In Fidem inc., de Montréal, d'une nouvelle offre de service en sécurité des applications. L'organisation affirme sur son site corporatif que « Nos experts conçoivent des stratégies et des solutions de sécurité applicatives simples, concrètes et efficaces en s'inspirant du modèle international ISO 27034:2011. Ces stratégies sont arrimées et adaptées à vos processus et méthodologies de développement. » (In Fidem, 2011).

Janv. 2012 Utilisation du modèle SA : acquisition et utilisation de la norme ISO 27034-1 par Élections Canada, pour intégrer la sécurité dans les processus d'acquisition, de déploiement et d'utilisation de l'application de votation par Internet au Canada.

L'utilisation d'éléments du modèle SA tels que le modèle de référence de la SA (Morin, 2012, p. 7), le principe que la sécurité doit être démontrée, l'intégration de la sécurité à l'intérieur du système ainsi que la définition d'une application de votation par Internet sécuritaire (Morin, 2012, p. 9). L'identification et l'ajustement des processus de l'organisation (Morin, 2012, pp. 10-11) ont directement impacté la portée, les processus et les résultats attendus par le projet.

Mai 2012 Prise de connaissance du modèle SA : présentation de la norme ISO 27034 par Tak Chijiiwa, consultant chez Security Compass, lors d'une rencontre du chapitre de Toronto d'OWAPS, qui a eu lieu le 10 mai 2012 (Chijiiwa, 2012).

Mai 2013 Prise de connaissance du modèle SA : support officiel de Reavis Consulting Group, LLC affirmant: « *This standard publication is a significant milestone in industry efforts to secure software and improve risk management through greater transparency. … An international standard such as ISO/IEC 27034-1 is becoming the baseline of practices for producing trusted software, and can help any organization demonstrate due care within their software development lifecycle.* » (Reavis, 2013, p. 2), et encourage les entreprises en TI, à se conformer à la norme 27034 « *… ISO/IEC 27034-1 is not about producing security overkill, but using risk-based methodologies to achieve a targeted level of trust. … We should encourage the entire industry – competitors, partners, and customers – to work together to assure that the principles of ISO/IEC 27034-1 and secure software development become as pervasive as software itself.* » (Reavis, 2013, p. 15).

Mai 2013 Prise de connaissance du modèle SA : l'équipe de rédaction du journal Web Mag Securs a présenté dans son article du 15 mai « Le développement sécurisé et le standard ISO 27034 aiment la SDC2013 » que « Durant le keynote d'ouverture, Microsoft, par la voix de Scott Charney VP du TrustWorthy Computing Group, a émis une déclaration de conformité au standard ISO 27034-1, mettant ainsi en lumière cette norme très récente et en faisant le thème central de cette édition 2013 de la SDC. ISO 27034-1 est le premier standard international à spécifiquement cibler les pratiques de développement sécurisé et l'infrastructure organisationnelle dans laquelle le code est développé. Il définit les concepts, frameworks et processus pour aider les organisations à intégrer la sécurité au cœur de leur cycle de vie des développements logiciels. » (Mag Securs, 2013).

Mai 2013 Adoption du modèle SA : Steve Lipner, directeur de la Security Engineering Strategy pour Microsoft annonce sur son Blogue corporatif, la conformité de Microsoft à la norme ISO 27034 : « *This morning Scott Charney announced in*

his keynote at the Security Development Conference that the Microsoft Security Development Lifecycle (SDL) meets or exceeds the guidance published in ISO/IEC 27034-1. » (Lipner, 2013).

Mai 2013 Prise de connaissance du modèle SA : dans leurs articles des 14 et 15 mai 2013, les magazines web ComputerWeekly et InfoSecurity rapportent les propos qu'à tenus M. Scott Charney, vice-président corporatif de Microsoft Trustworthy Computing, lors de sa présentation au Security Development Conference 2013 à San Francisco : « ...the standard provides a way to measure and improve security in a way that is scalable and repeatable. », « We encourage others in the software industry to conform and software users to ask for conformance as part of their procurement processes ». Puis, ComputerWeekly complète son article avec les propos de Steve Lipner « ... ISO 27034 applies to all software, not just security software. ... Microsoft Word, for example, is not a security product, but it still needs to be developed securely, so while the Common Criteria would not apply, ISO 27034 does, ... » (Ashford, 2013).

De son côté, rapportant le même événement, l'équipe d'InfoSecurity titre son article : « Microsoft Declares Conformity to ISO 27034-1 and Scott Charney Calls for Industry to Follow » et rapporte ses propos en écrivant que la norme 27034 « allows the even measurement of security. » (d'InfoSecurity, 2013).

Mai 2013 Prise de connaissance du modèle SA : le magazine Web The Age, rapporte dans son article du 15 mai 2013 « If it's worth coding, it's worth securing » les propos d'Howard Schmidt, présenté comme le « former cyber tsar to US President Barack Obama, now a cyber security consultant and board member of the Software Assurance Forum for Excellence in Code (SAFECode), a non-profit organisation aimed at making the internet safer. » « Schmidt is asking software writers, application developers and the organisations buying from

them to adhere to a relatively new security standard for software development, ISO 27034. » L'auteur complète en écrivant « The 18-month old standard is being pushed by large software makers in the US, including Microsoft, Adobe, Cisco and SafeCODE, as a way to ensure security is written into computer code at the initial stages, not as an afterthought. » (Timson, 2013).

Juin 2013 Acquisition de la norme ISO 27034 et implication de Schneider Electric dans le projet ISO 27034.

Sept. 2013 Utilisation du modèle SA : acquisition de la norme ISO 27034 et annonce par l'entreprise PECB (*Professional Evaluation and Certification Board*) du développement de trois nouvelles certifications professionnelles internationales basées sur le modèle, soit : « Certified ISO 27034 Foundation » (PECB, 2013a), « Certified ISO-27034 Lead implementer » (PECB, 2013c) et « Certified ISO 27034 Lead auditor » (PECB, 2013b).

Avril 2015 Arrimage au modèle SA : l'entreprise Microsoft corporation inc. a réalisé un projet pilote afin d'évaluer la faisabilité et l'impact de l'arrimage de la conversion des mesures de sécurité de son *Secure Development Lifecycle* (SDL v6.5) vers la structure XML des CSA proposée par le modèle SA.

Cette liste non exhaustive démontre l'intérêt grandissant d'organisations de différents secteurs de l'industrie à faire adopter et à utiliser le modèle SA produit par cette recherche. Le soutien ou la mise en place du modèle SA par des organisations comme Microsoft, EMC, Adobe, Cisco et SafeCODE aux États-Unis, Élections Canada, nurun, In Fidem, Security Compass, PECB, Cogentas et le Mouvement Desjardins au Canada, Altirian et l'université Tudor au Luxembourg, Orsys en France, laisse présager les impacts que le modèle aura sur l'industrie des TI et sur les organisations qui les utilisent.

8.5 Travaux futurs

Il sera utile, le moment venu, de définir un processus formel pour réaliser une certification de SA. Le défi à relever concernera la définition des contextes, des bibliothèques des CSA et des niveaux de confiance qui serviront de référence à une certification reconnue de la SA qui pourra tenir compte, notamment, de la valeur de l'application pour l'organisation, de ses spécifications et de son environnement d'exécution (contextes juridiques, d'affaires, technologiques).

L'annonce par OWASP, en janvier 2014, du démarrage d'un nouveau projet concernant la conversion des risques de sécurité présenté par le document « OWASP Top 10 Security Risks » en CSA, afin de les rendre disponibles aux entreprises désirant atténuer ces risques de sécurité de leurs applications en utilisant des éléments définis dans le modèle (Marcil, 2014).

Premiers contacts du gouvernement du Luxembourg et de l'entreprise Atirian signifiant leur intérêt au démarrage d'un laboratoire de tests de sécurité qui, notamment, utiliserait pour certifier la sécurité d'applications et d'entreprises du pays, le modèle SA proposé par la norme ISO 27034.

ANNEXE I

TABLEAUX ET FIGURES

I.1 Relations du modèle avec d'autres normes, méthodes, règlements et bonnes pratiques

La Figure-A I-1 positionne le modèle SA avec une sélection des principaux documents pouvant être utilisés dans les domaines des TI, durant le cycle de vie d'une application.

I.2 Activités clés de la méthodologie de recherche

La Figure-A I-2 présente un schéma sommaire global des activités clés réalisées durant ce projet de recherche, ainsi que les intrants et les extrants de chaque phase de recherche.

I.3 Résultats consolidés des commentaires traités par cycle et des votes d'approbation de passage aux stades suivants réalisés durant le projet

Le Tableau-A I-1 présente une synthèse du nombre des commentaires reçus par cycle Delphi, de la façon dont ces commentaires ont été traités, du nombre de pays inscrits au SC27 à la fin de chaque cycle, ainsi que du résultat de leur vote approuvant ou non la progression du document.

I.4 Processus de gestion des risques de SA proposé par la méthode ASIA

La Figure-A I-3 présente la méthode ASIA et son alignement avec la norme ISO 27005.

NOTE Le Tableau-A I-1 et les Figures-A I-2 et I-3 nécessitent l'utilisation de papier de format 11 x 17 pour pouvoir s'imprimer correctement.

La Figure-A I-1 positionne le modèle SA avec une sélection des principaux documents qui présentent des principes, des normes, des processus, des méthodes et de bonnes pratiques pouvant être utilisés dans les domaines des TI, durant le cycle de vie d'une application.

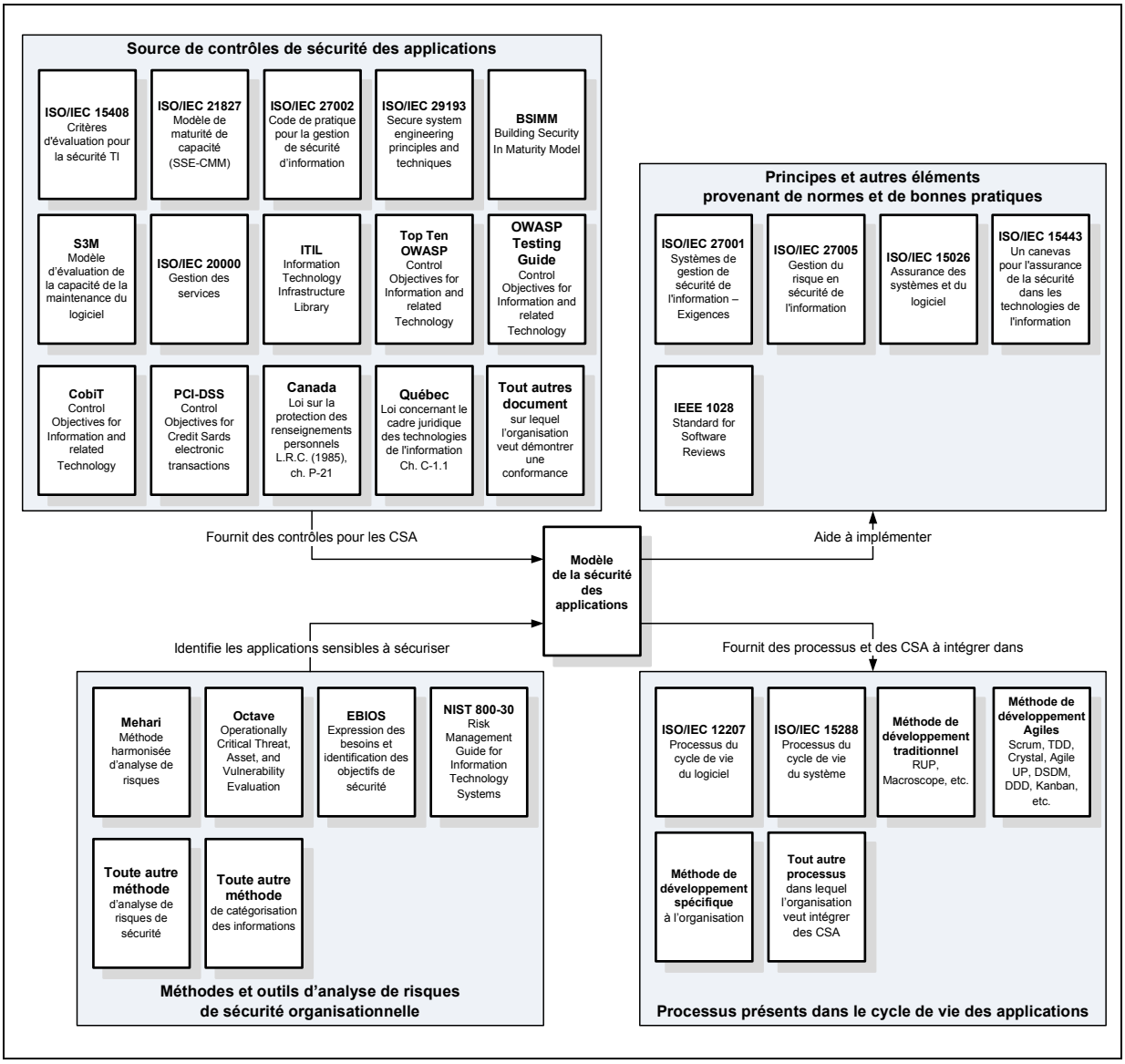


Figure-A I-1 Relations du modèle avec d'autres normes, méthodes, règlements et bonnes pratiques
Traduite et adaptée de (ISO/IEC, 2011d)

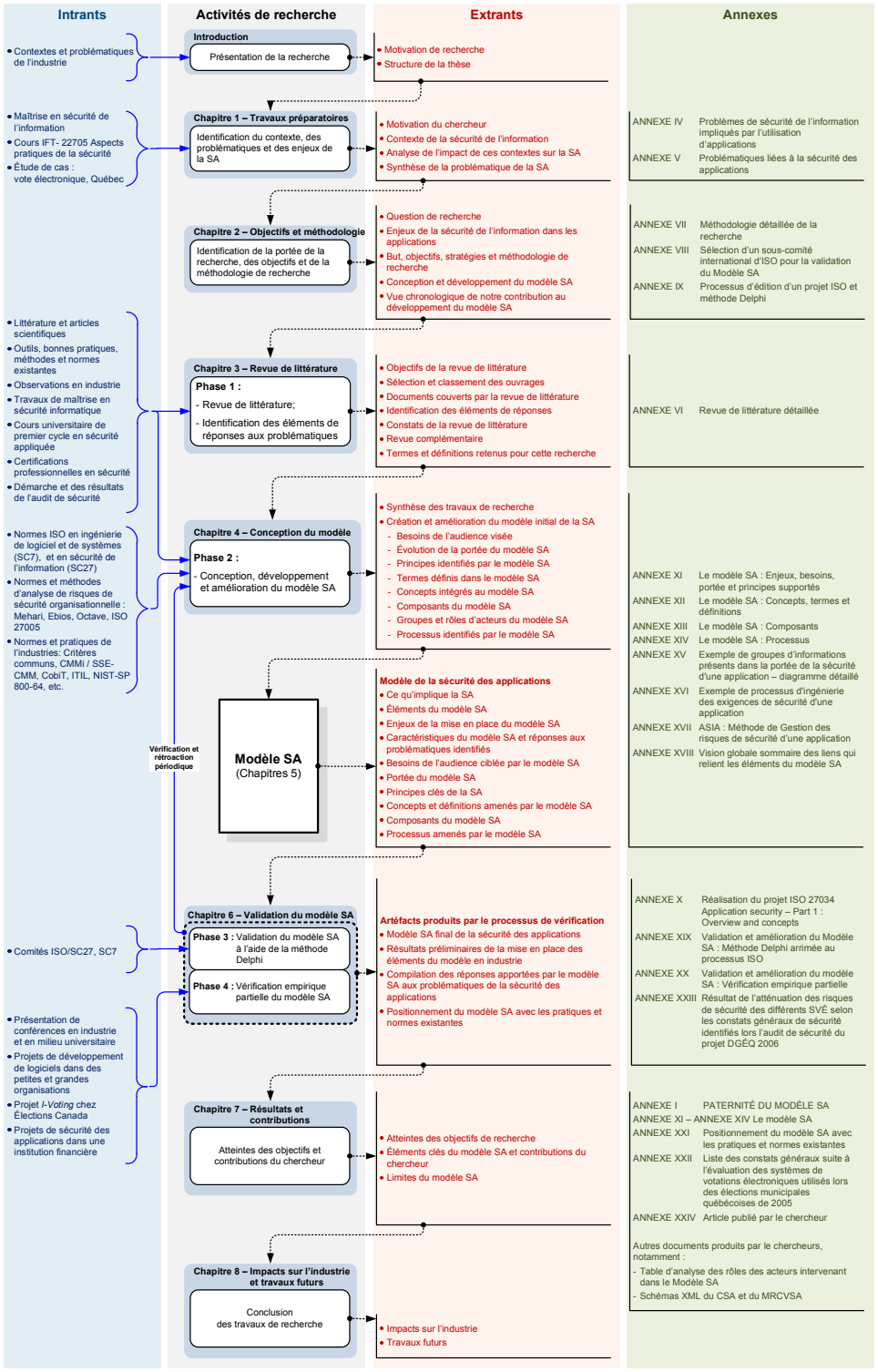


Figure-A I-2 Activités clés de la méthodologie de recherche

(Insérez ici la Figure-A I-2 en format 11 x 17)

Tableau-A I-1 Résultats consolidés des commentaires traités par cycle et des votes d'approbation de passage aux stades suivants réalisés durant le projet

Stade # --->		00. - Stade préliminaire Call for contributions to WG 4, Study Period on Application Security Johannesburg, (Afrique du Sud) Novembre 2006	10. - Stade de proposition New Work Item Proposal on Guidelines for ISMS implementation security Moscou, (Russie) Mai 2007	20.0 - Stade de préparation Version préliminaire du document de travail Lucerne, (Suisse) Octobre 2007	20.1 Document, version de travail 1 Kyoto, (Japon) Avril 2008	20.2 Document, version de travail 2 Limmasol, (Cypre) Octobre 2008	20.3 Document, version de travail 3 Beijin, (China) Mai 2009	30.1 - Stade de comité Document, version de comité 1 Redmond, (US) Novembre 2009	30.2 Document, version de comité 2 Melaka, (Malaysie) Avril 2010	40.1 - Stade d'enquête Document, version de comité finale Berlin, (Allemagne) Octobre 2010	40.2 Document, version de comité finale révisée Singapour, Avril 2011	50. - Stade d'approbation Document, version finale avant publication Secretariat SC27 - DIN, Berlin, (Allemagne) Octobre 2011	60. - Stade de publication Standard international ISO/IEC 27034 - Application Security, part 1 Secretariat ISO, Genève (Suisse), Novembre 2011	Nombre de commentaires traités	Pourcentage des commentaires traités
Rapport des éditeurs		(SC27/WG4, 2006d)	(ISO/IEC, 2007d)	(SC27/WG4, 2007)	(SC27/WG4, 2008a)	(SC27/WG4, 2008b)	(SC27/WG4, 2009, pp.	(SC27/WG4, 2009b)	(SC27/WG4, 2010)						
Document de travail ou norme ISO publiée															
Commentaires	Acceptés	0	6	28	210	81	88	139	14	81	9	0		656	57%
	Acc. en principe	0	2	3	0	0	1	18	5	2	3	0		34	3%
	Acc. avec modif.	0	0	12	68	18	20	22	5	4	4	0		153	13%
	Notés	0	1	36	95	61	13	23	3	4	5	0		241	21%
	Rejetés	0	0	0	11	14	11	14	2	4	0	3		59	5%
Total de commentaires reçus par cycle :		0	9	79	384	174	133	216	29	95	21	3		1143	100%
% de commentaires reçus acceptés par cycle :		-	100%	100%	97%	92%	92%	94%	93%	96%	100%	0%			
Total de commentaires reçus par stade :		0	9				770		245		116	3			
% de commentaires reçus acceptés par stade :		-	100%				95%		93%		98%	0%			
Résultats des votes des pays participants		Total %	Total %				Total %		Total %		Total %	Total %			
Nombre de pays inscrits		35	42				42		42		44	46			
Nombre de pays qui ont fourni des commentaires ou des contributions		6	5	10	6	5	5	10	3	7	6	2			
Nbombre de pays qui ont voté	Soutient : Oui	9 100%	20 87%				18 86%		14 70%		14 67%	35 97%			
	Soutient : Non	0 0%	3 13%				3 14%		5 25%		7 33%	1 3%			
	s'abstenint	0	13				13		16		8	10			
Nombre Pays qui ont participé au vote		9	23				34		35		29	36			
Nombre de pays qui n'ont pas voté		0	6				8		6		15	0			

(Insérez ici le Tableau-A I-1 en format 11 x 17)

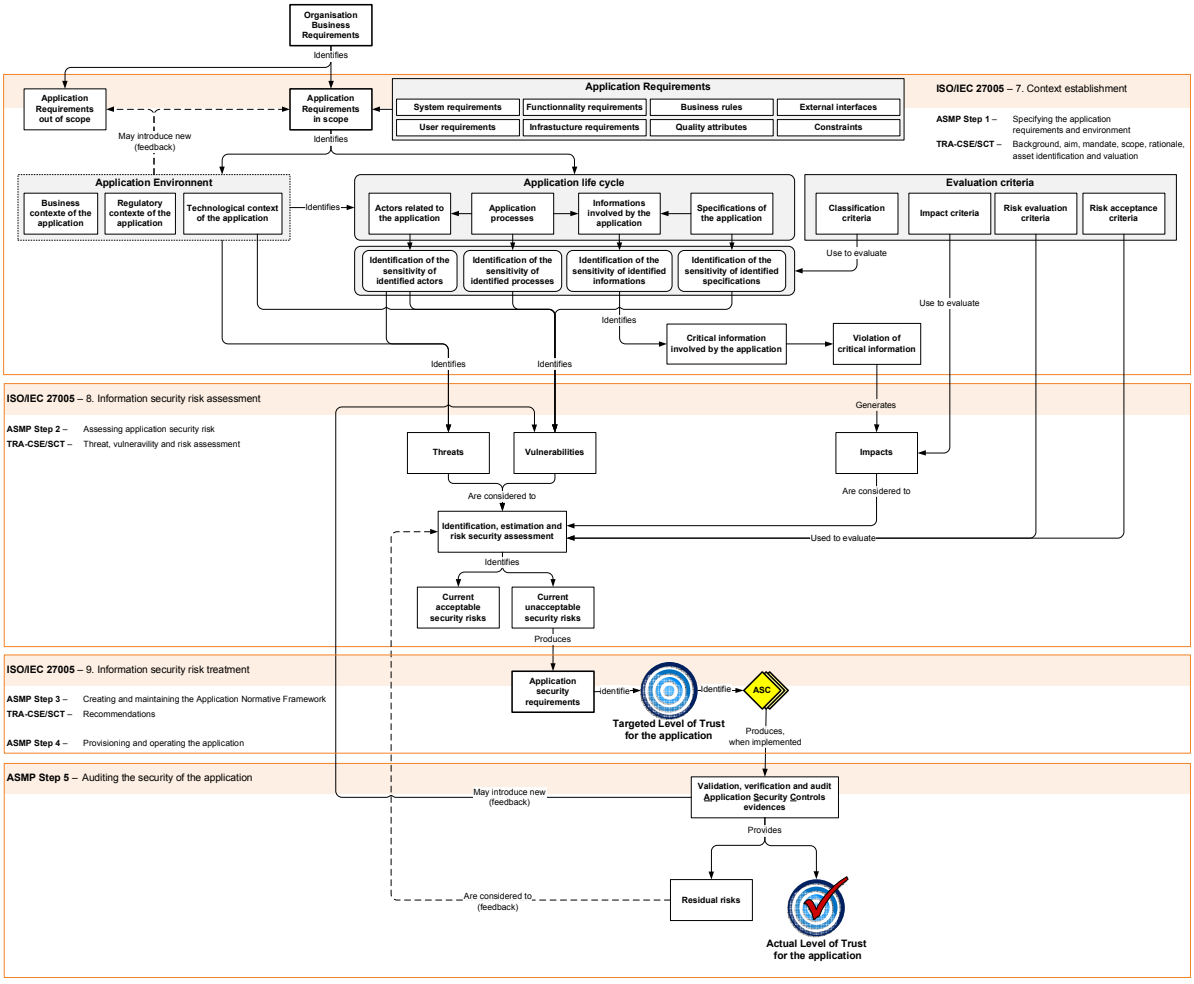


Figure-A I-3 Processus de gestion des risques de SA proposé par la méthode ASIA

(Insérez ici le Figure-A I-3 en format 11 x 17)

ANNEXE II

PATERNITÉ DU MODÈLE SA

Cette annexe présente trois lettres de confirmation de la paternité du chercheur envers les travaux et les résultats de cette recherche.

1) **M. Meng-Chow Khan** *CISSP, PhD*
   Director, Information Security
   Cisco Systems inc.
   Meng-Chow.Khan@Cisco.com

2) **M. Bruno Guay** *CISA, CISM, CRISC, CASLI*
   Conseiller senior en sécurité de l'information
   nurun inc.
   Bruno.Guay@nurun.com

3) **M. Johann Amsenga** *ing.*
   Researcher – Armscor SOC Ltd
   Ambassador – International Council on Systems Engineering (INCOSE)
   Johann.Amsenga@incose.org

Friday, June 27th 2014

To the members of the doctorate evaluation committee
Department of Software Engineering and IT
École de Technologie supérieure, Montréal (Canada)

I currently work as a Director of the Information Security group for Cisco Systems, Inc. My credentials include a Master's degree in Information Security and a Ph.D in Information Risk Management. I am also a holder of the $(ISC)^2$ Certified Information Systems Security Professional (CISSP) certification since 1998.

In November 2006, following Mr. Luc Poulin's presentation to the ISO/SC27 international meeting held in South Africa, I invited Mr Poulin to the position of editor to the ISO/IEC 27034 project.

His presentation in 2006 introduced to the SC27 group his Application Security model defining keys elements and concepts to integrate security into the life cycle of an application.

During this ISO/SC27 project, Mr Poulin, in addition to his role as the lead editor, also contributed as its redactor and a key contributor by introducing his research work into this ISO/IEC 27034 project.

As the WG4 convener supervising this project since its inception till July 2012 (where my services ended), I can confirm that M. Poulin introduced his set of application security concepts and elements for comments and reviews by all National Experts involved in the SC27 works.

Since November 2006, Mr. Poulin had led and overseen the development and drafting of various parts of the ISO/IEC 27034 standard and the results of his research on security applications are considered as keys contribution to the standard.

Regards

- Signature removed ---

Meng-Chow Kang, CISSP, PhD
Director, Information Security,
Cisco Systems Inc.

mengchow@cisco.com

Lundi, le 30 juin 2014

Au comité d'évaluation du doctorat
Département de génie logiciel
École de Technologie supérieure

Messieurs,

Je travaille présentement comme conseiller senior en sécurité de l'information pour la firme de consultation en informatique *nurun* inc.

J'ai été invité par M. Luc Poulin afin de l'assister en tant que co-éditeur de la norme ISO/IEC 27034 part 1 après qu'il ait débuté à présenter son modèle au groupe de travail 4 (WG4), du sous-comité 27 (SC27) d'ISO.

Durant les 6 années pendant lesquelles j'ai participé à ce projet, mon rôle a principalement consisté à aider M. Poulin à « challenger » les principes, concepts et élément du modèle qu'il développait et intégrait dans la norme mentionnée ci-haut, et à effectuer les révisions techniques des diverses versions anglaises de la norme.

Ayant assisté M. Poulin depuis presque le tout début de ce projet ISO, et ayant été témoin de l'évolution de son travail de recherche sur la création du modèle de la sécurité des applications, ainsi que des commentaires et contributions reçus des autres délégués nationaux impliqués dans la réalisation de ce projet, je suis en mesure de confirmer que M. Poulin est l'unique auteur du modèle de la sécurité des applications, tel que présenté dans sa thèse et dans la norme internationale ISO/IEC 27034 : *Application Security part 1 – Concepts and overview*.

Cordialement

- Signature removed ---

Bruno Guay,
Conseiller senior en sécurité de l'information
nurun inc.
Bruno.Guay@nurun.com

Monday, July 30th 2015

To the members of the doctorate evaluation committee

Department of Software Engineering and IT

École de Technologie supérieure, Montréal (Canada)

I currently work as a researcher for Armscor SOC Ltd in South Africa. My credentials include a Baccalaureus Ingeneriae (Bing) in Electronic Engineering and a Magister Ingeneriae (Ming) in Computer Engineering, both from the University of Pretoria, South Africa. I am also an ambassador for the International Council on Systems Engineering (INCOSE)

I started participating with Mr. Luc Poulin on the development of the International Standard for Application security (ISO/IEC 27034) at the international meeting of ISO/IEC JTC 1/SC 27 (IT Security techniques) meeting held in Russia, May 2007.

Mr. Poulin proposed an application security model defining key elements and concepts to integrate security into the life cycle of an application. This is now presented and explained in seven parts of ISO/IEC 27034 as follows:

PART 1: **Application security – Overview and concepts**
Part 1 provides an overview of application security. It introduces definitions, concepts, principles and processes involved in application security. This part was published in 2011.

PART 2: **Application security – Organization normative framework**
Part 2 provides an in-depth discussion of the Organization Normative Framework, its components and the organization-level processes for managing it. This part was published in 2015.

PART 3: **Application security management process**
Part 3 provides an in-depth discussion of the processes involved in an application project: determining the application requirements and environment, assessing the application security risks, creating and maintaining the Application Normative Framework, realizing and operating the application and validating its security throughout its life cycle.

PART 4: **Application security validation**
Part 4 provides detail of the application security validation, audit and certification process for organizations, applications and people.

PART 5: **Protocols and application security controls data structure**
Part 5 gives the minimal set of essential attributes of Application Security Controls (ASC) and further details the Application Security Life Cycle Reference Model in order to facilitate the implementation of the 27034 AS framework, as well as the communication and exchange of ASCs.

PART 5-1: **Protocols and application security controls data structure – XML Schemas**
Part 5 presents and explains two XML Schemas examples, describing the Application Security Control (ASC) and the Application Security Life Cycle Reference Model (ASLCRM) components.

PART 6: **Cases studies**
Part 6 provides case studies and examples of ASCs tailored for specific application security requirements.

Mr. Poulin is the overall project editor of all parts of ISO/IEC 27034. In addition to this role, he also provides valuable contributions from his research.

As an South African expert that contributed and commented on the projects, and as the convener (since 2012) of the SC 27 working group responsible for the project, I can confirm that Mr. Poulin submitted his set of application security concepts and elements for comment and review by experts from all member organisations involved in the work of SC 27. Member organisations consist of the national bodies of countries, and liaison organisations.

Mr. Poulin has led and overseen the development of the various parts of ISO/IEC w7034 since May 2007. The results of his research on application security are considered as key contributions to the project.

Regards,

- Signature removed ---

Mr. Johann Amsenga *ing.*

Researcher – Armscor SOC Ltd
Ambassador – International Council on Systems Engineering (INCOSE)
Johann.Amsenga@incose.org

ANNEXE III

LISTE DES APPENDICES

Les appendices suivants sont référencés dans cette thèse et sont inclus sur le CD-ROM « POULIN, Luc – Projet THÈSE 2015 – CD des Annexes » ci-joint.

#	Nom du fichier	**Nom du document** Description du contenu
A	POULIN Luc, Projet THÈSE 2015 – ANNEXES III à XXII.pdf	**DOCUMENT DES ANNEXES** ANNEXE IV Problèmes de sécurité de l'information impliqués par l'utilisation d'applications ANNEXE V Problématiques liées à la sécurité des applications ANNEXE VI Revue de littérature détaillée ANNEXE VII Méthodologie détaillée de la recherche ANNEXE VIII Sélection d'un sous-comité international d'ISO pour la validation du Modèle SA ANNEXE IX Processus d'édition d'un projet ISO et méthode Delphi ANNEXE X Réalisation du projet ISO 27034 Application security – Part 1 : Overview and concepts ANNEXE XI Le modèle SA : Enjeux, besoins, portée et principes supportés ANNEXE XII Le modèle SA : Concepts, termes et définitions ANNEXE XIII Le modèle SA : Composants ANNEXE XIV Le modèle SA : Processus ANNEXE XV Exemple de groupes d'informations présents dans la portée de la sécurité d'une application – diagramme détaillé ANNEXE XVI Exemple de processus d'ingénierie des exigences de sécurité d'une application ANNEXE XVII ASIA : Méthode de Gestion des risques de sécurité d'une application ANNEXE XVIII Vision globale sommaire des liens qui relient les éléments du modèle SA ANNEXE XIX Validation et amélioration du Modèle SA : Méthode Delphi arrimée au processus ISO

#	Nom du fichier	**Nom du document** Description du contenu
		ANNEXE XX Validation et amélioration du modèle SA : Vérification empirique partielle ANNEXE XXI Positionnement du modèle SA avec les pratiques et normes existantes ANNEXE XXII Liste des constats généraux suite à l'évaluation des systèmes de votations électroniques utilisés lors des élections municipales québécoises de 2005 ANNEXE XXIII Résultat de l'atténuation des risques de sécurité des différents SVÉ selon les constats généraux de sécurité identifiés lors l'audit de sécurité du projet DGÉQ 2006 ANNEXE XXIV Article publié par le chercheur
B	Canadian Contribution - Unified Roles Table ISO_IEC-27034, v1.2.xlsx	**Table d'analyse des rôles des acteurs intervenant dans le Modèle SA** Liste consolidée des rôles identifiés dans les documents normes, méthodes et pratiques SCRUM, OpenUP, Quebec Gov, ISO/IEC 27001, ISO/IEC 27034-1, ISO/IEC 12207, COBIT, SQUARE et Microsoft SDL.
C	ISO27034-5-1-ASC_XML_Schema_ 2015-07.xsd	**Schéma XML du CSA et du MRCVSA** Version préliminaire du schéma XML contenant la description formelle du CSA et du modèle de référence du cycle de vie de la sécurité des applications (MRCVSA).

Bibliographie

(ISC)², Transcends Technology 2013a. « CISSP®-ISSMP®: Information Systems Security Management Professional ». In *(ISC)² - Inspiring a safe and secure cyber world®*. En ligne. < https://www.isc2.org/issmp/default.aspx >. Consulté le 22 novembre 2013.

(ISC)², Transcends Technology 2013b. « CISSP® - Certified Information Systems Security Professional ». Document électronique. (ISC)² Transcends Technology 6p.

(ISC)², Transcends Technology 2013c. « CSSLP® - Certified Secure Software Lifecycle Professional ». Document électronique. (ISC)² Transcends Technology 6p.

Abran, Alain. 2010. *Software metrics and software metrology*, Nouv. ed. Livre. Hoboken (N.J.), Los Alamitos (Calif.): Wiley; IEEE Computer Society, xix, 328 p.

Alberts, Christopher J., Audrey J. Dorofee, James Stevens et Carol Woody. 2005. « OCTAVE-S Implementation Guide, Version 1.0 ». Manuel électronique. Pittsburg, PA, : Software Engineering Institute, Carbegie Mellon university, 199 p.

All, Carnegie Mellon University et. 2003. *Systems Security Engineering Capability Maturity Model (SSE-CMM), v3.0*. Livre électronique. Carnegie Mellon University, 340 p.

Amsanga, Johann. 2008. *Appendix from ZA*. Rapport électronique. Coll. « 20.1 Kyoto ». Kyoto Japon: Luc Poulin, 17 p.

Andress, Amanda. 2003. *Surviving security: how to integrate people, process, and technology* (2003), 2. Livre. Auerbach Publications, 502 p.

Anonymous. 2003. *Maximum security*. Livre. Sams, 945 p.

ANSSI. 2004. *Expression des Besoins et Identification des Objectifs de Sécurité*. Guide technique électronique. Paris, France: Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information, Sous-direction des opérations, Bureau conseil, 22 p.

April, Alain, et Alain Abran. 2008. *Software Maintenance Management: Evaluation and Continuous Improvement* (2008). Livre. John Wiley & Sons, 314 p.

Ashford, Warwick. 2013. « Microsoft declares conformance with ISO 27034-1 ». In *ComputerWeekly.com*. En ligne. < http://www.computerweekly.com/news/2240184149/Microsoft-declares-conformance-with-ISO-27034-1 >. Consulté le 17 février 2014.

Avramescu, G., M. Bucicoiu, D. Rosner et N. Tapus. 2013. « Guidelines for Discovering and Improving Application Security ». In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on*. (29-31 May 2013), p. 560-565.

Baker, W. H., et L. Wallace. 2007. « Is Information Security Under Control? - Investigating Quality in Information Security Management ». *Security & Privacy, IEEE,* vol. 5, n^{o} 1, p. 36-44.

Barman, Scott. 2002. *Writing information security policies*. Livre. Indianapolis, Ind.: New Riders, xviii, 216 p. p.

Ben-Natan, Ron. 2005. *Implementing database security and auditing: a guide for DBAs, information security administrators and auditors* (2005). Livre. Elsevier Digital Press, 413 p.

Beznosov, Konstantin, et Philippe Kruchten. 2005. « Towards Agile Security Assurance ». In *Proceedings of the workshop on New security paradigms*. (16 October 2005), p. 47-54.

Booch, Grady, Ivar Jacobson et James Rumbaugh. 1999. *The unified software development process*. Livre. Coll. « The Addison-Wesley object technology series ». Boston ; Montreal: ACM Press/Addison Wesley, xxix, 463 p. p.

Borek, Marian, Nina Moebius, Kurt Stenzel et Wolfgang Reif. 2012. « Model-Driven Development of Secure Service Applications ». In *Software Engineering Workshop (SEW), 2012 35th Annual IEEE*. (12-13 Oct. 2012), p. 62-71.

BSI, Federal Office for Information Security of Germany. 2005a. *BSI Standard 100-1: Information Security Management Systems (ISMS)*. Rapport électronique. Coll. « 20.2 Limassol ». Bonn, Allemagne: Federal Office for Information Security (BSI), 35 p.

BSI, Federal Office for Information Security of Germany. 2005 b. *BSI Standard 100-2: IT-Grundschutz Methodology*. Rapport électronique. Coll. « 20.2 Limassol ». Bonn, Allemagne: Federal Office for Information Security (BSI), 74 p.

BSI, Federal Office for Information Security of Germany. 2005c. *BSI Standard 100-3: Risk Analysis based on IT-Grundschutz*. Rapport électronique. Coll. « 20.2 Limassol ». Bonn, Allemagne: Federal Office for Information Security (BSI), 19 p.

Canada, Ministre de la Justice du. 13 novembre 2013. *Loi sur la protection des renseignements personnels*. Loi-règlement. Ottawa(Ont.), 63 p.

Carlstedl, Anders. 2006. « Security standards and Practices in Sweden ». In *00.0 Johanesbourg*. sous la dir. de Carlstedl, Anders, p. 20. accenture.

Caulkins, J. P., E. D. Hough, N. R. Mead et H. Osman. 2007. « Optimizing Investments in Security Countermeasures: A Practical Tool for Fixed Budgets ». *Security & Privacy, IEEE,* vol. 5, n° 5, p. 57-60.

Chen, T. M., et J. M. Robert. 2004. « Worm epidemics in high-speed networks ». *Computer,* vol. 37, n° 6, p. 48-53.

Chijiiwa, Tak. 2012. « Application Security ISO ». In *Security Compass*. (Toronto, Ontario, 10 mai 2012) Vol. 2014, p. 37. Security Compass inc. < https://docs.google.com/gview?url=https://www.owasp.org/images/6/64/ISO_27034_review_%2528OWASP_Toronto_May_10%252C_2012%2529.pdf&chrome=true >.

Chriqi, A., H. Otrok et J. M. Robert. 2009. « SC-OLSR: Secure Clustering-Based OLSR Model for Ad Hoc Networks ». In *Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on*. (12-14 Oct. 2009), p. 239-245.

CLUSIF. 2005. *MEHARI V3 - Manuel de référence des services de sécurité*. Manuel électronique. Paris, France: Club de la sécurité des systèmes d'information Français, 215 p.

CMMI, Product Team. 2006. « CMMI for Developpement ». Rapport technique. Software Engineering Institute, Carnegie Mellon University, 561 p.

CNN. 2010. « Toyota: Software to blame for Prius brake problems ». *CNN Web - Edition International*. Article-journal. 5 février 2010, p. 2. < http://edition.cnn.com/2010/BUSINESS/02/04/japan.prius.investigate/index.html?eref=rss_latest&utm_source=feedburner&utm_medium=feed& >.

d'InfoSecurity, Équipe. 2013. « Microsoft Declares Conformity to ISO 27034-1 and Scott Charney Calls for Industry to Follow ». In *info security*. En ligne. < http://www.infosecurity-magazine.com/view/32405/microsoft-declares-conformity-to-iso-270341-and-scott-charney-calls-for-industry-to-follow-/ >. Consulté le 17 février 2014.

DCSSI, Bureau conseil de la. 2004. *EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité*. Guide technique électronique. Paris, France: Bureau conseil de la DCSSI, 22 p.

Dejun, Mu, Hu Wei, Mao Baolei et Ma Bo. 2014. « A bottom-up approach to verifiable embedded system information flow security ». *Information Security, IET,* vol. 8, n° 1, p. 12-17.

Deming, W. Edwards. 2000. *Out of the Crisis*. Livre. Cambridge (MA): The MIT Press, 523 p.

Denham, Elisabeth 2009. *Report of findings into the complaint filed by the Canadian Internet Policy And Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection And Electronic Documents Act*. Rapport électronique. 16 juillet 2009. Ottawa: Office of the Privacy Commissioner of Canada, 113 p.

DGEQ. 2006. *Élections municipales de novembre 2005 : Rapport d'évaluation des nouveaux mécanismes de votation*. Rapport électronique. Québec: Le directeur général des élections du Québec, 230 p.

DHS, Department of Homeland Security. 2007. *Security in the software lifecycle - Making Software Development Processes - and Software Produced by Them - More Secure*. Rapport électronique. Coll. « 20.0 Lucerne ». US: Department of Homeland Security, 219 p.

Dianxiang, Xu, et K. E. Nygard. 2006. « Threat-driven modeling and verification of secure software using aspect-oriented Petri nets ». *Software Engineering, IEEE Transactions on,* vol. 32, n° 4, p. 265-278.

Evans, S., D. Heinbuch, E. Kyle, J. Piorkowski et J. Wallner. 2004. « Risk-based systems security engineering: stopping attacks with intention ». *Security & Privacy, IEEE,* vol. 2, n° 6, p. 59-62.

Garcia, L. F., et J. M. Robert. 2009. « Preventing Layer-3 wormhole attacks in ad-hoc networks with multipath DSR ». In *Ad Hoc Networking Workshop, 2009. Med-Hoc-Net 2009. 8th IFIP Annual Mediterranean*. (June 29 2009-July 1 2009), p. 15-20.

Goertzel, Karen Mercedes, Theodore Winograd, Holly Lynne McKinley, Lyndon Oh, Michael Colon, Thomas McGibbon, Elaine Fedchak et Robert Vienneau. 2007. *Software Security Assurance: A State-of-the-Art Report (SOAR)*. Rapport électronique. Coll. « 20.0 Lucerne », SC27N6125_Att4. US, 396 p.

Goldberg, Ian, David Wagner, Randi Thomas et Eric Brewer. 1996. « A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker) ». In *Sixth USENIX UNIX Security Symposium*. (Berkeley, California, Juillet 1996). USENIX Association.

Gregoire, J., K. Buyens, B. De Win, R. Scandariato et W. Joosen. 2007. « On the Secure Software Development Process: CLASP and SDL Compared ». In *Software Engineering for Secure Systems, 2007. SESS '07: ICSE Workshops 2007. Third International Workshop on*. (20-26 May 2007), p. 1-1.

Group, CC. 2009. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*. Livre électronique, 93 p.

Guay, Bruno , et Luc Poulin. 2002. « Aspects pratiques de la sécurité ». In *Syllabus de cours*. p. 5. Département d'informatique et de génie logiciel, Université Laval.

Haley, Charles B. , Robin Laney, Jonathan D. Moffett et Bashar Nuseibeh. 2008. « Security Requirements Engineering: A Framework for Representation and Analysis ». *IEEE Transactions on software engineering,* vol. 34, n° 1, p. 21.

Howard, Michael, et David LeBlanc. 2002. *Writing secure code 2*. Livre. Microsoft Press.

Howard, Michael, David LeBlanc et John Viega. 2005. *19 Deadly Sins of Software Security*. Livre. McGraw-Hill/Osborne.

Hsu, Chia-Chien, et Brian A. Sandford. 2007. « The Delphi Technique: Making Sense of Consensus ». *Practical Assessment, Research & Evaluation,* vol. 12, n° 10, p. 8.

Huang, Zhitao, P. Zavarsky et R. Ruhl. 2009. « An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002 ». In *Computational Science and Engineering, 2009. CSE '09. International Conference*. (Vancouver, BC 29-31 août 2009) Vol. 3, p. 386-391.

IEEE. 1990. *IEEE Standard Glossary of Software Engineering Terminology*. Norme Internationale, 610.12-1990: IEEE Computer Society, 84 p.

IEEE. 1997. *IEEE Standard for Software Reviews*. Norme, 47 p.

In Fidem. 2011. « Stratégies d'intégration de la sécurité dans le cycle de développement d'applications (SDLC) ». In *IN FIDEM*. En ligne. < http://www.infidem.biz/services/formation/strategies-dintegration-de-la-securite-dans-le-cycle-de-developpement-dapplications-sdlc/ >. Consulté le 16 février 2014.

ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Manuel électronique. ISACA, 94 p. < http://books.google.ca/books?id=1iLKVlOIg9EC >.

ISACA®. 2013a. « CISA® (Certified Information System Auditor™) ». In *ISACA® - Section de Québec*. En ligne. < http://www.isaca-quebec.ca/cisa.htm >. Consulté le 22 novembre 2013.

ISACA®. 2013 b. « CISM® (Certified Information Security Manager®) ». In *ISACA® - Section de Québec*. En ligne. < http://www.isaca-quebec.ca/cisa.htm >. Consulté le 22 novembre 2013.

ISO/IEC. 2001. *Software engineering - Product quality - Part 1: Quality model*. Norme Internationale, ISO/IEC IS 9626-1: International Standards Organization; International Electronic Commission, 25 p.

ISO/IEC. 2002. *Software engineering: software measurement process*. FDIS 15939. Genève: International Standards Organization; International Electronic Commission, 37 p. p.

ISO/IEC. 2004a. *Concepts and models for information and communications technology security management*. Norme Internationale, ISO/IEC IS 13335-1: International Standards Organization; International Electronic Commission.

ISO/IEC. 2004 b. *ISO/IEC Directives - Part 1: Procedures for the technical work*. Norme Internationale, ISO/IEC Directives-1. Genève, Suisse: International Standards Organization; International Electronic Commission, 62 p.

ISO/IEC. 2004c. *ISO/IEC Directives - Part 2: Rules for the structure and drafting of International Standards, 5th edition, 2004*. Norme Internationale, ISO/IEC Directives-2. Genève, Suisse: ISO/IEC, 69 p.

ISO/IEC. 2004d. *Software engineering: system life cycle processes*. IS 15288. Genève, Suisse: International Standards Organization; International Electronic Commission, vi, 62 p. p.

ISO/IEC. 2005a. *Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements*. FDIS 15408-2. Geneva, Switzerland: International Standards Organization; International Electronic Commission, 250 p.

ISO/IEC. 2005 b. *Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements*. Norme internationale, ISO/IEC FDIS 15408-3. Geneva, Switzerland: International Standards Organization; International Electronic Commission, 164 p.

ISO/IEC. 2005c. *Information technology - Security techniques - Information security management systems - Code of practice for information security management*. Norme Internationale, ISO/IEC FDIS 27002. Berlin, Allemagne: Organisation International Standards Organization; International Electronic Commission, 42 p.

ISO/IEC. 2005d. *Information technology - Security techniques - Information security management systems - Requirements*. Norme Internationale, ISO/IEC FDIS 27001. Berlin, Allemagne: International Standards Organization; International Electronic Commission, 42 p.

ISO/IEC. 2005e. *Information Technology - Service management - Part 2: Code of practice*. Norme Internationale, ISO/IEC IS 20000-2:2005. Genève: International Standards Organization, iv, 34 p. p.

ISO/IEC. 2005f. *Information technology : Security technique - A framework for IT security assurance: part 1: Overview and framework*. TR 15443-1, ISO/IEC TR 15443-1. Genève, Suisse: International Standards Organization; International Electronic Commission, v, 24 p.

ISO/IEC. 2005 g. *Systems and software engineering - Software life cycle processes - Maintenance*. Norme internationale, ISO/IEC FDIS 14764. Genève: ISO/IEC, vi, 45 p.

ISO/IEC. 2005 h. *Technologies de l'information : gestion des services : partie 1 : spécifications*. Norme Internationale. Genève: Organisation internationale de normalisation, v, 19 p. p.

ISO/IEC. 2006a. *Information technology - Security techniques - System Security Engineering - Capability Maturity Model (SSE-CMM)*. Norme internationale, ISO/IEC FCD 21827. Geneva, Switzerland: ISO/IEC, 134 p.

ISO/IEC. 2006 b. *Software engineering: software measurement process*. FDIS 15939. Genève: International Standards Organization; International Electronic Commission, v, 37 p.

ISO/IEC. 2007a. *Call for contributions to WG 4 Study Period on Application Security*. Rapport électronique. Coll. « 00.0 Johanesbourg ». Berlin, Alemagne, 9 p.

ISO/IEC. 2007 b. *Guidelines for application security and comments on SC 27 N5737 - Preliminary Draft for NP 27034*. Rapport électronique. ISO/IEC JTC 1/SC 27 N6093. Berlin, Germany: DIN, 29 p.

ISO/IEC. 2007c. *Information technology - Security techniques - Application security - Part 1: Guidelines for application security*. Norme internationale, ISO/IEC PD 27034-1. Berlin, Allemagne: ISO/IEC, 48 p.

ISO/IEC. 2007d. *Information technology : Security technique - A framework for IT security assurance - part 3: Analysis of ssurance methods*. TR 15443-3, ISO/IEC TR 15443-3. Genève, Suisse: ISO/IEC, vii, 67 p.

ISO/IEC. 2007e. *New Work Item Proposal on Guidelines for application security (27034)* Rapport électronique. Coll. « 10.0 Russie ». Berlin, Alemagne, 9 p.

ISO/IEC. 2007f. *Summary of contributions to WG4 Study Period on Application Security in response to SC 27 N5571 "Call for contributions"*. Rapport électronique. ISO/IEC JTC 1/SC 27 N5653. Berlin, Germany: DIN, 9 p.

ISO/IEC. 2007 g. *Systems and software engineering - System life cycle processes*. Norme internationale, ISO/IEC FDIS 15288. Genève: International Standards Organization; International Electronic Commission, x, 71 p. p.

ISO/IEC. 2008a. *Information technology - Security techniques - Application security - Part 1: Guidelines for application security*. Norme internationale, ISO/IEC WD2 27034-1. Berlin, Allemagne: ISO/IEC, 56 p.

ISO/IEC. 2008 b. *Information technology - Security techniques - Application security - Part 1: Guidelines for application security*. Norme internationale, ISO/IEC WD 27034-1. Berlin, Allemagne: ISO/IEC, 44 p.

ISO/IEC. 2008c. *Summary of National Body comments received on document SC 27 N6276 – ISO/IEC 1st WD 27034-1 – Information technology – Security techniques – Application security – Part 1: Guidelines to application security*. Rapport électronique. ISO/IEC JTC 1/SC 27 N6515. Berlin, Germany: DIN, 152 p.

ISO/IEC. 2008d. *Summary of National Body comments received on document SC 27 N6747 – ISO/IEC 2nd WD 27034-1 – Information technology – Security techniques – Application security – Part 1: Overview and concepts*. Rapport électronique. ISO/IEC JTC 1/SC 27 N6996. Berlin, Germany: DIN, 55 p.

ISO/IEC. 2008e. *Systems and software engineering - Software life cycle processes*. Norme internationale, ISO/IEC FDIS 12207. Genève: International Standards Organization; International Electronic Commission, xii, 123 p.

ISO/IEC. 2009a. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC WD3 27034-1. Berlin, Allemagne: ISO/IEC, 65 p.

ISO/IEC. 2009 b. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC CD1 27034-1. Berlin, Allemagne: ISO/IEC, 91 p.

ISO/IEC. 2009c. *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model*. FDIS 15408-1. Geneva, Switzerland: International Standards Organization; International Electronic Commission, 76 p.

ISO/IEC. 2009d. *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Norme Internationale, ISO/IEC FDIS 27000. Berlin: International Standards Organization; International Electronic Commission, 30 p.

ISO/IEC. 2009e. *Information technology - Security techniques - Information security management systems - Secure system engineering principles and techniques* Norme Internationale, ISO/IEC WD1 29193. Berlin, Allemagne: Organisation International Standards Organization; International Electronic Commission, 34 p.

ISO/IEC. 2009f. *Management du risque : principes et lignes directrices*. Norme internationale, ISO/IEC FDIS 31000. Genève: Organisation internationale de normalisation, 24 p. p.

ISO/IEC. 2009 g. *Software and systems engineering - Life cycle processes - Requirements engineering*. Norme internationale, ISO/IEC CD 29148. Genève: International Standards Organization; International Electronic Commission, 74 p.

ISO/IEC. 2009 h. *Summary of National Body comments received on document SC 27 N7176 – ISO/IEC 3nd WD 27034-1 – Information technology – Security techniques – Application security – Part 1: Overview and concepts*. Rapport électronique. ISO/IEC JTC 1/SC 27 N7533. Berlin, Germany: DIN, 40 p.

ISO/IEC. 2009i. *Summary of National Body comments received on document SC 27 N7176 – ISO/IEC 3nd WD 27034-1 – Information technology – Security techniques – Application security – Part 1: Overview and concepts*. Rapport électronique. ISO/IEC JTC 1/SC 27 N7533. Berlin, Germany: DIN, 70 p.

ISO/IEC. 2009j. *Systems and software engineering - Systems and software assurance - Part 1: Concepts and vocabulary*. Rapport technique, ISO/IEC TR 15026-1. Genève: International Standards Organization; International Electronic Commission, 91 p.

ISO/IEC. 2010a. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC FCD 27034-1. Berlin, Allemagne: ISO/IEC, 84 p.

ISO/IEC. 2010 b. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC CD2 27034-1. Berlin, Allemagne: ISO/IEC, 87 p.

ISO/IEC. 2010c. *Information technology - Security techniques - Application security - Part 2: Organization Normative Framework*. Norme internationale, ISO/IEC FCD 27034-2. Berlin, Allemagne: ISO/IEC, 71 p.

ISO/IEC. 2010d. *Information technology - Security techniques - Information security risk management*. Norme Internationale, ISO/IEC FDIS 27005. Berlin: International Standards Organization; International Electronic Commission, 70 p.

ISO/IEC. 2010e. *Summary of National Body comments received on document SC 27 N7176 – ISO/IEC 2nd CD 27034-1 – Information technology – Security techniques –*

Application security – Part 1: Overview and concepts. Rapport électronique. ISO/IEC JTC 1/SC 27 N7533. Berlin, Germany: DIN, 14 p.

ISO/IEC. 2010f. *Systems and software engineering - Systems and software assurance - Part 2: Assurance case*. Norme internationale, ISO/IEC TR 15026-2. Genève: ISO/IEC, 15 p.

ISO/IEC. 2010 g. *Systems and software engineering - Vocabulary*. Norme internationale, ISO/IEC IS 24765. Genève: International Standards Organization; International Electronic Commission, vi, 412 p.

ISO/IEC. 2011a. *Dispositions of comments received on ISO/IEC FDIS 27034-1:2011(E) (N10324) — Information technology — Security techniques — Application security — Part 1: Overview and concepts (in response to NB comments in [N10485])* Rapport électronique. ISO/IEC JTC 1/SC 27 N10486. Berlin, Germany: DIN, 3 p.

ISO/IEC. 2011 b. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC RFCD 27034-1. Berlin, Allemagne: ISO/IEC, 86 p.

ISO/IEC. 2011c. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC FDIS 27034-1. Berlin, Allemagne: ISO/IEC, 86 p.

ISO/IEC. 2011d. *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. Norme internationale, ISO/IEC IS 27034-1. Geneva, Switzerland: ISO/IEC, 82 p.

ISO/IEC. 2011e. *Summary of National Body comments received on document SC 27 N7176 – ISO/IEC FCD 27034-1 – Information technology – Security techniques – Application security – Part 1: Overview and concepts*. Rapport électronique. Coll. « 40.1 Berlin », ISO/IEC JTC 1/SC 27 N9096. Berlin, Germany: DIN, 23 p.

ISO/IEC. 2011f. *Summary of National Body comments received on document SC 27 N7176 – ISO/IEC RFCD 27034-1 – Information technology – Security techniques – Application security – Part 1: Overview and concepts*. Rapport électronique. ISO/IEC JTC 1/SC 27 N9960. Berlin, Germany: DIN, 17 p.

ISO/IEC. 2013a. *Information technology - Security techniques - Application security - Part 8: Protocols and application security controls data structure – XML Schemas* Norme internationale, ISO/IEC 27034-8, PDTS. Berlin, Allemagne: ISO/IEC, 42 p.

ISO/IEC. 2013 b. *Information technology - Security techniques - Information security management systems - Code of practice for information security management*. Norme

Internationale, ISO/IEC FDIS 27002. Berlin, Allemagne: International Standards Organization; International Electronic Commission, 80 p.

ISO/IEC. 2015. *Information technology - Security techniques - Application security - Part 5-1: Protocols and application security controls data structure – XML Schemas* Norme internationale, ISO/IEC 27034-5-1, WD3. Berlin, Allemagne: ISO/IEC, 42 p.

ISO/IEC/IEEE. 2010. *Systems and software engineering — Vocabulary*. Norme internationale, ISO/IEC/IEEE 24765:2010: International Standards Organization; International Electronic Commission; IEEE Computer Society, 410 p.

ITGI. 2007. *COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. Manuel électronique. IT Governance Institute, 213 p. Consulté le 2007.

ITIMF. 2013. « An Introductory Overview of ITIL® V3 - A high-level overview of the IT INFRASTRUCTURE LIBRARY ». Manuel électronique. IT Information Management Forum, Best Management Practice Partnership, 58 p.

ITU-T, SG17. 2007a. *ITU-T SG17 liaison statement to ISO/IEC JTC 1/SC27/WG 4 on new work item proposal on guidelines for application security (27034) (SC27 N5729) [in response to SC 27 N5911]*. Présentation électronique. Coll. « 20.0 Lucerne », SC27N06141rev1. Genève, Suisse: ITU-T SC17, 2 p.

ITU-T, SG17 WP2/17. 2007 b. *ITU-T SG 17 Liaison Statement to SC 27/WG 4 on collaborative work on Application Security (in response to SC 27 N 5498)* Rapport électronique. Coll. « 10.0 Russie ». Genève, Suisse: ITU-T, 3 p.

Johnson, M. E., et E. Goetz. 2007. « Embedding Information Security into the Organization ». *Security & Privacy, IEEE,* vol. 5, n^{o} 3, p. 16-24.

Jorshari, F. Z., H. Mouratidis et S. Islam. 2012. « Extracting security requirements from relevant laws and regulations ». In *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on*. (16-18 May 2012), p. 1-9.

Jürjens, Jan (309). 2005. *Secure systems development with UML*. Livre. Springer.

Justice, ministre de la. 2014. *Loi sur les banques*. Ottawa (Ont.): ministre de la Justice, 784 p.

Kacsuk, P. , A. Goyeneche, T. Delaitre, T. Kiss, Z. Farkas et T. Boczko. 2004. « High-Level Grid Application Environment to Use Legacy Codes as OGSA Grid Services ». In *GRID '04 Proceedings of the 5th IEEE/ACM International Workshop on Grid Computing*. (Washington, DC, USA), p. 428-435

Kaplan, Robert S., et David P. Norton. 1996. *The Balanced Scorecard: Translating Strategy into Action*, September-October 1996. Livre. Coll. « Strategy and Leadership ». Massachusetts: Harvard Business School Press, 322 p.

Kitchenham, Barbara Ann. 1996. « Evaluating software engineering methods and tool part 1: The evaluation context and evaluation methods ». *ACM SIGSOFT Software Engineering Notes,* vol. 21, n° 1, p. 11-14.

Ladd, David. 2009. *Case Study: Overview of the Security Development Lifecycle (SDL) as applied to the Organization Normative Framework*. Rapport électronique. Coll. « 30.1 Redmond ». Redmond, États-Unis, 17 p.

Leveson, Nancy G. 1995. *Safeware: System Safety and Computers*. Livre. Coll. « Addison-Wesley ». Addison-Wesley, 680 p.

Linstone, Harold A., et Murray Turoff. 2002. *The Delphi Method - Techniques and Applications*, 2002. Livre électronique. 616 p.

Lipner, Steve. 2013. « Microsoft SDL Conforms to ISO/IEC 27034-1:2011 ». In *Microsoft Security Development Lifecycle Blog*. En ligne. < http://blogs.msdn.com/b/sdl/archive/2013/05/14/microsoft-sdl-conforms-to-iso-iec-27034-1-2011.aspx >. Consulté le 16 février 2014.

LLC, PCI Security Standards Council. 2010. *Normes de sécurité des données - Secteur de la carte de paiement*. Norme privé, PCI DSS 2.0: PCI Security Standards Council LLC 86 p.

Long, Fred, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland et David Svoboda. 2011. *The CERT Oracle Secure Coding Standard for Java*. Addison-Wesley Professional, 774 p.

Ma, Antony. 2006. « Honk Kong IT Security ». In *00.0 Johanesbourg*. (Johannesburg, Afrique du sud), p. 6. PISA.

MacIntyre, Blair, Alex Hill, Hafez Rouzati, Maribeth Gandy et Brian Davidson. 2011. « The Argon AR Web Browser and Standards-based AR Application Environment ». In *Mixed and Augmented Reality (ISMAR), 2011 10th IEEE International Symposium*. (Basel, Switzerland, 26-29 octobre 2011), p. 65 - 74. IEEE.

Mag Securs. 2013. « Le développement sécurisé et le standard ISO 27034 animent la SDC2013 ». In *Mag Securs*. En ligne. < http://www.mag-securs.com/News/tabid/62/id/30797/Le-developpement-securise-et-le-standard-ISO-27034-animent-la-SDC2013.aspx >. Consulté le 17 février 2014.

Marcil, Jonathan. 2014. « OWASP ISO IEC 27034 Application Security Controls Project ». In *OWASP - Open Web Application Security Project*. En ligne. < https://www.owasp.org/index.php/OWASP_ISO_IEC_27034_Application_Security_Controls_Project >. Consulté le 21 janvier 2014.

McGraw, Gary, Brian Chess et Sammy Migues. 2010. *Building Security In Maturity Model - BSIMM2*. Livre électronique. 56 p.

Menzel, M., et C. Meinel. 2009. « A Security Meta-model for Service-Oriented Architectures ». In *Services Computing, 2009. SCC '09. IEEE International Conference on*. (21-25 Sept. 2009), p. 251-259.

Microsoft. 2007. *Introduction to the Security Development Lifecycle*. Rapport électronique. Coll. « 20.0 Lucerne », SC27N6125_Att3. Bellevue, Washington: Microsoft Corporation inc., 24 p.

Microsoft. 2010. *Security Development Lifecycle - Simplified Implementation of the Microsoft SDL*. Manuel électronique. Bellevue, Washington, 17 p. Consulté le 2010.

Microsoft. 2011. « Microsoft Security Development Lifecycle ». En ligne. < http://www.microsoft.com/security/sdl/default.aspx >. Consulté le 2001-08-04.

Morin, Lyne. 2012. « I-Voting Pilot Project - Executive committee, Status Update ». In. (Ottawa, janvier 2012), p. 14. Élections Canada.

Mouratidis, Haralambo, et Paolo Giorgini. 2007. *Integrating Security and Software Engineering: Advances and Future Visions*. Livre. Idea Group Pub., 288 p.

Nakao, Koji. 2006a. « Collaboration of Security Operation ». In *00.0 Johanesbourg*. (Johannesburg, Afrique du sud, 1 novembre 2006), sous la dir. de Nakao, Koji, p. 27. Telecom-ISAD Japan.

Nakao, Koji. 2006 b. « Monitoring and Detecting Malware and Cyber attacks - Design and implementation of nicter ». In *00.0 Johanesbourg*. (Johannesburg, Afrique du sud), sous la dir. de Nakao, Koji, p. 33. NICT, NICTER.

Neumann, Peter G. (384). 1994. *Computer-Related Risks* (28 octobre 1994). Livre. Coll. « ACM Press ». Addison-Wesley Professional.

Neumann, Peter G. 1996. « Illustrative Risks to the Public in the Use of Computer Systems and Related Technology ». *SIGSOFT Softw. Eng. Notes,* vol. 21, n° 1, p. 16-30.

Newman, Mark, Carl Thompson et Anthony P. Roberts. 2006. « Helping practitioners understand the contribution of qualitative research to evidence-based practice ». *EBN,* vol. 9, p. 4-7.

NIST. 2008. *Security Considerations in the Information System Development Life Cycle*. SP 800-64: National Institute ofstandatds and Technology, 67 p.

NIST. 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach*. SP 800-37 Rev 1: National Institute ofstandatds and Technology, 93 p.

NIST. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations* SP 800-53 Rev 4: National Institute ofstandatds and Technology, 457 p.

Nunes, F. J. B., A. D. Belchior et A. B. Albuquerque. 2010. « Security Engineering Approach to Support Software Security ». In *Services (SERVICES-1), 2010 6th World Congress on*. (5-10 July 2010), p. 48-55.

nurun. 2011. « Sécurité dans les développements ». In *nurun*. En ligne. < http://www.nurun.com/servicesconseils/fiche/securite-dans-les-developpements >. Consulté le 16 février 2014.

Nworie, John 2011. « Using the Delphi Technique in EducationalTechnology Research ». *TechTrends,* vol. 55, n° 5, p. 24-30.

OCDE, Organisation de Coopération et de Développement Économiques. 2002. *Vers une culture de la sécurité*. Manuel électronique. Coll. « Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité », 28 p.

Office, US Government Accountability. 2006. *Information Assurance: National Partnership Offers Benefits, but Faces Considerable Challenges*. Rapport électronique. 36 p. < http://www.gao.gov/search?search_type=Solr&o=0&facets=a%3A2%3A{s%3A7%3A%22docdate%22%3Bs%3A22%3A%222006-01-01to2006-12-31%22%3Bs%3A4%3A%22site%22%3Bs%3A12%3A%22Publications%22%3B}&q=%22Common+Criteria+evaluations%22 >.

OGC, Office of Government Commerce. 2007. *The Official Introduction to the ITIL Service Lifecycle*. Manuel électronique. Coll. « ITIL ». London: The Stationery Office.

Okoli, Chitu, et Suzanne D. Pawlowski. 2004. « The Delphi Method as a Research Tool: An Example, Design Considerations and Applications ». *Information & Management,* vol. 42, n° 1, p. 15-29.

OWASP. 2005. *A Guide to Building Secure Web Applications and Web Services*. Manuel électronique. Coll. « 2.0 Black Hat Edition », 293 p.

OWASP. 2006. *CLASP Project (Comprehensive, Lightweight Application Security Process) - Concepts* 1.2. Manuel électronique. OWASP Foundation, 16 p.

OWASP. 2008a. *Code review guide*, 1.1. Manuel électronique. 215 p.

OWASP. 2008 b. *Testing guide*, 3.0. Manuel électronique. OWASP Foundation, 350 p.

OWASP. 2010. *OWASP Secure Coding Practices - Quick Reference Guide*, 2.0. Manuel électronique. OWASP Foundation, 17 p.

OWASP. 2013. *OWASP Top 10 - 2013; Les Dix Risques de Sécurité Applicatifs Web les Plus Critiques*, 2013. Manuel électronique. OWASP Foundation, 22 p.

OWASP. 2014. « OWASP Secure Coding Principles ». In *OWASP - Open Web Application Security Project*. En ligne. < https://www.owasp.org/index.php/Secure_Coding_Principles >. Consulté le 21 janvier 2014.

Paquet, Catherine, et Warren Saxe. 2005. *The business case for network security: advocacy, governance, and ROI*. Livre. Coll. « Network Business Series ». Cisco Press.

Pavlidis, M., H. Mouratidis, S. Islam et P. Kearney. 2012. « Dealing with trust and control: A meta-model for trustworthy information systems development ». In *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on*. (16-18 May 2012), p. 1-9.

PECB. 2013a. « Certified ISO 27034 Foundation ». Document électronique. Montréal, Québec: Professional Evaluation and Certification Board, 1 p. < https://pecb.org/en/iso-27034 >.

PECB. 2013 b. « Certified ISO 27034 Lead auditor ». Document électronique. Montréal, Québec: Professional Evaluation and Certification Board, 4 p. < https://pecb.org/en/iso-27034 >.

PECB. 2013c. « Certified ISO 27034 Lead implementer ». Document électronique. Montréal, Québec: Professional Evaluation and Certification Board, 4 p. < https://pecb.org/en/iso-27034 >.

Peterson, Gunnar. 2010. « Don't Trust. And Verify: A Security Architecture Stack for the Cloud ». *Security & Privacy, IEEE,* vol. 8, n° 5, p. 83-86.

Pfleeger, Charles P. 1989. *Security in computing*. Livre. Englewood Cliffs, N.J.: Prentice-Hall, xxi, 538 p. p.

Pfleeger, Charles P. , et Shari Lawrence Pfleeger. 2008. *Security in computing*, 4ième édition. Livre. Upper Saddle River, NJ: Prentice Hall PTR, XXIX, 845 p.

PMI. 2008. *A guide to the project management body of Knowledge (PMBOK Guide)*, Fourth Edition. Livre électronique. Pennsylvania, USA: Project Management Institute, 459 p.

Poulin, Luc. 2002. « Méthodologie et politique de sécurité « Security Policy Markup Language » ». Mémoire de maîtrise. Québec, Université Laval, 184 p.

Poulin, Luc. 2006a. *Annexes du rapport d'audit détaillé des systèmes de votation électronique utilisés au Québec lors des élections municipales 2005*. Rapport électronique. Québec: CRIM, 101 p.

Poulin, Luc. 2006 b. « Application Security – Integration of security concerns in the system life cycle ». In. (Johannesburg, South Africa, 13 novembre 2006), p. 35. ISIQ.

Poulin, Luc. 2006c. *Rapport d'audit détaillé des systèmes de votation électronique utilisés au Québec lors des élections municipales 2005*. Rapport électronique. Québec: CRIM, 120 p.

Poulin, Luc. 2007a. « Application Security - Definition and scope ». In *10.0 Russie*. (MS Lenin, Russie, 6 mai 2007), sous la dir. de Poulin, Luc, p. 5.

Poulin, Luc. 2007 b. « Application Security - Integration of security concerns in the system life cycle ». In *10.0 Russie*. (MS Lenin, Russie, 7 mai 2007), sous la dir. de Poulin, Luc, p. 51. ISIQ.

Poulin, Luc. 2007c. « Application Security - SCPIP Quebec Gov Projects ». In *10.0 Russie*. (MS Lenin, Russie, 8 mai 2007), sous la dir. de Poulin, Luc, p. 8. Luc Poulin.

Poulin, Luc. 2007d. « ISO/IEC 27034 Application Security, Integration of application security measures in the system lifecycle - All Diagrams EN, 6.0 ». In *20.0 Lucerne*. (Québec, Québec, octobre 2007), sous la dir. de Poulin, Luc, p. 18. Luc Poulin.

Poulin, Luc. 2007e. « Un piège pour la démocratie? Systèmes de votations électroniques - Démarche et résultats de l'audit de sécurité réalisé sur les systèmes de votations électroniques utilisés lors des élections municipales 2005 au Québec ». In. (Québec, Canada, 21 juin 2007), sous la dir. de Poulin, Luc, p. 41.

Poulin, Luc. 2008a. *Arrimage des activités du cycle de vie de 27034 avec 12207 et 15288, partie 1*. Rapport électronique. Coll. « 20.1 Kyoto ». Kyoto Japon: Luc Poulin, 8 p.

Poulin, Luc. 2008 b. *Arrimage des activités du cycle de vie de 27034 avec 12207 et 15288, partie 2*. Rapport électronique. Coll. « 20.1 Kyoto ». Kyoto Japon: Luc Poulin, 18 p.

Poulin, Luc. 2008c. « La qualité - Une alliée essentielle dans la sécurité d'une application ». In. (Québec, Canada, 14 mai 2008), sous la dir. de Poulin, Luc, p. 39.

Poulin, Luc. 2008d. « La sécurité des applications - Approche pratique d'évaluation de la sécurité d'une application ou d'un système : étude de cas ». In. (Québec, Canada, 9 décembre 2008), sous la dir. de Poulin, Luc, p. 43.

Poulin, Luc. 2009a. *Alignment of ISO-27034 Application Security with ISO-27005 Security Risk Analysis*. Rapport électronique. Coll. « 20.3 Beijing ». Québec, Canada: Luc Poulin, 2 p.

Poulin, Luc. 2009b. *Arrimage cycle de vie - Securité vs 12207*. Rapport électronique. Coll. « 20.3 Beijing ». Québec, Canada: Luc Poulin, 20 p.

Poulin, Luc. 2009c. « ISO/IEC 27034 – Application Security: Overview – A standard to implement and maintain security in applications for their life cycles ». In. (Québec, Canada, 26 mars 2008), p. 36. Washinton DC, Maryland: ISIQ.

Poulin, Luc. 2009d. « ISO/IEC 27034 Application Security Management Processes - Diagrams ». In *20.3 Beijing* (4 janvier 2009), sous la dir. de Poulin, Luc Diagrammes électronique. p. 2. Québec, Québec: Luc Poulin.

Poulin, Luc. 2009e. « ISO/IEC 27034 Application Security: Overview - A standard to implement and maintain security in applications for their life cycles ». In *20.3 Beijing*. (Québec, Canada, 12 mai 2009), v3.1, p. 36. Luc Poulin.

Poulin, Luc. 2010a. *The concept of "Level of Trust" in ISO/IEC 27034*. Rapport électronique. Coll. « 30.2 Melaka ». Redmond, US: Luc Poulin, 4 p.

Poulin, Luc. 2010b. « Développer et maintenir un système sécuritaire : intégrer des activités de sécurité durant tout le cycle de vie de l'application ». In. (Québec, Canada, 28 mars 2010), sous la dir. de Poulin, Luc, p. 80. ISIQ, MSG.

Poulin, Luc. 2010c. « Développer et maintenir un système sécuritaire : réalité ou fiction ». In. (Montréal, Canada, 18 mai 2010), p. 17. ISIQ.

Poulin, Luc. 2011a. « L'intégration de la sécurité dans le cycle de développement d'une application : une approche gagnante ». In. (Montréal, Canada, 9 février 2011), p. 17. Cogentas inc.

Poulin, Luc. 2011b. « Projet 763B26 – Sécurité des applications Desjardins - Les principaux éléments ». In. (Montréal, Canada, 10 novembre 2011), p. 10. Mouvement Desjardins.

Poulin, Luc. 2013a. « La sécurité des applications - c'est plus que la sécurité dans le développement d'applications ». In. (Montréal, Canada, 11 novembre 2013), p. 44. Cogentas inc.

Poulin, Luc. 2013b. « Les systèmes de vote électronique : une stratégie de confiance ». In. (Québec, Canada, 27 février 2013), p. 54. Cogentas inc.

Poulin, Luc, et Stéphane Gagnon. 2009. « Développer un système sécuritaire - Réalité ou fiction? ». In. (Québec, Canada, 8 avril 2009), sous la dir. de Poulin, Luc, p. 76. ISIQ.

Poulin, Luc, et Bruno Guay. 2006a. « Module 1 - Introduction et concepts de base ». In (2006) Acétates électronique. p. 21. Coll. « IFT-22514 - Aspects Pratiques de la sécurité informatique ». Québec: Université Laval.

Poulin, Luc, et Bruno Guay. 2006b. « Module 8 - Applications, serveurs et systèmes - Développemetn d'applications ». In (2006) Acétates électronique. p. 70. Coll. « IFT-22514 - Aspects Pratiques de la sécurité informatique ». Québec: Université Laval.

Poulin, Luc, et Bruno Guay. 2006c. « Module 9 - Applications, serveurs et systèmes - Développement d'applications ». In (2006) Acétates électronique. p. 70. Coll. « IFT-22514 - Aspects Pratiques de la sécurité informatique ». Québec: Université Laval.

Poulin, Luc, et Bruno Guay. 2008. « ISO/IEC 27034 Application Security - Overview ». In *20.1 Kyoto*. (Kyoto, Japan, 14 avril 2008), sous la dir. de Poulin, Luc, p. 29. ISIQ.

Poulin, Luc, Laura Kuiper et Meng-Chow Kang. 2007. « Application Security - Meeting plan ». In *10.0 Russie*. (MS Lenin, Russie, 3 mai 2007), sous la dir. de Poulin, Luc, p. 26. Luc Poulin.

Poulin, Luc, et Denise Rouselle. 2007. *Relevant Standards who can be use to develop the Application Security standards*. Rapport électronique. Coll. « 10.0 Russie ». MSW Lenin, Russie: Luc Poulin, 24 p.

Poulin, Luc, Denise Rouselle et Johann Amsenga. 2008. *Relevant Standards who can be use to develop the Application Security standards*. Rapport électronique. Coll. « 20.1 Kyoto ». Kyoto Japon: Luc Poulin, 24 p.

Qun, Zhong, et Nigel Edwards. 1998. « Security control for COTS components ». *Computer,* vol. 31, n° 6, p. 67-73.

Reavis. 2013. *The emergence of software security standards: ISO/IEC 27034-1:2011 and your organization* Rapport électronique. Reavis Consulting Group, 15 p. Consulté le 22 mai 2013.

Ross, Ron, Marianne Swanson, Gary Stoneburner, Stu Katzke et Arnold Johnson. 2003. *Guide for the Security Certification and Accreditation of Federal Information Systems*. SP 800-37: National Institute ofstandatds and Technology, 62 p.

Runeson, Per, et Martin Höst. 2009. « Guidelines for conducting and reporting case study research in software engineering ». *Empir Software Eng,* vol. 14, p. 131-164.

Savard, Marco, et Luc Poulin. 2008. *Encadrer la profession informatique, maintenant une nécessité!* (juin 2008). Mémoire. Coll. « Mémoires de l'APIIQ ». Québec: Association professionnelle des informaticiens et informaticiennes du Québec, 127 p.

SC7, JTC1. 2003. *DTR 19759: Software Engineering - Guide to the Software Engineering Body of Knowledge (SWEBOK)*. Rapport électronique. Coll. « 30.1 Redmond ». Montréal, Québec: SC 7 Secretariat, 231 p.

SC27/WG4, JTC1. 2006a. *JTC 1/SC 27/WG 4 Liaison Statement to ITU-T SG17 on Collaborative work on Application Security*. Rapport électronique. Coll. « 00.0 Johanesbourg », SC27N5498. Berlin, Alemagne: DIN, Germany, 2 p.

SC27/WG4, JTC1. 2006b. *JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 7 on Collaborative work on Application Security*. Rapport électronique. Coll. « 00.0 Johanesbourg », SC27N5493: DIN, Germany, 2 p.

SC27/WG4, JTC1. 2006c. *JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 22 on Collaborative work on Application Security*. Rapport électronique. Coll. « 00.0 Johanesbourg », SC27N5494: DIN, Germany, 2 p.

SC27/WG4, JTC1. 2006d. *Report of the Application Security meeting, held in Glenburn Lodge (South Africa), Nov. 17th 2006*. Rapport électronique. Coll. « 00.0 Johanesbourg », SC27N5482: DIN, Germany, 7 p.

SC27/WG4, JTC1. 2007a. *ISO/IEC JTC 1/SC 27/WG 4 liaison statement to ITU-T SG17 on Collaborative work on Application Security*. Rapport électronique. Coll. « 10.0 Russie », SC27N5911: DIN, Germany, 2 p.

SC27/WG4, JTC1. 2007b. *ISO/IEC JTC 1/SC 27/WG 4 Liaison Statement to ITU-T SG17 on Guidelines for application security in response to SC 27 N6141rev1*. Rapport électronique. Coll. « 20.0 Lucerne », SC27N6027. Berlin, Alemagne: DIN, 2 p.

SC27/WG4, JTC1. 2007c. *ISO/IEC JTC 1/SC 27/WG 4 liaison statement to JTC 1/SC 7 on Collaborative work on Application Security*. Rapport électronique. Coll. « 10.0 Russie », SC27N5929: DIN, Germany, 2 p.

SC27/WG4, JTC1. 2007d. *ISO/IEC JTC 1/SC 27/WG 4 liaison statement to NESSI on Collaborative work on Application security*. Rapport électronique. Coll. « 10.0 Russie », SC27N5927: DIN, Germany, 2 p.

SC27/WG4, JTC1. 2007e. *JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 7 on Collaborative work on Application Security in response to SC 27 N6011 (SC 7 liaison statement)*. Rapport électronique. Coll. « 20.0 Lucerne », SC27N6080. Berlin, Alemagne: DIN, 2 p.

SC27/WG4, JTC1. 2007f. *JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 22 on Collaborative work on Application Security in response to SC 27 N5937 (SC 22 liaison statement)*. Rapport électronique. Coll. « 20.0 Lucerne », SC27N6033. Berlin, Alemagne: DIN, 2 p.

SC27/WG4, JTC1. 2007g. *Report of the SC27 WG4 Application Security meeting held on Lucerne, Switzerland, 1-5 october 2007*. Rapport électronique. Coll. « 20.0 Lucerne », SC27N5729: DIN, Germany, 4 p.

SC27/WG4, JTC1. 2008a. *ISO/IEC JTC 1/SC 27/WG 4 Liaison Statement to ITU-T SG17 on Collaborative work on Application security*. Rapport électronique. Coll. « 20.1 Kyoto », SC27N6782. Berlin, Alemagne: DIN, 2 p.

SC27/WG4, JTC1. 2008b. *JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 7 on Collaborative work on Application Security* Rapport électronique. Coll. « 20.1 Kyoto », SC27N6780. Berlin, Alemagne: DIN, 2 p.

SC27/WG4, JTC1. 2008c. *JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 22 on Collaborative work on Application Security*. Rapport électronique. Coll. « 20.1 Kyoto », SC27N6781. Berlin, Alemagne: DIN, 2 p.

SC27/WG4, JTC1. 2008d. *Report of the SC 27 WG 4 Application Security meeting held on Kyoto, Japan, 14-18 April 2008*. Rapport électronique. Coll. « 20.1 Kyoto »: DIN, Germany, 4 p.

SC27/WG4, JTC1. 2008e. *Report of the SC 27 WG 4 Application Security meeting held on Limassol, Cyprus, 6-10 October 2008*. Rapport électronique. Coll. « 20.2 Limasol »: DIN, Germany, 3 p.

SC27/WG4, JTC1. 2009a. *ISO/IEC JTC 1/SC 27/WG 4 Meeting No. 6, Beijing, P.R. China, May 4th to 8th, 2009 - Meeting Report*. Rapport électronique. Coll. « 20.3 Beijing », SC27/N7552. Beijing, P.R. China: DIN, Germany, 19 p.

SC27/WG4, JTC1. 2009b. *Report of the SC 27 WG 4 Application Security meeting held on Redmond, WA, USA, Nov. 2-6 2009*. Rapport électronique. Coll. « 30.1 Redmond », SC27/N7552. Redmond, US: DIN, Germany, 4 p.

SC27/WG4, JTC1. 2010a. *Report of the SC 27 WG 4 Application Security meeting held in Berlin, Germany, Oct. 4-8 2010*. Rapport électronique. Coll. « 40.1 Berlin ». Melaka, Indonésie: DIN, Germany, 3 p.

SC27/WG4, JTC1. 2010b. *Report of the SC 27 WG 4 Application Security meeting held on Melaka, Malaysia, 18-23 April 2010*. Rapport électronique. Coll. « 30.2 Melaka ». Melaka, Indonésie: DIN, Germany, 4 p.

SC27/WG4, JTC1. 2011. *Report of the SC 27 WG 4 Application Security meeting held in Singapore, April. 11th-15th, 2011*. Rapport électronique. Coll. « 40.2 Singapour ». Singapour: DIN, Germany, 7 p.

Schneier, Bruce. 1996. *Applied cryptography: protocols, algorithms, and source code in C* (1996), 2. Livre. Wiley & Son Inc., 758 p.

Schumacher, Marcus, Eduardo Fernandez-Buglioni, Duane Hyberston, Frank Bushmann et Peter Sommerlad (656). 2006. *Security patterns: integrating security and systems engineering*. Livre. John Wiley & Sons.

Seacord, Robert C. (Ed). 2013. *Secure Coding in C and C++*, 2nd Edition. Coll. « SEI Series in Software Engineering ». Addison-Wesley Professional, 600 p.

Seaman, Carolyn B. . 1999. « Qualitative Methods in Empirical Studies of Software Engineering ». *IEEE Transactions on software engineering,* vol. 25, n^{o} 4, p. 557-572.

SEI. 2007. *CERT C Programming Language Secure Coding Standard*. CERT N1255: Carnegie Mellon University, 488 p.

SEI, Software Engineering Institute. 2001. *OCTAVE Criteria, version 2.0*. Manuel électronique, CMU/SEI-2001-TR-016. Pittsburgh, PA: SEI, Software Engineering Institute, 143 p.

Sherief, N. H., A. A. Abdel-Hamid et K. M. Mahar. 2010. « Threat-driven modeling framework for secure software using aspect-oriented Stochastic Petri nets ». In *Informatics and Systems (INFOS), 2010 The 7th International Conference on*. (28-30 March 2010), p. 1-8.

Sinning, Daniel. 2011. « Projet 763B26 – Sécurité des applications Desjardins ». In *Les principaux éléments*. (Montréal, Québec, novembre 2011), p. 10. Mouvement Desjardins.

Skulmoski, Gregory J. , Francis T. Hartman et Jennifer Krahn. 2007. « The Delphi Method for Graduate Research ». *Journal of Information Technology Education,* vol. 6, p. 21.

Steel, Christopher, Ramesh Nagappan et Ray Lai. 2005. *Core security patterns: best practices and strategies for J2EE, Web services, and identity management*. Livre. Prentice Hall PTR, 1041 p.

Stoddart, Jennifer 2009. « Communiqués - Facebook accepte de répondre aux préoccupations de la commissaire à la protection de la vie privée. ». In *Commissariat à la protection de la vie privée du Canada*. Site Web.

Stoneburner, Gary, Alice Goguen et Alexis Feringa. 2002. *Risk Management Guide for Information Technology Systems*. SP 800-30. Falls Church, VA: National Institute of Standards and Technology, 55 p.

Stoneburner, Gary, Clark Hayden et Alexis Feringa. 2004. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*. SP 800-27 Rev A: National Institute of standatds and Technology, 35 p.

Takebe, Tatsuaki. 2009. « Processus de gestion de la sécurité d'une application ». In *30.1 Redmond* (29 juin 2009), sous la dir. de 27, Comité Japonais au SC, v3.0 Rapport électronique. Tokyo, Japon: Comité Japonais au SC 27.

Timson, Lia. 2013. « If it's worth coding, it's worth securing ». In *The Age*. En ligne. < http://www.theage.com.au/it-pro/security-it/if-its-worth-coding-its-worth-securing-20130515-2jlmr.html#ixzz2TPy22oeK >. Consulté le 17 février 2014.

van Lamsweerde, Axel. 2004. « Elaborating security requirements by construction of intentional anti-models ». In *Software Engineering, 2004. ICSE 2004. Proceedings. 26th International Conference on*. (23-28 May 2004), p. 148-157.

van Wyk, K. R., et Gary McGraw. 2005. « Bridging the gap between software development and information security ». *Security & Privacy, IEEE,* vol. 3, n^{o} 5, p. 75-79.

Venne, Michel. 1994. *Vie privée et démocratie à l'ère de l'information* (Janv. 1 1994). Livre. Coll. « Collection Diagnostic ». Presses de l'Université Laval Diffusion, 122 p. p.

Viega, John, et Gary McGraw. 2002. *Building secure software: how to avoid security problems the right way*. Livre. Addison-Wesley.

Walton, G. H., T. A. Longstaff et R. C. Linger. 2009. « Computational Evaluation of Software Security Attributes ». In *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*. (5-8 Jan. 2009), p. 1-10.

White, Jon, Duminda Wijesekera et Mark Hatton. 2008. « Executable misuse cases for modeling security concerns ». In *Software Engineering, 2008. ICSE '08. ACM/IEEE 30th International Conference on*. (10-18 May 2008), p. 121-130.

Whittaker, James A. , et Herbert H. Thompson. 2004. *How to break software security: effective techniques for security testing*. Livre. 185 p.

Wiegers, Karl Eugene. 2003. *Software requirements: practical techniques for gathering and managing requirements throughout the product development cycle*, Second Edition. Livre. Microsoft Press, 544 p.

Yi, Deng, Wang Jiacun, J. J. P. Tsai et K. Beznosov. 2003. « An approach for modeling and analysis of security system architectures ». *Knowledge and Data Engineering, IEEE Transactions on*. Article. Vol. 15, n^{o} 5, p. 1099-1119.

Zenah, N. H. Z., et N. A. Aziz. 2011. « Secure coding in software development ». In *Software Engineering (MySEC), 2011 5th Malaysian Conference in*. (13-14 Dec. 2011), p. 458-464.