L'évolution du modèle de la sécurité des applications

Un modèle utilisé pour intégrer la sécurité dans le cycle de vie des applications

Luc Poulin [a], Alain Abran [b] et Alain April [b]

[a] Cogentas – Institut de la sécurité des applications
10-1159 boulevard Jean-Talon O. Québec (Québec) Canada

[b] Département de génie logiciel et des TI
École de technologie supérieure – Université du Québec
1100, rue Notre-Dame Ouest, Montréal (Québec) Canada

RÉSUMÉ

Bien que beaucoup de processus, de méthodes et d'outils liés à la sécurité soient disponibles depuis des années, l'industrie du logiciel reste confrontée au défi de développer et de maintenir des applications sécuritaires. Un deuxième défi est lancé lorsque l'on demande à une organisation de démontrer, à l'aide de preuves vérifiables et répétables, la sécurité de son application. Un troisième défi apparaît lorsqu'il s'agit d'estimer et de gérer le coût de mise en place de la sécurité, et ce dans le respect des ressources et des capacités d'une organisation. La sécurité a un coût et toutes les organisations n'ont pas les mêmes besoins de sécurité.

Le modèle de la sécurité des applications (modèle SA) permet à une organisation de relever ces trois défis. Il lui permet notamment de déterminer un niveau de confiance mesurable et vérifiable, nécessaire pour utiliser une application de manière sécuritaire dans un environnement spécifique. Il lui permet aussi d'estimer les impacts des risques de sécurité ainsi que les coûts de mise en place des contrôles servant à atténuer ces risques, de manière à pouvoir en tenir compte lors du choix du niveau de confiance ciblé pour une application. Finalement, le modèle SA permet d'intégrer, de gérer et de vérifier les contrôles de sécurité tout au long du cycle de vie d'une application, afin d'améliorer la sécurité des informations sensibles qu'elle conserve, utilise et communique, et à fournir les preuves que le niveau de confiance ciblé pour son application a été atteint et est maintenu.

Même si plus de deux années se sont écoulées depuis la publication du modèle SA dans la norme ISO/IEC 27034 en décembre 2011, ce modèle est encore jeune et il évolue rapidement. Cet article introduit le modèle SA et présente certaines innovations amenées par son évolution.

Mots-clés: sécurité des applications, des systèmes de sécurité, ingénierie des systèmes, ISO 27001, ISO 27034, sécurité de l'information, ISO 15288, ISO 12207

I. INTRODUCTION

Les organisations doivent protéger leurs informations afin de demeurer en affaires. L'information des organisations

est de plus en plus mise en danger par les vulnérabilités des applications[1]. Il est donc essentiel que les organisations soient en mesure de gérer les risques et les coûts de la sécurité au niveau de l'application par la mise en œuvre des contrôles de sécurité de l'application, par la gestion des coûts de cette mise en œuvre et par l'obtention de preuves de l'efficacité de l'implémentation de ces derniers.

Bien que beaucoup de processus, des méthodes et des outils liés à la sécurité soient disponibles depuis des années (tels que les Critères Communs [1], le SSE-CMM [2] et les guides de l'OWASP [3-5]), l'industrie du logiciel reste confrontée au défi de développer et de maintenir des applications sécuritaires.

Sachant que les risques de sécurité des applications (SA), tout comme les risques de sécurité de l'information, proviennent principalement des personnes, des processus et de la technologie [6], ISO à publié dans une nouvelle norme un modèle de la sécurité des applications (modèle SA) qui aidera à atténuer ces risques en :

- définissant et encadrant l'implémentation de contrôles de sécurité des applications (CSA) vérifiables,
- tenant compte de l'estimation des coûts de la mise en place et de la vérification des CSA en fonction de l'impact des risques que les CSA permettent d'atténuer,
- aidant l'identification des qualifications requises par certains rôles et personnes, et
- permettant de définir des directives pour appliquer ces contrôles à des processus de l'application et aux technologies utilisées et supportées par ces personnes.

Le modèle SA permet notamment à une organisation d'intégrer, de gérer et de vérifier les contrôles de sécurité tout au long du cycle de vie d'une application, afin d'améliorer la sécurité des informations sensibles qu'elle conserve, utilise et communique. Il permet aussi lui fournir à l'organisation qui l'utilise les preuves que le niveau de confiance qu'elle a ciblée pour son application a été atteint et est maintenu.

Même si plus de deux années se sont écoulés depuis la publication du modèle SA dans la norme *ISO/IEC 27034 – Application Security, Part 1: Overview and concepts* [7] en décembre 2011, ce modèle, tout comme le domaine de la sécurité des applications, est encore jeune et il évolue rapidement.

Cet article présente sommairement l'évolution du modèle SA [8] depuis sa publication dans la norme. Il présente des figures alternatives servant à décrire certains concepts, incluant l'introduction d'un nouveau composant : la matrice de traçabilité de la SA.

Quatre groupes de personnes ont été ciblés pour ce modèle SA :

1) **les gestionnaires,** qui doivent gérer les risques, les exigences de sécurité, les ressources et qui peuvent être responsables de la sécurité des applications;
2) **les équipes de projet, les acquéreurs et fournisseurs,** qui doivent satisfaire aux exigences de sécurité pour la mise en œuvre et la gestion des contrôles de sécurité de l'application tout au long du cycle de vie de celle-ci;
3) **les auditeurs,** qui doivent vérifier et appliquer une vérification des réalisations de sécurité sur un champ d'application défini à l'aide d'outils pour obtenir des résultats reproductibles;
4) **les utilisateurs finaux,** qui ont besoin de faire confiance aux applications qu'ils utilisent.

Cet article est structuré de la façon suivante. La section « 2 Les fondements de sécurité des applications » introduit le contexte, les termes et définitions, les principes et les concepts sur lesquels s'appuie le modèle SA. La section « 3 Le modèle SA » présente une description sommaire des principaux composants et processus du modèle SA

[1] Système utilisant les technologies de l'information (TI), dont du logiciel, développé et utilisé pour répondre à des besoins d'affaires.

II. LES FONDEMENTS DE SÉCURITÉ DES APPLICATIONS

II.I Contexte

Le modèle élaboré pour la SA est utilisé pour identifier les risques et les exigences de sécurité, ainsi que pour mettre en œuvre des contrôles de sécurité des applications (CSA) adéquats et vérifiables afin de permettre un niveau de confiance approprié indiquant que la sécurité d'une application est suffisante, compte tenu de son environnement opérationnel.

Ce modèle SA vise à aider les organisations à intégrer la sécurité de façon transparente tout au long du cycle de vie de leurs applications en offrant des concepts, des principes, un cadre normatif, des composants et des processus. Il peut également être utilisé pour établir des critères d'acceptation pour l'acquisition d'applications, ou l'externalisation du développement et de l'exploitation de leurs applications.

II.II Termes et définitions

Une réponse à une des problématiques identifiées lors de la conception du modèle SA a été de préciser des termes qui, même si certains d'entre eux étaient déjà utilisés par des professionnels, n'avaient pas nécessairement la même définition ou la même portée, selon que le professionnel œuvrait dans le secteur de la gouvernance de la sécurité, de l'ingénierie logicielle ou des infrastructures TI. Cette problématique de vocabulaire pouvait, dans certaines circonstances, générer des risques sur la sécurité d'une application.

Les termes et définitions présentés au Tableau 1 ont été précisés durant la conception du modèle SA. Par exemple le terme « niveau de confiance ciblé » est défini dans le modèle SA comme « une étiquette identifiant les contrôles de sécurité des applications qui devraient être mis en œuvre durant le cycle de vie d'une application ».

Les notes ont été ajoutées au Tableau 1 pour présenter les précisions apportées par l'évolution du modèle SA.

Tableau 1 – Termes et définitions

Terme	**Définitions**
Application	Système TI supportant des besoins d'affaires de l'organisation. NOTE Cette définition est plus simple et plus claire que de celle publiée, tout en ayant la même portée.
Sécurité des applications (SA)	Protéger les informations impliquées par l'utilisation d'une application. NOTE Ce terme n'est pas défini dans le modèle SA initial. Il précise l'objectif ultime, pourquoi une organisation déciderait-elle de protéger une application.
Contrôle sécurité des applications (CSA)	Un contrôle incluant notamment des références à un niveau de confiance, à des exigences de sécurité, à une activité de sécurité et à une activité de mesure et de vérification. NOTE Un CSA doit obligatoirement décrire une activité de vérification associée à l'activité de sécurité qu'il contient. Lorsqu'elles sont définies, ces deux activités doivent obligatoirement être réalisées et produire les résultats escomptés pour que l'on considère que le CSA a bien été implémenté.
Niveau de confiance (NdC)	Étiquette identifiant une liste de CSA
Niveau de confiance ciblé	Étiquette assignée à une application, identifiant la liste de CSA qui devrait être mis en œuvre au cours de son cycle de vie.

Terme	Définitions
Niveau de confiance actuel	Étiquette identifiant une liste de CSA qui ont passé avec succès l'activité de mesure de vérification en produisant au moment prévu, les résultats escomptés.
Application sécuritaire	Application pour laquelle le niveau de confiance actuel est égal au niveau de confiance ciblé, tel que déterminé par l'organisation qui utilise ou qui possède l'application. NOTE Ajout du concept de détenteur dans la définition.
Cadre normatif de l'organisation (CNO)	Dépôt autoritaire contenant l'ensemble des processus et des éléments normatifs de SA approuvés par l'organisation. NOTE Ajout du concept de source autoritaire dans la définition.
Cadre normatif de l'application (CNA)	Dépôt autoritaire, extrait du CNO, contenant l'ensemble des processus et des éléments normatifs de SA nécessaires à la sécurisation d'une application. NOTE Ajout du concept de source autoritaire dans la définition.

II.III Principes

Le modèle SA est basé sur les principes suivants :

1) La sécurité d'une application doit être gérée

La SA est liée à la gestion des différents risques de sécurité amenés par l'utilisation d'une application dans un environnement spécifique. Sachant que l'on ne peut gérer ce qui n'est pas connu, tous les types d'activités des parties prenantes, ainsi que tous les aspects de leurs opérations dans l'environnement d'une application, doivent être identifiés et évalués régulièrement afin de pouvoir définir les exigences de sécurité qui devront être respectées.

NOTE Ce principe n'est pas implicitement défini dans le modèle SA initial, même s'il y est présent. Le fait de préciser ce principe indique qu'on ne peut considérer une application indéfiniment. Les critères indiquant la nécessité d'une nouvelle vérification de la sécurité d'une application font partie des paramètres à identifier lorsque le modèle SA est déployé dans une organisation.

2) La sécurité est une exigence

Les exigences de sécurité doivent être définies et analysées pour chaque étape du cycle de vie d'une application, traitées de façon adéquate et gérées sur une base continue.

3) La sécurité des applications est dépendante du contexte

Les besoins en sécurité sont identifiés et évalués à partir de trois perspectives :

a) le contexte d'affaires;

Le contexte d'affaires est défini à partir de la ligne d'affaires et des besoins d'affaires d'une organisation. Des applications médicales ne nécessiteront peut-être pas la même sécurité que des applications financières. Des commerces de cartier pourraient ne pas exiger la même sécurité pour leurs applications que celle qui serait exigée par une organisation gouvernementale ayant à gérer l'impôt sur le revenu de ses citoyens. Chaque organisation doit définir ses propres exigences de sécurité en fonction de son contexte d'affaires – en tenant compte, par exemple, des informations sensibles de leur secteur d'activité, des règles de l'organisation et des ressources dont elle dispose.

b) le contexte juridique;

Une application utilisée dans une province ou une région de n'importe lequel pays peut avoir à se conformer aux réglementations régionales et nationales. Une application peut être considérée comme étant sécuritaire aux États-Unis et ne pas l'être en Europe, car elle ne répondra qu'à la loi sur la protection des

renseignements personnels américaine. En outre, des règlements d'un pays peuvent exiger que les données de ses citoyens demeurent sur son territoire et qu'elles ne doivent pas être stockées ou sauvegardées dans une base de données qui serait localisée en dehors de ses frontières.

NOTE Le modèle SA précisait initialement le contexte règlementaire et non pas le contexte juridique. Il apparait aujourd'hui plus pratique de regrouper dans ce contexte l'identification des lois et règlements en vigueur à une région géographique, et de conserver dans le contexte d'affaires, les directives et règlements de l'organisation ainsi que ceux qui proviennent de sa ligne d'affaires.

c) le contexte technologique;

Les applications sont exposées à des risques qui dépendent de la technologie qu'elles utilisent ou qui les soutiennent : par exemple les applications fonctionnant sur Windows, Mac OS X ou Unix; les applications utilisant un réseau local, un réseau GSM ou le réseau Internet; les applications développées pour fonctionner sur le Web, sur un serveur mobile ou sur un poste de travail; les applications qui offrent des services de paiement en ligne, des services bancaires en ligne ou des services de communications chiffrés.

4) Des investissements appropriés à la sécurité d'une application doivent être réalisés

Une organisation gouvernementale qui utiliserait une application ne ferait certainement pas face aux mêmes impacts de sécurité qu'un commerce de détail ou qu'une banque si elles utilisaient toutes la même application : chaque organisation doit investir les ressources appropriées pour protéger adéquatement ses applications.

5) La sécurité d'une application doit pouvoir être démontrée

Chaque fois qu'une personne ou une organisation déclarera qu'une application est sécuritaire, celle-ci devra être en mesure de fournir des preuves tangibles et reproductibles qui soutiendront ces déclarations.

II.IV Concepts

II.IV.i Environnement de l'application

La Figure 1 illustre que l'environnement de l'application n'est plus limité qu'à la seule infrastructure technologique : il comprend également les contextes d'affaires, juridiques et technologiques, ainsi que les spécifications de l'application.

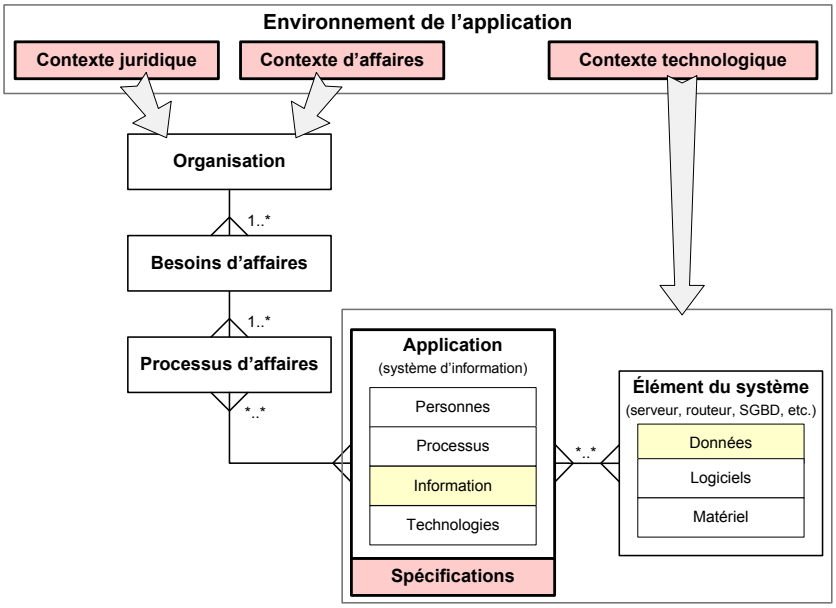

Figure 1 L'environnement de l'application

Les contextes d'affaires et juridiques dépendent de « pourquoi », « comment » et « où » l'organisation a besoin de l'application. Le contexte technologique dépend des personnes, des processus et de la technologie nécessaires pour développer, opérer et maintenir une application. Les spécifications sont spécifiées à partir des critères et des

exigences qui doivent être remplis et respectés par l'application via les fonctionnalités fournies.

Toute modification de l'un de ces quatre éléments peut avoir un impact significatif sur les risques de sécurité qui menacent l'information impliquée par une application.

NOTE Cette figure n'a pas été publiée avec le modèle SA initial.

II.IV.ii Portée de la sécurité d'une application

Pour être en mesure de protéger l'information impliquée par une application, cette information doit être définie.

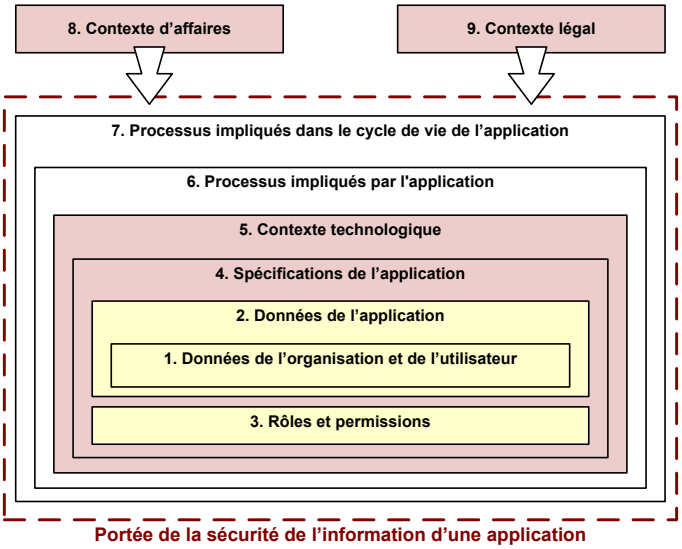

Figure 2 Portée de la sécurité de l'information d'une application *(traduit et adapté d'ISO 27034)* [2]

La Figure 2 présente différemment les neuf catégories dans lesquelles des groupes d'information peuvent être définis dans le modèle SA pour en préciser la portée.

NOTE Cette représentation permet de représenter les niveaux d'abstraction des différents groupes de données impliqués par une application, en partant en son centre, des données de l'organisation et de l'utilisateur (1), qui sont ultimement ce qui est à protéger. Puis en s'éloignant couche par couche, jusqu'au groupe d'information contenant la description des processus impliqués dans le cycle de vie de l'application (7), soit notamment de sont développement, de sa maintenance, de sa gestion, de son support et de son utilisation.

1) **Les données de l'organisation et des utilisateurs**, telles que les certificats, les clés privées, les transactions, les profils, les journaux, les documents et les fichiers.
2) **Les rôles et les permissions**, telles que les données d'identification et d'authentification et les données d'autorisation.
3) **Les données de l'application**, telles que les paramètres de configuration des applications, le code binaire de l'application : la gestion des versions de code, stockage, le code source, les composants et les bibliothèques commerciales.
4) **Les spécifications de l'application**, telles que les spécifications, les critères et les fonctions requis ou offerts par l'application, autant du côté client que du côté serveur.
5) **Le contexte technologique**, tel que les composants et les périphériques autorisés, le système d'exploitation, les configurations et les services extérieurs nécessaires à l'application, y compris son infrastructure technologique.
6) **Les processus impliqués par l'application**, tels que les processus de déploiement, d'installation, d'exploitation, de gestion, de sauvegarde et de contingence.

[2] Certaines figures provenant de la norme ISO/IEC 27034 ont été adaptées dans cet article afin de permettre l'intégration des changements amenés par l'avancement de nos travaux de recherches.

7) **Les processus impliqués dans le cycle de vie de l'application**, tels que les processus associés à des services et à des applications connexes, des processus de formation, de développement, de gestion de projet, de gestion des versions, de contrôle, incluant aussi les processus définissant et désignant les rôles, les responsabilités et les qualifications de tous les acteurs concernés par l'application.

8) **Le contexte d'affaires**, tel que les réalités et les contraintes amenées par l'organisation ou par sa ligne d'affaires, incluant ses politiques internes, ses directives et ses règlements, ses processus d'affaires et ses façons de faire en vigueur.

9) **Le contexte juridique**, tel que des ensembles de lois, les politiques et les règlements régionaux qui s'appliquent ou limitent l'utilisation de l'application.

II.IV.iii Quatre secteurs d'intervention en SA

Pour être en mesure de protéger l'information impliquée par une application, quatre secteurs d'intervention en SA doivent travailler ensemble :

1) **L'équipe de gestion**, qui doit gérer l'entreprise et les applications et veiller à ce que seules les personnes autorisées aient accès aux informations pertinentes.

2) **L'équipe de l'infrastructure TI**, qui a besoin d'installer, de supporter et de maintenir tous les composants de l'infrastructure TI, incluant les environnements de développement, de tests et d'opération.

3) **L'équipe de développement**, qui a besoin d'utiliser des outils pour développer, corriger, maintenir et supporter une application.

4) **L'équipe des auditeurs**, qui a besoin de vérifier et d'auditer une application.

Ces quatre groupes de personnes doivent partager la même vision, les mêmes concepts et le même vocabulaire de la SA. Leurs besoins en SA doivent être comblés par le modèle SA.

II.IV.iv Source des risques de la sécurité des applications

Les sources des risques de la sécurité d'une application sont multiples. Ils peuvent provenir autant des personnes, des processus et des technologies évoluant à l'intérieur de l'environnement de l'application durant son cycle de vie.

Les personnes peuvent volontairement ou involontairement faire des actions qui vont provoquer une brèche de sécurité sur l'intégrité, la confidentialité, ou encore la disponibilité des informations impliquées par une application. Les processus de l'organisation peuvent être désuets ou inadaptés à l'utilisation d'une application et ainsi mettre en péril ses informations. Des composants TI peuvent échouer, être compromis ou être volés, ce qui fait que l'information, qui y était conservée pourrait être corrompue, divulguée ou perdue.

Par exemple selon le contexte d'affaires et juridique où est utilisée une application, la mise en œuvre d'un processus de contingence inadéquat pourrait causer un impact plus important que celui causé si sa fonctionnalité de paiement en ligne était attaqué de l'Internet.

NOTE Cet élément n'est pas précisé dans le modèle SA initial.

II.IV.v Intégration des contrôles de la sécurité des applications dans le cycle de vie de l'application

Afin de minimiser les efforts et les coûts de mise en œuvre de la sécurité dans un projet d'application, l'une des stratégies est d'intégrer les contrôles de sécurité de l'application (CSA) à l'intérieur des processus que l'organisation a mis en place pour couvrir les phases du cycle de vie qui la concerne, sans lui demander de modifier ses activités existantes. Étant respectueuse des façons de faire en vigueur dans l'organisation, cette stratégie permet également de réduire la résistance aux changements des personnes qui auront à la mettre en œuvre, à vérifier ou à utiliser l'application avec ses contrôles de sécurité.

Une organisation qui développe des applications pourra notamment intégrer des CSA dans ses processus existants de développement, de déploiement et de tests sans avoir à changer complètement ses façons de faire. De la même manière, une organisation qui a acquis une application pourra de sont coté intégrer des CSA dans ses processus de gestions, de support, de contingence ou d'archivages. Dans ces deux cas, l'organisation sera en mesure de démontrer, preuves à l'appui, que tous les CSA exigés par le niveau de confiance qu'elle aura assignée à son application, ont été mis en œuvre, ont été vérifiés et qu'ils fonctionnent tous, tel que prévu.

III. LE MODÈLE SA

Le modèle SA propose des éléments qui doivent être choisis et mis en œuvre par l'organisation, en fonction de ses priorités et des ressources dont elle dispose. Cette section présente les principaux composants et processus, fournis par le modèle SA, qui peuvent être mis en œuvre par une organisation pour sécuriser ses applications.

III.I Les composants du modèle SA

Cette section présente les six composants clés du modèle SA.

III.I.i Le modèle de référence du cycle de vie de la sécurité d'une application

La Figure 3 présente le modèle de référence du cycle de vie de la sécurité d'une application. Il est composé de quatre couches, de cinq étapes, de 15 zones d'activité et de nombreux rôles identifiant les acteurs qui y sont impliqués. Les couches du modèle de référence permettent d'aligner les activités des personnes œuvrant dans les quatre secteurs d'intervention.

Le cycle de la SA a été défini pour être utilisé comme un modèle de référence de processus qui sert à :

1) fournir une référence commune pour les couches, les phases, les zones d'activité, les activités et les acteurs présents dans le cycle de vie d'une application typique et qui peuvent avoir un impact sur sa sécurité;
2) aider les organisations à identifier les éléments manquants qui pourraient être nécessaires à leurs besoins de sécurité;
3) aligner toute méthode de développement, de maintenance, de gestion de l'infrastructure TI ou de cycle de vie, telle que le PMI, OpenUP, ITIL, ou Cobit, déjà en usage dans la plupart des organisations;
4) identifier les CSA (voir Figure 4) servant à préciser « quand » une activité de sécurité et une activité de vérification doivent être réalisées, soit : avant, pendant ou après une activité définie dans l'une des couches, stades et zones d'activité de ce modèle de référence;

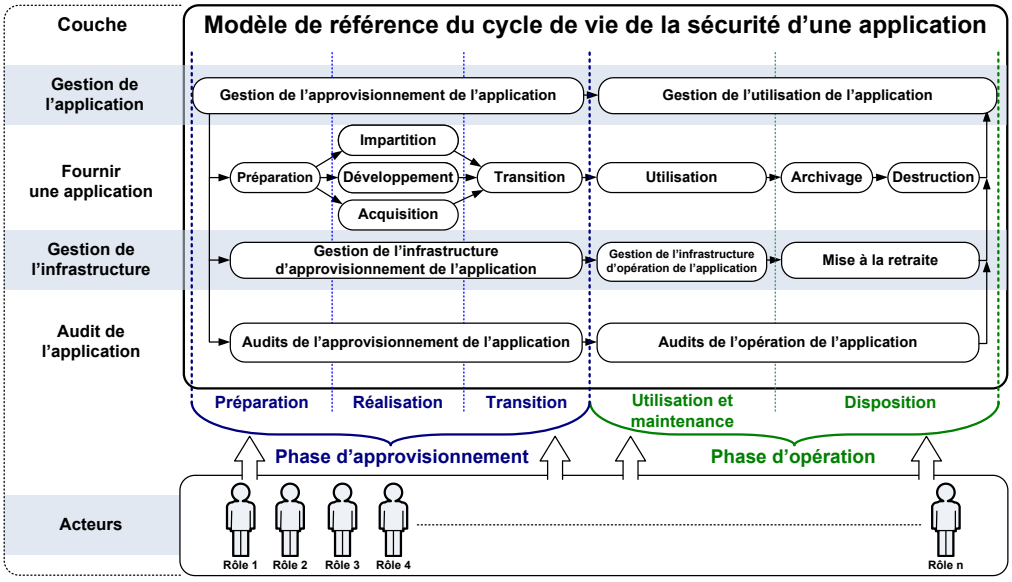

Figure 3 Représentation simplifiée du modèle de référence du cycle de vie de la SA *(traduit et adapté d'ISO 27034)*

NOTE Le nom initial de la couche « approvisionner et opérer l'application » a été changé dans la Figure 3 pour « Fournir une application » afin d'éviter de répéter les noms des phases du cycle de vie dans le nom de cette couche. Les phases « Archivage » et « Destruction » du modèle de référence initial ont été fusionnées dans la phase « Disposition » afin d'améliorer son alignement avec les phases de cycle de vie présentées dans les normes ISO/IEC 15288 et ISO/IEC 12207.

III.I.ii Le contrôle de la sécurité des applications (CSA)

Dans le modèle SA, un contrôle de sécurité des applications (CSA) décrit formellement ce qui devra être fait pour répondre à un besoin de sécurité, et ainsi atténuer un risque de sécurité spécifique (Figure 4).

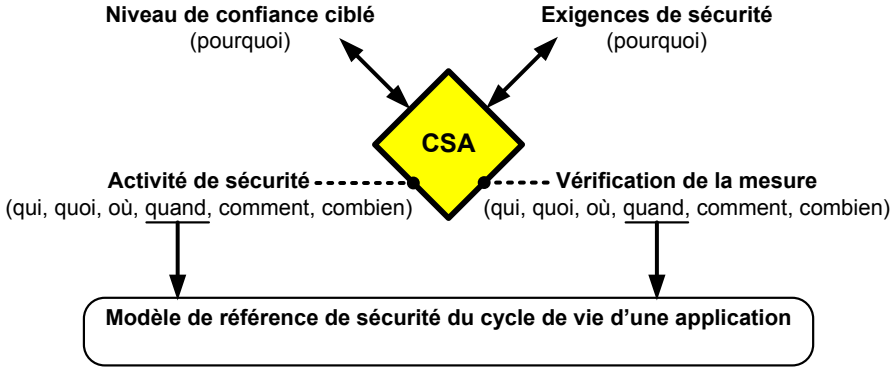

Figure 4 Le contrôle de la sécurité des applications *(traduit et adapté d'ISO 27034)*

Un CSA comprend quatre éléments d'information :

1) Les niveaux de confiance ciblés associés à ce CSA.
2) Les exigences de sécurité visées par le CSA.
3) L'activité de sécurité, décrivant le « quoi » (les résultats attendus), le « comment », le « où » et par « qui » cette activité doit être réalisée. Une évaluation de « combien » il en coûtera pour la mettre en œuvre doit également être précisée dans cette section.
4) La vérification de la mesure, quant à elle, utilise les mêmes caractéristiques pour décrire l'activité de vérification.

La caractéristique « quand » des deux derniers éléments du CSA permettent d'identifier à quel moment une activité devra être réalisée, en pointant sur une des activités du modèle de référence du cycle de vie de la sécurité d'une application, et en précisant si celle-ci doit être réalisée avant, pendant ou après l'activité du modèle de référence identifiée.

En identifiant les « qui », ces éléments doivent également préciser les rôles et les qualifications requises pour réaliser l'activité qui y est décrite.

NOTE La Figure 4 a légèrement été modifiée afin d'indiquer plus clairement, quel est l'attribut des activités de sécurité et de vérification de la mesure, qui réfèrent à une activité présente dans le modèle de référence du cycle de vie de la sécurité des applications.

III.I.iii La bibliothèque des contrôles SA

Les CSA utilisés par une organisation pour ses projets de développement doivent être approuvés au préalable, et rassemblés dans un référentiel. Ce référentiel, aussi nommé « bibliothèque de CSA » – voir Figure 3, constituera alors la source d'information fiable pour communiquer les CSA au sein de l'organisation.

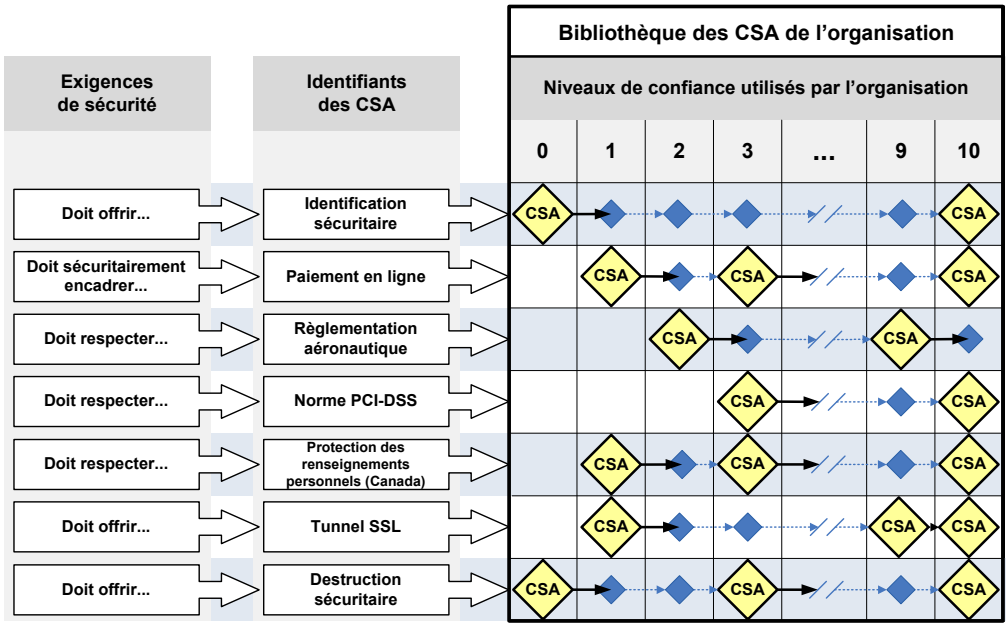

Figure 5 La bibliothèque CSA *(traduit et adapté d'ISO 27034)*

La bibliothèque des CSA regroupera les CSA qui ont été assignés par l'organisation à un ou plusieurs niveaux de confiance et exigences de sécurité. Le principal objectif de la mise en œuvre de cette bibliothèque est de s'assurer que le niveau de confiance ciblé, attribué à une application spécifique selon ses exigences de sécurité, soit clairement identifié et communiqué et qu'il permette identifier à l'avance les CSA qui devront être mis en œuvre puis vérifiés.

La sélection d'un niveau de confiance par une organisation, soit la liste de CSA à mettre en œuvre, prend notamment en compte de leurs coûts d'implémentation et de vérification, versus l'atténuation des impacts pour l'organisation, des risques ciblés par ces contrôles.

NOTE Le modèle SA initial présentait à la gauche de la figure de la bibliothèque de CSA, deux colonnes nommées : « Source des spécifications et des contraintes » et « Spécifications et contraintes ». Ces dernières ont été remplacées dans la Figure 3 afin de représenter les « exigences de sécurité » requise par une application ainsi que les « Identifiants des CSA » associé à celles-ci. Les deux éléments d'information retirés de cette figure, qui de fait représentaient les sources des risques de sécurité pouvant menacer une application, ont été inclus dans un nouveau composant du modèle : la matrice de traçabilité de la SA de l'organisation.

III.I.iv La matrice de traçabilité de la SA de l'organisation

La matrice de traçabilité de la SA est un référentiel utilisé pour aider une organisation à garder une trace des changements, ainsi que les liens qui associent les risques de SA aux exigences de sécurité, aux CSA et aux applications de l'organisation.

L'objectif visé par l'introduction de ce nouveau composant dans le modèle SA est de fournir à l'organisation qui l'utilisera, un outil permettant d'avoir une vision globale de l'ensemble des risques, des exigences de SA et des CSA de chacune de ses applications afin de lui permettre d'identifier, d'évaluer et de réagir rapidement a tous changements de risques de SA les concernant. Ces changements au niveau des risques de sécurité viendront inévitablement des contextes d'affaires, juridique ou technologique.

La **Error! Reference source not found.** est une représentation graphique sommaire des informations clés contenues dans la matrice de traçabilité de la SA de l'organisation telles que proposées par le modèle.

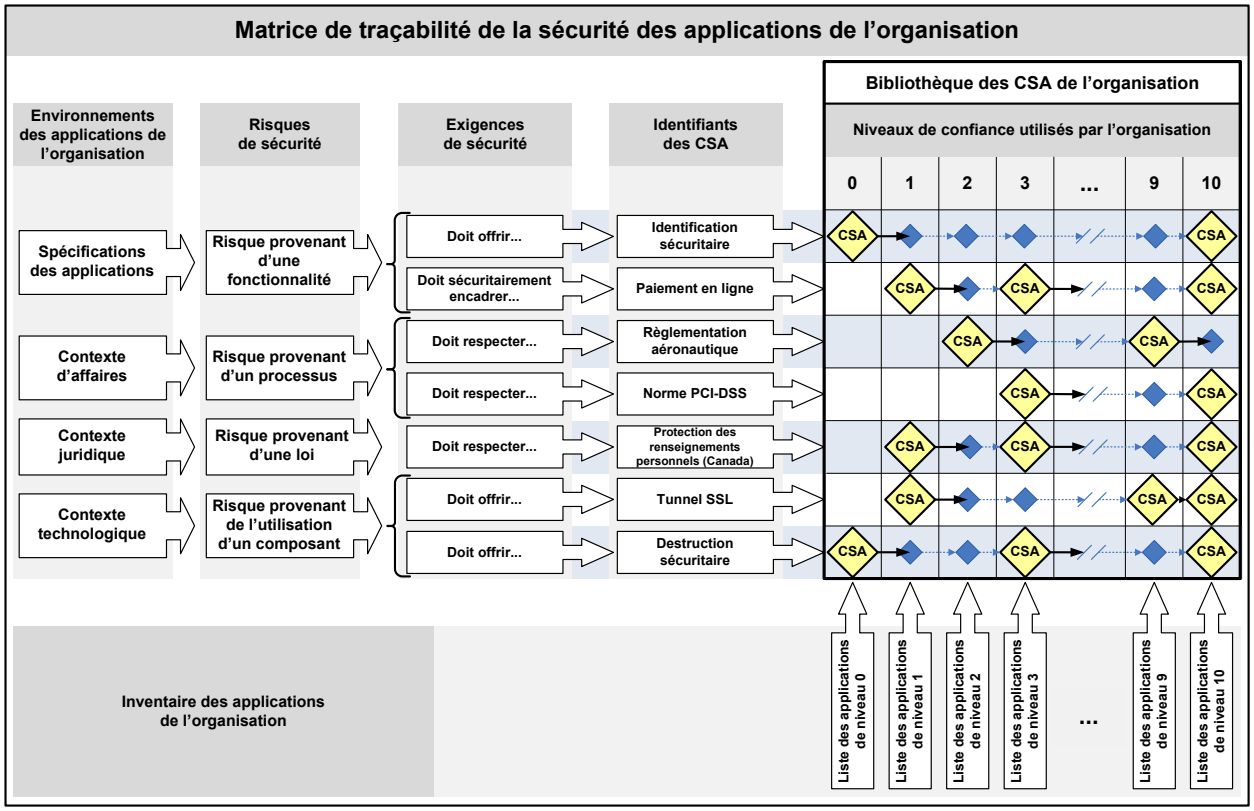

Figure 6 Matrice de traçabilité de la SA de l'organisation

La matrice de traçabilité peut être représentée comme un tableau contenant cinq groupes d'informations inter-reliés, soit :

1) Une table des éléments des environnements incluant les spécifications des applications d'où peuvent provenir des risques de sécurité;
2) Une table des risques de sécurité de toutes les applications de l'organisation;
3) Une table des exigences de sécurité à satisfaire, liées aux risques correspondants;
4) La bibliothèque des CSA offrant un choix de niveaux de confiance possible pour les applications de l'organisation; et
5) L'inventaire des applications de l'organisation auxquelles ont été assignées un niveau de confiance de la bibliothèque des CSA.

III.I.v Le cadre normatif de l'organisation (CNO)

Le modèle nécessite la conservation des éléments dans un cadre normatif de l'organisation (CNO), afin d'assurer leur gestion et leur communication à l'intérieur de l'organisation.

Les éléments clés du CNO sont :

- les contextes d'affaires, juridique et technologique;
- le dépôt des spécifications des applications;
- les processus liés à la sécurité des applications;
- le dépôt des rôles, des responsabilités et des qualifications;
- les contrôles de la sécurité des applications (CSA);
- la bibliothèque de CSA de l'organisation; et
- le modèle de référence du cycle de vie de la sécurité d'une application.

Chaque élément défini dans le CNO doit être vérifiable et être approuvé par l'organisation.

Le CNO est la source autoritaire de tous les éléments du modèle SA mis en place par l'organisation. Les éléments du CNO sont validés, vérifiés, approuvés et mis à la disposition de tout projet d'application.

III.I.vi Le cadre normatif d'une application (CNA)

Le CNA est un sous-ensemble du CNO et contient seulement les composants et les processus approuvés appartenant à une application spécifique. Un CNA devrait être défini pour chaque application sécurisée avec ce modèle SA. Il est utilisé pour conserver tous les documents, les décisions, les composants et les processus rédigés ou sélectionnés pour une application.

III.II Les processus clés du modèle SA

Cette section présente les deux processus clés du modèle SA, soit le processus de gestion du CNO et le processus de la gestion de la SA.

III.II.i Le processus de gestion du CNO

Le processus de gestion du CNO (Figure 7) est proposé par le modèle SA pour aider les organisations à gérer les éléments de la SA à travers l'organisation de façon uniforme.

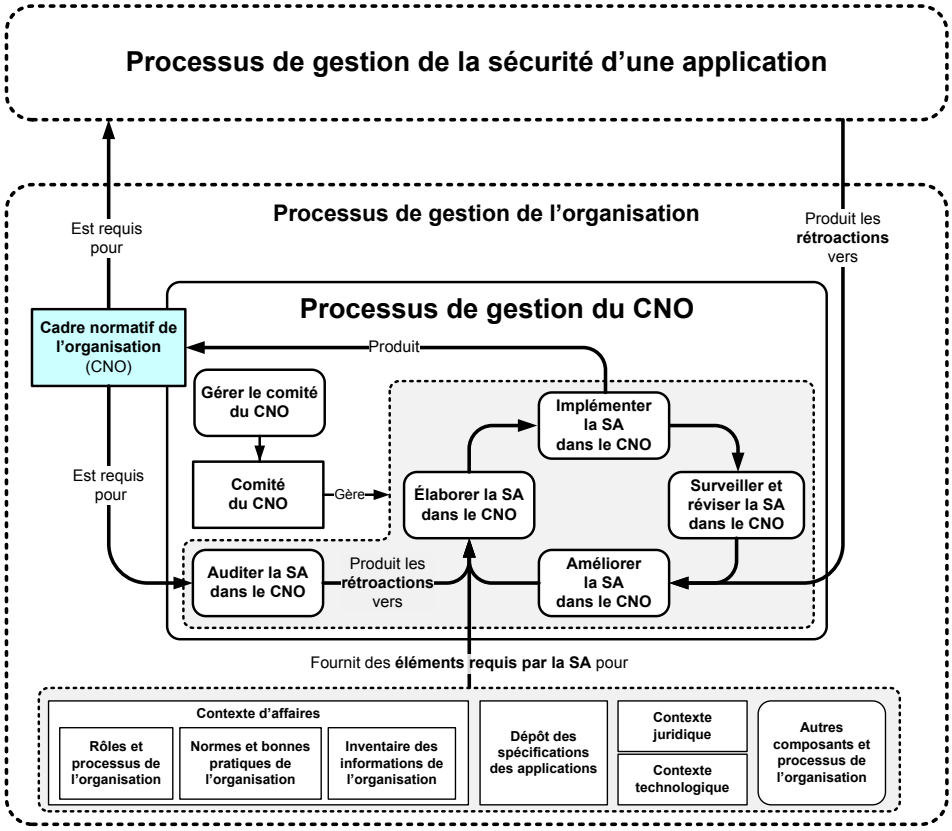

Figure 7 Le processus de gestion du CNO *(traduit et adapté d'ISO 27034)*

Le processus de gestion du CNO comprend six sous-processus qui seront utilisés au niveau de l'organisation, afin de mettre en œuvre le modèle SA. Ces six sous-processus sont :

1) gérer le comité du CNO;
2) élaborer la SA dans le CNO;
3) implémenter la SA dans le CNO;

4) surveiller et réviser la SA dans le CNO;

5) améliorer la SA dans le CNO; et

6) auditer la SA dans le CNO.

NOTE La représentation du processus de gestion du CNO présentée à la Figure 7 a été bonifiée afin d'y préciser la source des éléments requis par la SA, qui sont nécessaires à l'élaboration et à la mise en place de la SA dans le CNO de l'organisation. Le processus « Établir le comité du CNO » a été renommé « Gérer le comité du CNO » et ce comité a aussi été introduit dans la figure. Finalement les cinq processus qui sont directement impliqués dans la gestion et l'amélioration continue du CNO ont été regroupés dans une zone grisée.

III.II.ii Le processus de gestion de la SA

Le processus de gestion de la sécurité de l'application (Figure 8) est le processus global de gestion de la sécurité pour chaque application produite ou utilisée par une organisation. Ce processus contient cinq étapes :

1) Identifier les besoins et l'environnement de l'application.

2) Évaluer les risques de sécurité amenés par l'application, et déterminer le niveau de confiance nécessaire pour cette application.

3) Créer et maintenir le cadre normatif de l'application.

4) Réaliser et opérer l'application.

5) Vérifier la sécurité de l'application.

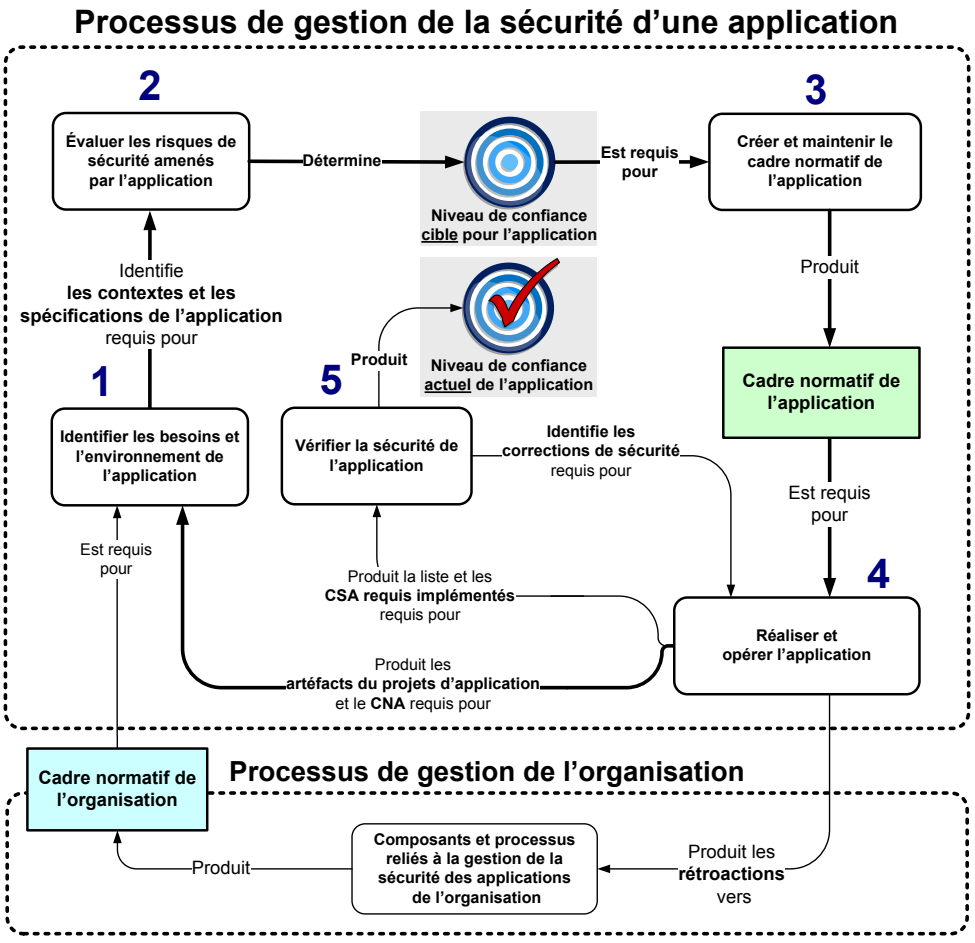

Figure 8 Le processus de gestion de la SA *(traduit et adapté d'ISO 27034)*

En utilisant des éléments préapprouvés du CNO, le processus de gestion de la sécurité de l'application aidera les projets à cibler, mettre en œuvre et à maintenir un niveau de confiance vérifiable qui a été identifié pour chaque application, en fonction de son environnement spécifique.

NOTE La représentation du processus de gestion de la sécurité d'une application présentée à la Figure 8 a légèrement été bonifiée afin de mettre en évidence le positionnement, les intrants et les extrants des composants « Cadre normatif de l'organisation » et « cadre normatif de l'application ».

IV. CONCLUSION

Peu d'approches et de modèles permettent de déclarer une application sécuritaire et d'appuyer cette déclaration avec des preuves vérifiables. Encore moins peuvent permettre à une organisation de définir le niveau de sécurité désiré, dans le respect de ses ressources et de ses capacités. Le nouveau modèle SA (modèle SA 1.1) permet à une organisation de rencontrer de manière encore plus efficiente ces trois défis.

Non seulement le modèle SA 1.1 permet à une organisation d'identifier et de gérer globalement les risques de sécurité présents dans les contextes d'affaires, juridique et technologique, que ces risques proviennent des personnes, des processus ou des technologies, il permet aussi à cette organisation d'associer cet ensemble de risques de sécurité à un niveau de confiance ciblé, dont l'atteinte sera exigée pour considérer une application sécuritaire.

Tout comme pour la première version, le modèle SA 1.1 exige que chaque CSA intègre un processus de vérification approuvé qui, lorsque le contrôle de sécurité est bien implémenté, produira des résultats attendus qui ont déjà été considérés comme les preuves acceptables de leur bonne implémentation et de leur bon fonctionnement.

Sachant qu'un niveau de confiance identifie une liste des CSA à mettre en œuvre, sachant que tout CSA doit notamment décrire une activité de sécurité et une activité de vérification et sachant que les coûts de réalisation de ces activités doivent être estimés, le modèle SA permet à une organisation de faire cet exercice de gestion globale des risques de sécurité et de sélection du niveau de confiance ciblé dans le respect de ses ressources et de ses capacités. De plus, cette gestion globale est maintenant facilité par l'ajout de la matrice de traçabilité de la SA de l'organisation dans le modèle SA.

La vérification de tous les CSA identifiés par le niveau de confiance ciblé d'une application permettra de collecter les preuves requises pour faire la démonstration qu'une application peut être considérée sécuritaire par l'organisation, dans un environnement spécifique. Cette démonstration est réalisée en comparant ce niveau de confiance mesuré, au niveau de confiance ciblé.

Le modèle SA 1.1 propose des composants et des processus permettant d'évaluer les risques de sécurité d'utiliser une application, de lui attribuer un niveau de confiance ciblé et de préciser les exigences de sécurité et les CSA correspondants, nécessaires à sa sécurisation.

Pour avoir plus d'information sur la version initiale 1.0 du modèle SA voir la norme *ISO/IEC 27034 – Application Security, Part 1: Overview and concepts* [7].

RÉFÉRENCES

1. ISO/IEC, *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model*. 2009, ISO/IEC: Geneva, Switzerland. p. 76.
2. ISO/IEC, *Information technology - Security techniques - System Security Engineering - Capability Maturity Model (SSE-CMM)*. 2006, ISO/IEC: Geneva, Switzerland. p. 134.
3. OWASP, *OWASP Top 10 - 2013; The Ten Most Critical Web Applicayion Security Risks*. 2013, OWASP Foundation. p. 22.
4. OWASP, *Code review guide*. 2008. p. 215.
5. OWASP, *Testing guide*. 2008, OWASP Foundation. p. 350.
6. Andress, A., *Surviving security: how to integrate people, process, and technology*. 2 ed. 2003: Auerbach Publications. 502.

7. ISO/IEC, *Information technology - Security techniques - Application security - Part 1: Overview and concepts*. 2011, ISO/IEC: Geneva, Switzerland. p. 82.
8. Poulin, L., *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*, in *Département de génie logiciel et des TI* 2014, École de technologie supérieure - Université du Québec: Montréal, Québec. p. 541.