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

DOCUMENT DES ANNEXES

MONTRÉAL, LE 15 SEPTEMBRE 2015

TABLE DES MATIÈRES

Page

LISTE DES TABLEAUX

LISTE DES FIGURES

ANNEXE IV

PROBLÈMES DE SÉCURITÉ DE L'INFORMATION IMPLIQUÉS PAR L'UTILISATION D'APPLICATIONS

Cette annexe présente, par domaines d'affaires, les problèmes de sécurité de l'information qui ont été identifiés lors de cette recherche et qui impliquaient l'utilisation d'applications.

IV.1 Secteur médical

1) *Perte de l'intégrité d'une information :* L'appareil de radiothérapie Therac-25 produit par l'entreprise Atomic Energy Commission Limited (AECL) du gouvernement canadien a provoqué six cas de radiation massive sur des patients, dont trois mortels, entre juin 1985 et janvier 1987. (Leveson, 1995)

   Le principal problème informatique à l'origine des cas de mal fonctionnement résultait d'une course critique (race condition) des processus de l'application de l'appareil. (Neumann, 1994) Une course critique se produit lorsqu'un processus informatique écrit dans un espace mémoire, un message destiné à un deuxième processus. Mais avant que ce dernier puisse le lire, un troisième processus remplace le message initial par le sien, en écrivant lui aussi dans le même espace. En écrivant dans le même espace mémoire, le troisième processus a produit une perte d'intégrité de l'information envoyée par le premier processus.

2) *Perte de la confidentialité d'une information :* 2000 employés de la Commission de la santé et de la sécurité du travail(CSST), ont accès à tous les fichiers des bénéficiaires, et aucun mécanisme de journalisation n'avait été mis en place. Il n'était donc pas possible de retracer la source d'une fuite si elle se produisait, et des fuites se sont effectivement produites.

À l'été 1993, une employée ayant accès dossiers des bénéficiaires, transmet certaines informations confidentielles à son conjoint, qui opère un lucratif commerce d'information. Mais l'application de la CSST n'avait pas été conçue pour conserver des preuves d'accès irréfutables. (Venne, 1994, p. 35)

3) *Perte de la confidentialité de l'information :* « On n'éliminera jamais totalement la fraude, car c'est une composante de la nature humaine [...]. Mais la technologie amplifie le risque. Et le problème, c'est que des organismes fonctionnent souvent sans filet. On a découvert que les 2000 employés de la Commission de la santé et de la sécurité du travail ont accès à tous les fichiers des bénéficiaires et que chaque fois qu'un employé consulte un dossier, sa manœuvre n'est pas enregistrée. De sorte qu'il est impossible de retracer la source d'une fuite lorsqu'elle se produit. Une employée de cet organisme public porta à mon attention, à l'été 1993, l'existence dans son bureau d'un trafic de renseignements. Une dame transmet à son mari, qui opère un commerce lucratif d'information, des renseignements tirés des dossiers des bénéficiaires. Mais le système informatique est conçu de telle sorte qu'il est à peu près impossible d'en faire la preuve. » (Vie privée et démocratie à l'ère de l'informatique, Michel Venne, IQRC, 1994, page 35.)

4) *Perte d'intégrité de l'information :* croyant être atteinte d'une maladie incurable, une patiente tue sa fille de quinze ans, tente de tuer son fils puis de se suicider. Une application était à la source de ce faux diagnostic. (Neumann, 1994, p. 7)

IV.2 Secteur des transports

1) écrasement du vol 965 à Cali, de Korean Air à Guam (Aircraft Accident Report, Aeronautica Civil of the Republic of Colombia, American Airlines Flight 965, Boeing 757-223, N651AA, Near Cali, Colombia, December 20, 1995.)

2) *Perte de l'intégrité de l'information :* système de transport rapide BART à San Francisco.

Une mauvaise gestion des paramètres du système d'information par les opérateurs du système l'ont amené à transmettre des demandes d'actions erronées aux différents trains du métro, dont l'activation des freins et l'ouverture des portes lorsqu'ils étaient en marche. (Neumann, 1994, p. 57) (Computer-Related Risks, p. 54.)

3) *Perte de disponibilité de l'information :* Toyota a annoncé qu'une panne de logiciel est à blâmer pour les problèmes de freinage dans le modèle Prius 2010.
   Le problème était dû au délai de traitement d'information du système informatique de freinage qui pouvait prendre jusqu'à une seconde avant de produire son résultat. (CNN, 2010)

4) *Perte de la disponibilité de l'information :* panne dans un système de réservation de billets d'avion. La panne du système de réservation du 2 février 2000 était reliée à une mauvaise gestion de la mémoire dynamique par l'application logicielle. (*Voir* http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=3161)

IV.3 Secteur financier

1) Perte de la disponibilité de l'information :
   Tous ces cas présentés dans cette section ont principalement mené à une perte de la disponibilité des services des financiers des institutions concernés.

   4 juin 2004 : Au cours de l'été 2004, plus de 2,5 millions de clients de la Banque Royale du Canada (RBC) n'ont pu accéder pleinement à leurs comptes. L'institution bancaire a déclaré que cette situation était attribuable à une mise à niveau informatique qui avait mal tourné, ce qui, essentiellement, a empêché l'inscription des opérations effectuées le 31 mai et le 1er juin (des dépôts, des retraits et des paiements) au solde des comptes des clients.

« Il s'agit de la coïncidence d'une combinaison invraisemblable d'erreurs et d'événements, explique David Moorcroft. Tous les éléments étaient en place pour envenimer la crise : erreurs de frappe, tests d'assurance qualité non effectués, changement de programmation mis en œuvre au début de la semaine plutôt que le vendredi. RBC a dû corriger manuellement chaque opération, ce qui a entraîné un retard de plusieurs jours et des erreurs supplémentaires. »

Erreur humaine, problème d'exploitation, négligence de la part du personnel des TI? Quoi qu'il en soit, le programme qui aurait dû s'intégrer sans problème n'a pas fonctionné comme prévu.

(« Un bogue Royal », Radio-Canada, le vendredi 4 juin 2004, un reportage de Julie Marcoux, http://www.radio-canada.ca) (John Cooper, La gestion de crise, CMA Management Web Magazine, http://www.managementmag.com/8/0/1/6/index2.shtml)

29 juillet 2004 : panne à la Banque CIBC (« CIBC computer glitch headache for clients », CBC, 29 juillet 2004. http://ottawa.cbc.ca)

18 janvier 2007 : La Banque CIBC a perdu les informations de 470,000 Canadiens. « The personal information of nearly half-a-million customers at a CIBC mutual fund subsidiary has gone missing, prompting fears of a potential security breach and inciting an investigation from Canada's federal privacy commissioner.

A backup computer file containing application data for 470,000 investors at Montreal-based Talvest Mutual Funds disappeared in transit on the way to Toronto recently, the bank said in a news release Thursday." (SINCLAIR STEWART, Globe and Mail Update,

18/01/07
http://www.theglobeandmail.com/servlet/story/RTGAM.20070118.wcibc0118/BNStory/Business/home)

31 juillet 2004 : panne technique à la Banque Nationale (« Panne technique à la Banque Nationale », le samedi 31 juillet 2004, http://www.radio-canada.ca)

15 septembre 2004 : panne généralisée chez Desjardins (« Retour à la normale aux guichets Desjardins », Radio-Canada, le mercredi 15 septembre 2004, http://www.radio-canada.ca)

10 novembre 2004 : problèmes informatiques à la Banque Scotia. (Presse canadienne, 10 novembre 2004.)

Lors de tous ces événements, les comptes bancaires des personnes et entreprises impactés par ces incidents n'étaient plus accessibles et aucune transaction ne pouvait y être effectuée. Vu le grand nombre de comptes impactés, les conséquences de ces pannes ont varié selon les situations, pouvant aller d'une conséquence nulle si la personne n'a réalisé aucune transaction, jusqu'à une conséquence plus importante, si un paiement ou une transaction d'affaires stratégiques devait être réalisé durant cette période.

IV.4 Secteur gouvernemental

1) Perte de la disponibilité de l'information : L'Agence du revenu du Canada a suspendu certaines applications liées à l'impôt sur le revenu des particuliers, en raison de problèmes dans l'entretien des logiciels.

   (http://lapresseaffaires.cyberpresse.ca/economie/200901/06/01-676861-limpot-federal-en-panne-informatique.php)

2) *Perte de l'intégrité, de confidentialité et de disponibilité de l'information :* problèmes des systèmes de votations électroniques utilisés lors des élections municipales de 2005 au Québec.

   Des erreurs de conception, d'analyse, de programmation, de maintenance et d'utilisation des systèmes de votation électroniques ont mené à douter des résultats des élections de 140 municipalités au Québec. (DGEQ, 2006, p. 5) Le Tableau 6.18 présente sommairement les résultats de l'évaluation 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. (*Voir* l'appendice A – ANNEXE XXIII pour plus de détails.)

3) Perte de la confidentialité de l'information : Voir l'annexe « Études de cas d'incidents informatiques » du document des annexes, section 1.7.2 Descriptions des cas – Vol de données confidentielles sur 120 000 contribuables canadiens, Radio-Canada, Un reportage de Nicole Chiasson, le mardi 30 septembre 2003.

4) Perte d'intégrité et de disponibilité de l'information – problèmes des systèmes de votations électroniques utilisés lors des élections municipales de 2005 au Québec.

5) *Perte de la confidentialité de l'information :* La confidentialité des fichiers des conducteurs contenus dans les systèmes d'information de la SAAQ était mal protégée. Ce qui à mené à la divulgation d'information personnelle de certaines personnes.
   (*Voir* http://www.cyberie.qc.ca/dixit/20010105.html et « La confidentialité des fichiers de la SAAQ mal protégée », Radio-Canada, le mercredi 13 décembre 2000.)

6) *Perte de la disponibilité de l'information* : « Des milliers d'étudiants sans prêts et bourses pour la rentrée » La panne du système de l'organisme gouvernemental autorisant l'approbation et le paiement des prêts aux bouses étudiants du Québec a occasionné des retards qui ont été préjudiciables a plusieurs d'entres-eux.
   (*Voir* Radio-Canada, le lundi 2 août 2004, http://www.radio-canada.ca)

IV.5 Secteur des systèmes de communication

1) *Perte de la disponibilité de l'information :* Le système informatique 999 de répartition d'appels de Londres, similaire au système 911 nord-américain, connaît des ratés importants; on estime que 20 décès auraient pu être évités avec un système informatique pleinement opérationnel.

   Le 7 février 1992, un opérateur ferme par inadvertance son ordinateur, perdant ainsi quatre appels d'urgence. Un patient rappelle trente minutes plus tard, et on lui redemande les mêmes renseignements en lui expliquant qu'ils ont été perdus par l'ordinateur. Le patient ne sera pas secouru à temps et décèdera.

   Les 26 et 27 octobre 1992, la performance du système se dégrade à un point tel que des retards sont signalés dans la répartition des véhicules d'urgence; à quelques reprises, plusieurs ambulances sont envoyées pour le même appel, alors que, d'autres fois, un véhicule d'urgence se trouvant loin de l'incident est sollicité alors qu'il y avait un véhicule disponible à proximité.

   Le 4 novembre 1992, le système tombe en panne généralisée durant une période de onze heures. (Neumann, 1994, p. p. 72)

2) *Perte de confidentialité de l'information :* Une faille dans passer le mot de passe peut donner accès au routeur Cisco. Après la découverte d'une vulnérabilité de mot de passe potentiel grave, Cisco a exhorté les utilisateurs d'une version particulière de son système d'exploitation de le mettre à jour.
   (Voir John Leyden, The Register, 25/04/2003,
   http://www.theregister.co.uk/content/55/30402.html)

IV.6 Secteur de la défense et de l'aérospatial

1) Raté au décollage d'un vol d'Air Canada à Toronto (Voir la référence donnée à l'annexe « Incidents d'aviation » du document des annexes, section Computer Contributes to 747 Tail Scrape.)

2) *Perte de la disponibilité de l'information :* Le 17 juin 2011 à 8h15, heure de New York, une panne informatique qui a touché les applications de départs de vol et de traitement de réservations, a retardé les vols d'Unided Airline durant plus de 6 heures, cette panne a un impact sur les vols à la grandeur des États-Unis.

3) *Perte d'intégrité de l'information :* Le logiciel des missiles antimissiles de type Patriot contenait une faille informatique qui, lorsque qu'en fonction pendant plus de huit heures consécutives, provoquait la perte d'intégrité d'une information utile au processus de calcul du temps du système de guidage du missile.

   Des missiles antimissiles de type Patriot sont utilisés durant la guerre du Golfe, pour intercepter les missiles Scud envoyés par les forces irakiennes. Pour réaliser l'interception, ces missiles exécutaient un logiciel qui leur permettait de calculer la trajectoire de collision avec les missiles ennemis. Malheureusement, ce logiciel contient une faille informatique qui, lorsque le missile était en fonction pendant plus de huit heures consécutives, provoquait la perte d'intégrité d'une information de temps sensible. Cette perte d'intégrité était provoquée par une erreur de précision cumulative d'une valeur stockée en nombres à virgule flottante, du processus de calcul du temps du système de guidage du missile.

   En février 1991, le logiciel a calculé de manière erronée la trajectoire d'un missile Patriot, à cause de cette faille informatique. Non seulement le missile Patriot n'a pas réussi à intercepter le missile irakien Scud, mais il a terminé sa trajectoire en frappant une

baraque de l'armée américaine. Constat : 29 soldats tués et 97 blessés dans le camp américain à Dharan, en Arabie Saoudite. (Neumann, 1994, p. P 34.)

IV.7 Secteur personnel

1) *Perte de confidentialité, de disponibilité et d'intégrité de l'information :* Firefox update plugs « critical » holes (Joris Evers et Staff Writer, 2010)
« Selon l'organisation Mozilla, la vulnérabilité la plus grave pouvant être exploitée permettrait à des personnes malveillantes de prendre le contrôle d'un ordinateur vulnérable. La société Mozilla, qui supervise le développement de Firefox, a publié les avis de sécurité pour chacun des défauts réparés par la mise à jour. » ... « Firefox 1.5.0.5 est une mise à jour de sécurité qui fait partie de notre programme continu visant à fournir une expérience Internet sécuritaire à nos clients » (CNET News.com, July 27, 2006, http://news.com.com/Firefox+update+plugs+critical+holes/2100-1002_3-6099254.html)

2) *Perte de confidentialité de l'information :* Ces données privées que les applications mobiles transmettent à votre insu « Localisation, âge, sexe, identifiants : la plupart des applications sur téléphone mobile envoient des données privées à des régies publicitaires sans que l'utilisateur en soit informé, selon une enquête du Wall Street Journal. Sur 101 applications populaires étudiées par le journal américain, moitié sur iPhone, moitié sur Android, 56 transmettent l'identifiant unique du téléphone, 47 donnent la localisation de l'utilisateur, et 5 livrent l'âge et le sexe du mobinaute sans qu'il se doute de rien. » ... « Le Wall Street Journal pointe deux faiblesses dans la protection de la vie privée des mobinautes : l'impossibilité de désactiver a posteriori le traçage, et l'absence d'obligation pour les applications de disposer de règles de confidentialité, aussi bien sur l'Apple Store que sur l'Android Market. »
(LEMONDE.FR, 20.12.10 – 16h00, mis à jour le 20.12.10 – 16h44, http://www.lemonde.fr/technologies/article/2010/12/20/ces-donnees-privees-que-les-applications-mobiles-transmettent-a-votre-insu_1455982_651865.html#ens_id=1244271&xtor=RSS-3208)

ANNEXE V

PROBLÉMATIQUES LIÉES À LA SÉCURITÉ DES APPLICATIONS

Cette annexe présente les problématiques identifiées durant ce travail de recherche, et qui sont liées à la sécurité des applications.

V.1 Absence d'une vision globale de la sécurité des applications

Il faut reconnaitre que les professions et que le domaine des TI sont encore jeunes. Il ne faut retourner qu'en 1946, à l'arrivé de l'ENIAC (Electronic Numerical Integrator and Computer) premier ordinateur électronique programmable basé sur les travaux de M. Alan Mathison Turin, pour identifier la période marquant le début de l'informatique. D'un monde où l'ordinateur n'existait pas à aujourd'hui, il aura fallu environ 60 ans pour améliorer cette technologie et se mettre à l'utiliser dans presque toutes les sphères de notre société.

Les problèmes puis les concepts de sécurité de l'information ne sont eux, arrivés que beaucoup plus tard. Premièrement par les besoins d'intégrités, de rigueurs et d'audits requis pour la mise en place de systèmes de gestion comptables des organisations. Ces besoins d'intégrités provenaient du contexte légal qui existait déjà au Canada en 1940 (Justice, 2014, p. 71). Puis ces besoins en sécurité de l'information ont rapidement évolué, s'étendant au domaine des TI et au domaine du développement des applications, par l'arrivé de la micro-informatique, des réseaux, de l'Internet, puis par l'explosion et la convergence simultanées des domaines d'application et des besoins d'affaires pouvant être comblés par les TI.

Il aura fallu attendre jusqu'en 2002, pour que soit développé à l'université Laval le premier cours universitaire de premier cycle qui fit un lien entre les quatre domaines de connaissances impliqués dans la sécurité de l'information, soit : la gouvernance de la sécurité de l'information, la sécurité des infrastructures technologiques, la sécurité dans le développement et la maintenance des applications, et la vérification et les audits de sécurité.

Ce cours, qui est toujours aujourd'hui au programme du premier cycle du département d'informatique et de génie logiciel de l'université, présente une vision systémique globale de la sécurité de l'information ainsi que les relations entre ses quatre domaines de connaissances. (Guay et Poulin, 2002) Mais cette vision est-elle adéquate, si on désire l'appliquer à la sécurité des applications?

Notre travail de recherche devra inclure la définition d'une vision globale de la sécurité des applications.

V.2 Absence d'une vision permettant d'identifier et de tenir compte des risques et des contextes d'utilisation d'une application

La réponse à cette question dépend notamment des risques amenés par les contextes d'utilisation de l'application. Prenons ces trois exemples :

1) L'application ne doit pas réaliser aucune transaction de paiement électronique, ou au contraire elle doit permettre l'achat de produits valant plusieurs milliers de dollars et conserver des informations résultant de ces transactions électroniques. Ces deux besoins d'affaires différents devraient avoir un impact sur le choix des activités de vérification à réaliser menant à l'évaluation de la sécurité de cette application. Selon cet exemple, nous pouvons déduire que les besoins provenant du contexte d'affaires d'une organisation devraient avoir un impact sur les besoins de SA qu'elle utilise.
2) L'application est hébergée sur des serveurs situés aux États-Unis et elle contient 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 lois américaines? Selon les lois canadiennes? Selon cet exemple, nous pouvons déduire que le contexte juridique peut aussi avoir un impact sur le résultat d'une évaluation de la sécurité d'une application.
3) L'application requiert un lien internet afin d'avoir accès à des données partagées sur des serveurs externes, ou au contraire l'application conserve l'ensemble de ses données sur le poste de travail de l'utilisateur et ne requiert aucun lien externe pour fonctionner. Il est ici facile de comprendre d'une application qui requiert un lien Internet est plus à risque à voir

ses données compromises qu'une application autonome. Selon cet exemple, nous pouvons déduire que le contexte technologique peut aussi avoir un impact sur le résultat d'une évaluation de la sécurité d'une application.

À la lumière de ces exemples, nous pouvons déduire qu'il sera difficile d'évaluer et de vérifier la SA sans utiliser une méthode d'évaluation des risques de sécurité qui tiendra en compte son environnement d'utilisation. Malheureusement, il ne semble qu'aucune norme ou méthode n'évalue la SA en considérant ces trois contextes simultanément.

C'est de fait, l'interprétation et l'adaptation incomplète ou erronée des systèmes de votation électroniques (SVÉ) aux risques de sécurité provenant des contextes juridiques (lois régissant les élections municipales québécoises), d'affaires et technologiques des municipalités qui ont été mise en évidence dans le rapport de 2005 du Directeur général des élections du Québec. (DGEQ, 2006)

Notre travail de recherche devra présenter une solution qui permet de tenir compte des risques et des contextes d'utilisation d'une application.

V.3 Absence d'un modèle de sécurité des applications pouvant s'adapter aux besoins de sécurité des organisations

Sachant que les organisations n'ont pas toutes les mêmes besoins de sécurité, ni les mêmes moyens mis à leur disposition; sachant également que les contextes d'affaires, juridiques et technologiques peuvent différer d'une organisation à l'autre simplement parce que ces organisations ne sont pas situées dans les mêmes pays; est-il possible de définir un cadre normatif de SA qui pourrait s'adapter aux besoins de SA des grandes, des moyennes et des petites organisations?

Lors du projet du DGÉQ, l'ensemble du préparatoire pour réaliser un audit de sécurité des systèmes de votation électronique impartial, répétable et vérifiable nous demandé d'identifier

les éléments qui devaient être inclus dans la vision de la SA et de les placer à l'intérieur d'un cadre et de les mettre en relations les uns avec les autres afin d'en identifier notamment les types, les dépendances, les priorités et leurs préséances.

Sans ce cadre de référence, l'affirmation qu'une application est sécuritaire ou qu'elle est non sécuritaire est sans valeurs, car elle devient l'interprétation personnelle d'une personne. Et il existera toujours un deuxième expert qui pourra le contredire et affirmer que l'application n'est pas assez sécuritaire à ses yeux.

Comment régler ce problème de mesure de la sécurité d'une application? Serait-il intéressant pour les organisations de pouvoir utiliser un modèle de SA reconnu pouvant s'adapter à ses besoins de sécurité?

Notre travail de recherche devra être en mesure de fournir un cadre normatif de SA pouvant s'adapter aux besoins de sécurité des organisations.

V.4 Absence d'une approche permettant de sélectionner les solutions de sécurité des applications requises par une organisation en fonction de ses besoins de sécurité et de ses ressources économique

Plusieurs grandes, et la majorité des petites et moyennes entreprises n'ont pas les moyens ou ne ressentent pas le besoin d'implémenter, d'obtenir et de maintenir une certification comme celle proposée par les Critères Communs ou le CMMi. Premièrement, ces certifications concernent les organisations qui développent les produits technologiques, deuxièmement les coûts associés à ces certifications de sécurité sont généralement trop élevés pour elles et finalement, qu'elles soient certifiées ou non, leurs applications trouveront preneur étant donné que dans la majorité des cas, aucune contrainte légale ou d'affaires n'exige de certification de sécurité de produit.

Lors de l'audit de sécurité des systèmes de votation électronique (SdVÉ), nous nous sommes aperçus que personne n'avait une vision globale de l'ensemble des éléments, des

informations, des risques et des contrôles qui pouvaient être impliqués dans la sécurité de ces systèmes. Ni les clients, les diverses municipalités qui ont fait l'acquisition ou la location des SdVÉ, n'avaient exprimé leurs besoins de sécurité, ni leurs fournisseurs de services et de produits ne leur en avaient demandé.

Par exemple, les constats généraux 1, 2 et 3 (CG1, CG2, CG3) démontraient qu'aucun fournisseur ne possédait une documentation claire et détaillée des rôles, responsabilités et qualifications requises ni des membres de son équipe de projet, ni de l'équipe de développement, de l'équipe de formation ou de l'équipe d'infrastructure tant en ce qui a trait au développement, aux tests qu'au soutien technique. Dans tous les cas, les municipalités qui ne connaissant pas le domaine d'expertise de la sécurité, se sont fiées à leurs fournisseurs.

Non seulement nous avons constaté qu'aucune entreprise n'avait appliqué de pratiques de sécurité dans leurs projets, mais aucune n'avait cru nécessaire de réaliser une analyse de risques de sécurité formelle qui aurait pu leur permettre d'évaluer les risques critiques de sécurité, puis d'identifier les besoins de sécurité de leurs clients. C'est ces lacunes ainsi que l'ensemble des problèmes de sécurité qui sont survenus lors des élections municipales québécoises de 2005 qui ont mené en fin de compte, à la demande de l'audit technique de sécurité que nous devions réaliser.

Les risques de sécurité et constats faits lors de cet audit de sécurité ont démontré que les entreprises qui ont développé les SVÉ n'avaient pas identifié la portée de la sécurité de leurs applications.

La solution proposée par notre travail de recherche devra donc pouvoir s'adapter aux besoins d'affaires et être économiquement accessible à la majorité des organisations qui désireront la mettre en place. Elle devra pouvoir fournir les éléments permettant à l'industrie d'estimer, de mesurer et d'évaluer les coûts de la sécurité d'une application. De cette manière, l'organisation sera en mesure de gérer ses coûts de sécurité en fonction des risques encourus lorsqu'elle implantera et utilisera une application dans son environnement.

V.5 Absence d'un vocabulaire et de références communes en sécurité des applications

Qu'est-ce qu'une application? Quelle est la différence y a t'il entre une application et un système? La définition d'une application couvre elle les mêmes éléments que ceux requis pour définir la sécurité d'une application? Nous nous sommes rapidement aperçus au début de nos recherches, qu'il y avait plusieurs définitions à ces termes, et que la définition donnée et la portée de ce qu'elle représente pour chacun d'eux variaient selon la formation et le domaine d'intervention de la personne qui répondait à la question.

Durant plusieurs années, trois domaines d'intervention spécifiques : celui de la vérification comptable, celui des infrastructures technologies et celui du développement d'applications, ont travaillé en vase clos afin de répondre principalement aux besoins des personnes œuvrant dans un quatrième domaine : celui du domaine de la gestion d'affaires de l'organisation.

Ces quatre groupes ont une définition différente de ce qu'est une application. Pour les uns, il s'agit de la composante logicielle d'un système[32], pour les autres c'est un ensemble plus grand qui comprend non seulement le logiciel, mais aussi les composants et les processus nécessaires à son fonctionnement.

De par leurs cheminements académiques différents, leurs milieux de travail complètement séparés sans communication formelle réelle, les personnes œuvrant dans ces quatre domaines d'interventions ont au fil du temps, développé en vase clos leurs méthodes, leurs concepts et leurs vocabulaires, bien à eux. De ce fait, ils ont aussi chacun développé leur propre vision de la sécurité (*Voir* l'XII.1.1, Figure-A XII-1).

---

[32] Application software: software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself. (ISO/IEC 18019)

Aujourd'hui, les personnes de ces quatre groupes utilisent parfois des mots semblables pour désigner des concepts différents, mais aussi des mots différents pour désigner une seule et même chose. La problématique posée par le vocabulaire n'est cependant pas nouvelle et est généralement le résultat de rencontres de travail d'intervenants issus de plusieurs domaines de connaissances différents, lors de la maturation d'une discipline.

De plus, certains termes tels que « système » et « processus », largement utilisés dans le monde des TI sans qualificatif, pour désigner l'un et l'autre. Par exemple, le terme « système » est habituellement utilisé par les personnes œuvrant au niveau de l'infrastructure technologique pour désigner un ordinateur physique, tandis qu'il sera utilisé par les personnes œuvrant en génie logiciel pour désigner un ensemble de composants, qui parfois inclue aussi des personnes et des procédures. Voyons-y de plus près.

L'institut canadien des comptables agrée définit un système comme un ensemble composé d'un ou de plusieurs ordinateurs en réseau, des périphériques, du logiciel d'exploitation, des logiciels d'application et des installations de réseau, coordonné de manière à permettre le traitement et l'échange d'informations. (© Institut canadien des Comptables agréés, 2006)

Le sous-comité 7 d'ISO définit, dans la norme ISO 15288 :2008, un système comme *une combinaison d'élément en interaction, organisé pour atteindre un ou plusieurs objectifs énoncés*.

L'IEEE définit dans sa norme IEEE 1233-1998 (R2002) IEEE Guide for Developing System Requirements Specifications, un système comme étant *un groupe interdépendant de personnes, d'objets et de procédures, constitué pour atteindre des objectifs définis ou quelques rôles opérationnels, en réalisant des procédures (fonctions) spécifiées*.

Dans le domaine des infrastructures technologiques, ITIL définit le terme système comme *un nombre de choses en relation, qui travaillent ensemble à l'atteinte d'un objectif global*. Puis,

donne en exemple des spécifications tel que « système informatique », « système de gestion », « système de gestion de données » et « système d'exploitation ».

Le terme « application », est défini dans la norme ISO 24570:2005 du sous-comité 7 (SC7) d'ISO, comme un *système pour collecter, sauvegarder, traiter et présenter des données par l'utilisation d'un ordinateur*[33], et par la norme ISO 20968 comme étant *une collection cohérente de procédures et de données automatisées qui supportent un objectif d'affaires*[34].

Comme on peut le constater, le vocabulaire utilisé par les divers intervenants œuvrant en TI est sur la bonne voix de formalisation, mais n'est malheureusement pas encore mature.

Dans le cas de la discipline de la sécurité des applications, des ajustements et des arrimages dans le vocabulaire de ces quatre domaines d'interventions, devront être réalisés sur afin de définir formellement les concepts importants en sécurité des applications. Sachant que le vocabulaire diffère d'un domaine de connaissances à l'autre, il est important de pouvoir proposer un vocabulaire commun, qui fera consensus, et qui pourra être utilisé par les divers intervenants du secteur de la sécurité des applications.

Notre travail de recherche devra permettre de définir les bases d'un vocabulaire et des références communes en sécurité des applications.

---

[33] Traduction libre de: "a system for collecting, saving, processing, and presenting data by means of a computer" (Source: ISO/IEC 24570:2005 Software engineering – NESMA functional size measurement method version 2.1 – Definitions and counting guidelines for the application of Function Point Analysis)

[34] Traduction libre de: "a coherent collection of automated procedures and data supporting a business objective" (Source: ISO/IEC 20968:2002 Software engineering – Mk II Function Point Analysis – Counting Practices Manual, 10)

V.6 Absence d'une définition de la portée de la sécurité d'une application

N'ayant pas une définition claire de ce qu'est une application, il nous ait assez difficile d'en définir la portée de sa sécurité. Pour certains, une application est un logiciel que l'on installe sur un ordinateur comme, par exemple : MS Word, Excell ou iTune. Pour d'autres, une application est un ensemble de logiciels, de matériel technologique et de processus qui sont mis en place et utilisés pour répondre à un besoin d'affaires d'une organisation, par exemple : l'application Amazon, ou Canada411.

Sans connaître la portée d'une chose, il est assez difficile de pouvoir déclarer ce qu'elle est, et surtout, affirmer qu'elle est correctement protégée. Une définition précise d'une application et de la portée de la SA devront donc être précisée, avant de pour pouvoir être en mesure de déclarer une application sécuritaire.

Notre travail de recherche devra proposer une définition de la portée de la sécurité d'une application.

V.7 Absence d'une définition claire de ce que c'est qu'une application sécuritaire

Nous savons que la sécurité absolue n'existe pas. Mais dans quels contextes une application doit-elle être considérée comme sécuritaire? Comment fait-on pour savoir si on peut avoir confiance qu'une application soit suffisamment sécuritaire pour nos besoins? Est-ce que, pour une même application, il pourrait y avoir plusieurs évaluations différentes et simultanées du niveau de confiance, selon l'environnement de son utilisation et les besoins de l'organisation?

De fait, les éléments permettant à une organisation de mettre en place une application qu'elle jugera sécuritaire, soit une application dont elle a fixé et validé le niveau de confiance, devraient pouvoir être normalisés. Cependant, les divers éléments qui seront utilisés pour introduire les contrôles de sécurité dans le cycle de vie de cette application spécifique et

produire les preuves attendues devraient être assez flexibles pour pouvoir répondre aux besoins des grandes et des petites organisations, en fonction de leurs contraintes, de leurs limitations et de leurs contextes spécifiques.

C'est donc un problème comportant plusieurs facettes que le domaine de la SA doit affronter. Afin de permettre aux organisations d'implanter et d'assurer la sécurité de l'information d'une application, il faudra éventuellement identifier et être en mesure d'évaluer des éléments précis, permettant de soutenir leurs affirmations.

Notre travail de recherche devra proposer une définition claire de ce que c'est qu'une application sécuritaire.

Et qu'en est-il du cycle de vie de la sécurité d'une application? En avons-nous besoin ? Si oui, ce cycle de vie commence-t'-il dès la conception de l'application ou commence-t'-il à son installation dans l'organisation? Ces questions nous ont permis d'identifier les autres problématiques amenées par la sécurité des applications.

V.8 Absence d'un modèle de référence du cycle de vie de la sécurité d'une application

Si une faille de sécurité a été introduite lors de la conception, de la réalisation, de l'implémentation, de la maintenance ou de l'utilisation d'une application, peut-on considérer cette application sécuritaire? Si, à chacune de ces étapes du cycle de vie de l'application, des activités de sécurité avaient dû être réalisées, il est facile de conclure qu'afin de pouvoir préciser la portée de la sécurité d'une application, il faut aussi en connaitre le cycle de vie.

Malheureusement, même s'il existe plusieurs modèles de cycle de vie de système et d'application logicielle, ils ne présentent pas tous les mêmes phases et utilisent généralement un vocabulaire différent pour les identifier.

Un modèle de cycle de vie permet notamment d'identifier et de mettre en relation un ensemble de processus, d'activités, d'intervenants, d'intrants et d'extrants dans une vision globale cohérente afin d'en clarifier la portée et d'en faciliter la communication.

Malheureusement nous savons que, non seulement la définition de la portée du cycle de vie d'une application varie d'un secteur d'intervention à l'autre, mais que cette définition peut aussi varier à l'intérieur d'un même secteur. Par exemple, dans le secteur du développement d'applications, certains processus de développement comme XP[35] terminent le cycle de vie d'une application à sa livraison, tandis que d'autres comme EUP[36] terminent le cycle de vie de cette même application à la phase de son retrait.

De plus, en SA plus que dans tout autre secteur des TI, l'interdépendance temporelle et les interrelations entres processus et les activités des différents secteurs d'interventions, ainsi que la qualification et l'expérience des intervenants qui doivent les réaliser ou les vérifier, peuvent avoir des conséquences importantes sur l'atteinte d'un niveau de confiance ciblé pour une application spécifique.

Lors de l'audit du DGEQ, il nous avait été demandé de réaliser une révision du code source des applications afin d'identifier si des failles de sécurité s'y trouvaient. Cette demande du DGEQ aurait pu être une bonne idée, mais était ici complètement inutile, car aucun des fournisseurs des SVÉ n'avait mis en place un processus ou un contrôle permettant de garantir que le code qui serait révisé était celui qui avait été installé dans les différents SVÉ. De plus, l'audit a mis en lumière que le logiciel de certains SVÉ avait été mis à jour quelques jours avant l'élection, sans qu'aucun processus de transition formel ne l'encadre. Finalement, certains SVÉ ont disparu alors qu'ils étaient en transit, vers les municipalités auxquels elles étaient destinées. Ce qui démontre que des personnes ont pu avoir des accès physiques à

---

[35] Extreme Programming

[36] Enterprise Unified Process

certains SVÉ et qu'au lieu des les subtiliser, ils auraient pu y installer un nouveau logiciel sans que personne ne s'en aperçoivent.

Notre travail de recherche devra proposer un modèle de référence du cycle de vie de la sécurité d'une application, afin d'offrir une compréhension globale et commune de l'ensemble des activités, des acteurs et des interdépendances qui s'y rapportent.

V.9 Absence de sources claires des exigences de sécurité d'une application

Dans le domaine des TI, une exigence est une réponse formelle à un besoin qui a été exprimé. Depuis que des personnes développent du logiciel, des méthodes de travail ont été développées. L'une d'elles consiste à réaliser diverses analyses de besoins, permettant notamment d'identifier, selon le cas, les exigences d'affaires, d'utilisateurs, de systèmes, ou fonctionnelles, requit pour définir ou préciser les spécifications de la nouvelle application. (Wiegers, 2003) Mais qu'en est t'il des exigences de sécurité?

Les exigences de sécurité proviennent des besoins de sécurité, qui sont l'expression de la diminution d'un risque de sécurité à un niveau acceptable. Donc pour pouvoir identifier les besoins de sécurité, les risques de sécurité doivent préalablement avoir été identifiés. De nouvelles approches sont proposées pour développer les contrôles de sécurité, mais il n'existe malheureusement pas à ce jour, aucune méthode qui permette l'analyse et l'évaluation des risques de sécurité au niveau de l'application elle-même.

Bien sûr, il existe plusieurs méthodes d'analyse de risques de sécurité organisationnelles, qui commencent à être utilisées par nos organisations. Nommons ici la méthode OCTAVE du Software Engineering Institute (SEI), la méthode harmonisée d'analyse des risques (MÉHARI) du CLUSIF ainsi que la méthode EBIOS de l'Agence nationale de la sécurité de l'information de France. En excluant nos travaux de recherches que nous réalisons avec le CLUSIF sur ce domaine, aucune de ces méthodes ne devrait être utilisée pour réaliser une analyse de sécurité applicative, car aucune d'entre elles n'a été développée avec cet objectif.

Les mesures d'elles utilisent permettent d'identifier et d'évaluer des risques de sécurité pour l'organisation à utiliser des TI, mais ne permettent pas d'identifier les risques de sécurité à utiliser une application particulière, dans le contexte particulier de cette organisation, avec les informations spécifiques que l'organisation y aura placées. Ne pouvant identifier les risques, ces méthodes ne pourront donc pas identifier les exigences de sécurité, ni les contrôles de sécurité à mettre en place à l'intérieur ou autour de l'application.

Cette problématique est très importante, car toute l'approche de la mise en place de la sécurité de l'information par la gestion du risque amenée par les organisations internationales comme notamment l'ISO, avec sa série de normes ISO 27000, ou l'ISACA avec son code de bonnes pratiques de gestion de la sécurité de l'information COBIT, deviennent impossibles à réaliser. Comment pouvons-nous démontrer que les risques de sécurité amenés par l'utilisation d'une application ont correctement été diminués si on ne peut identifier ces risques? De plus, comment peut-ont affirmer qu'une application est sécuritaire, si on ne peut arrimer les contrôles de sécurité qui ont été mis en place, avec les risques de sécurité devant être mitigés?

Le cycle de vie de la SA devra permettre d'identifier les moments ou d'une méthode d'identification et des sources des exigences de SA devraient être réalisé. Ceci afin d'être en mesure de répondre à ces interrogations et de permettre à une organisation de mettre les contrôles de sécurité adéquats qui diminueront les risques de sécurité applicative à un niveau acceptable.

Notre travail de recherche devra proposer les sources et une démarche d'identification des exigences de sécurité d'une application.

De fait, sans une de méthode l'identification des sources des exigences de sécurité d'une application, il sera très difficile d'en évaluer la sécurité. Ce qui nous amène à une autre problématique.

V.10 Absence d'une méthode d'évaluation de la SA

Évaluer la SA n'est pas toujours aussi simple qu'il n'y parait. Peut-on évaluer la SA sans tenir compte de ses environnements de réalisation et d'utilisation? Comme nous l'avons vu précédemment, la révision du code source d'une application est une activité qui peut amener à l'identification de faille de sécurité tel qu'une mauvaise implémentation d'un protocole de chiffrement, mais doit-on vérifier tout le code? Sachant que l'on peut prouver que le code vérifié est bien celui qui sera utilisé par l'application, vérifier le code permettra-t-il d'identifier toutes les vulnérabilités d'une application? Si, suite à la révision du code, l'organisation qui utilisera l'application décide de faire réaliser des tests de vulnérabilités permets d'identifier de nouvelles failles, est-ce que ces deux activités seront suffisantes pour déclarer l'application sécuritaire? Y a-t-il d'autres activités de sécurité qui devraient être réalisées? Si oui, lesquelles? Et si on réalise toutes ces activités, allons-nous en avoir fait trop pour protéger cette application? Si une organisation décide d'implémenter tous les contrôles et bonnes pratiques de sécurité proposés, peut-être que la valeur de cette application et des informations à protéger ne justifiaient pas un tel investissement de la part de l'organisation.

Le cycle de vie de la SA défini dans ce projet devra donc permettre d'identifier les moments ou une méthode d'évaluation de la SA devrait être réalisée. Ceci, afin d'être en mesure de répondre à ces interrogations et de permettre à une organisation de déclarer une application sécuritaire, et d'être en mesure de fournir les éléments appuyant cette affirmation.

Notre travail de recherche devra proposer un processus d'évaluation de la sécurité d'une application.

V.11 Absence d'un processus reconnu, permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de sécurité de l'organisation

Non seulement on ne considère généralement pas les risques et l'environnement d'utilisation d'une application avant de la déclarer sécuritaire, mais il n'existe que peut, sinon pas de

processus reconnu permettant une évaluation reconnue de la SA selon les besoins de sécurité de l'organisation.

Les Critères Communs est un de ces outils. Il permet d'identifier un profil de protection ainsi qu'une cible de sécurité, qui permettront d'identifier les critères de sécurité selon lesquelles une version d'une application sera évaluée. (Group, 2009) Mais l'évaluation de la sécurité d'un produit par cette méthode est très dispendieuse à réaliser et peu d'organisations ont les moyens de l'utiliser (Office, 2006).

Dans la majorité des cas, selon les circonstances et le budget disponible de l'organisation, une application pourra être déclarée sécuritaire à la suite d'un test de vulnérabilité et de pénétration, ou à la suite d'une révision du code de l'application. Ces deux méthodes son généralement les moyens les plus utilisés par l'industrie de la sécurité pour évaluer la sécurité d'une application. Mais qu'en est-il vraiment?

Afin de pouvoir vérifier la sécurité d'une application, serait-il important de pouvoir utiliser une méthode d'évaluation formelle, répétable qui tiendrait compte des besoins de sécurité de l'organisation?

Sachant que la SA doit être vérifiable, dans quel contexte de référence les résultats d'une vérification de la SA doivent-ils être mesurés et interprétés pour que cette dernière soit considérée comme sécuritaire? Nous savons que les organisations utilisant des applications commencent à exiger des preuves de sécurité plus concrètes que la simple réputation des organisations et le professionnalisme des intervenants du secteur des TI.

Si ces preuves existent, le présent projet devra être en mesure de déterminer les mécanismes permettant de les fournir, et de cerner les éléments ainsi que le contexte de référence permettant d'énoncer une définition claire de ce qu'est une application sécuritaire.

Notre travail de recherche devra proposer un processus permettant la vérification des éléments de sécurité d'une application, en fonction des besoins de sécurité de l'organisation.

V.12 Absence d'arrimage entre les approches, méthodes, acteurs et outils existants pour mettre en place la sécurité des applications

Il existe toute une panoplie de méthodes, de normes, de bonnes pratiques et d'outils de sécurité qui sont reliés à la sécurité des applications.

Nous pouvons les diviser en deux groupes, ceux qui implémentent la sécurité en améliorant la qualité et la maturité des processus du projet d'application, et ceux qui implémentent la sécurité en améliorant la qualité du produit, soit de l'application elle-même.

La Figure-A V-1 présente les quatre P de l'ingénierie logicielle (Booch, Jacobson et Rumbaugh, 1999) qui propose une bonne vision simplifiée des éléments : personnes, projet, produit et processus d'un projet d'ingénierie logicielle, mais il n'en précise pas les relations.

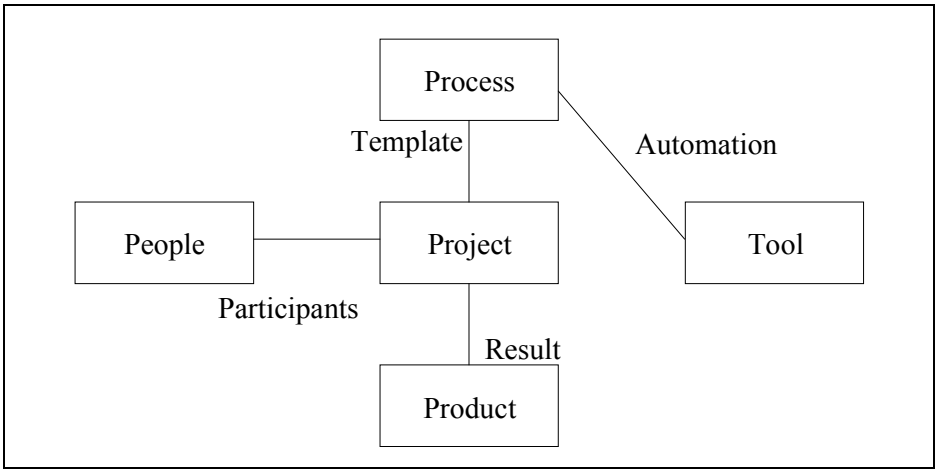


Figure-A V-1 Les quatre P de l'ingénierie logicielle selon Booch, Jacobson et Rumbaugh
Tiré de (Booch, Jacobson et Rumbaugh, 1999)

La figure ci-dessus présente les relations qui unis ces quatre P, soit : que les personnes participant au développement d'un produit, peuvent utiliser des outils pour automatiser

certains processus qui sont requis lors de la réalisation d'un projet menant à un produit. Par contre, les auteurs ne précisent pas les rôles de ces personnes, ni leurs implications respectives dans un projet de développement de produit logiciel.

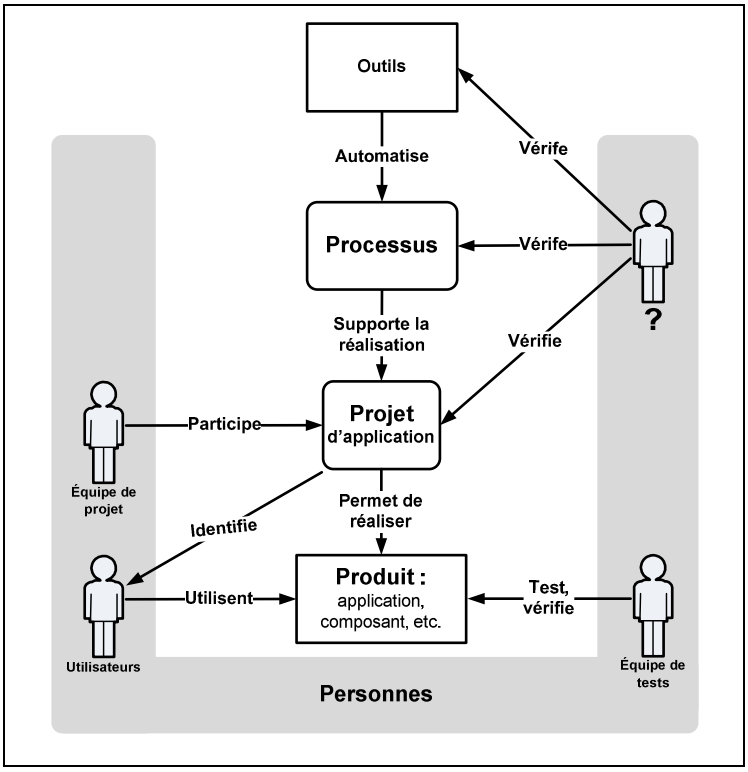


Figure-A V-2 Identification des principaux rôles des personnes impliquées dans l'ingénierie logicielle selon Booch, Jacobson et Rumbaugh

La figure Figure-A V-2 reprend le « modèle des 4 P » du développement de logicielle en tentant d'identifier les principaux rôles des personnes ainsi que les principales actions réalisées par les ces dernières lorsqu'elles sont impliquées dans un projet. Deux questions viennent immédiatement à l'esprit. Quelles sont les personnes qui sont impliquées dans la sécurité d'une application? Ces personnes devraient-elles avoir des responsabilités et qualifications supplémentaires concernant la sécurité d'une application?

Pourquoi est-il important de pouvoir identifier ces principaux acteurs et leurs actions respectives? Simplement parce que trop souvent, des personnes qui peuvent avoir un impact important sur la sécurité d'une application, soit parce qu'elles peuvent être une source de

risques de sécurité, soit parce qu'elles pourraient mettre en place des contrôles de sécurité permettant de diminuer ces risques, sont simplement absente de la description d'un projet ou ne savent pas qu'elles devraient aussi réaliser des activités de sécurité.

Les approches, méthodes et outils existants, qui ont été développées pour aider l'industrie à mettre en place la SA ont été par secteur d'intervention. La majorité d'entre eux sont excellents, mais quelques problèmes subsistent.

Voici un premier exemple, ou l'identification des rôles de cas d'utilisation peut avoir un impact sur la sécurité des informations d'une application :

- Lors du processus d'identification des cas d'utilisation d'une application, durant sa phase de développement, les cas d'utilisation impliquant des rôles d'acteurs comme notamment : le « root », l' « admin » et le « DBA », sont généralement manquants. Ces rôles donnent généralement des accès privilégiés aux personnes ou processus qui en obtiennent la l'assignation. Par exemple, lors de l'audit de sécurité des SVÉ du DGÉQ, il s'est avéré qu'un technicien a réalisé une intervention dans un bureau de votation, pour réparer la panne d'un système de votation, durant la période de votation. N'ayant pas été identifié, ce scénario n'avait pas défini et aucune procédure n'existait pour encadrer cette intervention.

  Le problème ici étant qu'aucun contrôle ni mesure de sécurité n'avait été mis en place, ni dans le SVÉ, ni dans aucun processus de maintenance, pour garantir que tous les votes qui avaient été enregistrés dans la mémoire du système de votation, y étaient toujours, intactes, après l'intervention du technicien.

Plusieurs ouvrages en sécurité sont disponibles aujourd'hui, tels que : Security System Development with UML, Security Patterns, Software vulnerability guide, Writing Secure Code, Implementing Database Security Auditing. Plusieurs normes et bonnes pratiques de sécurité sont aussi disponibles à qui veux bien les utiliser, comme notamment : ISO 27001, SSE-CMM, CC. Et finalement plusieurs normes existent aussi pour aider les développeurs à

implémenter la sécurité dans leurs systèmes, tels que : SP 800-64 Series Security Considerations in the Information System Development Life Cycle, ISO 15443 *Information technology – Security techniques – A framework for IT security assurance*. Mais aucune norme ou méthode propose un cadre normatif d'éléments et d'activités permettant de relier tous ces ouvrages normes et bonnes pratiques pour y intégrer les éléments de SA de façon globale, complémentaires et vérifiables.

Voici un deuxième exemple, ou d'arrimage entre les approches, méthodes et outils existants, peuvent avoir un impact sur la sécurité des informations d'une application :

- L'organisation OWASP propose une série de bonnes pratiques de sécurité dans le développement de logiciel, dont une pratique qui recommande la révision du code source afin d'y détecter les failles de sécurité. Cette pratique est excellente en elle-même, mais est complètement inutile sans la mise en place d'un contrôle, qui garantirait que le code révisé est bien celui qui s'exécutera dans le système concerné.

  Ce cas a aussi été mis en évidence lors de l'audit de sécurité des SVÉ. Le DGÉQ nous a demandé de réaliser une révision du code de toutes les SVÉ qui ont été utilisées lors des élections municipales québécoises de 2005. La demande était intéressante, surtout que certaines entreprisse avait affirmé que le code source de leurs systèmes avait déjà été audité. Malheureusement, non seulement aucune entreprise n'a été en mesure de nous fournir des preuves de ces audits, ni des preuves que les versions des logiciels audités étaient bien celui qui avaient été utilisés dans les SVÉ le jour de l'élection.

  Un fournisseur nous a même avoué que des personnes inconnues avaient eu un accès physique à ses SVÉ, la nuit où ils étaient en transit dans ses entrepôts de livraison, et que le logiciel sauvegardé dans la mémoire de ces systèmes aurait pu être modifié sans qu'on puisse le détecter. L'audit a aussi mis en lumière qu'un fournisseur avait mis à jour le logiciel de certains SVÉ, sans processus formel, le jour même de l'élection.

Notre projet de recherche devra faciliter l'arrimage entre les approches, méthodes et outils existants pour mettre en place la sécurité des applications.

V.13 Absence de mécanismes permettant d'assigner aux principaux rôles pouvant avoir un impact sur la sécurité d'une application, les qualifications requises pour chacune de ces responsabilités

Elle aussi devra fournir les mécanismes permettant d'assigner aux principaux rôles requis pour définir, gérer, réaliser et vérifier les activités de sécurité des applications, les qualifications requises par chacune de ces responsabilités.

V.14 Les méthodes et outils existants de génie logiciel ne tiennent pas toujours compte de la sécurité de l'information

La majorité des méthodes de développement, des normes nationales, internationales et bonnes pratiques n'incluent pas toujours la sécurité et quand elles le font, c'est soit en termes vagues et généraux, qui présentent généralement une vérité de La Palice (ISO/IEC, 2008e) (ISO/IEC, 2007g), soit en termes qui essaie de décrire des activités ou des éléments de sécurité qui devraient être réalisés de manière plus précise (LLC, 2010) (OWASP, 2010). Il n'existe pas d'outils permettant de dégager une vision globale permettant d'identifier les activités de sécurité qui devraient être réalisées lors d'un projet spécifique, ni d'identifier les connaissances et qualifications qui devraient être requises pour réaliser ces activités de sécurité correctement.

Bien sûr, plusieurs organisations présentent leurs méthodes et outils, comme « LA » solution miracle. Mais l'est-elle réellement? Comment l'évaluer?

Notre projet de recherche devra faciliter l'intégration des contrôles de sécurité des applications 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 par

rapport aux approches, aux méthodes et aux outils existants pour mettre en place la sécurité des applications.

V.15 Implémenter la sécurité en intégrant des contrôles de sécurité à l'intérieur des processus impliqués dans la réalisation et l'opération de l'application

Même si elles n'en sont pas toujours conscientes, toutes les organisations et personnes qui développent ou utilisent des applications suivent des processus. Certaines ont atteint un niveau de maturité leur permettant d'avoir accès a des processus formels, documentés, vérifiables et vérifiés, tandis que d'autres utilisent des processus informels et immatures. Dans la plupart des cas, elles considéreront que les méthodes et processus qu'elles utilisent sont adéquats pour leurs besoins et ne voient pas toujours l'intérêt de les changer ou de les améliorer.

Certaines méthodes et outils tentent d'améliorer la sécurité en bonifiant les processus existant à l'intérieur d'une organisation avec de nouvelles activités et processus de sécurité, tel que le processus de révision de code ou le processus de développement sécuritaire d'OWASP, ou d'améliorer le processus d'audit de sécurité de l'organisation en mettant en place la méthode d'audit COBIT. Mais si les organisations n'ont pas les ressources de leurs ambitions, ou qu'elles ne voient pas les bénéfices concrets qu'elles peuvent y retirer, ces nouvelles méthodes ne seront jamais implantées.

Que l'on désire utiliser des méthodes de développement sécuritaire tel que notamment, le SDL de Microsoft (Microsoft, 2011), en passant par les pratiques de programmation sécuritaire (OWASP, 2005), du guide de révision de code (OWASP, 2008a) et du guide de tests (OWASP, 2008b) d'OWASP, des normes ISO 15504 : Process Assessment (SPICE) , aux normes SP 800-64 Series : Security Considerations in the Information System Development Life Cycle, et SP 800-8 : Security Issues in the Database Language SQL du FIPS/NIST, ou la certification professionnelle CSSLP Certified Secure Software Lifecycle Professional de l'$(ISC)^2$.

Avec cette panoplie de méthodes et d'outils disponibles, servant à intégrer la sécurité dans les processus d'une application, on pourrait conclure que cette intégration est bien maîtrisée. Malheureusement, quatre questions se posent toujours, au sujet des contrôles de sécurité à intégrer aux processus impliqués dans le développement et l'utilisation d'une l'application :

1) tous ces « outils » offrent des visions, des activités et des contrôles de sécurité, menant à l'introduction de la sécurité des processus impliqués par une application, qui ne semblent pas nécessairement cohérente et compatibles entres-elles et risque de cohabiter difficilement;
2) aucun ne me permet d'identifier toutes les activités, contrôles ou méthodes de sécurité qui devraient être intégrés dans les processus de mon organisation, ni quelles en sont leurs priorités respectives;
3) aucun n'arrime tout ces contrôles, activités et processus en un tout cohérent menant à l'affirmation qu'une application est ou sera sécuritaire;
4) les coûts d'implémentation de certains de ces outils sont astronomiques, d'autres sont beaucoup plus abordables. Comment justifier le retour sur l'investissement en fonction de l'amélioration du niveau de sécurité obtenue par l'intégration des éléments de sécurité dans les processus de l'organisation?

De plus, en développement d'application comme dans bien d'autres milieux, la résistance des personnes impliquées par un changement est un facteur non négligeable d'échec de l'objectif visé par ce changement et il doit être considéré afin maximiser le succès de l'implémentation des activités de sécurité des applications. Par exemple, le changement d'une méthode de développement jugé adéquate pour les besoins immédiats d'une organisation, par une bien meilleure ne sera pas nécessairement bien acceptée, ni par les dirigeants de l'organisation qui y verront des coûts supplémentaires inutiles et une perte de productivités des équipes impliquées, ni des personnes elles-mêmes, qui y verront généralement un surplus de travail important pour des résultats mitigés de sécurité.

En intégrant les activités de sécurité qui sont jugées prioritaires, ou celles qui offrent le meilleur retour sur l'investissement, de manière ordonnée, directement dans les processus

existants de l'organisation, les problèmes de résistances aux changements et de justification des priorités et des coûts de SA sont grandement diminués.

Notre projet de recherche devra proposer une méthode et un cadre normatif de SA qui permet d'évaluer, de développer, de valider et de vérifier les activités et contrôles de sécurités jugées 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. Finalement il pourra servir à normaliser ses activités et contrôles de sécurité à l'intérieur de tous ses projets d'applications.

V.16 Implémenter la sécurité en intégrant des contrôles de sécurité à l'intérieur de l'application

Certaines méthodes et outils ont été développés afin d'améliorer la sécurité en bonifiant le produit, tel que les CC, le guide de tests d'OWASP, et les outils de tests de sécurité automatique tels qu'AppScan d'IBM.

Ici encore, les quatre mêmes questions se posent, mais cette fois-ci, au sujet des contrôles de sécurité à intégrer à l'application :

1) tous ces « outils » offrent des visions, des activités et des contrôles de sécurité, menant à l'amélioration de la sécurité d'une application, qui ne semblent pas nécessairement cohérente et compatibles entres-elles et qui risque de cohabiter difficilement;
2) aucun ne me permet d'identifier tous les contrôles et activités de sécurité qui devraient être intégrés dans mon application, ni quelles en sont leurs priorités respectives;
3) aucun n'arrime tout ces contrôles, activités et processus en un tout cohérent menant à l'affirmation qu'une application est ou sera sécuritaire;
4) les coûts d'implémentation de certains contrôles de sécurité sont astronomiques, d'autres sont beaucoup plus abordables. Comment justifier le retour sur

l’investissement en fonction de l’amélioration de la sécurité obtenue par l’intégration des contrôles de sécurité dans l’application?

ANNEXE VI

REVUE DE LITTÉRATURE DÉTAILLÉE

Cette annexe présente le détail de la revue de littérature qui a été réalisée durant cette recherche.

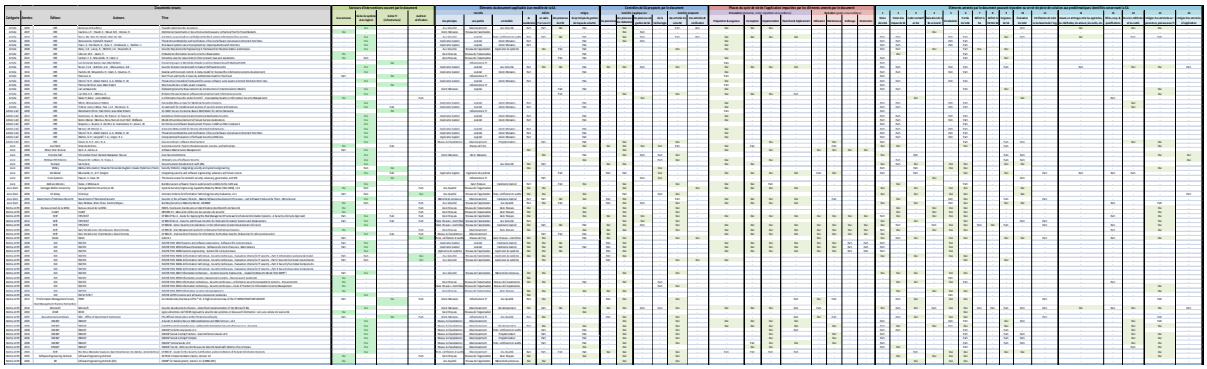
VI.1 Recensement et analyse des problèmes de sécurité liés à l'utilisation d'applications

La revue de littérature a été réalisée en identifiant et regroupant les sources des documents selon 4 catégories :

1) les publications, dont notamment les articles scientifiques et les livres,
2) les normes et pratiques recommandées, provenant d'organisations nationales et internationales dont notamment l'OCDE, ISO, IEEE, ITIL, l'ISACA et l'OWASP,
3) les modèles et outils offerts par l'entreprise privée, dont notamment : le SDL de Microsoft et BSIMM2.

NOTE Le Tableau-A VI-1 nécessite l'utilisation de papier de format 11 x 17 pour pouvoir s'imprimer correctement.

Tableau-A VI-1 Synthèse de la revue de littérature selon les domaines, les éléments et les problématiques



(Insérez ici le Tableau-A VI-1 en format 11 x 17)

VI.2 Liste des normes du SC7 : *Software Engineering* qui ont été considérées durant ce travail de recherche

Les normes suivantes ont été considérées et analysées sommairement.

ISO/IEC 6592	Information technology – Guidelines for the documentation of computer-based application systems
ISO/IEC 9126	Software engineering – Product quality: Quality model, External metrics, Internal metrics, Quality in use metrics
ISO 9127	Information processing systems – User documentation and cover information for consumer software packages
ISO/IEC TR 9294	Information technology – Guidelines for the management of software documentation
ISO 10007:2003	Quality management systems - Guidelines for configuration management
ISO/IEC 11411	Information technology – Representation for human communication of state transition of software
ISO/IEC TR 12182	Information technology – Categorization of software
ISO/IEC 14143	Information technology – Software measurement – Functional size measurement,
ISO/IEC TR 14471	Information technology – Software engineering – Guidelines for the adoption of CASE tools
ISO/IEC 14568	Information technology – DXL: Diagram eXchange Language for tree-structured charts
ISO/IEC 14598	Information technology – Software product evaluation: General overview, Planning and management, Process for developers, Process for acquirers, Process for evaluators, Documentation of evaluation modules
ISO/IEC 14750	Information technology – Open Distributed Processing – Interface Definition Language
ISO/IEC 14753	Information technology – Open Distributed Processing – Interface references and binding

ISO/IEC 14764	Software Engineering – Software Life Cycle Processes – Maintenance
ISO/IEC 15026	Information technology – System and software integrity levels
ISO/IEC TR 15271	Software Engineering – Software life cycle processes - Guide for ISO/IEC 12207 (Software Life Cycle Processes)
ISO/IEC 15289	Systems and software engineering – Content of systems and software life cycle process information products (Documentation)
ISO/IEC 15443-1	Information technology – Security techniques - A framework for IT security assurance – Part 1: Overview and framework
ISO/IEC 15443-2	Information technology – Security techniques - A framework for IT security assurance – Assurance methods
ISO/IEC 15443-3	Information technology – Security techniques - A framework for IT security assurance – Analysis of assurance methods
ISO/IEC 15910	Information technology – Software user documentation process
ISO/IEC 15939	Software engineering – Software measurement process
ISO/IEC 15940	Information Technology – Software Engineering Environment Services
ISO/IEC 16085	Systems and software engineering – Life cycle processes – Risk management
ISO/IEC TR 16326	Software engineering – Guide for the application of ISO/IEC 12207 to project management
ISO/IEC 18019	Software and system engineering – Guidelines for the design and preparation of user documentation for application software
ISO/IEC 18045	(To be published), Information technology – Security techniques – Methodology for IT security evaluation
ISO/IEC 19501	Information technology – Open Distributed Processing – Unified Modeling Language (UML)
ISO/IEC TR 19759	Software Engineering – Guide to the Software Engineering Body of Knowledge (SWEBOK)
ISO/IEC TR 19760	Systems engineering – A guide for the application of ISO/IEC 15288 (System life cycle processes)

ISO/IEC 19761	Software engineering – OSMIC-FFP – A functional size measurement method
ISO/IEC 19770	Information technology – Software asset management
ISO/IEC TR 19791	Information technology – Security techniques – Security assessment of operational systems
ISO/IEC 20000	Information technology – Service management
ISO/IEC 24744	Software Engineering – Metamodel for Development Methodologies
ISO/IEC TR 24748	System and Software Engineering - Guide for life cycle management
ISO/IEC 24765	(To be published), Systems and software engineering vocabulary
ISO/IEC 24774	System and Software Engineering - Life Cycle Management - Guidelines for process definition
ISO/IEC 25001	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Planning and management
ISO/IEC 25010	(To be published), Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Quality model
ISO/IEC 25012	(To be published), Software Engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Data Quality Model
ISO/IEC 25020	(To be published), Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Measurement reference model and guide
ISO/IEC TR 25021	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Quality measure elements
ISO/IEC 25023	(To be published), Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Measurement of External Quality
ISO/IEC 25024	(To be published), Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Measurement of Quality in Use
ISO/IEC 25030	Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Quality requirements

ISO/IEC 25040	(To be published), Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Evaluation reference model and guide
ISO/IEC 25051	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing
ISO/IEC 25062	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability test reports
ISO/IEC 26702	(To be published?), IEEE Standard for Application and Management of the Systems Engineering Process
ISO/IEC 29382	(To be published?), Corporate Governance of Information and Communication Technology
ISO/IEC 42010	(To be published?), Systems and software engineering - Recommended practice for architectural description of software-intensive systems
ISO/IEC 90003	Software engineering – Guidelines for the application of ISO 9001:2000 to computer software
ISO/IEC TR 90005	Systems engineering – Guidelines for the application of ISO 9001 to system life cycle processes

VI.3 Liste des normes du *Federal Information Processing Standard* (FIPS) et du *National Institute of Standards and Technology* (NIST) qui ont été considérés durant ce travail de recherche

Les normes suivantes ont été considérées et analysées sommairement.

FIPS PUB 140-2 Security Requirements for Cryptographic Modules – 01 May 25 (Supersedes FIPS PUB 140-1, 1994 January 11)

FIPS PUB 161-2 Electronic Data Interchange (EDI) – 96 May 22 - FIPS 161-2 adopts, with specific conditions, the families of EDI standards known as X12, UN/EDIFACT and HL7 developed by national and international standards developing organizations. FIPS 161-2 does not mandate the implementation of EDI systems within the Federal government, but requires the use of the identified families of standards when Federal agencies and organizations implement EDI systems.

FIPS PUB 193 SQL Environments

FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems, 2004 February. FIPS 199 addresses one of the requirements specified in the Federal Information Security Management Act (FISMA) of 2002, which requires all federal agencies to develop, document, and implement agency-wide information security programs for the information and information systems that support the operations and the assets of the agency, including those provided or managed by another agency, contractor, or other source. FIPS 199 provides security categorization standards for information and information systems. Security categorization standards make available a common framework and method for expressing security. They promote the effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities. Such standards also enable consistent

	reporting to OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
FIPS PUB 200	Minimum Security Requirements for Federal Information and Information Systems, 2006 March. FIPS 200 is the second standard that was specified by the Federal Information Security Management Act of 2002 (FISMA). It is an integral part of the risk management framework that NIST has developed to assist federal agencies in providing levels of information security based on levels of risk. FIPS 200 specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements.
NIST IR-7316	Assessment of Access Control Systems
SP 800-2	Public-Key Cryptography, April 1991
SP 800-3	Special Publication 800-3: Establishing a Computer Security Incident Response Capability (CSIRC), November 1991. As of January 2004, 800-3 has been superceded by 800-61 Computer Security Incident Handling Guide
SP 800-4	Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiatiors, Contracting Officers, and Computer Security Officials, March 1992. As of October 2003, 800-4 has been superceded by 800-64 Security Considerations in the Information System Development Life Cycle
SP 800-5	A Guide to the Selection of Anti-Virus Tools and Techniques, December 1992
SP 800-6	Automated Tools for Testing Computer System Vulnerability, December 1992
SP 800-7	Security in Open Systems, July 1994
SP 800-8	Security Issues in the Database Language SQL, August 1993
SP 800-9	Good Security Practices for Electronic Commerce, Including Electronic Data Interchange, December 1993

SP 800-10	Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, December 1994
SP 800-11	The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security, February 1995
SP 800- 23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800- 26	Security Self-Assessment Guide for Information Technology Systems - Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings.
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800- 28	Guidelines on Active Content and Mobile Code,
SP 800- 29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2,
SP 800- 30	Risk Management Guide for Information Technology Systems,
SP 800- 31	Intrusion Detection Systems (IDS),
SP 800- 32	Introduction to Public Key Technology and the Federal PKI Infrastructure,
SP 800- 33	Underlying Technical Models for Information Technology Security,
SP 800- 34	Contingency Planning Guide for Information Technology Systems,
SP 800- 35	Guide to Information Technology Security Services,
SP 800- 36	Guide to Selecting Information Technology Security Products,
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems,
SP 800- 38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques,
SP 800- 40	Version 2 Creating a Patch and Vulnerability Management Program
SP 800- 45A	Draft Special Publication, Guidelines on Electronic Mail Security
SP 800- 46	Security for Telecommuting and Broadband Communications,
SP 800- 47	Security Guide for Interconnecting Information Technology Systems,

SP 800- 52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,
SP 800- 53	Recommended Security Controls for Federal Information Systems, including:
	Annex 1: Baseline Security Controls for Low-Impact Information Systems
	Annex 2: Baseline Security Controls for Moderate-Impact Information Systems
	Annex 3: Baseline Security Controls for High-Impact Information Systems
SP 800- 55	Security Metrics Guide for Information Technology Systems,
SP 800- 57	Recommendation on Key Management,
SP 800- 59	Guideline for Identifying an Information System as a National Security System,
SP 800- 60	Guide for Mapping Types of Information and Information Systems to Security Categories,
SP 800- 63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
SP 800-64 Series	Security Considerations in the Information System Development Life Cycle
SP 800- 68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800- 70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers
SP 800- 73	Interfaces for Personal Identity Verification (PIV)
SP 800- 78-1	Draft Special Publication, Cryptographic Standards and Key Sizes for Personal Identity Verification
SP 800-80	Draft Special Publication 800-80, Guide for Developing Performance Metrics for Information Security
SP 800- 83	Guide to Malware Incident Prevention and Handling

SP 800- 84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800- 85A	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance),
SP 800- 85B	PIV Data Model Conformance Test Guidelines
SP 800- 92	Draft Special Publication, Guide to Computer Security Log Management
SP 800- 94	Draft Special Publication, Guide to Intrusion Detection and Prevention (IDP) Systems
SP 800- 95	Draft Special Publication, Guide to Secure Web Services
SP 800- 97	Draft Special Publication, Guide to IEEE 802.11i: Robust Security Networks
SP 800-100	Draft Special Publication, Information Security Handbook: A Guide for Managers
FIPS PUB 132	Guideline for Software Verification and Validation Plans (ANSI/IEEE 1012-1986)

VI.4 Liste des normes du *Institute of Electrical and Electronics Engineers – Computer-Society* (IEEE CS) qui ont été considérées durant ce travail de recherche

Les normes suivantes ont été considérées et analysées sommairement.

IEEE 730	IEEE Standard for Software Quality Assurance Plans
IEEE 828	IEEE Standard for Software Configuration Management Plans
IEEE 829	IEEE standard for software test documentation
IEEE 830	IEEE recommended practice for software requirements specifications
IEEE 982.1	IEEE Standard Dictionary of Measures of the Software Aspects of Dependability
IEEE 892.2	IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software
IEEE 983	IEEE Guide for Software Quality Assurance Planning
ANSI/IEEE 1002	IEEE Standard Taxonomy for Software Engineering Standards
ANSI/IEEE 1008	IEEE Standard for Software Unit Testing
IEEE Std 1012	IEEE Standard for Software Verification and Validation and Validation Plans
IEEE Std 1016	IEEE Recommended Practice for Software Design Descriptions
IEEE Std 1028	IEEE Standard for Software Reviews
ANSI/IEEE 1042	IEEE Guide to Software Configuration Management
IEEE Std 1044	IEEE Standard Classification for Software Anomalies
IEEE 1045	IEEE standard for software productivity metrics
IEEE Std 1058	IEEE Standard for Software Project Management Plans
IEEE Std 1059	IEEE Guide for Software Verification and Validation Plans
IEEE Std 1061	IEEE Standard for a Software Quality Metrics Methodology
IEEE Std 1062	IEEE Recommended Practice for Software Acquisition
IEEE Std 1063	IEEE Standard for Software User Documentation
IEEE Std 1074	IEEE Standard for Developing Software Life Cycle Processes
IEEE Std 1175	IEEE Trial-Use Standard Reference Model for Computing System Tool Interconnections

IEEE Std 1209	IEEE Recommended Practice for the Evaluation and Selection of CASE Tools
IEEE Std 1219	IEEE Standard for Software Maintenance
IEEE Std 1220	IEEE Standard for Application and Management of the Systems Engineering Process
IEEE Std 1228	IEEE Standard for Software Safety Plans
IEEE Std 1233	IEEE Guide for Developing System Requirements Specifications
IEEE Std 1298	Software Quality Management System Part 1: Requirements
IEEE Std 1320	IEEE Standard for Functional Modeling Language
IEEE Std 1348	IEEE Recommended Practice for the Adoption of Computer-Aided Software Engineering (CASE)
IEEE Std 1362	IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps)
IEEE Std 1420	IEEE Standard for Information Technology – Software Reuse – Data Model for Reuse Library, Software Reuse
IEEE Std 1430	IEEE Guide for Information Technology – Software Reuse – Concept of Operations for Interoperating Reuse Libraries
IEEE Std 1471	IEEE Recommended Practice for Architectural Description of Software-Intensive Systems
IEEE Std 1490	Adoption of PMI Standard, A Guide to the Project Management Body of Knowledge
IEEE Std 1517	IEEE Standard for Information Technology – Software Life Cycle Processes – Reuse Processes
IEEE Std 1540	IEEE Standard for Software Life Cycle Processes – Risk Management
IEEE Std 610	IEEE Standard Glossary of Software Engineering Terminology
IEEE Std 730	IEEE Standard for Software Quality Assurance Plans
IEEE Std 828	IEEE Standard for Software Configuration Management Plans
ANSI/IEEE 829	IEEE Standard for Software Test Documentation
IEEE Std 830	IEEE Recommended Practice for Software Requirements Specifications

IEEE Std 982 IEEE Standard Dictionary of Measures to Produce Reliable Software

VI.5 Liste des normes du *Organization for the Advancement of Structured Information Standards* (OASIS) qui ont été considérés durant ce travail de recherche

Functional Elements Specification, Primer, OASIS Open, Version 1.0, October 2006, 17pp.

Functional Elements Specification, Committee Specification, Version 1.0, OASIS Open, October 2006, pp274

Functional Elements Specification, Related Standards and Technologies, Documentations URL, OASIS Open, November 2006, 8pp.

Functional Elements Requirements, Requirements Document, OASIS Open, October 2005, 31pp.

List of Web Service-Related Standards, Japanese Contribution for ISO/IEC JTC 1 WSSG, January 2007, Excell file.

ANNEXE VII

MÉTHODOLOGIE DÉTAILLÉE DE LA RECHERCHE

Cette annexe présente la méthodologie détaillée de ceprojet de recherche.

VII.1 Phase 1 –Identification des principaux principes, concepts, et autres éléments à être inclus dans le modèle SA

Cette première phase d'identification sera réalisée par une revue de littérature des principales sources d'information sélectionnées en fonction de la crédibilité dans leur milieu respectif, soit du développement de logiciels, soit des domaines liés à la sécurité de l'information, incluant les organisations de normalisation en sécurité des TI telles que : IEEE, ISO, NIST, OWASP, CERT et ITU T.

Afin d'identifier les éléments utiles à nos travaux de recherche, les éléments suivants seront identifiés :

1) l'ouvrage présente une approche, un principe, une méthode, un processus ou un mécanisme servant à guider la mise en place ou l'amélioration d'un élément de sécurité à un système TI, répondant ainsi à une problématique identifiée. Cet élément peut s'appliquer autant à une personne qu'à un processus ou un composant technologique de l'application, tel que son logiciel ou encore un de ses composants matériels;
2) l'ouvrage ne se limite pas qu'à présenter un seul élément, tel qu'un mécanisme de chiffrement, un processus de gestion du risque ou la qualification des acteurs, ou qu'un seul niveau d'intervention (gouvernance, développement logiciel, et infrastructure) de la sécurité de l'information, mais présente une vision plus large regroupant au moins deux de ces éléments ou niveaux combinés.

La sélection des documents sera réalisée en deux étapes :

1) l'identification des ouvrages répondant aux deux premiers critères, permettant ainsi d'identifier la couverture des éléments et de faire l'inventaire des éléments qui

concernent la sécurité de l'information puis, plus spécifiquement, la sécurité des applications TI;

2) l'identification des ouvrages qui ont marqué le domaine, soit en évaluant informellement leur adoption par l'industrie ou les gouvernements, soit qu'ils sont déjà reconnus comme des incontournables dans le domaine de la sécurité de l'information.

Une fois ces éléments de solution sélectionnés, leurs analyses permettront de :

- distinguer leurs complémentarités;
- éliminer les duplications qui s'adressent aux mêmes objectifs ou problématiques; et
- identifier les éléments manquants qui doivent être développés.

VII.2 Phase 2 – Conception du modèle SA

Le modèle SA sera conçu en intégrant les éléments identifiés à la phase 1, et complété en ajoutant des éléments complémentaires requis pour répondre aux problématiques identifiées.

Une cible importante porte sur la maximisation de la réutilisation des éléments existants, provenant des principaux secteurs professionnels de la sécurité de l'information, afin de réduire la résistance aux changements auquel le modèle devra faire face lors de son implémentation en industrie.

VII.3 Phase 3 – Validation du modèle SA

Le processus de validation est réalisé en parallèle avec le développement du modèle. Le cycle de validation de la méthode Delphi qui sera utilisé dans la méthodologie de la présente recherche est présenté en détail à la section 6.1.

VII.4 Phase 4 – Vérification empirique partielle des éléments du modèle SA

Tel que présenté dans l'axe de la stratégie de vérification du modèle SA, la démarche de vérification empirique partielle de l'acceptabilité et de l'applicabilité des éléments du modèle SA par les organisations est réalisée en concurrence avec les phases de développement (phase 2) et de vérification du modèle SA (phase 3) de la méthodologie de recherche.

Le Tableau-A VII-1 présente les activités à réaliser pour effectuer la vérification empirique partielle des éléments du modèle SA, ainsi que les intentions visées par chercheur pour chacune de ces activités.

Tableau-A VII-1 Activités de déploiement et de vérification empirique partielle du modèle SA

Activité	**Intention**
Réaliser au moins un audit de SA développée, selon une approche traditionnelle, afin d'obtenir un état initial des règles de l'art en sécurité des applications	1) Identification des éléments de sécurité des applications actuellement en place en industrie
Présenter le modèle de sécurité des applications à l'industrie, par des présentations et des conférences, puis recueillir les commentaires	2) Présentation du modèle 3) Vérification empirique de son acceptabilité
Implémenter les principes, les concepts et les éléments du modèle de sécurité des applications dans un projet d'application en industrie	4) Présentation du modèle 5) Vérification empirique de son acceptabilité 6) Vérification de son utilité

Cette vérification empirique partielle consistera à :

1) présenter les éléments du modèle SA lors d'événements publics et privés touchant la sécurité de l'information. Un minimum de quatre représentations ciblant des professionnels d'organisation utilisant des TI devra être réalisé;
2) rendre disponibles les éléments du modèle à des organisations de taille et de domaines d'affaires différentes (c.-à-d., entreprises commerciales, agences gouvernementales,

organisations à but non lucratif, etc.) pour qu'elles puissent les utiliser lors de la réalisation de projets d'application. Un minimum de deux implémentations partielles du modèle SA devra être réalisé dans des projets d'applications en industrie;

3) évaluer et vérifier de manière empirique l'acceptabilité et de l'applicabilité des éléments du modèle SA. Un processus de vérification empirique partielle devra être utilisé pour évaluer les événements et les projets qui auront été réalisés durant cette étape de la méthodologie de recherche.

De plus, cette démarche permettra de recevoir des commentaires d'organisations qui sont aux faits des réalités et des défis auxquels elles font face concernant la sécurité de leurs applications. Ces commentaires, même s'ils sont émis de manière informelle, pourront servir à améliorer le modèle SA.

Le processus qui a été utilisé pour vérifier l'applicabilité et l'acceptabilité des éléments du modèle SA par les organisations est présenté à la section 6.2.1.

ANNEXE VIII

SÉLECTION D'UN SOUS-COMITÉ INTERNATIONAL D'ISO POUR LA VALIDATION DU MODÈLE SA

Parce que le processus de gestion de projet ISO utilise un processus de validation formel reconnu et documenté et qu'il rassemble des instances nationales compétentes provenant de plus 145 pays dans des sous-comités, la décision de soumettre les résultats préliminaires et finaux de notre recherche au processus de révision et de validation formel d'ISO a été intégrée à la méthodologie de développement de ce travail de recherche.

Sachant que cette recherche couvrira autant des domaines de connaissances impliqués dans la sécurité de l'information que celui du développement de systèmes d'information, il était important, pour rencontrer notre objectif de validation, d'identifier un sous-comité d'ISO qui soit en mesure de favoriser la participation d'un grand nombre d'experts vérificateurs des domaines de connaissances requises, appartenant autant au milieu de la recherche académique qu'à celui de l'industrie. Le sous-comité 27 (SC27) a ainsi été identifié comme groupe de validation, car ses travaux, auxquels participent plus de 35 pays[37], portent spécifiquement sur l'élaboration de techniques de sécurité des TI. Le SC27 encadre la réalisation de projets concernant la sécurité de l'information et implique la participation d'experts provenant notamment des secteurs de la gouvernance de la sécurité, du l'ingénierie logicielle et des infrastructures technologiques dont des chercheurs universitaires, des architectes de systèmes TI, des développeurs d'applications, des vérificateurs techniques et des représentants nationaux, responsables de l'approbation des documents. Tous ces experts sont délégués par les nations participantes.

L'accès et la consultation d'un grand nombre d'experts reconnus internationalement constituent donc le principal avantage de cette approche pour effectuer une validation

[37] Nombre de pays membres du SC27 en octobre 2006.

crédible des éléments du modèle. Ce sont ces instances nationales qui participeront à la validation des éléments du modèle, puis à l'approbation de leur intégration à un projet de norme de l'organisation internationale ISO.

ANNEXE IX

PROCESSUS D'ÉDITION D'UN PROJET ISO ET MÉTHODE DELPHI

Le processus d'édition d'un projet de l'organisation ISO se divise en sept étapes consécutives, appelées individuellement « stade ». La Figure-A IX-1, illustre sommairement les activités du processus habituel de réalisation de projet d'une norme ISO, tel que présenté dans la cinquième édition de *ISO/IEC Directives, Part 1 – Procedures for the technical work* (ISO/IEC, 2004b), et *ISO/IEC Directives, Part 2 – Rules for the structure and drafting of International Standards* (ISO/IEC, 2004c).

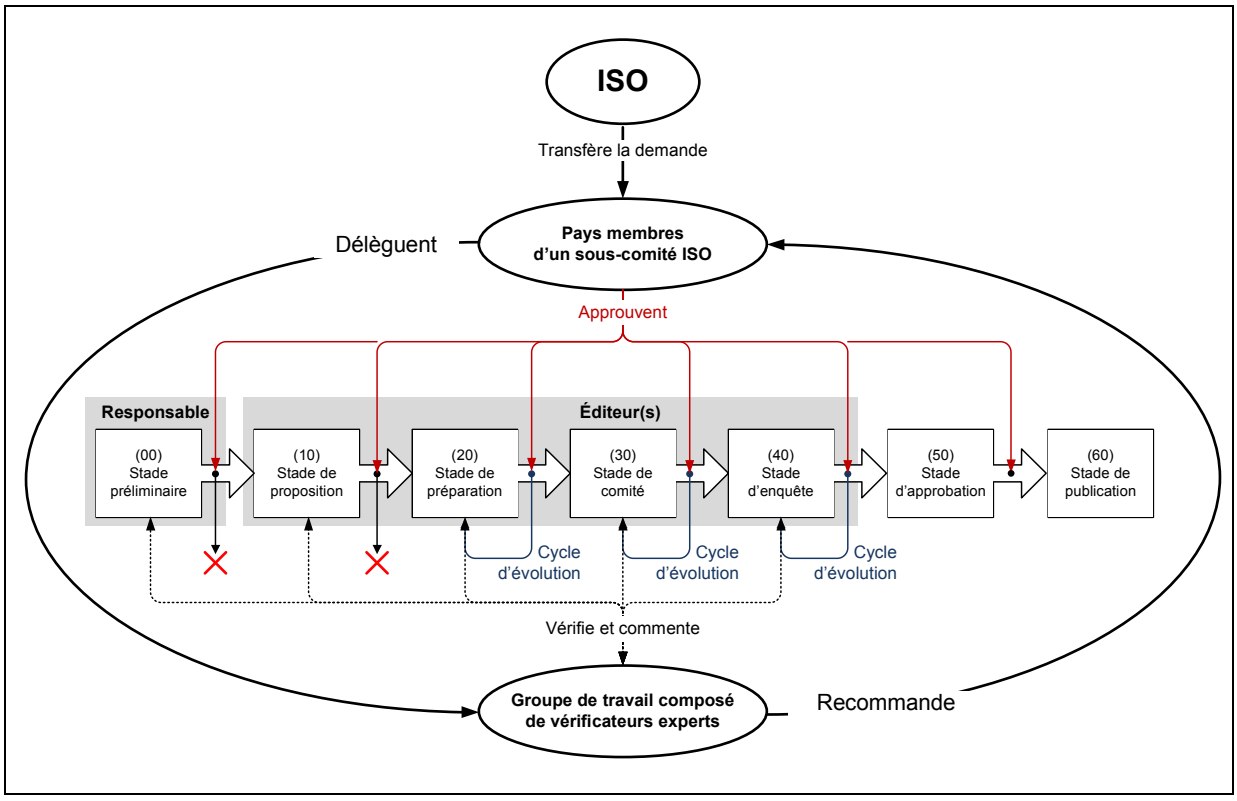


Figure-A IX-1 Processus d'édition d'un projet ISO

Tous les stades du processus d'ISO comportent au moins un cycle de validation. Chacun de ces cycles équivaut à un cycle Delphi. Tout comme proposé par la méthode Delphi, un cycle de validation d'ISO se divise en étapes successives, soit :

1) **L'étape de conception et d'amélioration**

   Un cycle débute lorsque l'éditeur génère une version du document après y avoir appliqué les actions des décisions découlant des commentaires reçus des experts délégués. C'est à cette étape que l'éditeur applique au document les résolutions des commentaires reçus. Une fois complétée, cette version est envoyée au secrétariat du SC27.

2) **L'étape de distribution**

   Le secrétariat du SC27 distribue une nouvelle version du document aux pays membres, pour validation et commentaires.

3) **L'étape de d'analyse et de remise de commentaires**

   C'est en utilisant les formulaires de projets ISO que les experts délégués par chacun des pays participants analyse et valide les éléments du modèle SA et émettent leurs commentaires et recommandations à leur comité national respectif. Chacun de ces comités consolide les commentaires et les recommandations reçus en remplaçant le nom des experts participants par le nom du pays qu'ils représentent pour en faire une position nationale officielle, qui est ensuite formellement transmise au comité de travail ISO.

4) **L'étape d'agrément sur le traitement des commentaires**

   Tous les commentaires nationaux reçus sont traités au cours de réunions de projet et un consensus sur le traitement de chacun d'eux est établi.

5) **L'étape d'approbation des recommandations**

   À la fin de chacune de ces réunions de projet, les experts qui y ont participé émettent des recommandations à leur représentant national respectif (soutenir, ne pas soutenir, s'abstenir). Chaque représentant national présentera par la suite, à travers un processus de

votation formel, la position officielle de son pays selon que ce dernier considère qu'un document est assez mature et qu'il supporte ou non une décision du sous-comité le concernant.

Pour simplifier, retenons que dans la majorité des situations, le processus de votation d'ISO considère qu'un document est approuvé lorsque plus de 66 % des représentants nationaux des pays votant soutiennent son passage au stade suivant. Le processus de décision d'ISO est détaillé dans le document *Directives, Part 1* (ISO/IEC, 2004b).

Les moyens de communication et de distribution mis en place par ISO permettent également de faciliter la distribution des résultats de nos travaux de recherche aux experts des pays impliqués, à travers les diverses organisations nationales membres du sous-comité concerné. Par la suite, lorsque la norme contenant les éléments de nos travaux de recherche sera publiée, elle sera accessible aux organisations intéressées à mettre en place un modèle SA.

Voici une description sommaire des activités qui sont généralement entreprises pour mener à terme les sept stades[38] du processus d'édition d'un projet de l'organisation ISO (*Voir* appendice A – ANNEXE IX pour une description plus détaillée).

(00) Stade préliminaire – Demande aux organisations et aux délégués participant aux comités ISO d'étudier et de valider la demande de l'industrie ou d'un organisme.

Voici un sommaire des étapes réalisées durant ce stade :

1) L'organisation internationale de normalisation (ISO) reçoit une demande et, selon le sujet, la transfère à un sous-comité spécifique aux fins d'étude.
2) Le sous-comité crée un groupe de travail et initie une période d'étude. La demande est soumise à ce groupe de travail et ses membres retransmettent cette demande aux

---

[38] La section 6.1 de ce document constitue un résumé des sections 2.2 à 2.8 du document *ISO/IEC Directives – Part 1: Procedures for the technical work*, 5th Edition, 2004, p. 62.

industries et aux organisations des divers pays, en leur demandant de leur retourner des informations, des documents ou tout autre commentaire pertinent.

3) Présentation des travaux des différents chercheurs et industries.
4) Une personne est nommée par le groupe de travail pour consolider et classer les contributions reçues des divers pays. Par la suite, celle-ci rédigera la proposition du nouveau sujet de travail.
5) Vote national : si les contributions ne sont pas suffisantes, les pays membres du sous-comité ISO peuvent décider d'arrêter un projet à ce stade.

- Version du document à ce stade du projet : période d'étude.

(10) Stade de proposition – Nomination de l'éditeur qui gèrera l'évolution du document du projet. Rédaction des versions préliminaires du contenu de la norme et validations périodiques de son contenues par les membres nationaux de l'équipe de projet ISO. Les vérificateurs sont des praticiens ou des chercheurs universitaires sélectionnés et encadrés par chacune des nations participantes.

Voici un sommaire des étapes réalisées durant ce stade :

1) Les personnes intéressées par le sujet se regroupent en équipe de projet et révisent ensemble les contributions consolidées par le responsable.
2) Selon la quantité et la qualité des contributions reçues, l'équipe de projet décide si un nouveau projet de norme doit être ou non démarré.
3) Un spécialiste du domaine est nommé « éditeur » par l'équipe de travail, et ce, pour la durée du projet. À cette étape du projet, son rôle consiste à déterminer la portée du document, à en monter la structure, à y insérer les contributions reçues et à retourner le nouveau document à tous, aux fins de commentaires. Il doit ensuite produire la première version du document de projet de travail et l'envoyer à tous pour qu'ils lui transmettent leurs commentaires.

4) Vote national : si les contributions ne sont pas suffisantes ou que ce projet ne semble pas répondre aux attentes, les pays membres du sous-comité ISO peuvent décider d'arrêter le projet à ce stade.

- Version du document à ce stade du projet : copie préliminaire.

(20) Stade de préparation – Rédaction de la norme et validation périodique de son contenu par les vérificateurs experts, membres de l'équipe de projet. Les vérificateurs experts sont des experts de l'industrie et des chercheurs universitaires du domaine.

Voici un sommaire des étapes réalisées durant ce stade :

1) L'équipe de projet se réunit pour commenter le contenu du document et soumettre de l'information additionnelle pour le bonifier. Pendant ce stade, le document demeure sous la forme de projet de travail.
2) Après la réunion, l'éditeur rédige une nouvelle version du document de projet de travail. Il produit cette nouvelle version conformément aux décisions prises par l'équipe de projet, à la suite de la révision des commentaires et des contributions des participants.

3) Cette nouvelle version du document est ensuite envoyée à tous, afin que de nouveaux commentaires et de nouvelles contributions soient apportés. Pendant ce stade, le contenu, le vocabulaire et la forme peuvent être remis en question à tout moment.

- Vote national : si l'équipe de travail considère que le document est assez étoffé, une recommandation est faite aux représentants des pays en vue de le soumettre en version de comité de projet; sinon il demeure au stade de version de travail et accomplit un cycle d'amélioration de plus. Par contre, si le projet ne semble pas répondre aux attentes et n'offre pas de perspectives d'amélioration, les représentants des pays membres du sous-comité ISO peuvent décider d'arrêter ce projet à ce stade.
- Version du document à ce stade du projet : copie de travail.

- Date ciblée pour la fin de ce stade : 6 mois après le début des travaux (ISO/IEC, 2004b, p. 21).

(30) Stade de comité – Bonification de la norme et validations périodiques de son contenu par les membres délégués par les pays participants. Ce stade constitue l'étape principale du processus d'édition d'une norme ISO. C'est le moment où les commentaires techniques nationaux sont pris en considération dans un objectif de consensus. Plusieurs cycles de validation et d'amélioration successives peuvent être nécessaires.

Voici un sommaire des étapes réalisées durant ce stade :

1) Vote national : comme pour le stade précédent, ce stade de comité se termine lorsque tous les commentaires techniques ont été résolus et que le document est approuvé pour passer au stade suivant.
2) Version du document à ce stade du projet : copie du comité.
3) Date ciblée pour la fin de ce stade : 12 mois après le début des travaux.

(40) Stade d'enquête – Distribution du document à tous les pays membres du SC27 pour un dernier tour de validation avant d'être soumis à un vote d'approbation. À ce stade, le vote d'approbation peut être accompagné de commentaires de réserve.

Voici un sommaire des étapes réalisées durant ce stade :

1) Vote national : comme pour le stade précédent, ce stade d'enquête se termine lorsque tous les commentaires ont été résolus.
2) Version du document à ce stade du projet : copie finale du comité.

- Date ciblée pour la fin de ce stade : 24 mois après le début des travaux.

(50) Stade d'approbation – Distribution du document à tous les représentants du SC27 pour être soumis à un vote final d'approbation sans réserve. À ce stade l'approbation finale doit se faire sans réserve. Seules des corrections d'édition sont autorisées.

À ce stade l'approbation finale doit se faire sans réserve. Seules des corrections éditoriales sont autorisées.

1) Prise de décision : les règles d'approbation du document sont les mêmes que celles mentionnées au stade d'enquête.
2) Version du document à ce stade du projet : copie finale du standard international.

- Date ciblée pour la fin de ce stade : 33 mois après le début des travaux.

(60) Stade de publication – Publication et distribution de la norme par l'organisation ISO :

1) Les dernières corrections peuvent être apportées au document, puis la norme est disponible pour impression et distribution par l'organisation ISO à tous ceux qui en font la demande.
2) Ce stade se termine à la publication du document.
3) Version du document à ce stade du projet : standard international.

- Date ciblée pour la fin de ce stade : 36 mois après le début des travaux.

Durant tout ce processus, le rôle habituel de l'éditeur d'un projet de norme ISO en est un de secrétaire. Ses responsabilités se limitent usuellement à :

1) consolider les contributions reçues des divers participants;
2) diriger les rencontres internationales afin d'obtenir des consensus sur le traitement des commentaires reçus;
3) intégrer les décisions des participants aux commentaires dans la prochaine version du document; et

4) produire, puis remettre à la direction du SC27, la nouvelle version cohérente du document pour distribution.

ANNEXE X

RÉALISATION DU PROJET ISO 27034 APPLICATION SECURITY – PART 1 : OVERVIEW AND CONCEPTS

C'est au début de chacun des cycles Delphi/ISO de 6 mois que nous avons introduit les nouveaux éléments du modèle de la sécurité des applications ainsi que les éléments qui avaient été bonifiés à la suite des commentaires du cycle précédent. Pour la préparation d'un nouveau cycle, notre travail consistait à réaliser les activités de recherche suivantes :

1) Recherche exploratoire, appuyée par des questionnements et des prototypes de solutions;
2) Recherche de normes et de bonnes pratiques dans le domaine de la sécurité des applications;
3) Définition et bonification itérative du modèle SA;
4) Édition et rédaction de la norme ISO 27034 *Application Security*;
5) Proposition de solutions pratiques permettant la mise en place des éléments et des processus du modèle SA;
6) Participation ponctuelle à des événements et des conférences permettant une certaine vérification empirique (acceptabilité);
7) Vérification ponctuelle de l'utilisation d'éléments du modèle à l'intérieur de projets de solutions pratiques en industrie (acceptabilité et implémentabilité).

Durant les 65 mois qu'a duré ce projet, le modèle SA a été tour à tour bonifié par le chercheur puis validé par les experts délégués par les 46[39] pays et les 4 organisations[40] participants, durant plus de 11 cycles de conception et de validation. C'est durant la réalisation de ces cycles que le chercheur a reçu des représentants nationaux des pays

---

[39] Selon les rapports de résultats de votes inclus dans certaines versions du document de travail du projet *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.

[40] Les quatre organisations contactées pour participer à la vérification du modèle de la sécurité des applications sont : ISO/JTC1/SC7, ISO/JTC1/SC22, ITU-T/SG17 et NESSI.

participants, analysé puis traité plus de 1 140 commentaires et 17 contributions, lui permettant de bonifier le modèle SA.

Cette annexe offre une vue d'ensemble de l'évolution des principaux éléments du modèle SA qui ont eu lieu au cours de ce projet de recherche.

Les annexes X.1 à X.7 présentent les événements clés provenant du traitement des commentaires et des contributions reçus ainsi que les publications qui ont été réalisées durant l'avancement des travaux de cette recherche. Les événements sont amenés dans ces sections, soit parce qu'ils concernent une contribution du chercheur, soit parce qu'ils concernent une amélioration ou une réorientation du modèle SA, suite au traitement d'un commentaire ou par l'ajout d'une contribution provenant des représentants nationaux des pays participants. Ces sections mentionnent aussi les principaux documents qui ont été produits durant chacun des stades de ce projet.

X.1 Stade préliminaire (00)

Étude et validation d'une demande de l'industrie ou d'un organisme.
Présentation et validation des principaux concepts et de l'idée générale du modèle SA produits lors de la revue de littérature et des travaux d'analyse complémentaires.

Période : 6 mois, de novembre 2006 à mai 2007.

X.1.1 Avancement des travaux de recherche durant ce stade

Afin de mettre l'accent sur l'origine des éléments du modèle ainsi que ce qui a influencé leur développement, la description de l'avancement des travaux de chaque stade est présentée en trois points, soit : 1) Éléments clés proposés par le chercheur qui ont été intégrés au modèle SA durant ce stade, 2) Commentaires et contributions clés proposées par les pays participants et qui ont eu un impact sur l'orientation du modèle, et 3) Commentaires et

contributions clés proposées par les pays participants et qui ont eu un impact sur un des éléments du modèle.

Événements clés :

1) Première participation du chercheur à une rencontre internationale du SC27 : novembre 2006, à Johannesburg, en Afrique du Sud.
2) Présentation sommaire des principaux éléments du modèle SA par le chercheur lors de la conférence *Application Security – Integration of security concerns in the system life cycle* (Poulin, 2006b).
3) Nomination du chercheur au poste de responsable de la rédaction d'une nouvelle proposition de projet ISO.
4) Rédaction par le chercheur du document *Call for contributions to WG 4 Study Period on Application Security* (ISO/IEC, 2007a) contenant une première version de la couche « Fournir une application » du cycle de vie de la sécurité d'une application.
5) Des 35 pays participants au SC27, neuf d'entre eux ont approuvé le passage au stade suivant, aucun pays n'a voté contre le projet.

X.1.2 Éléments clés proposés par le chercheur qui ont été intégrés au modèle SA durant ce stade

Lors de cette rencontre de projet, le chercheur a sommairement présenté la vision, les concepts, la portée et les principaux éléments du modèle SA proposé par ce travail de recherche qui pourraient être insérés dans la version préliminaire du document du projet ISO *Application Security*, aux fins de validation (Poulin, 2006b). Ce modèle introduit le cycle de vie de la SA comme un ensemble de phases et d'activités couvrant une période qui commence à l'initiation du projet de l'application et qui se termine à la destruction des données qu'elle impliquait. Il s'articule autour du principe de ne pas créer un nouveau processus de sécurité, mais plutôt d'intégrer les activités de sécurité à l'intérieur des processus de la méthode de développement en vigueur dans l'organisation, puis d'étendre les activités de sécurité aux processus requis par l'environnement d'opération.

Le modèle SA, dont l'élaboration a été initiée lors de nos travaux propédeutiques[41], incluait notamment :

1) Les trois contextes de l'application : affaires, juridique et technologique (Poulin, 2006b, p. 5).
2) Le concept de « niveau de confiance » reliant les besoins de sécurité avec l'information à protéger et le contexte d'exécution d'une application (Poulin, 2006b, p. 5).
3) La proposition d'une vision globale de la sécurité de l'information et les quatre domaines d'interventions qui la composent (Poulin, 2006b, p. 6).
4) Une définition préliminaire d'application sécuritaire qui intègre le principe que la sécurité doit être démontrée (Poulin, 2006b, p. 7).
5) Les trois éléments essentiels à considérer afin de protéger l'information impliquée par l'utilisation d'une application, et comment ces éléments influencent un projet d'application sécuritaire, soit : les personnes, les processus et la technologie (Poulin, 2006b, p. 8).
6) Le cadre normatif de l'organisation (Poulin, 2006b, p. 12).
7) Deux des quatre niveaux du cycle de vie d'un système TI, soient : le niveau concernant le développement et celui de la gestion des infrastructures nécessaires aux divers environnements de l'application (Poulin, 2006b, pp. 16-27).
8) Trois rôles d'acteurs (audience ciblé) impliqués dans la sécurité des applications (Poulin, 2006b, pp. 29-31).

Les commentaires et contributions proposés par les experts lors de l'étape de validation de ce stade sont présentés aux annexes XIX.3 à XIX.8 de cette thèse.

[41] Travaux postmaitrise et prédoctoraux.

X.1.3 Publication des éléments du modèle SA

Les principaux éléments et concepts du modèle amenés par la présentation du chercheur (Poulin, 2006b) ont été acceptés comme base de travail et distribués aux pays participants aux fins de commentaires (ISO/IEC, 2007c).

X.2 Stade de proposition (10)

Définition de la portée du projet et consolidation des contributions reçues.
Présentation et validation du modèle initial de la sécurité des applications.
Période : 6 mois, de mai à octobre 2007.

X.2.1 Avancement des travaux de recherche durant ce stade

Lors de la rencontre de projet qui a débuté ce stade, trois experts et le chercheur délégués respectivement par le Japon, Hong Kong, la Suisse et le Canada ont présenté des éléments concernant la sécurité des applications.

Événements clés :

1) Distribution par ISO du document aux fins de contributions et de commentaires : *Call for contributions to WG 4 Study Period on Application Security* (ISO/IEC, 2007a).
2) Traitement des neuf commentaires reçus (ISO/IEC, 2007f) ainsi que de la contribution du SG17 d'ITU-T (ITU-T, 2007b), lors de la rencontre du SC27 qui a eu lieu en Russie, en mai 2007.
3) Nomination du chercheur au poste de responsable de la rédaction de la proposition de projet et d'éditeur du projet ISO/IEC 27034 – *Application Security*. Cette responsabilité consistait notamment :
    a) à rédiger et proposer la portée du projet, soit « ... de spécifier un cycle de vie de sécurité de l'application, pouvant intégrer des activités de sécurité et de contrôle,

concernant des applications développées à l'interne, développées à l'externe, acquise, ou un mélange de ces approches. »[42] (ISO/IEC, 2007e, p. 2);

b) à proposer un diagramme préliminaire du cycle de vie de la SA (Poulin, 2007b, p. 22);

c) à rassembler dans une version préliminaire cohérente du document de travail (ISO/IEC, 2007c) tous les éléments du modèle SA. Distribuer cette version préliminaire, aux fins de validation et de commentaire, durant la phase de préparation (20), à tous les représentants des différents pays, afin qu'ils puissent la faire vérifier par leurs experts vérificateurs nationaux respectifs, puis consolider et faire parvenir leurs commentaires et leurs contributions au chercheur.

4) Présentation par le chercheur des principaux éléments du modèle SA (Poulin, 2007b) précisant l'orientation et la portée proposées pour élaborer le modèle SA.
5) Publication du document suivant : *New Work Item Proposal on Guidelines for application security (27034)* (ISO/IEC, 2007e).
6) Des 42 pays participants au SC27, 20 d'entre eux ont soutenu le passage du projet au stade suivant et trois pays ont voté contre, soit : l'Afrique du Sud, les États-Unis et le Royaume-Uni.

X.2.2 Éléments clés proposés par le chercheur qui ont été intégrés au modèle SA durant ce stade

Une présentation sommaire des principaux éléments du modèle SA (Poulin, 2007b) suggérant que les préoccupations de sécurité devraient être tenues en compte durant tout le cycle de vie d'une application et directement intégrées au document du projet soit les principes du modèle SA ainsi que les éléments et les concepts clés qui pourraient être contenus dans la nouvelle norme.

---

[42] Traduction libre de la portée décrite dans le document d'ISO.

C'est lors de cette rencontre de travail que le chercheur a proposé pour la première fois les éléments suivants :

1) Précision des concepts « d'environnement cible d'exécution » et de « degré de confiance », reliant les besoins de sécurité avec l'information à protéger et le contexte d'exécution d'une application (Poulin, 2007b, p. 5).
2) Identification des trois contextes (affaires, juridique et technologique) d'où proviennent les risques de sécurité d'une application, et comment ceux-ci influencent l'évaluation de la SA d'une organisation (Poulin, 2007b, p. 6).
3) Définition de la SA qui tient compte des besoins des acteurs œuvrant dans les quatre domaines de connaissances (Poulin, 2007b, p. 7).
4) Présentation d'une définition d'une application sécuritaire tenant en compte le niveau de confiance ciblé, les types d'information impliqués le contexte d'exécution ciblé, ainsi que l'importance de soutenir par des preuves toute affirmation confirmant l'atteinte et le maintien d'un niveau de confiance préalablement établi (Poulin, 2007b, p. 8).
5) Les besoins de l'audience ciblée par le modèle, soit : les gestionnaires, les développeurs (l'équipe d'exécution), les auditeurs et les utilisateurs, ainsi que leurs besoins respectifs concernant la SA (Poulin, 2007b, pp. 9-11).
6) La première version du cycle de vie de la SA (Poulin, 2007b, p. 22) ainsi que des exemples d'activités pouvant être intégrées dans chaque phase du cycle de vie de la SA (Poulin, 2007b, pp. 26-36).
7) L'élément appelé « point de contrôle de sécurité de l'application » qui contient l'activité de sécurité et l'activité de vérification, servant à s'assurer de la conformité de l'application aux exigences du cadre normatif de l'organisation telles qu'un règlement, une loi ou une pratique (Poulin, 2007b, pp. 23-25).
8) Une vision globale des éléments clés du modèle SA (*Voir* l'ANNEXE XVIII, Figure-A XVIII-1) présenté à partir du processus de vérification de la SA jusqu'à la liste des points de contrôles, en passant par les contextes de l'application, le cadre normatif de l'organisation, le cadre normatif de l'application, la liste des activités impliquées, les normes et pratiques recommandées, etc. (Poulin, 2007b, pp. 38-42).

Le chercheur a réalisé une présentation et dirigé une discussion afin d'obtenir un consensus sur la définition et la portée du terme « application » (Poulin, 2007a) visant à offrir une vision systémique d'une solution TI. Cependant, la définition proposée ne faisait pas l'unanimité, car elle présentait une portée différente de certaines autres définitions provenant de certains secteurs de l'industrie. En effet, selon le domaine de connaissances et le métier qu'ils exerçaient, les experts participants au groupe de travail avaient une définition différente du terme « application ». Étant essentiel en début de projet d'essayer d'obtenir un consensus sur cette définition, notamment afin de pouvoir partager une vision commune de la portée de la sécurité de l'application et d'orienter la suite des travaux, la majorité des discussions qui eurent lieu pendant cette séance de travail concernait ce qui devait être inclus et exclu d'un système TI appelé « application ». N'ayant pu obtenir un consensus clair, les éléments, les concepts et la portée du modèle présentés par le chercheur ont été acceptés, et un temps de réflexion a été proposé pour régler le différend concernant la définition de ce terme.

Le chercheur a déposé le document *Standards proposition to include in AS Purpose, v1.6* (Poulin et Rouselle, 2007) qui propose une liste de normes devant être considérées lors de la construction du modèle SA. Ce document avait préalablement été révisé par un expert vérificateur du Canada.

Avant de conclure cette rencontre de travail, le chercheur a présenté aux membres du groupe de travail 3 (sécurité en génie logiciel) et aux membres du groupe de travail 4 (sécurité technique), la portée et l'orientation qu'il allait donner au projet (Poulin, 2007c) afin d'obtenir l'approbation des experts présents et s'assurer de l'arrimage de ce projet avec tous les autres projets et les normes sous la responsabilité de ces deux groupes de travail. Il a aussi présenté les objectifs visés par certains éléments du modèle et qui ont été mis en place au Gouvernement du Québec (Poulin, 2007c) dont, notamment, l'utilité pour une organisation de définir et de mettre en place un cadre normatif pour la sécurité des applications.

Les commentaires et contributions proposés par les experts lors de l'étape de validation de ce stade sont présentés à la section XIX.4 de l'ANNEXE XIX de cette thèse.

X.2.3 Publication des éléments du modèle SA

Durant ce stade le chercheur a présenté une liste de documents à tenir en compte ainsi que les éléments du modèle SA qui ont été vérifiés par les experts des pays participants, puis qui seront intégrés dans la première version du document de projet « 27034 – Application Security ».

À titre d'éditeur, le chercheur a produit et déposé pour distribution, dès la fin de la rencontre, le document *New Work Item Proposal on Guidelines for application security (27034)* (ISO/IEC, 2007e). Par la suite, il a produit et envoyé au secrétariat du SC27 la version préliminaire du document de la norme *ISO/IEC 27034 Application Security – Part 1: Guidelines for application Security* (ISO/IEC, 2007c) pour distribution aux pays participants.

Tel que présenté à la Figure-A XVIII-1, la vision globale des éléments du modèle SA a été définie dès le début des travaux (ISO/IEC, 2007c, p. 38). Cette figure introduit et arrime (A) les éléments clés du modèle. Elle présente (B) le cadre normatif de l'organisation, qui contient notamment : (B.1) la liste des contrôles de sécurité des applications avec leur niveau de confiance, (B.2) les normes et pratiques recommandées, (B.3) les listes des activités et des rôles impliqués dans le cycle de vie de la sécurité d'une application, et (B.4) les contextes de l'organisation. La figure présente aussi (C) le cadre normatif de l'application, qui inclut notamment : (C.1) les contextes de l'application et (C.2) le processus d'évaluation de la sécurité, qui englobe également le niveau de confiance cible et le niveau de confiance actuel d'une application. Finalement, la figure introduit également une description sommaire de la structure d'un CSA, permettant d'en comprendre les principaux attributs. Cette description introduit sommairement le schéma XML, qui sera utilisé pour décrire le CSA dans un langage formel.

Ce modèle a évolué en fonction de deux facteurs principaux, soit :

1) en fonction des commentaires reçus des vérificateurs experts des différents pays impliqués dans le projet qui identifiaient des éléments d'amélioration, et ce, afin de mieux arrimer les termes et définitions de certains éléments du modèle avec des éléments ou un vocabulaire existant déjà utilisés dans un domaine particulier;
2) en fonction des travaux de recherche que nous avons réalisés lorsque nous découvrions qu'un élément, un concept ou une définition présentée par le modèle soulevait plus d'interrogations qu'il amenait de réponses.

C'est en fonction de ses deux facteurs combinés que le modèle SA a évolué et que de nouveaux éléments, dont notamment des processus, des acteurs, des termes et des définitions ont été créés ou bonifiés pour s'arrimer aux concepts et vocabulaires existants dans les domaines de la gouvernance, du génie logiciel, des infrastructures TI, de la vérification et du contrôle.

Voici la liste des éléments clés du modèle SA qui ont été intégrés et publiés dans cette version du document de travail :

1) Le processus de gestion de la SA (ISO/IEC, 2007c, p. 7) qui devrait être utilisé pour supporter un SGSI, tel que défini par la norme ISO 27001.
2) Le processus de gestion du cadre normatif de l'organisation (ISO/IEC, 2007c, p. 18).
3) Le cadre normatif de l'organisation (ISO/IEC, 2007c, p. 16) et celui de l'application (ISO/IEC, 2007c, p. 23).
4) Le cycle de vie de la SA (ISO/IEC, 2007c, p. 25).
5) Les principes de SA (ISO/IEC, 2007c, p. 9).
6) Les contextes d'affaires, juridiques et technologiques d'une application (ISO/IEC, 2007c, p. 12).
7) Les niveaux de confiance ciblés et actuels d'une application (ISO/IEC, 2007c, p. 13).
8) Le répertoire des mesures de sécurité des applications[43] (ISO/IEC, 2007c, p. 19).

[43] Élément qui s'appelle maintenant La bibliothèque de CSA.

9) Le processus de gestion du risque de SA (ISO/IEC, 2007c, p. 22).
10) Une version préliminaire du cycle de vie de la SA comprenant les quatre niveaux : la gouvernance, le développement logiciel, la gestion de l'infrastructure et les acteurs (ISO/IEC, 2007c, p. 25).
11) Le processus d'évaluation et les principaux éléments à considérer lors de la vérification de la SA (ISO/IEC, 2007c, pp. 32-33).
12) Une description sommaire de la mesure de sécurité d'une application, soit son en-tête, son activité de sécurité et son activité de vérification (ISO/IEC, 2007c, p. 36).
13) Les principaux éléments du modèle SA ainsi que leurs relations (ISO/IEC, 2007c, p. 38).

X.3 Stade de préparation (20)

Rédaction de la norme et validations périodiques de son contenu par les membres de l'équipe de projet durant quatre cycles.

Période : 25 mois, d'octobre 2007 à novembre 2009 – 4 cycles Delphi.

X.3.1 Avancement des travaux de recherche durant ce stade

À cette étape, quatre rencontres de projet ont eu lieu, commençant ainsi chacun des cycles de ce stade. Le chercheur y a présenté les divers éléments du modèle SA qui ont par la suite été vérifiés et introduits dans différentes versions du document de projet.

N'ayant reçu aucune contribution pouvant influer sur la structure du document, le travail d'éditeur s'est ainsi transformé en travail d'auteur et de rédacteur, car l'ensemble des résultats de nos travaux de recherche devenait la principale source de contribution à l'avancement du projet. Dès lors, notre responsabilité a consisté à définir les principes, les concepts et les divers éléments du modèle nécessaires à la sécurité des applications qui devront être intégrés dans la norme. Pour ce faire, nous avons effectué un travail de recherche appliquée, nous permettant de faire évoluer les concepts et les modèles présentés. Nous avons rédigé, présenté et fait approuver le document de travail préliminaire ainsi que

les diverses versions des documents de travail de la norme sur la sécurité des applications (vision systémique) jusqu'à sa version de comité.

C'est durant ce stade que nous avons présenté la portée du terme *application* selon une vision systémique. Cette portée a été amplement discutée, car le groupe de travail réunissait dans une même pièce des personnes provenant des quatre secteurs d'interventions de la sécurité de l'information. Nous avons présenté les définitions du terme *application*, selon chacun des domaines de connaissance, et le groupe de travail a statué pour conserver la portée systémique du concept amené par le document, mais en le nommant *application d'affaires*[44].

Événements clés :

1) Nomination du chercheur au poste d'éditeur et de chef de projet de la norme ISO 27034. C'est à ce titre qu'il a :
   a) Réalisé une présentation sommaire du modèle SA et des éléments qui le composent (Poulin et Guay, 2008), (Poulin, 2009e);
   b) Présenté les éléments du modèle SA aux vérificateurs experts des pays participants en publiant quatre versions du document de travail de la norme *ISO/IEC 27034 Application Security – Part 1: Guidelines for application Security* (ISO/IEC, 2007c), (ISO/IEC, 2008b), (ISO/IEC, 2008a) et (ISO/IEC, 2009a), et ce, afin de recevoir leurs commentaires et ainsi réaliser quatre cycles de validation des résultats de cette recherche;
   c) Présenté lors de différentes réunions de travail, tenues à tour de rôle avec les représentants des États-Unis, de l'Angleterre et de la Suisse, les diagrammes exposants les divers éléments, principes et concepts (Poulin, 2007d) qu'il désirait intégrer au document de travail, pour expliquer le modèle;

---

[44] Le terme *business application* a été utilisé dans les versions WD1 et WD2, puis a été changé pour revenir au terme *application* à partir de la version WD3 de la norme.

d) Dirigé quatre rencontres et recommandé M. Bruno Guay comme coéditeur de projet pour l'assister à titre de vérificateur expert canadien et de réviseur linguistique (anglais) des divers documents produits.

2) Traitement des 770 commentaires émis par dix-huit pays participants et une organisation, lors des rencontres qui ont eu lieu en octobre 2007, à Lucerne, en Suisse (ISO/IEC, 2007b), en avril 2008, à Kyoto, au Japon (ISO/IEC, 2008c), en octobre 2008, à Limassol, à Chypres (ISO/IEC, 2008d), et en mai 2009, à Beijing, en Chine (ISO/IEC, 2009i).
3) Des 42 pays participants au SC27, 18 d'entre eux ont soutenu le passage du projet au stade suivant et trois pays ont voté contre, soit : l'Afrique du Sud, l'Australie et le Japon.

X.3.2 Éléments clés qui ont évolué ou qui ont été intégrés au modèle SA par le chercheur durant ce stade

Événements clés :

1) Présentation et évolution de la structure du projet 27034 (ISO/IEC, 2009a, pp. 6-7), qui se conclut comme suit :
   - Partie 1 – Vue d'ensemble et concepts, qui présente l'ensemble du modèle SA et ses principaux éléments.
   - Partie 2 – Cadre normatif de l'organisation, qui présente les composants et les processus qui sont nécessaires à la mise en place et à la gestion du CNO.
   - Partie 3 – Processus de gestion de la sécurité d'une application, qui présente les composants et les processus concernant un projet d'application, qui sont nécessaires à la gestion de la sécurité d'une application.
   - Partie 4 – Vérification et certification de la sécurité des applications, qui présente les composants et les processus d'audits et de certification qui sont nécessaires à la gestion de la sécurité des applications.
   - Partie 5 – Protocoles et structure de données des CSA, qui présente les protocoles et les schémas XML qui serviront à valider la structure des CSA et du MRCVSA afin d'aider les organisations à communiquer, vérifier, mettre à jour et utiliser leurs CSA.

2) Vision globale des éléments clés du modèle SA
   a) Figure présentant la vision globale du modèle (*Voir* l'ANNEXE XVIII, Figure-A XVIII-1) qui avait été placé en annexe du document de travail (ISO/IEC, 2007c, p. 38), fut retiré parce que trop complexe;
   b) Description des quatre domaines d'interventions impliqués dans la protection des informations sensibles en sécurité de l'information, ainsi que dans la protection des informations sensibles, et qui sont aussi impliquées dans l'utilisation d'une application (Poulin et Guay, 2008, p. 3);

3) Principes clés sous-jacents au modèle
   a) Présentation de trois des principes clés de la sécurité des applications, des processus et des éléments clés, tels que le CNO, le CNA, le cycle de vie d'une application générique, les trois contextes, la bibliothèque des contrôles, les contrôles de sécurité, qui ont été introduits avec la publication de la version préliminaire du document (ISO/IEC, 2007c, p. 9);
   b) Ajout (ISO/IEC, 2007c, p. 9) et retrait (ISO/IEC, 2008b, p. iv) des attributs de sécurité de l'information de la liste des principes de la sécurité des applications, soit ceux qui concernaient la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation d'une application;
   c) Bonification des principes de la sécurité des applications (Poulin, 2009e, p. 10);
   d) Fusion et amélioration des énoncés et des descriptions des principes de la sécurité des applications (ISO/IEC, 2009a, p. xii).

4) Portée de la sécurité d'une application
   a) Explications concernant la portée de la sécurité des applications, soit l'identification des sept différents types (groupes) d'information dont la protection doit être assurée lors de l'utilisation d'une application (ISO/IEC, 2009a, p. 9);
   b) Définition de la portée des informations impliquées par la sécurité des applications (ISO/IEC, 2009i, p. 14).

5) Objectifs et bénéfices visés par le modèle
   a) Présentation des objectifs clés visés par l'utilisation d'un modèle de référence du cycle de vie d'une application dans le modèle SA (Poulin, 2009e, p. 18);
   b) Énumération des bénéfices amenés par le modèle SA, tant pour l'organisation au sens large que pour les intervenants, tels que : les gestionnaires, les équipes de réalisation, les auditeurs et les utilisateurs (Poulin, 2009e, p. 35).

6) Définition d'une application
   a) Représentation des différents types d'applications : autonome, client-serveur, N-tier et Web (Poulin et Guay, 2008, pp. 4-7);
   b) Présentation de la portée de la SA (personnes, processus et technologie) et de la définition du terme application comme étant une « application d'affaires » (Poulin et Guay, 2008, p. 2);
   c) Affinement de la définition d'une application sécuritaire (Poulin et Guay, 2008, p. 10);
   d) Amélioration de la définition d'une application sécuritaire (Poulin, 2009e, p. 15).

7) Composant : cycle de vie de la sécurité d'une application
   a) Description d'un cycle de vie générique de la SA comportant quatre couches afférentes aux domaines de connaissances, de leurs processus et de leurs acteurs (Poulin et Guay, 2008, p. 11);
   b) Présentation de l'alignement du cycle de vie générique de la SA aux normes ISO 12207 et ISO 15288 (Poulin et Guay, 2008, p. 12);
   c) Changements de nom de divers éléments du modèle, dont celui de l'objet « Cycle de vie générique de la sécurité d'une application » pour « Modèle de référence du cycle de vie de la sécurité d'une application » (Poulin, 2009e, p. 17), (ISO/IEC, 2008a, p. 31);
   d) Précisions sur l'arrimage entre le modèle présenté et les normes ISO 12207 et ISO 15288 (Poulin et Guay, 2008, p. 12) basé sur les travaux du chercheur (Poulin, 2008b), (Poulin, 2008a).

8) Composant : types d'acteurs, rôles et responsabilités
   a) Présentation des types d'acteurs et de l'importance d'identifier leurs rôles, responsabilités et qualifications (Poulin et Guay, 2008, p. 13).

9) Composant : contrôle de sécurité d'une application (CSA)
   a) Modification du nom « point de contrôle » pour « mesure de sécurité » d'une application (Poulin et Guay, 2008, p. 14);
   b) Changement de nom de l'élément « mesure de sécurité d'une application » pour « contrôle de sécurité d'une application » (ISO/IEC, 2008a, p. 28), (Poulin, 2009e, p. 17).

10) Composant : structure d'un contrôle de sécurité d'une application
   a) Affinement de la définition de la mesure de sécurité en y intégrant le niveau de confiance cible (pourquoi), les caractéristiques de l'application, les normes et les bonnes pratiques (pourquoi), l'activité de sécurité (qui, quand, quoi, coût), et l'activité de contrôle (qui, quand, quoi, coût) (Poulin et Guay, 2008, p. 14);
   b) Précisions sur les composants « mesures de sécurité des applications » qui introduisent l'existence de relations Parents – Enfants entres des CSA (ISO/IEC, 2008b, pp. 13-14), et de la figure démontrant qu'ils peuvent être liés en graphe (Poulin et Guay, 2008, p. 15), (ISO/IEC, 2009a, p. 24).

11) Composant : bibliothèque des contrôles de sécurité des applications
   a) Introduction de la bibliothèque des mesures de sécurité d'une organisation qui regroupe les mesures de sécurité par niveau de confiance, selon les contextes (affaires, juridique et technologique) et les caractéristiques, ainsi que les fonctionnalités d'une application (Poulin et Guay, 2008, p. 18).

12) Composant : cadre normatif de l'organisation (CNO)
   a) Introduction du cadre normatif de l'organisation (CNO) où doivent être conservés les éléments requis par le modèle SA : contexte technologique, contexte d'affaires,

contexte légal, caractéristiques des applications de l'organisation, rôle, responsabilités et qualifications requis, la bibliothèque des mesures de sécurité des applications de l'organisation, le processus de vérification de la sécurité des applications, le cycle de vie générique de la sécurité des applications, ainsi que les cadres normatifs des applications de l'organisation (Poulin et Guay, 2008, p. 19).

13) Processus : création, validation et vérification des CSA
    a) Identification des processus de création et de validation des mesures de sécurité des applications (Poulin et Guay, 2008, pp. 16-17);
    b) Présentation du processus de vérification de la SA qui tient compte des éléments du cadre normatif et des mesures de sécurité identifiées par le niveau de confiance cible d'une application, permettant de valider l'atteinte du niveau de confiance ciblé (Poulin et Guay, 2008, p. 20);
    c) Introduction des processus d'utilisation et de vérification des mesures de sécurité des applications dans un projet d'application (Poulin et Guay, 2008, pp. 22-25).

14) Processus : analyse de risques de la sécurité d'une application
    a) Introduction des principales étapes du processus d'analyse de risques de la SA menant à l'identification du niveau de confiance cible (Poulin et Guay, 2008, p. 21);
    b) Présentation du chercheur explicitant l'alignement du modèle avec la norme ISO 27005 concernant la gestion du risque de sécurité (Poulin, 2009a);
    c) Alignement du processus de gestion des risques de sécurité des applications à la norme ISO 27005 concernant la gestion des risques de sécurité de l'information (ISO/IEC, 2009a, p. 49).

15) Processus : gestion de la sécurité d'une application
    a) Simplification de la représentation du processus de gestion de la SA (Poulin et Guay, 2008, p. 27);
    b) Processus de gestion de la SA figé à la première version de travail de la norme (ISO/IEC, 2008b, p. 6);

c) Arrimage du modèle avec la norme ISO 12207 (Poulin, 2009b), ajustement de la Figure-A XIV-5 afin de clarifier les processus de gestion de la SA proposés par le modèle (Poulin, 2009d), une présentation de l'évolution du modèle (Poulin, 2009e);
d) Amélioration du processus de la gestion de la SA (Poulin, 2009e, p. 16).

16) Processus : gestion de la sécurité des applications d'une organisation
   a) Introduction du processus de gestion de la sécurité des applications d'une organisation (Poulin, 2009e, p. 16);
   b) Présentation des distinctions entre les processus organisationnels (Processus organisationnels de gestion de la sécurité des applications) et ceux concernant la SA spécifique (ISO/IEC, 2009a, p. 14);
   c) Introduction du processus de maintenance du cadre normatif de l'organisation (CNO) qui présente le comité du CNO comme étant le responsable de la gestion et de la mise à jour du contenu des éléments du CNO ainsi que des CSA, en fonction de l'évolution des contextes d'affaires, juridiques et technologiques de l'organisation (Poulin, 2009e, p. 24);
   d) Alignement du processus organisationnel de gestion de la sécurité des applications à la roue de Deming (Deming, 2000), soit au modèle « Prévoir, Faire, Vérifier, Réagir »[45], afin de pouvoir s'aligner au SGSI proposé par la norme ISO 27001 (ISO/IEC, 2009a, p. 34).

17) Processus : vérification de la sécurité d'une application
   a) Amélioration du schéma décrivant le processus de vérification de la SA (Poulin, 2009e, p. 32).

Les commentaires et contributions des experts lors de l'étape de validation de ce stade sont présentés à la section XIX.5 de l'ANNEXE XIX de cette thèse.

---

[45] Plan, Do, Check, Act.

X.3.3 Publication des éléments du modèle SA

Suite à chacun des cycles de validation, le chercheur a produit, et envoyé au SC27 pour publication, une version du modèle de sécurité des applications intégrée au document de travail de la norme *ISO/IEC 27034 Application Security – Part 1: Guidelines for application Security* (ISO/IEC, 2007c), (ISO/IEC, 2008b), (ISO/IEC, 2008b), (ISO/IEC, 2008a), (ISO/IEC, 2009a) comprenant les éléments du modèle qui ont été accepté.

X.4 Stade de comité (30)

Bonification de la norme et validation périodique de son contenu par les membres d'un comité élargi de vérificateurs experts délégués par les pays participants.

Période : 11 mois, de novembre 2009 à octobre 2010.

X.4.1 Avancement des travaux de recherche durant ce stade

Événements clés :

1) Les pays membres du SC27 ont approuvé le passage du projet au stade de comité. Durant ce stade la validation du modèle est transmise à une plus large audience de vérificateurs experts de chacun des pays participants;
2) Le chercheur a produit deux versions du document de travail présentant les ajustements aux éléments du modèle SA (ISO/IEC, 2009b), (ISO/IEC, 2010b);
3) Le traitement des commentaires provenant des différents pays a été produit en novembre 2009, à Redmond, aux États-Unis (ISO/IEC, 2009h) et en avril 2010, à Melaka, en Malaisie (ISO/IEC, 2010e);
4) Un commentaire, provenant des experts de l'Afrique du Sud, a amené des discussions et le changement du terme « processus » dans le modèle de référence du cycle de vie de la sécurité des applications, pour un « ensemble d'activités » afin d'éviter tout conflit de vocabulaire avec le terme « processus » utilisé dans les normes du SC7, dont notamment les normes ISO 12207 et ISO 15288 (ISO/IEC, 2009h, p. 29);

5) Cycle de la préparation et de la validation de la première version comité du modèle :
   a) version comité #1 distribuée pour commentaires (ISO/IEC, 2009b);
   b) éléments importants amenés par le traitement des commentaires (ISO/IEC, 2009h) et approuvés par les pays participants;
   c) contribution du Japon détaillant la figure du processus de gestion de la SA (Takebe, 2009);
   d) contribution des États-Unis concernant une étude de cas de l'application d'un cycle de vie de développement sécuritaire sur le cadre normatif de l'organisation (CNO) (Ladd, 2009);
   e) contribution du Japon présentant un exemple de conversion d'un contrôle de sécurité provenant de la norme NIST 800-53 vers le patron de CSA (ISO/IEC, 2009b, p. 62);
   f) contribution du SC7 concernant le Software Engineering Body of Knowledge (SWEBOK) (SC7, 2003);
   g) contribution du chercheur concernant le nom et le concept du niveau de confiance d'une application à l'intérieur du modèle (Poulin, 2010a);
   h) rapport produit à la fin de la rencontre (SC27/WG4, 2009b);
   i) retrait de l'utilisateur, de l'audience ciblée par le modèle (ISO/IEC, 2009b, p. xi);
   j) contribution du chercheur présentant une description des relations entre le modèle et les normes ISO de la famille 27000 (ISO/IEC, 2009b, p. 12).
6) Cycle de la préparation et de la validation de la deuxième version comité du modèle
   a) deuxième version comité distribuée pour commentaires (ISO/IEC, 2010b);
   b) éléments importants amenés par le traitement des commentaires (ISO/IEC, 2010e) approuvés par les pays participants;
   c) rapport produit à la fin de la rencontre (SC27/WG4, 2010b);
   d) ajout du rôle « personnel d'acquisition » dans l'audience ciblée par le modèle (ISO/IEC, 2010b, p. 3).
7) Des 42 pays participants au SC27, 14 d'entre eux ont soutenu le passage du projet au stade suivant et cinq pays ont voté contre, soit : l'Afrique du sud, l'Australie, la France, l'Inde et le Japon.

X.4.2 Éléments clés qui ont évolué ou qui ont été intégrés au modèle SA par le chercheur durant ce stade

Événements clés :

1) Précision de la description de l'élément CNO du modèle, précisant que l'organisation possède déjà un CNO ainsi que des processus, et que le modèle SA vient simplement s'y intégrer sans tout changer (ISO/IEC, 2009b, p. 13);
2) Définition et description des sous-processus de gestion du CNO pour chacune des étapes de la roue de Deming (ISO/IEC, 2010b, p. 36).

Les commentaires et contributions des experts lors de l'étape de validation de ce stade sont présentés à la section XIX.6 de l'ANNEXE XIX de cette thèse.

X.4.3 Publication des éléments du modèle SA

Au début de chacun des deux cycles de validation, le chercheur a produit, et transmis pour publication au SC27, une version du modèle de sécurité des applications intégrée au document de travail de la norme *ISO/IEC 27034 Application security – Part 1: Overview and concepts*, (ISO/IEC, 2009b) et (ISO/IEC, 2010b) comprenant les éléments du modèle qui ont été acceptés.

X.5 Stade d'enquête (40)

Dernières validations avant que le document de travail de la norme soit soumis au vote d'approbation des pays membres du SC27.

Période : octobre 2011 à novembre 2011.

X.5.1 Avancement des travaux de recherche durant ce stade

Événements clés :

1) Distribution par ISO de la version comité finale du document (ISO/IEC, 2010a), puis de la version comité finale révisée (ISO/IEC, 2011b) aux fins de contributions et de commentaires;
2) Traitement des 116 commentaires émis par les représentants nationaux de neuf pays participants réunis en octobre 2010, à Berlin, en Allemagne (ISO/IEC, 2011e) et en avril 2011, à Singapour (ISO/IEC, 2011f);
3) Dépôt final et intégration de l'annexe A fourni par les experts des États-Unis (ISO/IEC, 2010a, p. 48);
4) Des 44 pays participants au SC27, 14 d'entre eux ont soutenu le passage du projet au stade suivant et sept pays ont voté contre, soit : l'Afrique du sud, l'Allemagne, la Côte d'Ivoire, l'Espagne, les États-Unis, la France et le Japon.

X.5.2 Éléments clés qui ont évolué ou qui ont été intégrés au modèle SA par le chercheur durant ce stade

À la suite d'un commentaire émis par le chercheur (ISO/IEC, 2011e, p. 7), réintroduction du rôle « utilisateur » parmi les rôles présentés dans la section « audience ciblée » afin de s'assurer que, même si ce document ne s'adresse pas spécifiquement à eux, les besoins des utilisateurs seront explicitement identifiés par le modèle (ISO/IEC, 2011b, p. xii).

Les commentaires et contributions des experts lors de l'étape de validation de ce stade sont présentés à la section XIX.7 de l'ANNEXE XIX de cette thèse.

X.5.3 Publication des éléments du modèle SA

Au début de chacun des deux cycles de validation, le chercheur a produit en envoyé, pour publication au SC27, une version du modèle de sécurité des applications intégrée au document de travail de la norme *ISO/IEC 27034 Application security – Part 1: Overview and*

concepts, (ISO/IEC, 2010a) et (ISO/IEC, 2011b) comprenant les éléments du modèle qui ont été acceptés.

X.6 Stade d'approbation (50)

Distribution du document à tous les pays du SC27 pour être soumis à un vote d'approbation final sans réserve.

X.6.1 Avancement des travaux de recherche durant ce stade

Événements clés :

1) Publication par le SC27 de la version « comité révisée finale » du document, distribuée aux 46 pays participants, pour validation et approbation finale (ISO/IEC, 2011c);
2) Traitement par le JTC1 des trois commentaires émis par les représentants nationaux du Danemark et du Japon (ISO/IEC, 2011a);
3) Des 46 pays participants au SC27, 35 d'entre eux ont supporté le passage du projet au stade suivant, soit la publication de la norme, et un seul pays a voté contre, soit le Japon.

X.6.2 Éléments clés qui ont évolué ou qui ont été intégrés au modèle SA par le chercheur durant ce stade

Aucun élément supplémentaire n'a été proposé par le chercheur durant ce cycle de validation.

Les commentaires et contributions des experts lors du l'étape de validation de ce stade sont présentés à la section XIX.8 de l'ANNEXE XIX de cette thèse.

X.6.3 Publication des éléments du modèle SA

Suite à ce cycle de validation, le chercheur a produit, et transmis pour publication au SC27, une version du modèle de sécurité des applications intégrée au document de travail de la

norme *ISO/IEC 27034 Application security – Part 1: Overview and concepts* (ISO/IEC, 2011c) comprenant les éléments du modèle qui ont été acceptés.

X.7 Stade de publication (60)

Publication et distribution de la norme par l'organisation ISO.

5) La version finale du document de la norme ISO/IEC 27034 – *Application Security – Part 1 : Overview and concepts* (ISO/IEC, 2011d) a été publié, mis en ligne sur le site Web d'ISO et distribué aux pays participants en début décembre 2011.

ANNEXE XI

LE MODÈLE SA : ENJEUX, BESOINS, PORTÉE ET PRINCIPES SUPPORTÉS

Cette annexe présente les enjeux, le besoins, la portée et les principes clés supportés par le modèle SA.

XI.1 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. Il s'agit de :

5) Priorisation des éléments du modèle à mettre en place;
6) Formalisation du CNO;
7) Engagement d'investissement des ressources appropriées; et
8) Participation des intervenants liés aux quatre domaines d'intervention couverts par le modèle SA.

XI.1.1 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, car selon le contexte d'affaires, le contexte juridique et le contexte technologique dans lesquels ce modèle sera mis en place, l'absence de certains de ces éléments peut rendre le modèle inefficace, soit

inapte à fournir les preuves vérifiables attendues, démontrant que des contrôles de sécurité requis ont été identifiés, validés, mis en place et qu'ils fonctionnent tel que prévu, en fonction du niveau de confiance ciblé par l'organisation pour son application.

De ce fait, la sélection des éléments du modèle à mettre en place sera effectuée en regard des besoins et priorités de sécurité de l'organisation.

XI.1.2 Formalisation du cadre normatif de l'organisation

Le modèle exige de l'organisation la conservation des éléments du modèle à l'intérieur d'un cadre normatif de l'organisation (CNO), 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.

Le CNO est le dépôt officiel de l'organisation qui sera utilisé comme source autoritaire de tous les éléments du modèle qui aura été mis en place par l'organisation.

Sans la mise en place d'un CNO formel, il sera notamment impossible pour l'organisation :

1) De normaliser les éléments de sécurité des applications afin d'assurer une mise en œuvre et une vérification normalisée des CSA;

2) D'améliorer sa maturité dans le secteur de la sécurité des applications par la formalisation et la révision de tous les éléments de sécurité des applications pour les mettre à jour quant à l'environnement de l'organisation;

3) De réduire au minimum le coût de la sécurité pour les projets d'applications en favorisant la réutilisation des éléments de sécurité des applications existants qui ont déjà été approuvés.

XI.1.3 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. Quels que soient ses choix, et ce, afin de réellement pouvoir rencontrer ses objectifs de sécurité, l'organisation doit savoir évaluer puis, à la lumière de ses capacités et priorités, décider d'investir les ressources appropriées dans la conception, la réalisation, l'utilisation et la maintenance des éléments sélectionnés. Il vaut mieux se fixer des objectifs modestes et obtenir les résultats attendus, que de se donner des objectifs de sécurité trop ambitieux et de ne pouvoir les atteindre. Le modèle permet une implémentation « pas à pas » qui permettra à l'organisation qui le décide, de se fixer des étapes selon ses limites et ses priorités d'affaires.

Selon le principe du modèle : « la sécurité des applications doit pouvoir être démontrée », il vaut mieux avoir un peu de sécurité vérifiable, qu'une grande illusion de sécurité invérifiable. Sans de solides fondations amenées par la rigueur de la vérification de chacune des étapes réalisées dans la mise en place du modèle, l'ouvrage entier peut devenir futile et inutilisable si l'un des quatre principes n'est pas respecté.

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. Dans tous ces cas, l'organisation devra être en mesure d'évaluer et d'investir les ressources nécessaires à l'identification des changements de risques de sécurité et à l'analyse des conséquences de ces changements sur l'efficacité des éléments du modèle.

XI.1.4 Participation des intervenants liés aux quatre domaines d'interventions couverts par le modèle SA

Les personnes qui interviennent dans les différents secteurs des quatre domaines de connaissances en sécurité de l'information (*Voir* Figure-A XII-1), interviennent aussi en sécurité des applications. 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.

En s'ajustant à cette nouvelle portée, la description de l'objectif de chacun de ces domaines d'interventions devient :

1) **Le domaine de la gestion de la sécurité des applications** qui vise à remédier aux problèmes relatifs à la protection de l'infrastructure technologique et physique de l'organisation nécessaire aux opérations des applications jugées sensibles par l'organisation;

2) **Le domaine de la sécurité des infrastructures technologiques** qui vise à remédier aux problèmes relatifs à la protection de l'infrastructure technologique et physique de l'organisation nécessaire aux opérations des applications jugées sensibles par l'organisation;

3) **Le domaine de la sécurité des applications et des systèmes d'information** qui vise à remédier aux problèmes relatifs à la SA pendant tout son cycle de vie;

4) **Le domaine de la vérification et du contrôle de la sécurité des applications** qui vise à fournir les preuves que les activités et les contrôles de sécurité, à appliquer dans les quatre domaines, ont été mis en place et fonctionnent tel que prévu, et ce, en y incluant les activités d'audits qui valident que les activités de vérification des CSA et autres éléments du modèle aient bien été réalisées.

XI.2 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;
2) les équipes d'approvisionnement et d'opération;

3) les vérificateurs et les auditeurs;
4) les acheteurs;
5) les fournisseurs; et
6) les utilisateurs.

XI.2.1 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 tout autres activités pouvant survenir au cours du cycle de vie d'une application (Figure-A XIII-6, couche : gestion de l'application).

Voici quelques exemples de gestionnaires :

1) les responsables de la sécurité des informations;
2) les gestionnaires de projet;
3) les administrateurs;
4) les acquéreurs de logiciels;
5) les gestionnaires de développement logiciel;
6) les propriétaires d'applications;
7) les gestionnaires supervisant des employés.

Les besoins de ces personnes sont notamment :

5) 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;
6) d'examiner les rapports du vérificateur recommandant l'acceptation ou le rejet de la sécurité d'une application, et basés sur le fait qu'elle a atteint et maintenu le niveau de confiance ciblé;
7) d'assurer la conformité avec les normes, les lois et les règlements en fonction du contexte juridique d'une application (Figure-A XII-3);
8) de superviser la mise en œuvre d'une application sécurisée;

9) d’autoriser le niveau de confiance ciblé en fonction des contextes spécifiques de l’organisation;
10) de déterminer quelles activités de sécurité et de vérification correspondantes doivent être mises en œuvre et testées;
11) de minimiser les coûts de vérification de la sécurité de l’application;
12) de documenter les politiques et les procédures de sécurité définies pour une application;
13) de fournir des sessions de sensibilisation, de formation ou de surveillance de sécurité à tous les acteurs;
14) de mettre en place des niveaux d’autorisations requis à l’aide de politiques et de procédures de sécurité de l'information;
15) d’être informés de tous les plans de sécurité concernant les systèmes dans toute l'organisation.

XI.2.2 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 (Figure-A XIII-6, couches : fournir une application, et gestion de l’infrastructure).

Voici des exemples de membres d’équipes d’approvisionnement et d’opération :

1) les responsables des architectures (applications, système, infrastructure, etc.),
2) les analystes;
3) les programmeurs;
4) les testeurs;
5) les administrateurs de système;
6) les administrateurs de base de données;
7) les administrateurs de réseau; et
8) les techniciens.

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 comprendre quels contrôles doivent être mis en œuvre dans l'application elle-même;
3) de réduire au minimum l'impact de l'introduction de contrôles dans les activités de développement, de test et de documentation dans le cycle de vie de l'application;
4) de veiller à ce que les contrôles introduits répondent aux exigences de sécurité qui leur sont associées;
5) d'obtenir l'accès à des outils et à de meilleures pratiques dans le but de rationaliser le développement, les essais et la documentation;
6) de faciliter l'examen par les pairs;
7) de participer à la planification et à la stratégie d'acquisition;
8) d'établir des relations d'affaires pour obtenir des biens et services nécessaires (par exemple : pour la sollicitation, l'évaluation et l'octroi de contrats); et
9) d'organiser l'élimination des éléments résiduels après le travail est terminé (par exemple : la gestion ou l'élimination des données utilisées pour des tests).

XI.2.3 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 (Figure-A XIII-6, couche : audit de l'application).

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) de s'assurer que les résultats de l'audit sont reproductibles;
3) 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; et

4) d’appliquer des procédés de vérification standardisés basés sur l'utilisation de preuves vérifiables.

XI.2.4 Besoins des acheteurs

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

Les besoins de ces personnes sont notamment :

1) de préparer des demandes de propositions qui incluent les exigences de sécurité;
2) de sélectionner les fournisseurs qui répondent à ces exigences;
3) de vérifier les preuves des contrôles de sécurité qui ont été mis en place par le fournisseur;
4) d’évaluer les applications en vérifiant les preuves que tous les contrôles de sécurité de l'application qui étaient requis pour répondre aux exigences de sécurité ont été implémentés.

XI.2.5 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 :

1) de répondre aux exigences de sécurité qui sont incluses dans les demandes de propositions;
2) de sélectionner et de mettre en place les contrôles de sécurité des applications requises pour répondre aux exigences en fonction de leurs coûts; et
3) de fournir les preuves que les contrôles de sécurité requis ont été correctement implémentés dans le produit ou le service proposé.

XI.2.6 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 (Figure-A XIII-6, couche : fournir une application, groupe d'activités : transitions et utilisation).

Les besoins de ces personnes sont notamment :

1) d'être confiant que l'utilisation et le déploiement de cette application sont sécuritaires;
2) d'être confiant qu'une application produit des résultats fiables, de manière cohérente et en temps opportun; et
3) d'être confiant que les contrôles et les procédures de vérification requis sont en place, et qu'ils fonctionnent correctement, tel que prévu.

XI.3 Portée du modèle SA

Le modèle SA vise à :

1) S'appliquer à tout type d'applications telles que les applications autonomes, les applications clients – serveurs, les applications N-tiers, les applications embarquées, les applications temps réel, les applications Web, les applications mobiles, les applications centrales, quel que soit l'infrastructure technologique utilisée : station de travail, téléphone, tablette, réseau local, réseau Web, hébergement infonuagique, etc.
2) S'appliquer aux logiciels ainsi qu'aux éléments qui peuvent avoir un impact sur la sécurité des informations impliquées par l'utilisation de ces applications, telles que les acteurs, les processus présents dans le cycle de vie de l'application et les technologies utilisées par celle-ci;
3) S'appliquer à toutes les tailles et à tous les types d'organisations exposées à des risques liés aux applications, par exemple, les entreprises commerciales, les organismes gouvernementaux et les organismes sans but lucratif.

Ce modèle SA ne fournira pas :

1) de ligne directrice en matière de sécurité physique et réseau;
2) des contrôles ou des activités de mesure de sécurité; ni
3) des spécifications de programmation sécuritaire.

XI.4 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.

XI.4.1 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. 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 afin de pouvoir définir les exigences de sécurité qui devront être respectées.

L'approche de la SA de ce travail de recherche est basée sur l'évaluation et la gestion du risque de sécurité, telle que proposée par la série de normes ISO 27000.

XI.4.2 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.

Le concept d'exigence est utilisé en génie logiciel pour définir formellement des besoins fonctionnels et non fonctionnels d'un système qui sont « exigés » par l'organisation qui en fait l'acquisition. Selon la norme ISO/IEC/IEEE 29148 *Requirements engineering*, les caractéristiques que devrait posséder une exigence sont qu'elle doit être nécessaire, abstraite, sans ambiguïté, cohérente, complète, concise, faisable, vérifiable et que l'on puisse en assurer la traçabilité (ISO/IEC, 2009g, p. 8).

Des exigences[46] 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.

XI.4.3 La sécurité d'une application est dépendante de son environnement

La SA doit être évaluée en fonction de l'évolution de son environnement. Tout au long de son cycle de vie, et à l'intérieur des différents environnements dans lesquels une application aura à évoluer, trois contextes seront toujours les sources de risques de sécurité.

L'environnement d'une application est notamment défini par trois contextes :

1) Le contexte d'affaires, défini à l'annexe XII.2.3, qui inclue les processus, les acteurs et les informations impliqués par l'utilisation de l'application;
2) Le contexte juridique, défini à l'annexe XII.2.4, qui inclue les lois et règlements en vigueur dans les régions où sera utilisée l'application;
3) Le contexte technologique, défini à l'annexe XII.2.5, qui inclue l'ensemble des technologies requises pour faire fonctionner l'application.

---

[46] 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)*

L'évaluation de la SA d'une application doit aussi prendre en compte les spécifications et les fonctionnalités de l'application, définies à l'annexe XII.2.6, qui évolue dans cet environnement.

Pour minimiser ces risques, des exigences de sécurité devront être fixées par l'organisation. Le type et la portée de ces exigences sont déterminés par la gravité des risques auxquels l'application est exposée et par le risque résiduel acceptable décidé par l'organisation, en fonction de l'environnement de l'application.

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. Qu'il s'agisse d'un changement dans la règlementation d'un pays, ou qu'il s'agisse de code malicieux implémenté par un des développeurs de l'équipe. Il pourrait aussi s'agir d'une erreur dans l'architecture de l'application due à une mauvaise documentation ou de l'utilisation d'un composant non sécuritaire due à un mauvais processus de sélection. Il peut aussi s'agir d'une mauvaise interprétation de la Loi, d'un environnement de production mal géré ou plus simplement, de l'abus de privilèges d'un des utilisateurs ou de personnes impliquées dans le développement, la maintenance et l'utilisation de l'application. Toutes ces circonstances peuvent survenir dans l'environnement de l'application et avoir un impact sur sa sécurité.

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 mitigés. Si l'infrastructure technologique de l'application est modifiée, de nouveaux risques de sécurité provenant de ces changements dans l'environnement technologique peuvent surgir. De la même manière, si l'organisation décide d'utiliser son application dans un autre territoire géographique comme un autre pays, ou qu'une Loi existante est modifiée, ces changements dans l'environnement juridique de l'application peuvent générer de

nouveaux risques de sécurité. Dès que l'un des trois contextes de l'environnement d'une application est modifié, de nouveaux risques de sécurité peuvent émerger, ce qui aura un impact sur l'évaluation de la SA qui devra être mise à jour.

XI.4.4 La sécurité d'une application 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*, qui énonce que la « sélection de l'option de traitement d'un risque la plus appropriée consiste à équilibrer les coûts et les efforts de mise en œuvre avec les avantages dérivés… »[47] (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.

Il est à noter que les coûts de la SA peuvent être considérés comme un investissement pour certaines organisations. En effet, ils permettent de réduire les coûts de contingence, de diminuer les conséquences juridiques d'une brèche de sécurité et de démontrer que le propriétaire de l'application a assumé ses responsabilités de protection de l'information impliquée par l'utilisation de cette application.

---

[47] Traduction libre de l'auteur.

XI.4.5 La sécurité d'une application doit pouvoir être démontrée

Une application ne peut être déclarée sécuritaire que si le propriétaire de l'application accepte que les preuves générées par les activités de vérification des contrôles de sécurité, identifiés par le niveau de confiance ciblé, démontrent que ce niveau a bien été atteint.

Sachant que tout comme la sécurité de l'information, la SA peut se résumer à la gestion du risque menaçant les informations qu'implique leur utilisation, et que le principe de gestion du risque présuppose la diminution de ce dernier à un niveau acceptable, il doit être possible de démontrer que ce niveau acceptable défini, par son propriétaire, a réellement été atteint pour l'environnement où il désire utiliser son application. 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). Une application devrait être considérée sécuritaire pour un contexte spécifique, à un moment précis, en fonction de preuves présentées à la suite d'un processus de vérification formel confirmant que le niveau de confiance ciblé par l'organisation a été atteint. Dès qu'un changement est apporté à l'application ou à son environnement, il n'est plus possible d'assumer que cette application maintient son niveau de confiance sans avoir recours à une nouvelle vérification. De ce fait, l'atteinte du niveau de confiance envers une application doit être appuyée par des preuves de sécurité connues et vérifiables. Une application ne peut pas être déclarée sécuritaire si les preuves de sécurité présentées à l'auditeur ne correspondent pas aux résultats attendus.

ANNEXE XII

LE MODÈLE SA : CONCEPTS, TERMES ET DÉFINITIONS

Cette annexe présente les principaux concepts utilisés dans cette thèse ainsi que les définitions des termes clés qui y figurent.

XII.1 Concepts, termes et définitions existants

XII.1.1 Domaines d'interventions en sécurité de l'information

Le secteur de la sécurité de l'information est occupé conjointement par quatre groupes d'intervention (Figure-A XII-1), qui comprennent : des personnes utilisant de l'information, des processus et de la technologie leur permettant d'intervenir dans la protection des informations sensibles (*Voir* XII.1.6) depuis leur domaine de connaissances respectif.

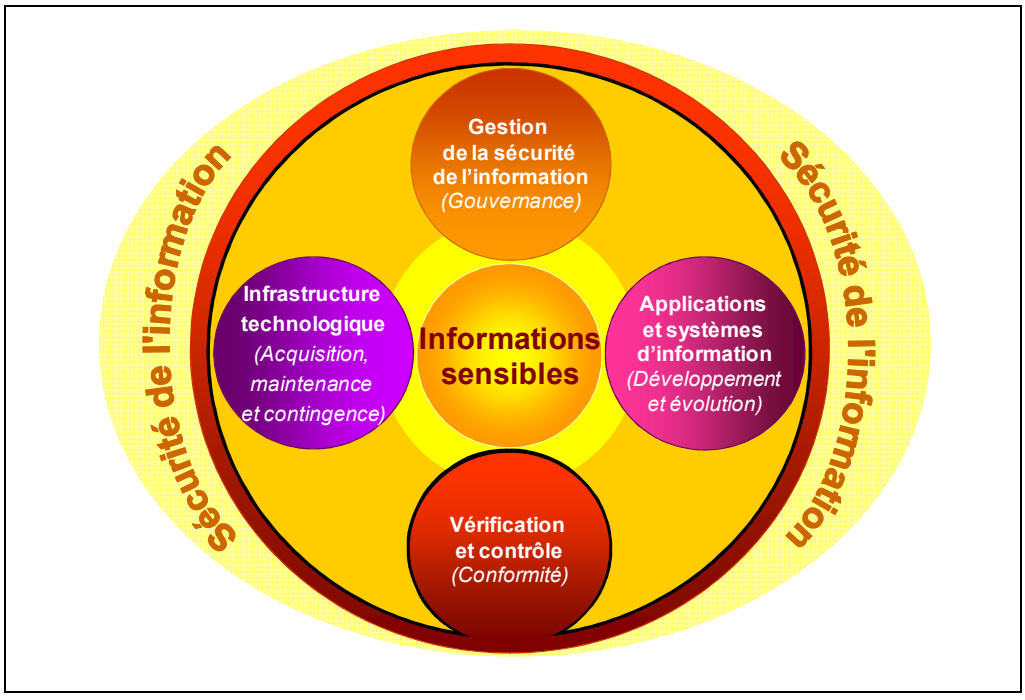


Figure-A XII-1 Les quatre domaines d'interventions couverts par le modèle en sécurité de l'information

Ces quatre domaines d'interventions sont :

1) **Le domaine de la gestion de la sécurité de l'information**, rattaché à la gouvernance de la sécurité de l'information. Ce domaine de connaissances vise non seulement la gestion de la sécurité de l'information à l'intérieur d'une organisation, mais aussi le développement d'une vision stratégique, l'atteinte des objectifs de sécurité ainsi que la gestion optimale, efficace et efficiente des risques et des ressources impliquées dans la protection des ressources informationnelles de l'organisation. Ce domaine est responsable de la coordination des activités liées à la sécurité de l'information en respect avec la vision, les objectifs et les ressources de l'organisation.

   Ce domaine comporte plusieurs secteurs d'interventions qui requièrent, de la part des intervenants, des compétences de gestion, et qui comprennent les processus visant à répondre aux problématiques relatives à la gestion de la sécurité de l'information dans l'organisation. Ils portent notamment sur la maturité des processus, les bonnes pratiques de gestion de la sécurité de l'information[48], les mesures de performance, les politiques, les rôles et les responsabilités, les directives, les objectifs stratégiques, les normes de sécurité, les cadres de gestion, la conformité aux lois, aux règlements et aux objectifs de sécurité, la continuité des affaires, etc.

2) **Le domaine de la sécurité des infrastructures technologiques** vise à remédier aux problèmes relatifs à la gestion de la protection de l'infrastructure technologique et physique d'une organisation. Il touche à l'ensemble des processus d'acquisition, de mise en place, de gestion, de maintenance et de contingence des divers éléments nécessaires au fonctionnement de ces infrastructures.

   Ce domaine comporte plusieurs secteurs d'interventions qui comprennent notamment la mise en place et l'utilisation de produits tels que les pare-feu, les systèmes de détection

[48] Information Security Management System, ISO/IEC 27000 Series.

d'intrusion, les mécanismes de gestion des incidents, les mécanismes de copies de sauvegarde, les antivirus, etc.

3) **Le domaine de la sécurité des applications et des systèmes d'information** vise à remédier aux problèmes relatifs à la SA pendant tout son cycle de vie, soit de la définition des besoins, sa réalisation, sa mise en place et sa gestion jusqu'à son archivage et à la destruction sécuritaire des informations sensibles qu'elle contient.

   Ce domaine touche à l'ensemble des processus de développement et de maintenance des applications et des systèmes d'information. Il comporte plusieurs secteurs d'interventions qui comprennent la réalisation et la maintenance de tous les types d'applications, notamment les systèmes de commerce électronique, les applications comptables, les systèmes de communication, les systèmes d'exploitation, les systèmes de gestion de base de données, etc.

4) **Le domaine de la vérification et du contrôle de la sécurité de l'information** est aussi connu sous le vocable « domaine de la conformité de la sécurité de l'information ». Ce domaine vise à fournir les preuves que les activités de sécurité et de vérification des contrôles de sécurité des quatre domaines ont été mises en place et fonctionnent, en y incluant les activités d'audit, qui valident la réalisation des activités de vérification.

XII.1.2 Domaines d'interventions en sécurité des applications

Étant donné que la sécurité de l'information concerne la protection de l'ensemble des informations utilisées par une organisation, et que la SA concerne la protection des informations impliquées par l'utilisation d'une application, on peut énoncer l'hypothèse que les acteurs provenant des quatre domaines d'interventions impliqués dans la sécurité de l'information (Figure-A XII-1), devraient aussi intervenir en sécurité des applications.

En tenant compte de leurs niveaux de connaissances et d'interventions complémentaires, les activités des acteurs des quatre domaines viseront le même objectif : la protection des informations sensibles impliquées par l'utilisation d'une application par l'organisation. Selon l'hypothèse énoncée, tout comme pour la sécurité de l'information, ces quatre domaines de connaissances devront être simultanément pris en compte dans la mise en place de contrôles et de mesures de sécurité sur l'application.

Les divers secteurs d'interventions compris dans ces domaines requièrent de leurs intervenants des connaissances et des compétences bien différentes, et la collaboration de ces quatre secteurs est essentielle pour permettre l'implantation de contrôles de sécurité efficaces qui peuvent être validés[49] et vérifiés[50].

XII.1.3 Acteur

Compte tenu de ce qui précède, un acteur se définit comme suit : quelqu'un ou quelque chose, à l'extérieur du système, qui interagit avec le système (ISO/IEC, 2010g, p. 10).

XII.1.4 Système

Tel que défini dans la norme ISO 15288 (clause 4.31) un système est une combinaison d'éléments interagissant entre eux, organisés pour atteindre un ou plusieurs états visés (ISO/IEC, 2007g, p. 6). Toujours selon cette même norme, un élément de système (clause 4.32) est un membre d'un ensemble de composants qui constitue le système (ISO/IEC, 2007g, p. 7). En pratique, l'interprétation de la portée d'un système est souvent clarifiée par l'utilisation d'un qualificatif, c.-à-d. système solaire, système juridique, système d'information.

---

[49] Validation : clause 4.54, ISO/IEC 12207: Systems and Software Engineering — Software Life Cycle Processes, p.8.

[50] Vérification : clause 4.55, ISO/IEC 12207: Systems and Software Engineering — Software Life Cycle Processes, p.8.

Selon cette définition, un système peut interagir avec d'autres systèmes ainsi qu'avec des éléments qui le composent (*Voir* Figure-A XII-2). L'identification des éléments et sous-systèmes qui composent un système n'est ainsi précisée que par l'interprétation de l'objectif qui lui est associé.

XII.1.5 Vulnérabilité

Une vulnérabilité est la conséquence de contrôles de sécurité insuffisants ou inexistants (ISO/IEC, 2009d, p. 6).

XII.1.6 Information sensible

Information qui, si elle est compromise par une perte d'intégrité, de confidentialité ou de disponibilité, causerait un impact qui serait jugé inacceptable par l'organisation ou la personne qui la possède.

XII.1.7 Propriétaire d'une application

Rôle organisationnel chargé de la gestion, de l'utilisation et de la protection de l'application et de ses données.

NOTE Le propriétaire de l'application prend toutes les décisions relatives à la sécurité de l'application. Le terme « détenteur » est considéré, dans ce document, comme un synonyme de « propriétaire » de l'application, car tous deux ont les mêmes responsabilités envers l'application qui leur appartient, ou qui leur a été assignée.

XII.2 Concepts, termes et définitions introduits par le modèle SA

Cette section présente et définit les principaux concepts ainsi que les termes clés en usage dans cette thèse.

XII.2.1 Application

Une application est un système d'information[51], qui a été construit pour automatiser un ou plusieurs processus afin de répondre à un nombre variable de besoins spécifiques qui proviennent généralement des processus et des exigences d'affaires d'une organisation (*Voir* Figure-A XII-3).

Plus concrètement, une application est une solution technologique qui inclue le logiciel, ses données et procédures, conçues pour aider les utilisateurs à effectuer des tâches particulières ou pour gérer des problèmes technologiques particuliers, en automatisant des processus ou des fonctions d'affaires. Il est à noter ici qu'un processus d'affaires inclue les personnes et la technologie.

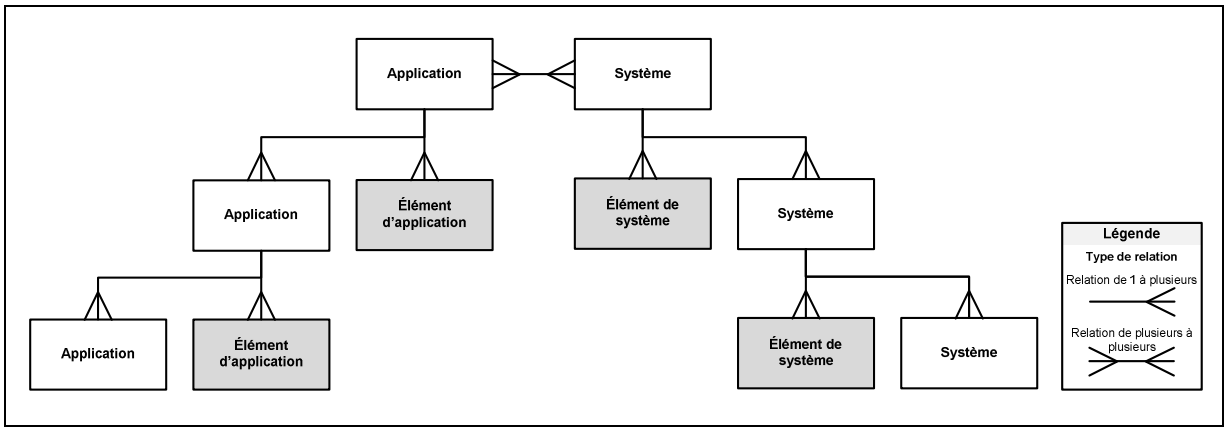


Figure-A XII-2 Une application selon le modèle SA versus un système selon la norme ISO 15288

Étant donné qu'une application est un type spécifique de système, elle peut, comme tout système, interagir avec des éléments qui lui sont propres ainsi qu'avec d'autres systèmes et applications. Par exemple, une application Web interagira avec ses propres composants logiciels, et pourra utiliser une application de gestion de base de données pour y conserver

[51] Aussi appelé système TI.

ses transactions. De plus, cette application pourra s'appuyer sur plusieurs serveurs d'applications et de données afin de pouvoir répondre efficacement à la demande d'un très grand nombre d'utilisateurs. De la même manière, plusieurs applications peuvent utiliser un seul et même serveur d'applications pour fonctionner, de même que plusieurs applications peuvent utiliser la même application de gestion de base de données pour y conserver leurs données respectives (*Voir* Figure-A XII-2).

Selon l'organisation ou le contexte d'utilisation, plusieurs termes peuvent être utilisés comme synonymes d'application, donc notamment : application logicielle, application Web, application d'affaires, ressource informationnelle et systèmes d'information.

XII.2.2 Environnement de l'application

L'évaluation de la SA d'une application doit tenir compte de l'environnement où celle-ci est ou sera réalisée et opérée. L'environnement d'une application peut être identifié de deux façons :

1) **L'environnement actuel d'une application** qui décrit et spécifie l'ensemble des contextes où est réalisée et opérée cette application; et
2) **L'environnement cible d'une application** qui décrit et spécifie l'ensemble des contextes où sera réalisée et opérée cette application.

L'environnement d'une application décrit et spécifie les caractéristiques des contextes d'affaires, juridiques et technologiques dans lesquels cette application est ou sera réalisée ou opérée. L'identification de cet environnement doit tenir compte des spécifications ainsi que de la description des groupes d'informations, des acteurs, des processus et des technologies qui sont ou seront impliqués dans sa réalisation ou son opération.

Aujourd'hui une organisation peut avoir son siège social à Montréal, héberger son application sur les serveurs de ses fournisseurs qui sont situés à Québec, à Toronto et à Boston, et autoriser l'utilisation des services de son application à des utilisateurs qui y

accèdent à partir de Vancouver, de New York, de Paris et de Moscou. Cet environnement d'utilisation permet déjà de soulever plusieurs questions. Seulement du côté légal, quels sont les lois et règlements qui s'appliquent pour définir ce qu'est un renseignement personnel? Est-ce que l'application contient des informations qui sont considérées personnelles par l'un ou l'autre des pays où celle-ci est utilisée? L'organisation doit-elle tenir compte de l'endroit où les données sont conservées?

Ces travaux de recherche étendent donc la définition d'un environnement traditionnellement « technologique » d'une application, pour y inclure le contexte juridique où elle est, ou sera utilisée (ensemble des lois canadiennes, des lois québécoises, des lois ontariennes, des lois américaines, des lois du Massachusetts, des lois françaises et russes, etc.), et le contexte d'affaires pour lequel l'organisation utilisera son application.

La Figure-A XII-3 présente le positionnement et les vecteurs d'influences des risques de sécurité provenant de l'environnement et des spécifications de l'application.

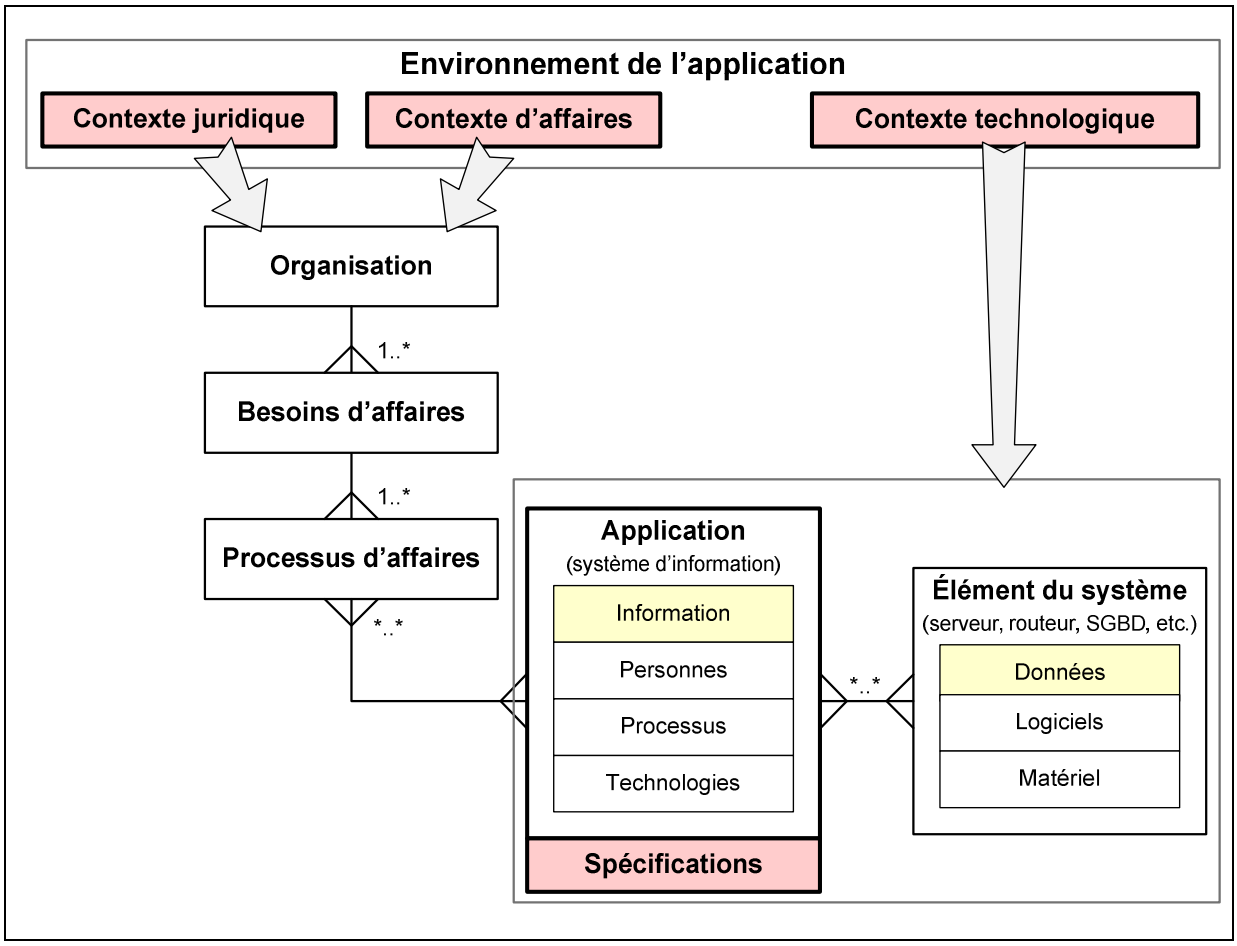


Figure-A XII-3 Les principales sources de risques de SA : l'environnement et les spécifications de l'application

Parce qu'une organisation utilise généralement une application pour répondre à au moins un de ses besoins d'affaires, les risques provenant du contexte juridique et du contexte d'affaires de cette organisation ont un impact direct sur les risques de sécurité existants dans l'environnement où est utilisée son application. Ceci inclut tous les acteurs, les processus et les produits TI, des quatre secteurs d'intervention impliqués dans la réalisation et l'opération de l'application. Le Tableau-A XII-1 présente les 12 sources des risques de SA.

Tableau-A XII-1 Sources des risques de SA liés à une application et à son environnement

Sources des risques de SA		Acteurs liés à l'application	Processus liés à l'application	Technologie liée à l'application
Environnement de l'application	Contexte technologique	✓	✓	✓
	Contexte juridique	✓	✓	✓
	Contexte d'affaires	✓	✓	✓
Spécifications de l'application		✓	✓	✓

Par exemple, si les contextes ou les spécifications d'une application ne sont pas bien identifiés, les risques de SA qu'ils amènent ne pourront être ni identifiés ni gérés et, de ce fait, on ne pourra pas définir s'il est sécuritaire ou non d'utiliser cette application dans cet environnement.

C'est, notamment, en tenant compte des contextes de l'environnement d'utilisation d'une application, qu'une organisation peut être en mesure d'identifier les risques qui peuvent menacer les données de son application. La Figure-A XII-3 montre comment ces trois contextes ont une influence sur l'évaluation de la sécurité de l'application par l'organisation.

Les trois sections suivantes décrivent le contenu des trois contextes : d'affaires, juridique et technologique qui ont été introduits à la section 1.4. L'information contenue dans ces contextes doit être continuellement mise à jour par le comité responsable de la gestion du CNO.

XII.2.3 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 (Figure-A XII-3). Ce contexte comprend aussi les descriptions et l'inventaire catégorisé des rôles et des informations impliquées par l’opération et l’utilisation de cette application.

C’est de ce contexte que proviennent les risques spécifiques découlant du domaine d'activité de l'organisation (compagnie de téléphone, compagnie de transport, gouvernement, etc.). Par exemple, une compagnie aérienne, une compagnie de transport et un gouvernement n’ont pas, en raison de leurs objectifs et processus d’affaires critiques, à gérer les mêmes risques de sécurité.

Le contexte d’affaires d’une organisation comprend notamment :

1) la gestion de projet, l’analyse des risques, les méthodes de développement, les procédures opérationnelles, les processus d'audit et de contrôle;
2) la politique de sécurité de l'organisation;
3) les pratiques pour le domaine des affaires;
4) la méthodologie de développement utilisée par l'organisation;
5) les meilleures pratiques pour tous les langages de programmation employés par l'organisation et énumérés dans le contexte technologique;
6) l'organisation du processus formel de gestion de projet;
7) les normes internes et les normes internationales pertinentes, telles que ISO 27001, ISO 27002 et ISO 15288.

Le contexte d’affaires d’une organisation se décrit comme l’ensemble des contextes d’affaires des applications de l’organisation. La documentation décrivant le contexte d’affaires de l’organisation (organigrammes, directives, règlements internes, processus, etc.) est conservée à l’intérieur de son cadre normatif (Figure-A XIII-1).

XII.2.4 Contexte juridique de l'application

Il s'agit de l'inventaire des différentes lois, règlements, directives et règles nationales inhérents à la juridiction, et au territoire où sera utilisée l'application, et qui s'appliquent à l'organisation (Figure-A XII-3) pour l'utilisation d'une de ses fonctionnalités ou de ses données.

C'est de ce contexte que proviennent les risques pour l'organisation de ne pas respecter un règlement territorial (Figure-A XII-3) dans une localisation géographique où elle fait des affaires et où son application est en usage (droits d'auteurs, lois sur la protection des renseignements personnels, etc.). Par exemple, les droits de propriété intellectuelle peuvent varier d'un pays à l'autre. Les restrictions sur les protections de chiffrement, mises en place dans un système d'information, peuvent aussi changer en fonction des régions où l'application sera utilisée. Le contexte juridique d'une application dépendra des lois et règlements édictés notamment par les pays, les régions et les municipalités.

Cet inventaire devra autant tenir compte de la localisation des serveurs qui hébergent l'application, que de la nationalité de ses utilisateurs ou de leur lieu de connexion.

Par exemple, une organisation qui déploie son application sur plusieurs continents, pour qu'elle soit utilisée par des utilisateurs de plusieurs pays, pourrait ne pas répondre adéquatement aux différentes législations des pays concernés.

Le contexte juridique d'une organisation se décrit comme l'ensemble des contextes juridiques qui régissent les territoires où sont utilisées ses applications. La documentation décrivant le contexte juridique de l'organisation (lois, règlements, etc.) est conservée à l'intérieur de son cadre normatif (Figure-A XIII-1).

XII.2.5 Contexte technologique de l'application

Il s'agit de l'inventaire des divers éléments utilisés ou nécessaires au fonctionnement de l'application (Figure-A XII-3), incluant notamment : les serveurs, leurs systèmes d'exploitation, leurs données de configuration, les ports et les liens de communication autorisés, les applications, les services et les périphériques. Ceci inclut les paramètres et les processus associés à ces éléments, tels que : les processus de qualification, les processus de maintenance, les processus de contingence et de relève.

Le contexte technologique englobe aussi les spécifications techniques, les processus et les configurations des éléments requises par l'application. Mentionnons, par exemple, les fonctionnalités de sécurité, les composants sécurisés, les spécifications des paiements en ligne, les connexions sécuritaires, la cryptographie et la gestion des autorisations, pour n'en nommer que quelque un.

C'est de ce contexte que proviennent les risques spécifiques découlant des personnes, des processus et des technologies impliqués par l'utilisation des composants technologiques dans le cours des activités d'une organisation. Ces risques peuvent notamment provenir :

1) des personnes impliquées dans la gestion, le support et la maintenance des composants technologiques de l'organisation;
2) des processus de relèves ou de contingences de l'organisation;
3) des composants technologiques requis par les environnements de production, de développement ou de tests de l'organisation (panne, mauvaise configuration, composant défectueux, etc.).

Du point de vue de la SA, le contexte technologique d'une organisation se décrit comme l'ensemble des contextes technologiques des applications de l'organisation. La documentation décrivant le contexte technologique de l'organisation (documentation, acteurs, processus, etc.) est conservée à l'intérieur de son cadre normatif (Figure-A XIII-1).

XII.2.6 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 (Figure-A XII-3).

Même si les spécifications et fonctionnalités requises pour une application font aussi partie de l'environnement, car ceux-ci proviennent du contexte d'affaires sous forme de besoins fonctionnels et non fonctionnels émis par l'organisation, il s'est avéré plus pratique de séparer les besoins du contexte d'affaires afin de les placer en évidence, car des risques particuliers peuvent provenir des spécifications et des fonctionnalités de l'application. Par exemple, une des spécifications d'une application indique que celle-ci doit pouvoir répondre à un événement spécifique à l'intérieur de 2 millisecondes, qu'elle doit soutenir une charge de 10 000 transactions par minute, ou encore, qu'elle soit offrir une fonctionnalité de paiement en ligne par carte de crédit. Ces spécifications et fonctionnalités pourraient amener des risques de sécurité tels que des risques d'indisponibilité ou des risques de fraudes qui n'auraient pas été présents si cette spécification ou fonctionnalité n'avait pas été exigée pour l'application.

XII.2.7 Groupes d'informations liées à la sécurité d'une application

La SA est la protection des groupes d'informations sensibles calculées, utilisées, stockées et transférées par une application, tel que requis par l'organisation. Cette protection assure non seulement la disponibilité, l'intégrité et la confidentialité des données, mais aussi l'authentification et la non-répudiation des actions de leurs utilisateurs. La sensibilité des données et des autres actifs informationnels doit être définie par l'organisation dans son processus d'évaluation des risques de sécurité.

Il s'agit de la liste et de la description des groupes d'informations liés à une application qui peuvent devoir être protégés. Ces informations ne proviennent pas seulement des données des éléments du système qui soutiennent l'application (Figure-A XII-3), mais elles

proviennent aussi des groupes d'informations de l'organisation et des personnes impliquées dans sa réalisation et son utilisation.

Par exemple, le code source d'une application spécifique peut être considéré par l'organisation comme étant des données de l'application qui a été catégorisée comme de l'information sensible, et qui nécessite une protection particulière (Figure-A XII-4, point 2).

La SA implique la protection de tous les éléments d'information dont une perte d'intégrité, de disponibilité ou de confidentialité produira un impact inacceptable pour l'organisation. Mais quels sont ces éléments d'information?

La Figure-A XII-4 présente, par une ligne pointillée, la portée des groupes d'informations à prendre en compte dans la SA. Elle présente aussi les types de groupes d'informations impliqués dans une application qui peuvent avoir une influence sur la protection des données sensibles de l'application. Un exemple de groupes d'informations présents dans la portée de la sécurité des informations d'une application est présenté, pour chacun des neuf types de groupes d'informations, à la Figure-A XV-1.

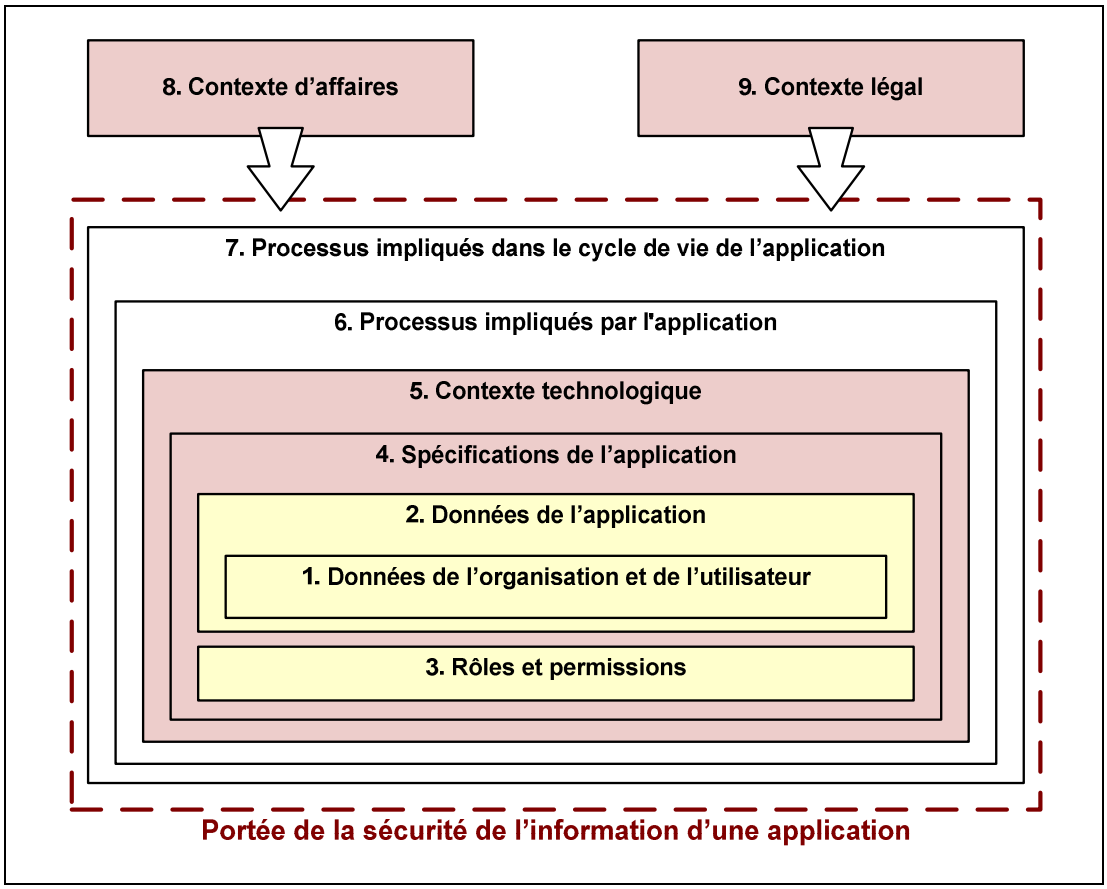


Figure-A XII-4 Les types de groupes d'informations liés à la sécurité d'une application
Traduite et adaptée de (ISO/IEC, 2011d)[52]

Identification sommaire des types de groupes d'informations liés à la SA :

1) **Les données de l'organisation et des utilisateurs de l'application**

   Le centre de l'attention de la SA se porte sur la protection adéquate de l'information et des données sensibles de l'organisation et de l'utilisateur. C'est cette information qu'il est primordial de protéger.

[52] Certaines figures provenant de la norme ISO 27034 présentées dans cette thèse ont été adaptées afin de pouvoir y intégrer les changements amenés par l'avancement de nos travaux de recherches.

Les données de l'organisation et celles des utilisateurs qui pourraient devoir être protégées sont notamment :

a) les certificats de clé publique;
b) les clés privées;
c) les transactions;
d) les journaux;
e) les paramètres de configuration;
f) les données de l'application (étiquettes, écrans, fichiers d'aides, etc.);
g) les données de l'organisation (listes des clients, d'employés, de produits, ou autre information de l'organisation conservée, transmise ou gérée par l'application); et
h) les données des utilisateurs (paramètres et profils des utilisateurs, préférences, ou autres informations des utilisateurs conservées, transmises ou gérées par l'application).

2) Les données de l'application

Si le code source, le code binaire ou les paramètres d'une application sont modifiés, sans autorisation, il est possible que l'information sensible qu'elle gère ne soit plus adéquatement protégée.

Les données de l'application qui pourraient devoir être protégées sont notamment :

a) les données de configuration d'application;
b) le code binaire de l'application;
c) le code source de l'application;
d) les librairies internes et commerciales; et
e) la documentation de l'application, de ses composants et de ses fonctionnalités.

3) Les rôles et permissions des différents acteurs

Si les informations concernant les permissions du rôle d'un acteur sont modifiées sans autorisation, et que ce changement permet à ce dernier d'avoir accès à de l'information à

laquelle il n'aurait pas dû avoir accès, il est possible que la confidentialité de cette information ne soit plus adéquatement assurée.

Les données décrivant les rôles et permissions des différents acteurs qui pourraient devoir être protégées sont notamment :

a) les données de gestion de l'identité;
b) les données d'identification et d'authentification des utilisateurs et des composants de l'application; et
c) les données d'autorisation.

4) Les spécifications et les fonctionnalités de l'application

Si une spécification ou une fonctionnalité est modifiée, retirée ou ajoutée à l'application, il est possible que ce changement amène un nouveau risque de sécurité et que l'information sensible qu'elle gère ne soit plus adéquatement protégée. (*Voir* XII.2.6)

Les données décrivant les spécifications et les fonctionnalités de l'application qui pourraient devoir être protégées sont notamment :

a) les spécifications et contraintes de bandes passantes, de dépôts de données, d'architecture matérielle et logicielle;
b) les spécifications fonctionnelles de l'application;
c) les spécifications de sécurité;
d) les spécifications des terminaux clients;
e) les spécifications des serveurs, les services et les composants d'une architecture N-Tiers;
f) les processus de qualification, d'installation, de configuration et de maintenance des divers produits et composants technologiques soutenant l'application.

5) Le contexte technologique de l'application

Si le contexte technologique de l'application change et qu'un des composants technologiques utilisés par l'application est ajouté, retiré, modifié ou reconfiguré, il est

possible que cette modification amène un nouveau risque de sécurité, et que l'information sensible que l'application gère ne soit plus adéquatement protégée (*Voir* XII.2.5).

Les données décrivant les spécifications et configurations des produits et composants technologiques soutenant l'application qui pourraient devoir être protégés sont notamment :

a) les consoles, les terminaux, les serveurs, les composants réseaux et autres périphériques autorisés, requis ou utilisés par l'application;
b) les systèmes d'exploitation, les configurations des différents composants et services externes requis par l'application;
c) les liens de transport et des ports de communication autorisés à être utilisés par l'application;
d) les logiciels commerciaux et autres produits, tels que les systèmes utilisés par l'application;
e) l'environnement physique et électrique requis par l'application; et
f) les processus de qualification, d'installation, de configuration et de maintenance des divers produits et composants technologiques soutenant l'application.

6) Les processus impliqués par l'application

Si un des processus requis par l'application est ajouté, retiré ou modifié, ou qu'un des processus existants de l'organisation n'est pas adapté à l'utilisation de l'application, il est possible que ce processus insère une faille dans l'utilisation, la gestion ou la maintenance de l'application et, qu'ainsi, l'information sensible gérée par l'application ne soit plus adéquatement protégée.

Les données décrivant les processus requis ou existants touchés par l'utilisation des fonctionnalités ou des informations de l'application qui doivent être protégées sont :

a) les processus d''utilisation et de gestion;
b) les processus d'entretien et de sauvegarde;
c) les processus de distribution et de déploiement; et

d) les processus impactés ou requis par l'application.

7) Les processus impliqués dans le cycle de vie de l'application

Si un des processus du cycle de vie de l'application est ajouté, retiré, modifié ou simplement mal réalisé (intentionnellement ou non) par l'acteur qui en est responsable et, que de ce fait, ce processus ne contient plus l'activité ou le contrôle de sécurité nécessaire à la sécurité de l'application, il est possible que l'information sensible gérée par cette application ne soit plus adéquatement protégée.

Les données décrivant les processus requis ou existants impliqués dans le cycle de vie de l'application qui doivent être protégées sont :

a) les processus de formation, d'audit et de qualification;
b) les processus de réalisation (développement, gestion de projet, maintenance, gestion des versions, des essais, etc.); et
c) les processus opérationnels.

8) Le contexte d'affaires de l'application

Si le contexte d'affaires de l'organisation change et que l'application qui était utilisée, par exemple, pour gérer les données des clients d'un club nautique via le Web, est maintenant utilisée pour gérer les données d'une clinique médicale privée, il est possible que l'information sensible gérée par l'application ne soit plus adéquatement protégée en fonction du nouveau contexte d'affaires où l'application est utilisée.

Le contexte d'affaires se réfère à toutes les bonnes pratiques, les règlements et les contraintes issus du domaine d'affaires de l'organisation (*Voir* XII.2.3).

9) Le contexte juridique de l'application

Si le contexte juridique d'un pays change et que l'application est utilisée à cet endroit, il est possible que l'information sensible gérée par l'application ne soit plus adéquatement protégée en fonction des nouvelles lois en vigueur.

Le contexte juridique se réfère à toutes les lois, règlements et règles communes, issues du territoire ou de la juridiction, qui ont un impact sur la fonctionnalité de l'application ou de son utilisation des données (*Voir* XII.2.4).

XII.2.7.1 Comparaison des types de groupes d'informations appartenant à l'application versus ceux impliqués dans sa sécurité

L'ensemble des types de groupes d'informations identifiés dans la Figure-A XII-4 ne signifie pas que tous ces éléments sont considérés comme faisant partie d'une application, mais plutôt que les éléments dans la portée doivent être protégés si l'on désire sécuriser une application. De fait, la portée de la SA est plus grande que la portée de l'application elle-même. Le Tableau-A XII-2 présente cette différence, soit les groupes types de d'information présents dans l'application ainsi que ceux qui sont présents dans la portée de la sécurité de cette dernière.

Tableau-A XII-2 Type de groupes d'informations inclus dans une application versus ceux inclus dans la portée de la sécurité d'une application

Type de groupe d'information	Présent dans l'application	Présent dans la portée de la sécurité d'une application
Données de l'organisation et de l'utilisateur		✓
Données de l'application	✓	✓
Rôles et permissions	✓	✓
Spécifications de l'application	✓	✓
Contexte technologique		✓
Processus impliqués par l'application		✓
Processus impliqués dans le cycle de vie de l'application		✓
Contexte juridique		✓
Contexte d'affaires		✓

Les groupes d'informations inclus dans la portée de la SA doivent être identifiés, puis associés ou intégrés à tous les processus, composants et acteurs critiques intervenant dans le

cycle de vie de l'application. Afin d'être complet, ces groupes d'informations doivent permettre d'identifier le type de groupes d'informations auxquels ils appartiennent, les noms des processus et les responsabilités des rôles des acteurs qui auront accès à ces groupes d'information, ainsi que les risques et les exigences de SA qui s'y réfèrent.

XII.2.8 Risques de sécurité d'une application

L'objectif de l'identification des risques de sécurité de l'information est de déterminer ce qui pourrait se produire pour provoquer la perte potentielle d'une information sensible appartenant à l'organisation (ISO/IEC, 2010d, p. 14). La sécurité d'une application suit le même objectif, mais l'identification des risques de sécurité ne concerne que les groupes d'informations liées à l'application elle-même (Figure-A XII-4). Il s'agit maintenant d'identifier la probabilité qu'un événement, qui menace une information sensible de l'application, survienne et génère un impact non désiré.

Les risques de SA peuvent provenir de 12 sources, soit des personnes, des processus et de la technologie impliqués par les contextes d'affaires, juridiques et technologiques de l'environmenent ou a été réalisée et est opérée l'application (Tableau-A XII-1).

La gestion d'un risque de sécurité se fait généralement par la mise en place d'un contrôle de sécurité de manière à diminuer un risque, et de le rendre acceptable par le détenteur ou l'organisation qui utilise l'application concernée. 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 requises par l'organisation pour cette application.

La Figure-A XII-5 présente les principaux éléments requis par le processus d'analyse de risque de la SA.

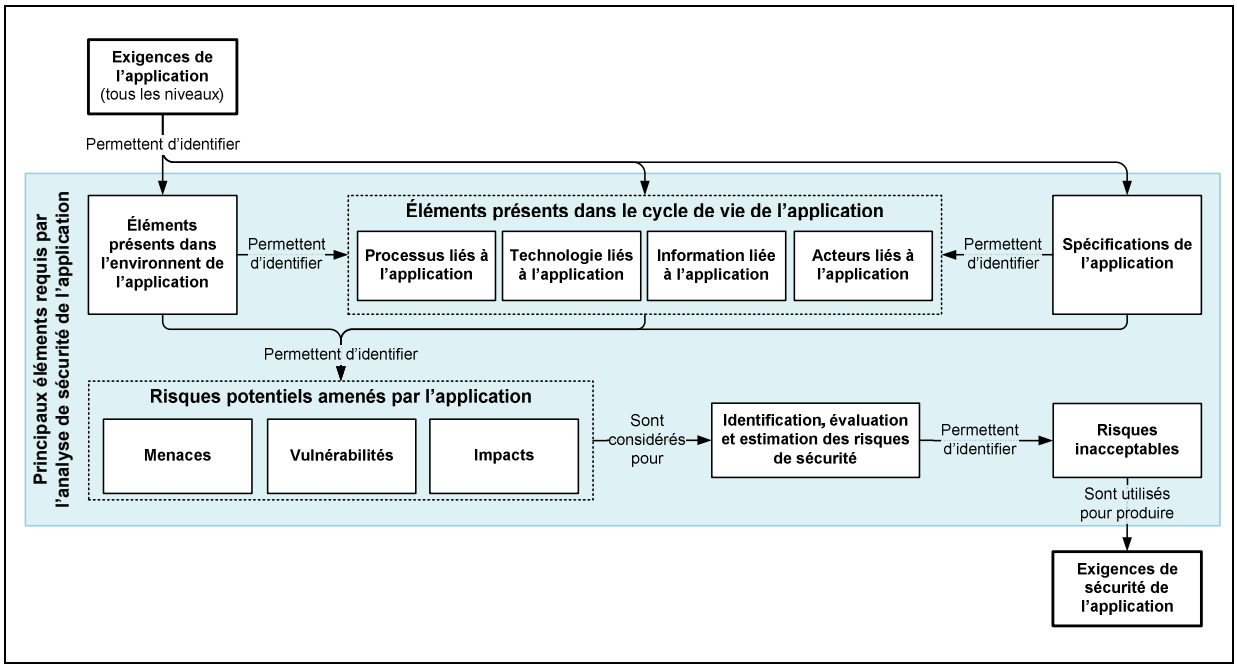


Figure-A XII-5 Vision sommaire des principaux éléments requis par l'analyse de sécurité d'une application

En plus de prendre en compte l'information liée à ces exigences, l'évaluation des risques de sécurité d'une application devra tenir compte de leurs impacts sur l'environnement d'utilisation de l'application, sur ses spécifications, les processus et les activités qui la concernent ainsi que sur les acteurs impliqués dans les activités impactées par ces exigences. L'objectif de cet exercice est de mieux identifier et comprendre les sources d'un risque de sécurité, soit : par qui, quand, comment, où et pourquoi cet événement pourrait se produire. Il s'agit ensuite de définir des exigences de sécurité qui permettront le développement et la mise en place de contrôles de sécurité visant à traiter et à diminuer ce risque à un niveau acceptable.

Par exemple, si l'organisation ne désire pas que l'application puisse effectuer des transactions à l'aide de cartes de crédit, tous les risques de sécurité provenant des éléments présents dans l'environnement de l'application, des acteurs, des processus et des informations liés à cette fonctionnalité seront inexistants et ne requerront donc pas la création d'exigences de sécurité.

Le processus de la gestion de la sécurité de l'application fait l'objet d'une présentation détaillée à l'annexe XIV.3.

XII.2.9 Exigences de sécurité d'une application

Description de ce qui est requis pour diminuer un ou plusieurs risques de SA et les ramener à un niveau acceptable.

Il faut noter que les exigences de sécurité ne proviennent que des risques de sécurité liés à une application. Étant donné que des risques peuvent provenir des spécifications et fonctionnalités offertes par une application, et que ces dernières proviennent des exigences préalablement émises pour une application, il devient évident que les exigences de sécurité ne peuvent être réalisées avant que les exigences de l'application n'aient été précisées (Figure-A XII-5).

Par exemple, une exigence de sécurité peut provenir d'un risque à ne pas se conformer correctement à la une loi de la protection des renseignements personnels d'un pays où l'organisation désire utiliser l'application. Une exigence peut aussi provenir d'un risque associé à un rôle, à une responsabilité ou à une qualification professionnelle obligatoirement requise pour réaliser un module de code identifié comme sensible. De fait, une exigence de SA peut provenir d'un risque de sécurité technologique, d'affaires ou juridique, présent dans l'un des contextes de l'application, ou encore il peut provenir directement d'une spécification ou d'une fonctionnalité de l'application de l'organisation.

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. L'exigence de sécurité est donc essentielle pour démontrer que la SA répond aux attentes.

Non seulement la définition d'exigences de sécurité est-elle requise (Viega et McGraw, 2002, p. 34), mais les mêmes caractéristiques des exigences logicielles, telles que définies par

ISO 29148, s'appliquent aux exigences de sécurité des applications. Elles doivent être fixées, puis traitées de manière identique aux exigences fonctionnelles ou aux exigences de qualité (ISO/IEC, 2001). Finalement, des exigences de sécurité liées au respect des limitations établies sur le risque résiduel devraient aussi être instituées.

XII.2.9.1 Types d'exigences de sécurité

Selon Wiegers, on peut cartographier les exigences logicielles selon deux catégories (fonctionnelles et non fonctionnelles) et trois niveaux (affaires, utilisateurs et fonctionnelles) (Wiegers, 2003). Le niveau des exigences d'affaires sert à répondre aux risques de sécurité stratégiques et tactiques de l'organisation tandis que les deux autres niveaux d'exigences servent généralement à répondre à des risques de sécurité plus opérationnels (NIST, 2010, p. 5).

Les exigences de SA se regroupent selon les mêmes catégories et niveaux que les exigences logicielles, sauf qu'un niveau supplémentaire sera nécessaire pour exprimer tous les types d'exigences de sécurité, soit : le niveau des exigences d'infrastructure. Ce dernier niveau est intégré au schéma des exigences de la SA afin de pouvoir répondre à des risques pouvant provenir de l'infrastructure où sera réalisée et utilisée l'application *(Voir* Figure-A XII-6).

Le type d'une exigence de sécurité est défini en identifiant l'acteur qui requiert cette exigence. Par exemple, si une exigence de sécurité spécifie qu'un utilisateur doit saisir un mot de passe, cette exigence sera identifiée comme une exigence d'utilisateur. Si une exigence de sécurité spécifie que l'application doit conserver un journal de certaines transactions sensibles, cette exigence sera identifiée comme une exigence de système.

La Figure-A XII-6, adaptée de la figure 1-1 de (Wiegers, 2003, p. 9) présente différents types d'exigences qui peuvent autant s'appliquer à des besoins logiciels, qu'à des besoins de sécurité d'une application.

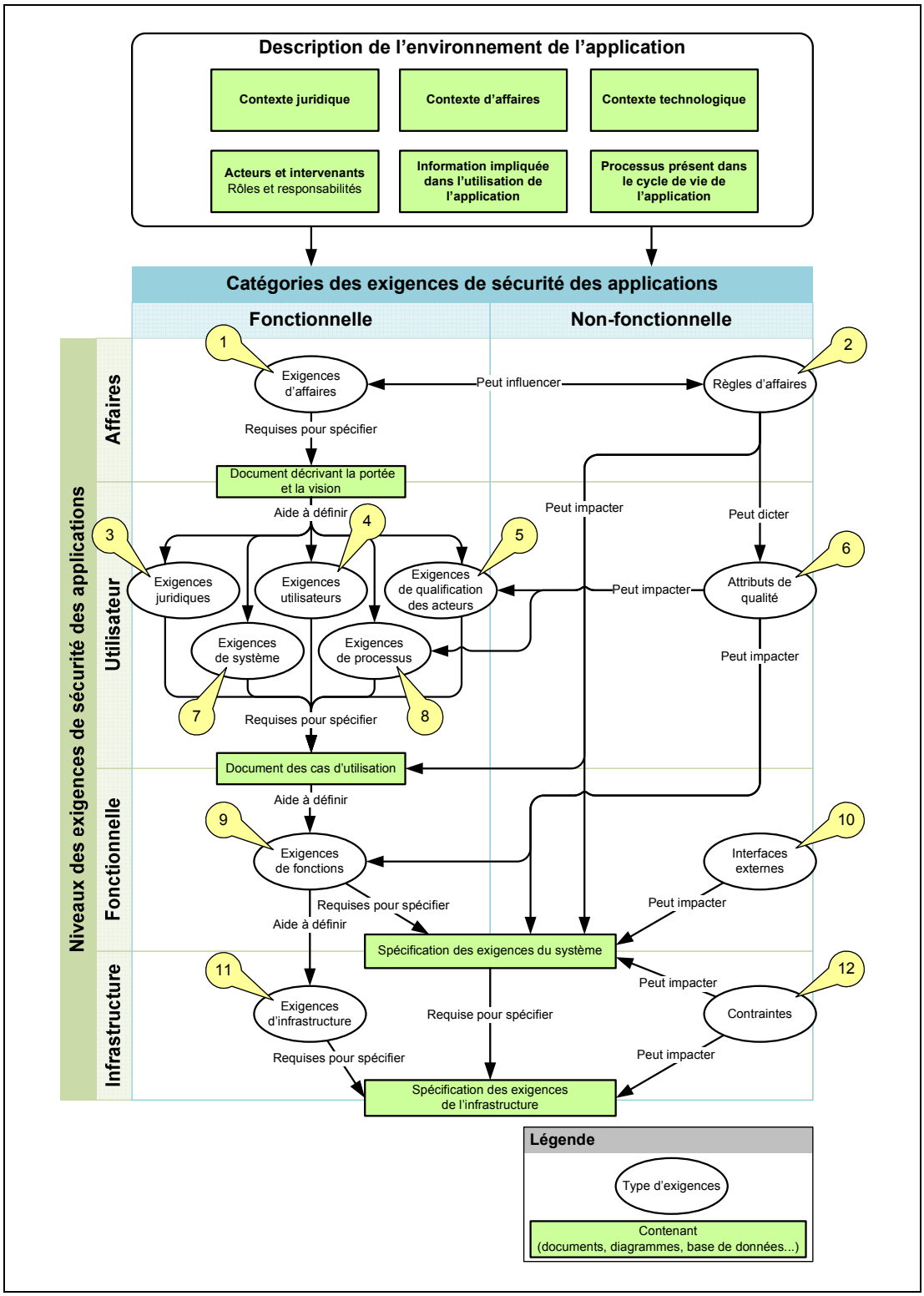


Figure-A XII-6 Schéma des exigences de sécurité des applications
Traduite et adaptée de (Wiegers, 2003, p. 9)

Les exigences de sécurité d'une application seront spécifiées à partir des risques de sécurité identifiés dans l'environnement de l'application. Ces exigences de sécurité peuvent se retrouver dans les douze types présentés dans la Figure-A XII-6 et serviront notamment à définir les contrôles de sécurité qui devront être mis en place.

1) Exigences d'affaires – Une exigence de sécurité d'affaires répond à au moins un risque de sécurité provenant du contexte d'affaires de l'organisation, tel que : les pratiques du domaine, les objectifs de l'organisation, les informations à protéger, la clientèle ciblée, etc.

2) Règles d'affaires – Une règle de sécurité d'affaires répond à au moins un risque de sécurité provenant de l'ensemble des règles de fonctionnement de l'organisation, tel que : les directives, les règlements internes, les codes de conduites, etc.

3) Exigences juridiques – Une exigence de sécurité juridique répond à au moins un risque de sécurité provenant du contexte légal auquel est assujettie l'organisation, du lieu où l'organisation prévoit utiliser son application, de l'endroit où les utilisateurs se connecteront à l'application, etc.

4) Exigences utilisateurs – Une exigence de sécurité utilisateur répond à au moins un risque de sécurité provenant des actions qui peuvent être réalisées par un acteur dans l'environnement d'opération de l'application, tel que : un gestionnaire, un membre de l'équipe technique, un opérateur, un utilisateur, un auditeur.

5) Exigences de qualification – Une exigence de sécurité de qualification répond à au moins un risque de sécurité provenant d'une contrainte ou d'une qualification concernant un acteur qu'il devra respecter lorsqu'il aura à réaliser une action dans les environnements de réalisation ou d'opération de l'application. Ce type d'exigences concerne soit une personne ou un élément du système.

   Par exemple, lorsqu'un un acteur est :

   a) une personne : avant qu'il ne soit autorisé à développer un nouveau composant Java, un développeur pourrait avoir à démontrer qu'il possède les qualifications nécessaires à réaliser son travail, soit un diplôme dans le domaine, un nombre minimal d'années d'expérience, des connaissances ou une certification professionnelle spécifique;
   b) un élément du système : avant qu'il ne soit autorisé à être déployé dans un environnement, on pourra avoir à démontrer qu'un élément du système est en mesure, par exemple de détecter et de réagir à une attaque distribuée de dénis de services, à une modification de données non autorisée ou à la panne d'un autre élément du système.

6) Attributs de qualité – Un attribut de qualité répond à au moins un risque de sécurité provenant d'une menace à l'atteinte des objectifs de qualité pour l'application, tel que : la réutilisabilité, l'utilisabilité, l'intégrité, la portabilité, l'interopérabilité, la maintenabilité, etc.

7) Exigences de système – Une exigence de sécurité de système répond à au moins un risque de sécurité provenant des services et fonctionnalités qui doivent être offerts par l'application.

8) Exigences de processus – Une exigence de sécurité de processus répond à au moins un risque de sécurité provenant des processus amenés ou impactés par l'application, notamment : les processus de développement, de déploiement, de délégation, d'utilisation, de maintenance, de contingence et d'archivage.

9) Exigences de fonctions – Une exigence de sécurité de fonction répond à au moins un risque de sécurité provenant des fonctionnalités qui sont offertes par le système, notamment : les fonctions d'authentification, de chiffrement, de surveillance, et de réaction automatique à un incident.

10) Interfaces externes – Une exigence de sécurité d'interface externe répond à au moins un risque de sécurité provenant des diverses interfaces offertes par le système, notamment : les interfaces Web et les interfaces de communication avec d'autres applications.

11) Exigences d'infrastructure – Une exigence de sécurité d'infrastructure répond à au moins un risque de sécurité provenant des contextes technologique, électrique et d'entreposage physique qui seront utilisés ou requis par l'application.

12) Contraintes – Une contrainte de sécurité répond à au moins un risque de sécurité provenant des restrictions de choix imposées à

> l'application. Par exemple, l'application doit être accessible via l'internet, aucun composant de l'application ne doit être développé en Java, ou encore une activité spécifique ne pourra être réalisée que par l'action simultanée de deux acteurs.

Pour minimiser toute ambiguïté, 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).

Il est toujours recommandé de préciser la raison pour laquelle une exigence de sécurité existe, et ce, pour deux raisons :

1) afin d'aider l'ingénieur, qui aura à satisfaire l'exigence, à comprendre dans quel contexte ce risque existe. Par exemple, cette raison pourrait référer à un risque provenant d'un article de loi qu'il faut respecter.
2) afin de mettre en place un mécanisme de gestion et de suivi des exigences permettant de démontrer que chaque risque inacceptable amené par l'application a engendré au moins une exigence de sécurité.

Il est à noter qu'une exigence de sécurité générale (de plus haut niveau) peut induire un ensemble d'exigences de sécurité plus spécifiques.

L'atteinte d'une exigence de sécurité doit être vérifiable : soit directement à l'aide d'une mesure, soit indirectement à l'aide d'une mesure qualitative donc le mécanisme de vérification sera préalablement défini et accepté par les parties.

XII.2.9.2 Sources des exigences de sécurité de l'application

Un risque est la probabilité qu'un événement menaçant une information sensible survienne de manière à causer un impact inacceptable pour l'organisation (ISO/IEC, 2010d). Le seul fondement pouvant amener une organisation à mettre en place des contrôles de sécurité réside dans les risques inacceptables qui menacent les informations sensibles d'une l'application. Sachant ces deux faits, on peut déduire que les sources des exigences de sécurité sont les risques pouvant menacer une information sensible appartenant à l'un des groupes d'informations liées à la sécurité de l'application (Figure-A XII-4).

Étant donné que des risques de sécurité peuvent provenir des exigences fonctionnelles et non fonctionnelles appartenant aux quatre niveaux d'exigences (Figure-A XII-6), ces exigences doivent donc avoir été préalablement identifiées avant de pouvoir identifier les exigences de sécurité correspondantes.

XII.2.9.3 Ingénierie des exigences de SA

Sachant que toutes les fonctionnalités, qualités, caractéristiques et contraintes d'une application devraient avoir été implémentées à la suite d'une exigence, les fonctionnalités, qualités et caractéristiques de SA devraient elles aussi avoir été implémentées à la suite d'une exigence de sécurité.

Tout comme l'ingénierie des exigences fonctionnelles et non fonctionnelles d'une application est réalisée à l'aide de processus qui prennent en compte les besoins d'affaires, d'utilisateurs et fonctionnels qui doivent être pris en compte par l'application, l'ingénierie des exigences de sécurité est réalisée à l'aide du même processus, mais en prenant en compte les besoins de sécurité qui doivent être satisfaits par l'application.

Le processus d'ingénierie des exigences de sécurité d'une application utilise ces exigences fonctionnelles et non fonctionnelles afin d'identifier les éléments qui pourraient être la cause

de risques inacceptables, car ils menacent des informations impliquées par l'utilisation de l'application.

Un exemple de l'adaptation du processus d'identification des exigences de système, basé sur la section 6.4.1 – *Stakeholder Requirements Definition Process* de la norme ISO 15288 (ISO/IEC, 2007g, p. 37), en processus d'ingénierie des exigences de sécurité d'une application, ainsi que des exemples d'exigences de SA sont présentés à l'appendice A – ANNEXE XVI.

XII.2.10 Contrôles de sécurité des applications

La notion de contrôle de sécurité est largement utilisée dans l'industrie de la sécurité de l'information. Un grand nombre de contrôles de sécurité sont déjà rendus disponibles par des organisations telles qu'ISO avec notamment la publication des normes ISO 27002 (ISO/IEC, 2005c) et ISO 15408-3 (ISO/IEC, 2005b), par l'organisation NIST avec notamment la publication de la norme NIST 800-53 (NIST, 2013) ou par l'organisation ISACA avec la norme COBIT 4.2 (ITGI, 2007).

Contrairement aux contrôles de sécurité qui sont habituellement utilisés en gestion de la sécurité de l'information, le modèle propose un concept de contrôle de sécurité des applications (CSA) qui inclut la 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. Cette description inclut aussi la spécification des activités de vérification de mesures qui doivent être réalisées pour démontrer que le contrôle implémenté fonctionne tel que prévu, et produit les résultats attendus. De plus, la description d'une activité requiert l'identification des éléments : qui, quoi, où, quand, comment et combien. (*Voir* l'appendice A – ANNEXE XIII.9 pour plus de détails.)

Les CSA et leurs objectifs doivent être choisis et mis en œuvre pour répondre aux exigences déterminées par l'évaluation et le traitement des risques (ISO/IEC, 2005d). Dans la sécurité des applications, le processus d'évaluation des risques de sécurité reliés aux informations inhérentes à l'application détermine les objectifs de contrôle, tels qu'exprimés par les exigences de sécurité des applications.

XII.2.11 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. C'est donc la conséquence de contrôles de sécurité insuffisants ou inexistants, suite à des exigences de sécurité qui n'auraient pas été correctement précisées ou qui n'auraient pas été satisfaites.

Voici quelques exemples de sources de vulnérabilités :

1) Les acteurs, tels que des programmeurs qui écrivent du code vulnérable, des utilisateurs qui font des erreurs en utilisant le logiciel ou des techniciens et des développeurs qui font des erreurs lors de la maintenance du logiciel ou de l'infrastructure de l'application;
2) Les processus, tels que des procédures de tests inadéquates, un mauvais processus de gestion de projets, une attention insuffisante sur l'intégration de la sécurité dans les processus du cycle de vie de l'application, les interactions imprévues entre les applications, les utilisateurs et les opérateurs, l'insuffisance des processus de gestion du changement;
3) Les éléments technologiques, tels qu'un mauvais choix d'architecture du réseau rendant accessibles des données sensibles à partir de l'Internet, ou l'absence d'un composant requis pour la redondance d'un service critique;
4) Les fonctionnalités de l'application, telles qu'un algorithme de chiffrement mal implémenté, un mécanisme d'authentification qui peut être contourné, ou des mots de passe intégrés en clair dans le code source.

XII.2.12 Niveau de confiance d'une application

Le niveau de confiance d'une application est représenté par le 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. Les CSA peuvent incluent des mécanismes de protection matérielle, logicielle et organisationnelle, qui ensemble mettent en œuvre la politique de sécurité de l'organisation.

Cette étiquette est définie par l'organisation elle-même dans le but d'identifier clairement et sans ambigüité un ensemble spécifique de CSA qui doivent s'appliquer à une application, dans son environnement spécifique, à un moment ou l'autre de son cycle de vie. Elle permet d'identifier et de communiquer facilement aux intervenants une liste de CSA à mettre en place dans le cycle de vie d'une application, et ce, de manière à s'assurer que tous les risques jugés inacceptables ont été correctement traités. Elle permet aussi d'étendre la traçabilité d'un risque de sécurité vers le ou les CSA requis pour l'atténuer adéquatement.

Le terme « niveau de confiance » proposé par le chercheur fût approuvé par consensus lors d'une réunion du SC27. Ce terme a été préféré à « niveau de sécurité » qui est communément utilisé pour définir un niveau non mesurable, habituellement évalué selon l'appréciation qualitative de l'évaluateur, et à « niveau d'assurance » qui a une définition différente associée, au contexte des Critères communs (ISO/IEC, 2009c). L'objectif de ce choix était de tenter d'éliminer toute confusion possible entre les personnes œuvrant dans les quatre domaines d'interventions.

L'assignation d'un niveau de confiance aux applications de l'organisation[53] permettra d'identifier les contrôles implémentés dans chacune d'elles, et ainsi faciliter la vérification, la

[53] Cette assignation a été effectuée à la suite de la réalisation d'une analyse de risques de sécurité organisationnelle.

maintenance et la mise à jour des CSA des applications de l'organisation, si la gravité d'un risque de sécurité venait à changer.

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

1) **Le niveau de confiance ciblé**

   Le niveau de confiance ciblé d'une application est une étiquette utilisée pour identifier et communiquer l'ensemble des CSA spécifiques, sélectionnés à partir de la bibliothèque de CSA, qui doivent être mis en place à différents moments du cycle de vie de la sécurité de l'application afin de pouvoir répondre aux exigences de sécurité.

   Le niveau de confiance ciblé d'une application est exigé par son détenteur afin qu'il ait une certaine assurance que les risques de sécurité qu'elle amène ont été diminués à un niveau acceptable. Il détermine l'ensemble des CSA qui doivent être mis en place et vérifiés à différents moments du cycle de vie de la sécurité de l'application.

2) **Le niveau de confiance actuel**

   Le niveau de confiance actuel d'une application est la conclusion du processus permettant de déterminer que tous les CSA d'une application, identifiés par leur niveau de confiance ciblé, ont été correctement implémentés et vérifiés, et qu'ils ont tous produit les résultats attendus.

   Le niveau de confiance actuel permet de démontrer la conformité d'une application aux exigences de sécurité requises et, ainsi, confirmer la diminution des risques de sécurité aux niveaux préalablement acceptés par l'organisation.

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.

XII.2.13 Application sécuritaire

Une application sécuritaire est une application pour laquelle le niveau de confiance actuel est égal ou supérieur au niveau de confiance ciblé.

Selon cette définition, une application sera jugée sécuritaire, lorsque la vérification de tous les CSA associés au niveau de confiance ciblé pour cette application aura produit les résultats attendus.

ANNEXE XIII

LE MODÈLE SA : COMPOSANTS

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.

Cette annexe présente les 14 composants clés du modèle SA, soit :

1) Comité de gestion du cadre normatif de l'organisation (*Voir* XIII.1);
2) Cadre normatif de l'organisation (CNO) (*Voir* XIII.2);
3) Contexte d'affaires (*Voir* XIII.3);
4) Contexte juridique (*Voir* XIII.4);
5) Contexte technologique (*Voir* XIII.5);
6) Dépôt des spécifications et des fonctionnalités des applications (*Voir* XIII.6);
7) Dépôt des rôles, responsabilités et qualifications (*Voir* XIII.7);
8) Dépôt des groupes d'informations catégorisés (*Voir XIII.8*);
9) Contrôle de sécurité des applications (CSA) (*Voir* XIII.9);
10) Bibliothèque de contrôles de sécurité des applications (*Voir* XIII.10);
11) Matrice de la traçabilité de la sécurité des applications de l'organisation (*Voir* XIII.11);
12) Modèle de référence du cycle de vie de la sécurité d'une application (MRCVSA) (*Voir* XIII.12);
13) Modèle du cycle de vie de la sécurité d'une application (*Voir* XIII.13);
14) Cadre normatif de l'application (CNA) (*Voir* XIII.14).

XIII.1 Comité de gestion du cadre normatif de l'organisation

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. Il présentera à la direction

de l'organisation, pour approbation, un plan d'action qui précisera ces objectifs et priorités de sécurité qui tiendra compte des priorités d'affaires et de la disponibilité des ressources de 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.

XIII.1.1 Objectifs visés par la mise en place du comité de gestion du CNO

Les objectifs visés par la mise en place d'un comité de gestion du CNO sont :

1) D'élaborer le plan d'action de la mise en œuvre de la SA en fonction des ressources et priorités de l'organisation;
2) De gérer l'intégration des composants et des processus identifiés par le plan d'action au CNO;
3) D'administrer les coûts de mise en œuvre et de maintenance du CNO;
4) De s'assurer que tous les éléments intégrés au CNO rencontrent les exigences de sécurité de l'organisation;
5) De s'assurer que le CNO puisse soutenir le SGSI de l'organisation;
6) De fournir des processus et des outils pour gérer la conformité de la SA aux normes, lois, directives et autres règlements en fonction des contextes juridiques et d'affaires de l'organisation;
7) De superviser la sensibilisation et la formation de tous les acteurs impliqués dans la SA;
8) De recevoir les rapports de vérification de la SI de l'organisation afin de s'assurer que le CNO répond adéquatement aux exigences de l'organisation; et
9) De promouvoir l'utilisation du CNO et s'assurer de la conformité de tous les projets d'application au cadre normatif de l'organisation.

XIII.1.2 Composition du comité de gestion du CNO

Dans de grandes organisations, ce groupe pourra être composé de directeurs qui, à l'intérieur du mandat du comité, répondront au chef de la sécurité de l'information de l'organisation (CIO). Dans des organisations plus modestes, il sera composé d'employés séniors qui ont une influence sur les décisions de l'organisation.

On retrouvera notamment dans ce groupe les noms de rôle décisionnel et de profil de compétence tels que :

1) Le responsable des opérations de l'organisation;
2) Le responsable des ressources humaines;
3) Le responsable de la sécurité des informations de l'organisation (CSIO);
4) Le responsable de l'infrastructure technologique de l'organisation et de l'acquisition des applications;
5) Le responsable du groupe de vérificateurs de l'organisation;
6) Le responsable du secteur juridique; et
7) Le responsable des projets de développement d'applications.

XIII.2 Cadre normatif de l'organisation (CNO)

Dépôt de données internes à l'organisation, contenant l'ensemble des éléments normatifs requis à la mise en place de la SA de l'organisation (*Voir* Figure-A XIII-1).

Bien qu'il soit souvent informel, toutes les organisations possèdent un cadre normatif. Dans bien des cas, il s'agit de toutes les habitudes, les façons de faire, les coutumes et les non-dits qui sont considérés comme allant de soi par les personnes travaillant dans l'organisation.

Le CNO est un dépôt de données qui contient toutes les meilleures pratiques reconnues par l'organisation. Il contient des éléments comme les politiques de l'organisation, ses règlements, ses pratiques, les rôles et responsabilités des postes clés, ainsi que ses processus

et façons de faire. Il peut être formalisé simplement par la mise en place d'un dépôt de documents officiels qui contiendra des éléments qui ont été approuvés et qui devront être suivis ou tenus en compte par les divers intervenants. Une fois formalisé, ce dépôt deviendra le cadre normatif de l'organisation (CNO), soit la source autoritaire des éléments qui normalisera le cadre des actions et des décisions prises par l'organisation.

Même s'il est incomplet, un CNO formel est essentiel à la mise en place du modèle SA. De par son rôle de recueil et de source autoritaire, le CNO est la fondation de l'implémentation du modèle SA dans toute organisation. Toutes les décisions et actions de l'organisation concernant la SA seront prises en tenant compte de ce cadre normalisé. Par exemple, une activité de revue de code ne pourra être réalisée comme un contrôle obligatoire de sécurité d'application que si les directives de programmation existent dans le CNO.

Dans le cadre du modèle, la portée du CNO concernera uniquement les éléments qui sont liés à la sécurité de ses applications tels que les pratiques recommandées de révision de code source reconnues par l'organisation, ainsi que les processus requis pour gérer et utiliser ses composants. Finalement, ce dépôt contient les processus de gestion du CNO ainsi que les éléments et processus nécessaires à la mise en place du modèle. L'objectif étant de ne pas dédoubler les éléments présents dans le cadre normatif de l'organisation.

Le CNO soutient l'architecture d'entreprise et le SGSI de l'organisation, lorsque ces deux derniers éléments existent.

Les organisations qui décident de créer et de maintenir un CNO devraient mettre en place un comité de gestion du CNO et s'assurer qu'il applique les principes suivants :

1) L'ordre de la mise en place des éléments de SA dans le CNO doit être réalisé en fonction des priorités de sécurité de l'organisation;
2) Le contenu du CNO doit être adapté aux besoins opérationnels de l'organisation;
3) Tout élément présent dans le CNO doit être vérifiable et avoir été approuvé par l'organisation;

4) Le contenu du CNO doit être communiqué et mis à la disponibilité de toute l'organisation;
5) Dans un contexte où les risques et menaces apparaissent et changent continuellement, l'organisation doit être en mesure de revoir et mettre à jour son CNO en réponse à ces changements.

XIII.2.1 Objectifs visés par la mise en place du CNO

Les objectifs visés par la mise en place d'un cadre normatif formel au sein de l'organisation sont de normaliser et de faciliter la communication de tous les processus et éléments de la sécurité des applications, et ainsi d'éviter les improvisations dans la réalisation d'activités ou la mise en place de contrôles concernant la sécurité d'une des applications de l'organisation.

Plus précisément, les objectifs de la mise en œuvre d'un CNO sont :

1) De normaliser les éléments (composants, processus, rôles et responsabilités, etc.) concernant la SA afin d'en assurer une mise en œuvre homogène et vérifiable;
2) D'assurer la communication de ces éléments en les conservant dans un dépôt accessible aux personnes concernées, et qui sera considéré comme la source autoritaire des éléments exigés par l'organisation;
3) De s'assurer que tous les éléments impliqués dans la SA sont approuvés par les décideurs appropriés et acceptés par les acteurs et parties prenantes;
4) De soutenir l'architecture d'entreprise et le SGSI de l'organisation;
5) De soutenir l'organisation dans sa capacité d'améliorer la maturité de ses processus par la formalisation et la révision de tous les éléments de sécurité contenus dans le CNO;
6) De limiter au minimum possible la résistance aux changements apportée par ces nouveaux éléments de sécurité des applications; et
7) De réduire au maximum l'impact du coût de la SA sur les projets en réutilisant des éléments existants de sécurité des applications, qui ont été validés et approuvés au préalable.

XIII.2.2 Éléments de sécurité des applications contenus dans le CNO

Une organisation peut décider de mettre en place plusieurs éléments afin de répondre aux défis engendrés par la sécurité des applications. Le CNO est le dépôt de tous ces processus et composants, approuvés et utilisés par l'organisation pour répondre et démontrer la sécurité de ses applications.

En conséquence, l'ensemble des processus liés à la définition, la gestion et la vérification de la SA dans l'organisation doit être décrit de manière formelle dans le CNO. La Figure-A XIII-1 présente une vue sommaire des composants et des processus types contenus dans le CNO d'une organisation.

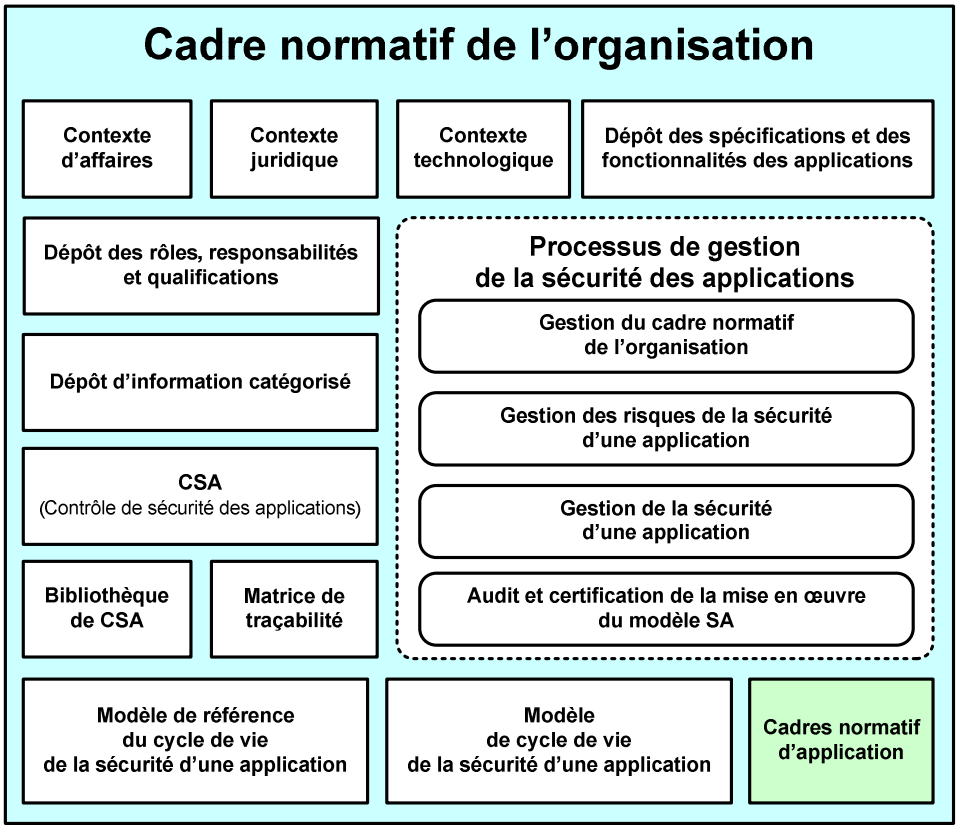


Figure-A XIII-1 Le cadre normatif de l'organisation
Traduite et adaptée de (ISO/IEC, 2011d)

Afin de pouvoir répondre correctement aux préoccupations de SA d'une organisation, le CNO devrait notamment contenir les éléments énumérés ci-dessous.

1) Les composants, soit :
   a) Contexte d'affaires (*Voir* XIII.3);
   b) Contexte juridique (*Voir* XIII.4);
   c) Contexte technologique (*Voir* XIII.5);
   d) Dépôt des spécifications et des fonctionnalités des applications (*Voir* XIII.6);
   e) Dépôt des rôles, responsabilités et qualifications (*Voir* XIII.7);
   f) Dépôt des groupes d'informations catégorisés (Voir XIII.8);
   g) Contrôle de sécurité des applications (CSA) (*Voir* XIII.9);
   h) Bibliothèque de contrôles de sécurité des applicat (*Voir* XIII.10);
   i) Matrice de la traçabilité de la sécurité des applications de l'organisation (*Voir* XIII.11);
   j) Modèle de référence du cycle de vie de la sécurité d'une application (MRCVSA) (*Voir* XIII.12);
   k) Modèle du cycle de vie de la sécurité d'une application (*Voir* XIII.13);
   l) Cadre normatif de l'application (CNA) (*Voir* XIII.14).
2) Les processus de gestion de la sécurité des applications, soit :
   a) Gestion du CNO (*Voir* XIV.1);
   b) Gestion des risques de la sécurité d'une application (*VoirXIV.2*);
   c) Gestion de la SA (*Voir XIV.3*).
   d) Audit et certification de la mise en œuvre du modèle SA (Voir XIV.4)

La description des composants du CNO est présentée ci-après, de l'annexe XIII.3 à XIII.14, tandis que celle des processus est présentée dans l'ANNEXE XIV.

XIII.3 Contexte d'affaires

À l'intérieur du CNO, le contexte d'affaires d'une organisation 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* XII.2.3).

Les activités impliquant ces applications peuvent générer des risques de sécurité et l'organisation se doit de déterminer les exigences de sécurité qui devront être satisfaites pour les atténuer. Par exemple, la politique de sécurité de l'organisation est généralement une source directe d'exigences de sécurité. Certaines d'entre elles sont pertinentes pour la sécurité des applications. Une non-conformité à la politique de sécurité de l'organisation est un risque qui n'est généralement pas accepté par le détenteur d'une application. Des CSA peuvent donc être conçus pour répondre aux exigences spécifiques de la politique de sécurité de l'organisation.

Par exemple, dans le domaine d'affaires de l'aéronautique, il peut y avoir des risques de sécurité élevés provenant du processus de développement d'une application qui sera utilisée pour le pilotage d'un avion. L'évaluation de ces risques permettra de définir les exigences de sécurité qui devront être satisfaites par l'introduction de CSA dans le processus utilisé pour le développement de ce type d'application.

XIII.3.1 Objectifs visés par l'identification du contexte d'affaires d'une organisation

Le contexte d'affaires permet de définir un cadre normalisé pour aider l'organisation à réduire les risques de sécurité provenant de ses activités opérationnelles dont, notamment, des personnes, des directives, des règlements et des processus impliqués dans les secteurs et lignes d'affaires ou seront utilisées les applications de l'organisation. Il sert aussi à définir les exigences de sécurité provenant du contexte d'affaires pouvant être référencées par les CSA. Il est principalement utilisé par l'approche de gestion de la sécurité d'une application, présenté par le modèle, pour permettre d'identifier et de réduire les risques associés aux différents domaines d'affaires où œuvre l'organisation.

XIII.3.2 Contenu du contexte d'affaires d'une organisation

Ce composant contient les rôles et processus impliqués par les applications de l'organisation, l'inventaire des groupes d'informations catégorisés, impliqués par ces processus, les normes, les règlements et les pratiques recommandés, approuvés par l'organisation, et qui peuvent générer des risques de sécurité incluant les projets concernant le développement ou l'utilisation d'applications, ainsi que les exigences de sécurité pouvant être référencées par les CSA de l'organisation.

Plus précisément, le contexte d'affaires devrait pouvoir fournir les éléments suivants :

1) Une liste de tous les domaines d'activités se rapportant à toutes les parties de l'organisation dans laquelle une application fonctionnera ou sera utilisée;

2) Pour chaque domaine d'activité, une liste des processus, des politiques et des pratiques recommandées, qui ont trait au développement, à l'utilisation et à la maintenance d'applications dans ce domaine, telle que :
   a) la politique de sécurité de l'organisation;
   b) une liste des applications de l'organisation avec leur classification de sécurité respective;
   c) les processus et les meilleures pratiques utilisés dans l'organisation concernant la gestion d'affaires, la gestion de projet, l'analyse des risques, l'utilisation, la maintenance, la gestion du changement, les vérifications et les audits impliqués par ces applications;
   d) les méthodes et processus d'acquisition (développement, impartition, achats) utilisés par l'organisation;
   e) les processus et les meilleures pratiques de déploiement, de gestion, de maintenance, de vérification et de contingences de tous les composants répertoriés dans le contexte technologique;
   f) les meilleures pratiques pour tous les langages de programmation utilisés par les applications de l'organisation; et

g) les normes approuvées par l'organisation, comme notamment les normes internationales et les normes de l'industrie auxquelles l'organisation doit se conformer.

3) Une matrice de traçabilité des risques de SA contenant des références, entre autres, aux facteurs suivant :
   a) l'inventaire des groupes d'informations catégorisées concernant les applications de l'organisation;
   b) la source d'un risque des applications pouvant menacer un de ces groupes, comme notamment : un article de loi, une exigence fonctionnelle, une directive de l'organisation ou un composant TI;
   c) les risques de sécurité associés à une source de risques sur un groupe d'informations de par l'utilisation d'une application de l'organisation dans son environnement spécifique;
   d) les exigences de sécurité concernant ces risques;
   e) les CSA et processus mis en place pour rencontrer ces exigences afin d'atténuer les risques identifiés aux niveaux attendus;
   f) les rôles, les processus, les applications et les technologies impliqués dans la mise en place et l'utilisation des CSA et des processus de SA;
   g) la liste de risques de la SA introduits par les politiques, les meilleures pratiques et les procédés identifiés au préalable;
   h) la liste des exigences de sécurité à combler pour diminuer les risques identifiés et les ramener à un niveau acceptable par l'organisation.

XIII.4 Contexte juridique

À l'intérieur du CNO, le contexte juridique 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* XII.2.4).

Le contexte juridique peut avoir un impact direct sur les exigences de sécurité et les spécifications d'une application. Une organisation qui déploie une application sur plus d'un territoire pourrait avoir à répondre aux exigences de sécurité différentes pour chaque pays où elle intervient. Un cas concret : le 27 août 2009, « Facebook a accepté d'ajouter de nouvelles mesures de protection des renseignements personnels significatives et d'apporter d'autres modifications (à son application) à la suite d'une enquête menée par la commissaire à la protection de la vie privée du Canada concernant les politiques et pratiques en matière de protection des renseignements personnels du populaire site de réseautage social. » (Stoddart, 2009).

XIII.4.1 Objectifs visés par l'identification du contexte juridique d'une organisation

Le contexte juridique permet de définir un cadre normalisé pour aider l'organisation à réduire les risques de sécurité provenant d'une non-conformité aux lois et règlements du lieu où sera utilisée son application. Il intervient principalement dans l'approche de gestion de la sécurité d'une application, présentée par le modèle, pour permettre d'identifier et de réduire les risques associés aux différentes lois et régulations pouvant assujettir les applications de l'organisation ainsi que pour définir les exigences de sécurité provenant du contexte juridique qui seront référencées par les CSA de l'organisation.

XIII.4.2 Contenu du contexte juridique d'une organisation

Le contexte juridique comprend les lois, règles et règlements des pays ou territoires où les applications de l'organisation seront développées, déployées ou utilisées. L'organisation se doit de déterminer les exigences juridiques de sécurité nécessaires à l'atténuation des risques de non-conformité aux lois et règlements s'appliquant à ses applications.

Plus précisément, le contexte juridique devrait pouvoir fournir les éléments suivants :

1) Une liste des lois et règlements en vigueur aux endroits où les applications de l'organisation sont utilisées, incluant les documents contenant les articles de chacun d'eux;
2) La liste de risques de SA introduites par les articles de ces lois et de ces règlements;
3) Une liste des exigences juridiques de sécurité à combler pour diminuer les risques associés à chacun des articles sensibles afin de les ramener à un niveau acceptable par l'organisation.

XIII.5 Contexte technologique

À l'intérieur du CNO, le contexte technologique 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 infonuagique, etc., incluant les paramêtres, les règles et les pratiques recommandées pour leurs mises en place dans l'organisation *(Voir* XII.2.5).

Les personnes, processus et technologies associés à ces composants peuvent générer des risques de sécurité qui pourraient avoir un impact autant dans l'utilisation opérationnelle d'une application que dans des projets concernant notamment le développement, l'utilisation ou la maintenance d'applications de l'organisation.

XIII.5.1 Objectifs visés par l'identification du contexte technologique d'une organisation

Le contexte technologique permet de définir un cadre normalisé pour aider l'organisation à réduire les risques de sécurité provenant des composants des infrastructures technologiques et physiques supportant les applications de l'organisation. Comme pour les deux autres contextes, il est principalement utilisé par l'approche de gestion de la sécurité d'une application, présentée par le modèle, pour permettre d'identifier et de réduire les risques de sécurité provenant des technologies identifiées dans ce contexte, ainsi que pour définir les

exigences de sécurité provenant du contexte technologique qui seront référencées par les CSA de l'organisation.

XIII.5.2 Contenu du contexte technologique d'une organisation

Il contient la description des risques et des exigences de sécurité provenant notamment des personnes, des processus TI, des dispositifs technologiques et de l'information impliqués dans la mise en place et la gestion des technologies nécessaires au développement, à l'utilisation et à la maintenance de l'application. Ce contexte contient aussi les documents des normes, des règlements et des meilleures pratiques TI, imposées ou adoptées par l'organisation, et qui pourraient avoir un impact sur les projets d'applications.

Plus précisément, le contexte technologique devrait pouvoir fournir les éléments suivants :

1) Une liste des composants technologiques utilisés par les applications de l'organisation incluant la description de ces composants, de leurs paramètres de configurations ainsi que la description des processus et des acteurs reliés à chacun d'eux;
2) La liste des risques de SA introduits par ces composants technologiques; et
3) Une liste des exigences de sécurité à combler pour diminuer les risques identifiés et les ramener à un niveau acceptable par l'organisation.

XIII.6 Dépôt des spécifications et des fonctionnalités des applications

À l'intérieur du CNO, le dépôt des spécifications des applications 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* XII.2.6).

En plus de pouvoir décrire des caractéristiques de sécurité telles que la disponibilité, la confidentialité et l'intégrité d'une application ou de l'un de ses éléments, les spécifications pourront, entre autres, décrire comment l'application devra :

a) interagir avec d'autres systèmes;
b) répondre aux événements et aux menaces provenant de l'infrastructure d'opération dont elle dépend; et
c) fournir des mécanismes de contrôle, des interfaces et des informations concernant son intégrité et celle de ses transactions, ainsi que la liste des contrôles au sein de l'environnement d'exécution.

XIII.6.1 Objectifs visés par la mise en place du dépôt des spécifications et des fonctionnalités des applications de l'organisation

Le dépôt des spécifications et des fonctionnalités des applications permet de définir un cadre visant l'implémentation normalisé de certaines solutions dans les applications de l'organisation. Ces solutions peuvent être des fonctionnalités, des services et des spécifications considérés sensibles, dans lesquels des CSA ont déjà été intégrés, et dont les processus et les moyens de mise en place ont été identifiés comme des pratiques recommandées obligatoires par l'organisation.

La mise en place de ce dépôt permet à une l'organisation d'harmoniser les implémentations, l'utilisation, la maintenance et les vérifications des spécifications et des fonctionnalités de ses applications. Il réduit les risques de sécurité ainsi que les coûts pouvant provenir d'une mauvaise implémentation ou d'une mauvaise utilisation d'un service ou d'une fonctionnalité, ou encore d'une mauvaise compréhension d'une spécification à mettre en place.

Ce dépôt est principalement utilisé lors de la réalisation du processus de gestion de la sécurité d'une application, tel que présenté par le modèle (XIV.3), pour permettre la réutilisation de composants approuvés ou les CSA y auraient déjà été intégrés.

XIII.6.2 Contenu du dépôt des spécifications et des fonctionnalités des applications de l'organisation

Le dépôt des spécifications et des fonctionnalités des applications de l'organisation contient des solutions préapprouvées concernant des fonctionnalités, des services ou des spécifications jugés sensibles, dont l'organisation veut assurer la bonne mise en œuvre. Ces solutions ont été intégrées au dépôt parce qu'elles ont déjà été requises ou ont été implémentées par un projet d'application, et qu'elles sont maintenant soit offertes soit utilisées par une des applications de l'organisation.

Ces solutions peuvent être conservées sous forme de document, de code source ou de fichiers binaires. Elles peuvent notamment inclure des instructions, des documents de références ou encore des documents décrivant des spécifications générales, des processus, des directives, des exigences fonctionnelles et de conceptions associées aux solutions préapprouvées par l'organisation. Ces solutions peuvent aussi contenir ou référer à l'utilisation de produits, de fichiers de paramètres, de composants précompilés ou de librairies de code qui devront être utilisés dans l'implémentation ou la vérification d'une solution.

Plus précisément le dépôt des spécifications et des fonctionnalités des applications inclut les éléments suivants :

1) Une liste de toutes les fonctionnalités et services jugés sensibles par l'organisation, qui ont été intégrés ou sont offerts par les applications de l'organisation, incluant notamment les paramètres et les spécifications encadrant la mise en place, l'utilisation, la maintenance et la vérification de ces fonctionnalités et services, lorsque ces derniers doivent notamment identifier, autoriser l'accès, accéder, recevoir, calculer, stocker, protéger ou transférer de l'information;

2) Pour chaque fonctionnalité, spécification et service décrits, les éléments suivants seront définis :
   a) une liste des processus et des meilleures pratiques, appropriées et approuvées par l'organisation, qui décrivent les moyens et les façons de faire concernant leur mise en œuvre, leur utilisation, leur entretien et leur vérification;
   b) les fichiers ou les références vers des produits, les fichiers de paramètres, les composants précompilés, le code source, le code binaire ou la librairie de code nécessaire à la mise en place, l'utilisation, la maintenance ou la vérification de cette solution;
   c) une liste des risques de sécurité concernant cette fonctionnalité, spécification ou service, qui inclut sa classification; et
   d) une liste des exigences de sécurité et de CSA requis pour atténuer les risques identifiés.

Tout comme pour les autres éléments du CNO, ces solutions sont révisées et améliorées à l'aide du processus de gestion du CNO.

XIII.7 Dépôt des rôles, responsabilités et qualifications

D'entrée de jeux, Andres spécifie, dans son livre « Surviving security », que la grande partie des risques de sécurité provient des personnes (Andress, 2003), soit des acteurs tenant un rôle quelconque dans le développement ou l'utilisation d'une application. Le dépôt des rôles, responsabilités et qualifications constitue l'outil permettant de résoudre le problème.

Sachant qu'un rôle peut être tenu par des personnes ou par des processus, celui-ci réfère à un ensemble de responsabilités associées aux activités auxquelles ce rôle participe. Les qualifications requises pour pouvoir tenir un rôle doivent aussi être spécifiées dans l'inventaire, en fonction des responsabilités qui lui sont associées. La catégorisation d'un rôle se fait en fonction de la sensibilité des informations qui seront accédées ou manipulées par un acteur tenant un rôle précis pour une application précise.

Le dépôt des rôles, responsabilités et qualifications du CNO est un inventaire catégorisé des rôles impliqués dans au moins une des activités amenées par les applications de l'organisation..

XIII.7.1 Objectifs du dépôt des rôles, responsabilités et qualifications

Ce dépôt permet de conserver l'inventaire catégorisé de tous les rôles, afin de faciliter l'identification des rôles les plus à risque et de pouvoir ainsi y placer les contrôles nécessaires à leur diminution, lorsque nécessaire.

En outre, il contient l'ensemble des responsabilités et qualifications des rôles (personnes et processus) impliqués à un moment ou un autre dans une des activités du cycle de vie des applications de l'organisation, afin de pouvoir catégoriser ces rôles en fonction des risques de sécurité qu'ils présentent dans l'environnement d'une application spécifique. Avec ce dépôt, on peut aussi identifier rapidement ceux auxquels une exigence de sécurité ou un CSA doit être associé.

Il permet également de s'assurer de l'identification et de la description des éléments suivants :

1) Tous les rôles importants impliqués dans les processus et activités des projets d'application;
2) Leurs responsabilités respectives en fonction des activités auxquelles ils participent;
3) Les critères de qualification requis pour tenir ces rôles en fonction des niveaux de confiance existants dans La bibliothèque de CSA de l'organisation;
4) Les conflits d'intérêts possibles dès la définition des rôles afin que les responsabilités conflictuelles soient assignées à deux ou plusieurs rôles lorsque nécessaires.

Finalement, ce dépôt permet d'assurer que les personnes désignées à chacun de ces rôles sensibles, pour un projet d'application spécifique, possèdent les qualifications et les

connaissances requises pour comprendre la portée et pleinement assumer les responsabilités qui lui sont assignées.

Par exemple, le rôle de réviseur de code java est défini par le dépôt des rôles du CNO de l'organisation. Pour les applications auxquelles on a assigné un niveau de confiance de 0 à 4, soit la majorité des projets d'applications dans l'organisation, tout développeur Java ayant lu les directives de programmation sécuritaire en Java de l'organisation est autorisé à tenir ce rôle et à effectuer le travail de révision de code. Par contre, l'organisation a émis une directive de sécurité spécifiant qu'un développeur Java ne peut, en aucune circonstance, réviser le code qu'il a lui-même écrit. De plus, si le niveau de confiance « 5 » ou plus élevé est assigné à une application, les qualifications requises par les personnes qui seront autorisées à tenir le rôle de réviseur pour ce projet ne consisteront plus uniquement à prendre connaissance des directives. Ils devront également avoir une expérience d'au moins 5 ans en programmation Java, détenir la certification processionnelle GSSP-JAVA[54] et avoir tenu ce rôle pour au moins 10 projets de révision de code pour des applications dans cette organisation.

XIII.7.2 Contenu du dépôt des rôles, responsabilités et qualifications

Ce dépôt contient notamment, les listes et les descriptions de tous les rôles, les responsabilités et les qualifications professionnelles nécessaires qui leur sont associées, pour chacun des niveaux de confiance présent dans La bibliothèque de CSA de l'organisation.

Cet ensemble de rôles comprend :

1) les acteurs impliqués dans la création, le maintien et la vérification du CNO et des CSA de l'organisation; ainsi que

---

[54] Certification processionnelle « Secure Software Programmer-Java » donnée par le « Global Information Assurance Certification », http://www.giac.org

2) les acteurs impliqués dans le cycle de vie des applications de l'organisation. Par exemple, les responsables de la sécurité de l'information, les chefs de projet, les administrateurs, les responsables des achats, les responsables du développement de logiciels, les propriétaires d'applications, les gestionnaires, les architectes, les analystes, les programmeurs, les testeurs, le personnel technique des administrateurs systèmes aux administrateurs de bases de données, incluant les administrateurs de réseaux.

Finalement, la mise en place de ce dépôt exige que le comité du CNO se dote d'une politique qui forcera l'organisation à s'assurer que tous les rôles impliqués dans les processus et les activités, existants dans le cycle de vie d'une application sensible, soient identifiés et que leur assignation à des personnes ne se réalise qu'à la suite de la vérification des qualifications exigées.

XIII.8 Dépôt des groupes d'informations catégorisés

À l'intérieur du CNO, le dépôt des groupes d'informations catégorisés contient l'inventaire des groupes d'informations catégorisés, liés aux applications de l'organisation qui peuvent devoir être protégés, ainsi que les noms des processus et les responsabilités des acteurs qui peuvent y avoir accès (Voir XII.2.7).

XIII.8.1 Objectifs du dépôt des groupes d'informations catégorisés

Les principaux objectifs visés par la mise en place d'un dépôt des groupes d'informations catégorisés sont de :

1) conserver un inverntaire tous les groupes d'informations catégorisés, utilisés par les aplications de l'organisation;
2) optimiser le processus de catégorisation de la sensibilité des groupes d'informations de l'organisation en réutilisant, lorsque applicable, les résultats des évaluations précédentes de groupes d'informations déjà catégorisés;

3) assurer une cohérence dans l'évaluation de la sensibilité des groupes d'informations utilisés par les aplications de l'organisation;
4) s'assurer que tous les groupes d'informations identifiés ont bien été catégorisés; et
5) identifier, pour chaque groupe d'informations catégorisé,
   a) le type du groupe d'informations auquel il appartient (*Voir XII.2.7*);
   b) les processus (de l'organisation et de l'application) ainsi que les responsabilités des rôles des acteurs qui y ont accès; et
   c) les médiums par lesquesl ils sont transférés ou conservés
   d) les risques et les exigences de sécurité des applications qui s'y réfèrent (*Voir* XII.2.8).

XIII.8.2 Contenu du dépôt des groupes d'informations catégorisés

Le modèle propose une structure d'information permettant de décrire un dépôt des groupes d'informations catégorisés.

1) Nom, identifiant et description du groupe d'information;
2) Nom du propriétaire du groupe d'information;
3) Catégorisation,
   a) Valeur de l'intégrité, la disponibilité, la confidentialité;
   b) Valeur monétaire (ex. valeur de la perte, ou coût pour retrouver l'information);
   c) Doit être archivé (ex.: oui/non, durée);
   d) Liste des dates et noms des responsables des précédentes évaluation;
4) Références,
   a) Type de groupe d'informations;
   b) Liste des groupes parents auquels ce groupe d'informations appartient;
   c) Liste des sous-groupes (enfants) contenu dans ce groupe d'information;
   d) Liste des risques et des exigences de sécurité liés à ce groupe d'information;
      i) Exigences (identifiant, nom, catégorie, type,
   e) Liste des applications liées à ce groupe d'informations;
      i) Liste des processus liés à ce groupe d'informations (entrée/sortie);

ii) Liste des responsabiltiés des rôles liés à ce groupe d'informations et des droits d'accès;
iii) Liste des emplacements ou ce groupe d'informations est conservé (addresse postale, nom du serveur, Système de gestion de base de données (SGBD), etc.).

XIII.9 Contrôle de sécurité des applications (CSA)

Le contrôle de la sécurité des applications (CSA) est un des composants centraux du modèle. Étant normalisé et vérifiable il permet, notamment, de décrire des activités de sécurité et de vérification, et 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 dans la réalisation ou l'opération d'une l'application.

Comme nous l'avons déjà mentionné, le composant « contrôle de sécurité » n'est pas nouveau (*Voir* XII.2.10). Ce qui est nouveau, c'est que pour être en mesure de respecter le principe « La SA doit pouvoir être démontrée » amené par le modèle (*Voir* 5.7.5), le CSA ne décrit plus seulement l'activité de sécurité à réaliser pour diminuer un risque à un niveau acceptable, mais il précise aussi les résultats attendus par la réalisation de l'activité de sécurité. De plus, il demande de définir l'activité vérification de la mesure qui sera appliquée à ce contrôle pour s'assurer que les résultats attendus sont bien ceux obtenus. Ces résultats seront conservés comme preuve de la mise en place et du bon fonctionnement du CSA concerné.

La Figure-A XIII-2 montre que le CSA fournit, à l'équipe de projet d'une application, une activité de sécurité à réaliser (permettant de réduire un risque de sécurité spécifique), et à l'équipe de vérification, une activité de vérification de la mesure à réaliser (permettant de confirmer que l'activité de sécurité a été réalisée avec succès, fournissant les preuves à l'appui). Le CSA permet donc de produire les résultats attendus requis pour fournir les preuves nécessaires à l'évaluation du succès de son implémentation et de l'atténuation désirée des risques ciblés.

Parce que l'ensemble des CSA sélectionnés pour un projet d'application, identifié par le niveau de confiance ciblé, provient directement de l'analyse des risques de sécurité de l'application concernée, l'organisation sait à l'avance qu'une fois leur mise en place complétée et vérifiée, ces CSA répondront aux exigences de sécurité amenées par l'utilisation de l'application, et permettront à l'organisation de fournir les justifications attendues, nécessaires à la déclaration de la sécurité de l'application.

Notons que pour les organisations utilisant le concept de cas d'assurance (ISO/IEC, 2010f), les CSA seront utiles pour simplifier la gestion des preuves et fournir en temps utile les éléments et les arguments nécessaires supportant les allégations de la sécurité d'une application. De plus, les processus proposés par le modèle pour la création, l'approbation, l'utilisation, la vérification de la mesure et ainsi que l'audit d'un CSA, permettront à l'organisation de fournir, de façon constante et répétitive, les preuves et arguments prévus pour soutenir les allégations d'atténuation des risques de sécurité au niveau de confiance ciblé.

XIII.9.1 Objectifs du CSA

Le principal objectif visé par la mise en place et l'intégration, dans le CNO, de CSA qui auront été préalablement approuvés par l'organisation, consiste à définir des activités de sécurité répétables et vérifiables qui ont été conçues, validées, qui pourront être mises en place et qui devront être vérifiées afin de pouvoir produire les résultats attendus. Ces résultats sont considérés comme étant les preuves requises servant à démontrer la réponse adéquate aux exigences de sécurité concernées et, ultimement, à l'atteinte d'un niveau de confiance ciblé pour une application. La définition formelle des éléments décrivant les activités d'un CSA permet de s'assurer que leur réalisation produira les mêmes résultats attendus, pour toutes les applications où elles seront mises en place.

Encadré durant sa conception, son développement, sa vérification et sa validation par le processus de Gestion du CNO (*Voir* XIV.1), puis encadré durant son implémentation et sa

vérification par le processus de Gestion de la SA (*Voir* XIV.3) le CSA permettra aussi à l'organisation d'identifier et d'augmenter la maturité de ses processus et activités sensibles jusqu'à les rendre complets, performants, gérables, définis, quantitativement gérés et optimisés (CMMI, 2006, p. 32).

Plus précisément, la bonification du contrôle de sécurité, qui a mené à la création et à l'intégration du composant « CSA » dans le modèle SA, permet d'aider une organisation à concevoir et à mettre en place des CSA qui pourront être :

1) Appliqués à un processus, à un composant technologique ou à un composant de l'application;
2) Sélectionnés en fonction des priorités, des exigences de SA prioritaires, des capacités et des impacts acceptables de leur mise en place;
3) Réutilisables, en identifiant la ou les exigences de sécurité auxquelles ils répondent, ainsi que l'environnement de l'application;
4) Validés, en s'assurant que les activités réalisées, que les résultats produits et que les impacts résiduels répondent adéquatement aux exigences de sécurité de ses applications, et ce, en fonction du niveau de confiance ciblé;
5) Vérifiables, en s'assurant que la réalisation de chaque activité de sécurité et de vérification soit en mesure de produire les résultats attendus;
6) Répétables, en précisant les descriptions du « qui », « quoi », « où », « quand » et « comment » des activités à réaliser, incluant la vérification des rôles, des responsabilités et des qualifications professionnelles des acteurs impliqués dans leur mise en place;
7) Approuvés, en s'assurant que les CSA qui ont été conçus et validés, pourront être mis en place, devront être vérifiés et audités;
8) Un vecteur d'amélioration de la maturité des processus de SA de l'organisation.

Les principaux objectifs visés par la mise en place d'un CSA sont de :

1) Diminuer à un niveau acceptable les risques de sécurité pouvant menacer l'information impliquée par l'utilisation d'une l'application;

2) Réaliser les mêmes activités de sécurité qui produiront les mêmes résultats attendus, pour les mêmes exigences de sécurité visant un même niveau de confiance;
3) Prévoir et fournir les preuves, les résultats attendus nécessaires à la démonstration de l'atteinte de la diminution des risques de sécurité concernés.

Afin de rencontrer ces objectifs, un CSA pourra être utilisé afin de :

1) Sécuriser un composant d'application, soit un logiciel, des données, un COTS, ou encore un composant de l'infrastructure technologique;
2) Sécuriser un processus utilisé à un moment ou à un autre du cycle de vie de l'application;
3) Vérifier un rôle, ses responsabilités, ses conflits d'intérêts, ainsi que les qualifications professionnelles requises pour pouvoir prendre ces responsabilités;
4) Déterminer le processus de mesure et d'évaluation des critères d'acceptation requis pour la vérification des composants ou des processus; et
5) Aider à déterminer le niveau de confiance actuel (mesuré) de l'application.

Les objectifs et les processus de mesure sur lesquels s'appuie le CSA, pour définir et mesurer son rendement et ses résultats (diminution du risque vs coûts), sont basés sur les principes du cadre de mesure du rendement, développé par Kaplan et Norton (Kaplan et Norton, 1996). Selon ces principes, la performance d'un CSA sera déterminée en fonction des critères suivants, soit que l'organisation doit :

1) S'assurer que la vision et la stratégie visées pour répondre à un besoin de sécurité
   a) soient claires, qu'elles permettent de diminuer les risques concernés à un niveau acceptable par l'organisation, et qu'elles produisent des activités précises, vérifiables et acceptables par les acteurs impliqués;
   b) soient valables, afin d'assurer la mesure des bons critères.
2) Concentrer l'attention des acteurs sur ce qui importe le plus pour le succès de leurs activités;
3) Permettre la mesure des activités effectuées ainsi que celle des réalisations (résultats attendus);
4) Fournir un langage commun pour faciliter la communication et éviter les ambigüités;

5) S’assurer que le CSA est vérifiable, pour assurer l'exactitude de la collecte de donnée.

XIII.9.2 Contenu du CSA

Le modèle propose une structure d'information permettant de décrire un CSA, qui devra être effectué à un moment précis du cycle de vie de l'application. Tel que présenté dans la Figure-A XIII-2, cette structure permet d’exprimer les quatre principaux groupes d’informations contenus dans un CSA, et qui sont nécessaires à sa description, son utilisation et sa vérification, soit :

1) Le ou les niveaux de confiance auxquels il est assigné;
2) Le ou les exigences de sécurité auxquelles il s’adresse;
3) L’activité de sécurité; et
4) L’activité de vérification de la mesure.

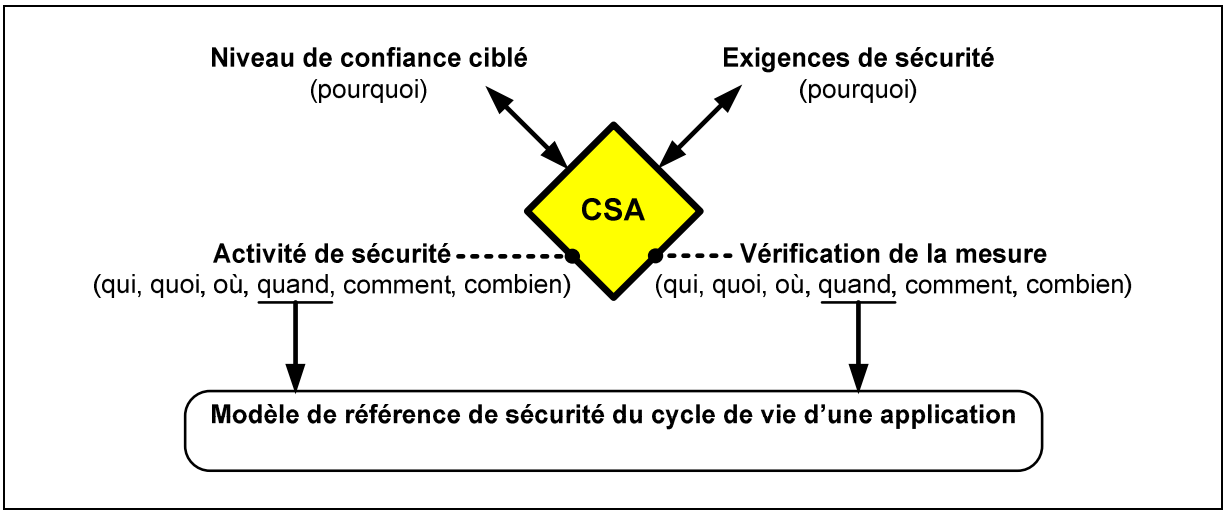


Figure-A XIII-2 Le contrôle de sécurité de l'application
Traduite et adaptée de (ISO/IEC, 2011d)

Ces groupes d’informations peuvent être divisés en deux catégories. La première répond à la question « Pourquoi ce CSA existe-t-il dans l’organisation? », la deuxième répond à la question « Qui fait quoi? ».

Dans un premier temps, lors de la conception d'un CSA, les experts doivent obligatoirement indiquer pourquoi ce CSA a été intégré au CNO, c'est-à-dire, quels sont :

1) le ou les niveaux de confiance concernés par celui-ci; et
2) les exigences de sécurité auxquels ce CSA répond incluant le type, la catégorie ainsi que le contexte auxquels sont associées ces exigences.

Dans un deuxième temps, les experts doivent définir et préciser le contenu de l'activité de sécurité et celui de la vérification de la mesure, soit :

1) L'activité de sécurité identifie l'acteur qualifié et précise la façon de mettre en place le contrôle de sécurité ; tandis que
2) l'activité vérification de la mesure du CSA identifie l'acteur qualifié et précise la façon de vérifier la preuve que l'activité de sécurité a été effectuée correctement et que les résultats attendus ont bien été obtenus.

Selon ce qui est requis, chacune de ces deux activités peut fournir les informations suivantes :

1) Qui – Les noms des rôles impliqués, incluant leurs responsabilités[55] (RASCI) et les qualifications respectives requises pour réaliser adéquatement l'activité. L'organisation doit s'assurer que les qualifications professionnelles requises pour chaque rôle/responsabilité sont acquises par les acteurs concernés et que le principe de la séparation des tâches est respecté. Un CSA pourrait être rédigé dans le but de vérifier les qualifications professionnelles requises par une personne pour pouvoir être assignées à un rôle;
2) Quoi – La description complète de l'activité, incluant les artéfacts et les résultats mesurables attendus (objectifs) produits par l'activité incluant, l'unité de mesure, la qualité des données et les seuils d'approbation;

---

[55] Basé sur la matrice des responsabilités RACI : *Responsable, Accountable, Consulted* et *Informed*.

3) Où – L'endroit où sera appliqué l'activité, telle que le code source, les paramètres d'application, un composant de l'application, un processus, sur un composant du serveur ou un composant du poste client;
4) Quand – Un identifiant et un attribut[56] pointant sur le nom d'une activité spécifique ou une description indiquant que l'activité du CSA sera réalisée soit avant, pendant ou après une activité spécifique modèle du cycle de vie de l'application (*Voir* Figure-A XIII-6);
5) Comment – La méthode et les outils utilisés pour mettre en place, ou vérifier ce CSA et obtenir les artéfacts désirés incluant, si nécessaire, la périodicité, la fréquence ou les événements qui déclencheront l'activité de vérification; et
6) Combien – Une estimation du coût de réalisation de l'activité qui pourra inclure, par exemple, des efforts en jours/personne, des coûts d'acquisition, d'utilisation, de location ou de services externes. Cette estimation, qui peut être révisée si nécessaire, aidera l'organisation à évaluer et à approuver le coût de la sécurité d'un projet d'application ou d'une offre de services, pour le niveau de confiance visé.

Finalement, le contenu d'un CSA, inclura aussi certaines informations de gestion telles que :

1) Son nom, son numéro d'identifiant original, son numéro d'identifiant unique donnés par l'organisation qui en a fait l'acquisition, son numéro de version, sa description et son objectif de sécurité;
2) Le nom et les coordonnées de l'auteur ainsi que la date de publication du CSA;
3) Des pointeurs, soit des numéros d'identifiant original ou des numéros d'identifiant unique donnés par l'organisation, des CSA parents et enfants du CSA concernés. Un CSA peut être représenté comme une structure de graphe (*Voir* Figure-A XIII-3);

---

[56] Les valeurs possibles de l'attribut de l'information quand sont : « BEFORE », « DURING », et « AFTER »

4) Les noms, coordonnées, date et signature électronique du propriétaire ainsi que des différents acteurs impliqués dans la gestion du CSA, durant toutes les phases de son cycle de vie soit :
    a) demande de création;
    b) conception;
    c) validation;
    d) développement;
    e) vérification;
    f) approbation;
    g) approbation finale;
    h) publication pour formation;
    i) actif; et
    j) expiré.

La Figure-A XIII-3 montre un exemple de cette relation graphique, dans laquelle un ensemble de CSA sont reliés entre eux sous la rubrique «paiement en ligne". Dans cet exemple, tous les CSA relatifs au paiement en ligne peuvent être utilisés comme un ensemble unique et cette complexité peut être dissimulée, si nécessaire.

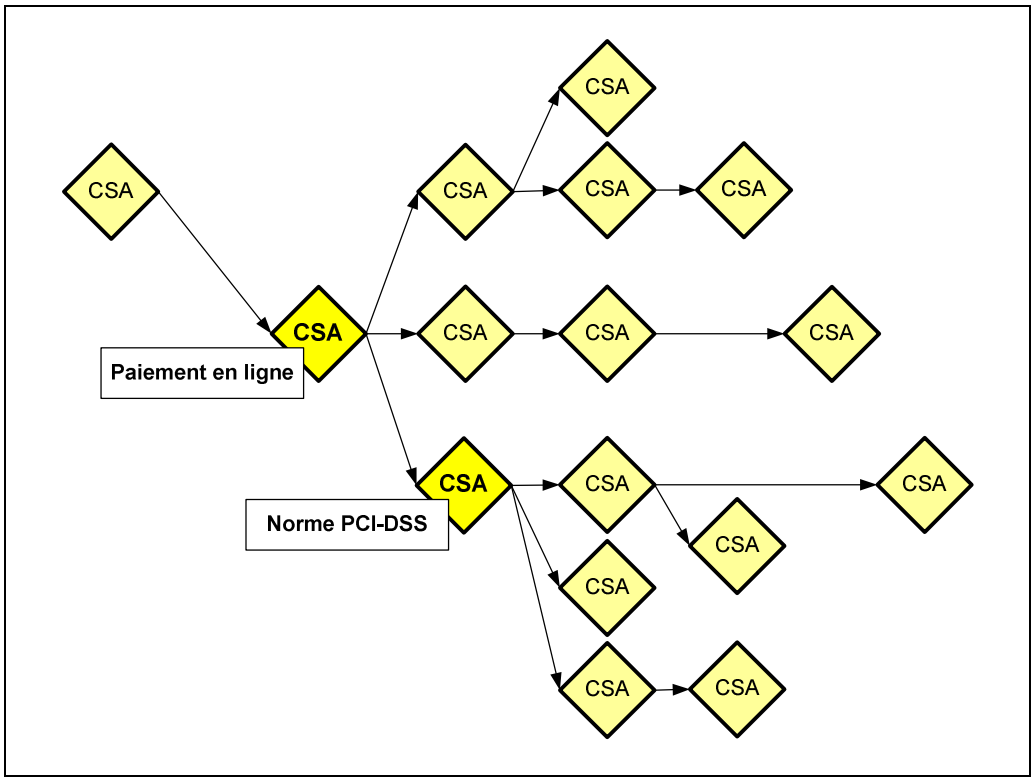


Figure-A XIII-3 Exemple de graphe de CSA
Traduite et adaptée de (ISO/IEC, 2011d)

Les CSA peuvent être liés ensembles dans un graphe, de sorte qu'une fois l'activité d'un CSA est effectuée, elle peut être suivie par les activités des CSA enfants. Cette caractéristique du CSA est utile pour :

a) Fournir uniquement les informations pertinentes aux différents acteurs, en dissimulant la complexité inutile;
b) Faciliter la communication en regroupant les CSA pertinents dans les rubriques et en utilisant un vocabulaire approprié. Par exemple, en utilisant un langage d'affaires pour communiquer avec des gestionnaires;
c) Favoriser la distribution des CSA en les regroupant en ensembles connexes;
d) S'assurer que toutes les activités de sécurité dans les CSA liées sont effectuées et qu'aucune n'a été oubliée.

Ce graphe de CSA permet de mettre en œuvre le concept de relation de confiance directe et indirecte (Pavlidis et al., 2012) afin d'obtenir un niveau de confiance acceptable que les risques visés par ce CSA ont été adéquatement atténué, basé sur le fait que tous les CSA requis ont tous été implémentés et vérifiés avec succès.

Le contenu de tous les CSA intégré au CNO doit préalablement avoir été approuvé par l'organisation.

XIII.9.3 Schéma XML du CSA

Un schéma XML a été développé pour préciser de manière formelle tous les attributs du CSA afin de pouvoir y intéger les éléments définis à l'annexe XIII.9.2. (*Voir* l'appendice A – ANNEXE XIII.12.3 pour plus de détails.)

XIII.10 Bibliothèque de contrôles de sécurité des applications

Selon le modèle, l'organisation doit commencer à se définir une bibliothèque dès l'approbation et la mise en place de ses premiers CSA. Dès ce moment, cette bibliothèque sera utilisée pour répertorier, documenter, regrouper et classer tous les CSA approuvés par l'organisation.

La Figure-A XIII-4 présente un exemple simple d'une bibliothèque de CSA d'une organisation. L'organisation qui a mis en place cette bibliothèque de CSA développe des applications dans le domaine de l'aéronautique. La bibliothèque contient tous les contrôles de sécurité que l'organisation a besoin pour atténuer les risques de sécurité pouvant provenir de l'implémentation des fonctionnalités de l'application, des normes, des lois et règlements applicables à l'environnement d'utilisation de l'application et, finalement, pour s'assurer de mettre en œuvre les pratiques recommandées s'appliquant à ces contextes.

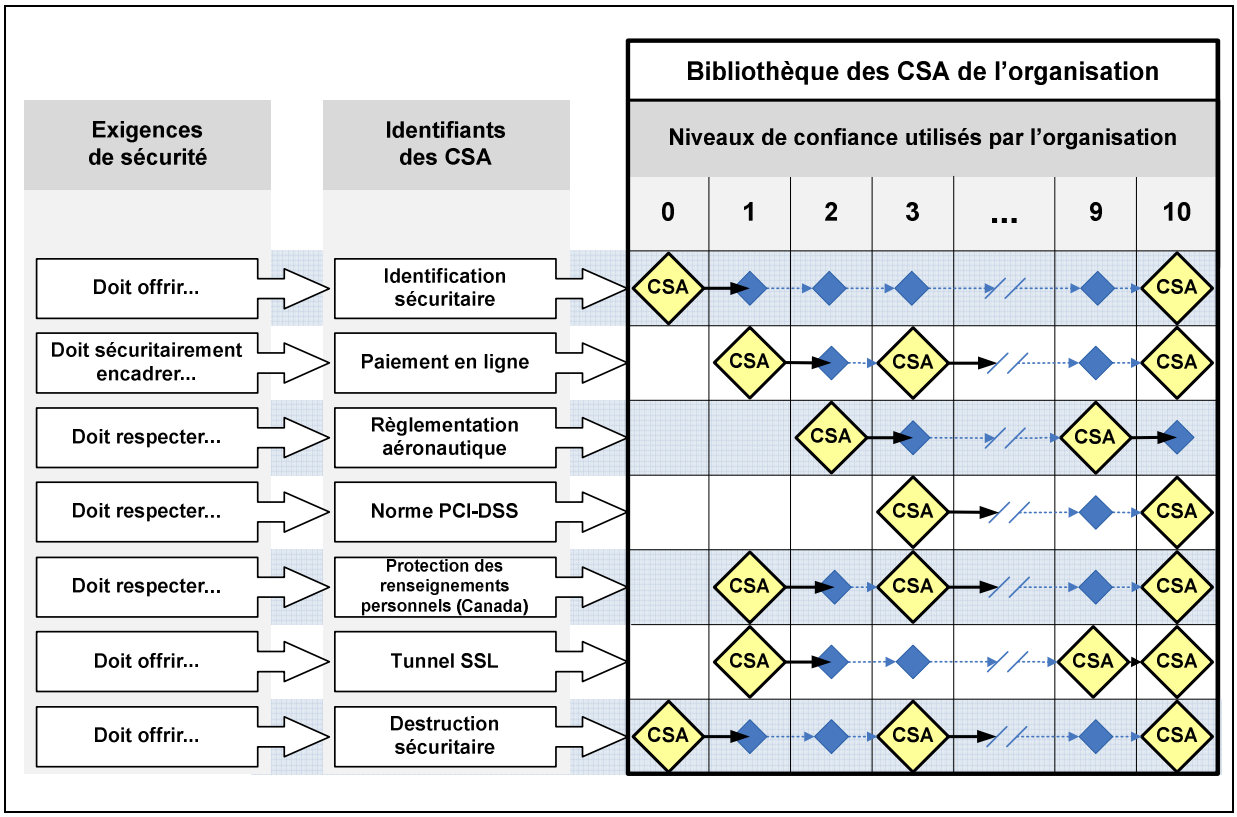


Figure-A XIII-4 Représentation graphique sommaire d'un exemple de la bibliothèque de CSA d'une organisation
Traduite et adaptée de (ISO/IEC, 2011d)

Dans cet exemple, l'organisation a défini onze niveaux de confiance, qu'elle a nommée respectivement de « 0 » à « 10 » indiquant que plus la valeur du nom du niveau est petite, plus le niveau de confiance associé à ce niveau est faible. Puis une directive a été émise spécifiant que toutes les applications de l'organisation doivent minimalement être conformes au niveau « 0 ». Ceci implique que l'implémentation des CSA de ce niveau doit obligatoirement avoir été effectuée et vérifiée pour les applications utilisées par l'organisation.

Plusieurs risques de sécurité inacceptables, provenant de l'environnement des applications, ont été identifiés. Le moyen d'atténuer ces risques a été défini par des exigences de sécurité, qui identifient les CSA à mettre en place. Par exemple, désirant que certaines de ses applications offrent un service de paiement en ligne sécuritaire, l'organisation a décidé de

définir trois CSA associés à cette fonctionnalité. Un premier CSA associé aux niveaux 1, 2 et 3, devra être mis en place dans toute application qui aura à gérer des transactions de moins de 100 $. Un deuxième CSA associé aux niveaux 4 à 9 devra être mis en place dans toute application qui aura à gérer des transactions entre 100$ et 1 000$. Puis finalement, un troisième CSA associé au niveau 10, niveau plus sécuritaire, mais plus compliqué à mettre en place, devra être implémenté dans toute application qui aura à gérer des transactions de plus de 1 000 $.

Désirant que certaines de ses applications soient autorisées à accepter des paiements par cartes de crédit VISA et MasterCard et sachant que le standard PCI DSS[57] est exigé par ces deux compagnies (LLC, 2010), l'organisation a défini une exigence de sécurité, et a décidé de mettre en place deux CSA pour assurer la conformité de ces applications à cette norme. Un premier CSA, associé au niveau 3, qui concerne les paiements par carte de crédit de moins de 1 000 $ et un deuxième, de niveau 10, pour les transactions de 1 000 $ et plus.

Tout territoire est assujetti à des lois ou à des règlements. Le contexte juridique permet d'identifier des risques et des exigences afin de regrouper les CSA qui permettront de démontrer la conformité aux lois et règlements des pays où sera utilisée l'application.

Finalement, désirant que certaines informations sensibles transmises et conservées par une application soient adéquatement protégées, l'organisation a défini des CSA qui devront être intégrés aux fonctionnalités de « communications chiffrées » et de « destruction sécuritaire de données », imposant l'implémentation et l'utilisation du protocole de connexion SSL ainsi qu'un mécanisme utilisant une méthode approuvée d'effacement sécuritaire de fichiers.

Cet exemple montre que l'identification et l'analyse des risques de sécurité provenant autant des spécifications et des fonctionnalités des applications de l'organisation, que des contextes

---

[57] PCI Data Security Standard (PCI DSS), développé par le PCI Security Standards Council.

d'affaires, juridiques et technologiques où sont utilisés les applications de l'organisation, a servi pour déterminer le contenu de La bibliothèque de CSA de l'organisation.

XIII.10.1 Objectif de La bibliothèque de CSA de l'organisation

La mise en place d'une bibliothèque de CSA et de ses niveaux de confiance vise à faciliter la sélection, la communication et la réutilisation de plans de sécurité normalisés devant s'appliquer aux applications de l'organisation.

Lorsqu'un niveau de confiance est associé à une application, cela permet de sélectionner les CSA qui doivent être mis en place pour diminuer les risques de son utilisation à un niveau acceptable. Associer un niveau de confiance à une application revient à identifier un plan de sécurité préapprouvé, précis, qui doit être réutilisé pour toutes les applications de l'organisation associées à ce niveau.

XIII.10.2 Contenu de la bibliothèque de CSA de l'organisation

La bibliothèque de CSA (*Voir* Figure-A XIII-4) peut être représentée comme un tableau contenant des colonnes correspondant à trois groupes d'informations :

1) Les risques de sécurité provenant de l'environnement de l'organisation et des spécifications de l'application;
2) Les exigences de SA précisant comment les risques de sécurité identifiés doivent être atténués;
3) Les niveaux de confiance utilisés par l'organisation pour identifier les différents niveaux de sécurité définis pour ses applications; et
4) Les CSA répondant aux exigences de sécurité et associés au niveau de confiance.

XIII.10.2.1 Exigences de sécurité des applications contenues dans la bibliothèque

Les exigences de SA forment un premier groupe d'informations contenues dans la bibliothèque. Il contient les exigences provenant des sources de risques, des contraintes ou des spécifications associées à une ou plusieurs applications de l'organisation. Ces exigences de SA ont été définies par l'organisation comme étant les objectifs vérifiables de la diminution d'un ou de plusieurs risques de sécurité. De fait, chacune de ces exigences doit être associée à au moins un risque de sécurité et doit conduire à la mise en place d'au moins un CSA servant à diminuer les risques identifiés à un niveau acceptable.

De cette façon, dès qu'un contexte, un risque ou une exigence change, il est facile d'identifier les CSA qui sont impactés par ce changement, puis de réaliser les actions nécessaires, soit notamment : d'évaluer le risque amené par ce changement, de créer et de faire approuver une nouvelle version des CSA concernés afin d'atténuer ce nouveau risque de sécurité à un niveau acceptable puis, à l'aide de la matrice de traçabilité (*Voir XIII.11*), d'identifier les applications ou ce nouveau CSA devra être mis en place.

Afin d'en faciliter le classement et la maintenance, les exigences de sécurité devraient aussi être réparties en sous-groupes. Par exemple, ils pourraient être simultanément regroupés par fonctionnalités et par objectifs de sécurité (*Voir* Figure-A XII-6), mais aussi par catégories, niveaux et types d'exigences (*Voir* Figure-A XII-6).

XIII.10.2.2 Nom du CSA

Le nom du CSA forme un deuxième groupe d'informations contenues dans la bibliothèque. Il contient notamment les informations nécessaires à l'identification et à la validation de l'intégrité de chacun des CSA contenus dans la bibliothèque.

XIII.10.2.3 Niveaux de confiance contenus dans la bibliothèque

Les niveaux de confiance utilisés par l'organisation sont le moyen privilégié par le modèle pour regrouper les CSA d'une organisation. L'association « CSA ←→ NdC » permet d'identifier rapidement, et sans ambigüité, la liste des CSA qui devront être mis en place par une équipe de développement, ou qui seront identifiés dans l'appel d'offres aux fournisseurs. Ce regroupement de CSA par « niveau de confiance » servira aussi pour informer les gestionnaires du degré de sécurité obtenu à partir d'un ensemble particulier de contrôles afin d'en faciliter l'approbation.

Toute organisation qui désire mettre en place le modèle devra définir sa propre série de niveaux de confiance. C'est le comité du CNO qui est responsable de nommer, de définir et de maintenir ces niveaux en fonction des besoins de sécurité de l'organisation pour ses applications.

Lors de la création d'une bibliothèque, le modèle recommande de définir un niveau de confiance minimal acceptable qui s'appliquera par défaut à toutes les applications de l'organisation auxquelles aucun niveau de confiance n'aura été assigné au préalable. Ce niveau de base identifie la liste minimale de CSA qui doit être obligatoirement appliquée à toute application utilisée par l'organisation. Ce niveau est représenté dans la Figure-A XIII-4 par le niveau de confiance « zéro ». Une organisation peut utiliser n'importe quel nom pour ce niveau de confiance.

La Figure-A XIII-4 montre qu'une organisation peut définir plusieurs niveaux de confiance et qu'un même CSA peut être associé à plusieurs de ces niveaux. Une fois intégré à la bibliothèque, tout CSA doit être assigné à au moins un niveau de confiance. Si des CSA sont associés à un niveau de confiance qui a été identifié comme un niveau faible, c'est qu'une fois qu'ils auront tous été mis en place et vérifiés, leurs actions combinées permettront d'offrir un niveau de protection limité à l'information de l'application concernée. Si un niveau de confiance est identifié à un niveau élevé, c'est qu'une fois que les CSA qui y sont

associés auront tous été mis en place et vérifiés, leurs actions combinées permettront d'offrir un niveau de protection beaucoup plus important pour l'information sensible de l'application concernée.

L'identification d'un niveau de confiance cible pour une spécification ou une contrainte spécifique, revient à sélectionner un CSA qui, s'il est mis en place, permettra de diminuer le risque qu'il concerne à un niveau qui a déjà été accepté par l'organisation. Par exemple, si le niveau de confiance « 5 » a été ciblé pour une application, et que celle-ci offre une fonctionnalité de paiement en ligne, on est a même de pouvoir identifier le CSA qui devra être mis en place. La sélection d'un niveau de confiance cible, pour l'ensemble de l'environnement d'une application, revient à sélectionner la liste des CSA présents dans la colonne. La mise en place des CSA associés à cette liste devient l'objectif de sécurité de l'équipe de projet de l'application. De plus, cette même liste de CSA devient, pour l'équipe de vérification, la portée de son audit, soit l'ensemble des contrôles à auditer pour vérifier la sécurité d'une application.

La bibliothèque ne demande pas nécessairement de développer des niveaux de confiance progressifs, mais exige que chaque niveau de confiance défini identifie une liste précise de CSA. Par exemple, une petite organisation qui possède un processus de classification de ses informations de 1 à 4, pourrait créer ses niveaux de confiance en fonction de ces critères, tel que présenté dans le Tableau-A XIII-1.

Tableau-A XIII-1 Exemple de niveaux de confiance d'une bibliothèque des CSA pour l'organisation ABC inc.

Niveaux de confiance		
Identifiant	**Nom**	**Description**
ABCinc_Min	Minimum	Application qui n'a été associée à aucun niveau de confiance.
ABCinc_A	A	Application possédant des informations classifiées 1 et 2, reliée à l'internet.
ABCinc_B	B	Application possédant des informations classifiées 3 et 4, reliée à l'internet.
ABCinc_C	C	Application possédant des informations classifiées 1 et 2, sans lien à l'internet.
ABCinc_D	D	Application possédant des informations classifiées 3 et 4, sans lien à l'internet.

Sachant que la mise en place et la vérification de tout contrôle ont un coût, et qu'un contrôle plus simple sera généralement moins dispendieux à implémenter qu'un contrôle plus complexe ou plus sécuritaire, une organisation sera en mesure de se servir des niveaux de confiance qu'elle aura définis pour gérer les coûts de la sécurité de ses applications.

XIII.11 Matrice de la traçabilité de la sécurité des applications de l'organisation

Toute organisation qui désire pouvoir démontrer que l'application qu'elle utilise maintient le niveau de confiance ciblé, doit être en mesure de détecter et de réagir à tout changement concernant les risques de sécurité présents dans l'environnement de cette application. Cette réaction vise ultimement à s'assurer que les CSA en place atténuent toujours adéquatement tous les risques de sécurité. Sinon, l'organisation se doit d'appliquer les changements requis aux CSA concernés puis de les redéployer dans l'application.

Le 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 se nomme « matrice de traçabilité » de la SA de l'organisation.

Les liens reliant les risques de sécurité jusqu'aux CSA de l'application sont conservés dans une matrice qui se définit comme suit :

1) Toute application de l'organisation est assignée à un niveau de confiance qui identifie les CSA devant y être appliqués (Figure-A XIII-4);
2) Tout CSA est assigné simultanément à un ou plusieurs niveaux de confiance, et à une ou plusieurs exigences de sécurité (Figure-A XIII-2);
3) Toute exigence décrit un besoin d'atténuation d'un ou plusieurs risques de sécurité présents dans l'un des environnements des applications de l'organisation ou amenés par une des spécifications de l'application (Figure-A XII-6).

XIII.11.1 Objectif visés par la matrice de traçabilité

La mise en place de la matrice de traçabilité de la SA d'une organisation permet de démontrer le maintien des niveaux de confiance ciblés pour chacune des applications, et ce, en fonction des risques de sécurité actuels qui les menacent. Elle permet de garder un lien précis entre un risque de sécurité, les CSA qui les atténuent et les applications impactées par ces risques. L'objectif est de pouvoir mettre à jour et de redéployer efficacement les nouveaux CSA dans les applications impactées par la détection de tout nouveau risque de sécurité afin de répondre aux exigences de SA et de maintenir l'atteinte des niveaux de confiance ciblés.

Par exemple, dès qu'un risque de sécurité change ou qu'un nouveau risque est détecté, que ce soit à la suite d'une modification d'un article de loi ou à l'ajout d'un nouveau composant technologique, ce nouveau risque sera évalué afin d'amener, si nécessaire, les ajustements correspondant aux exigences de sécurité qui s'y réfèrent. Ces changements peuvent à leur tour amener des modifications aux CSA qui ont été mis en place, ou plus encore, la création et la mise en place de nouveaux CSA permettant l'atténuation du risque à un niveau acceptable.

XIII.11.2 Contenu de la matrice de traçabilité

La Figure-A XIII-5 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.

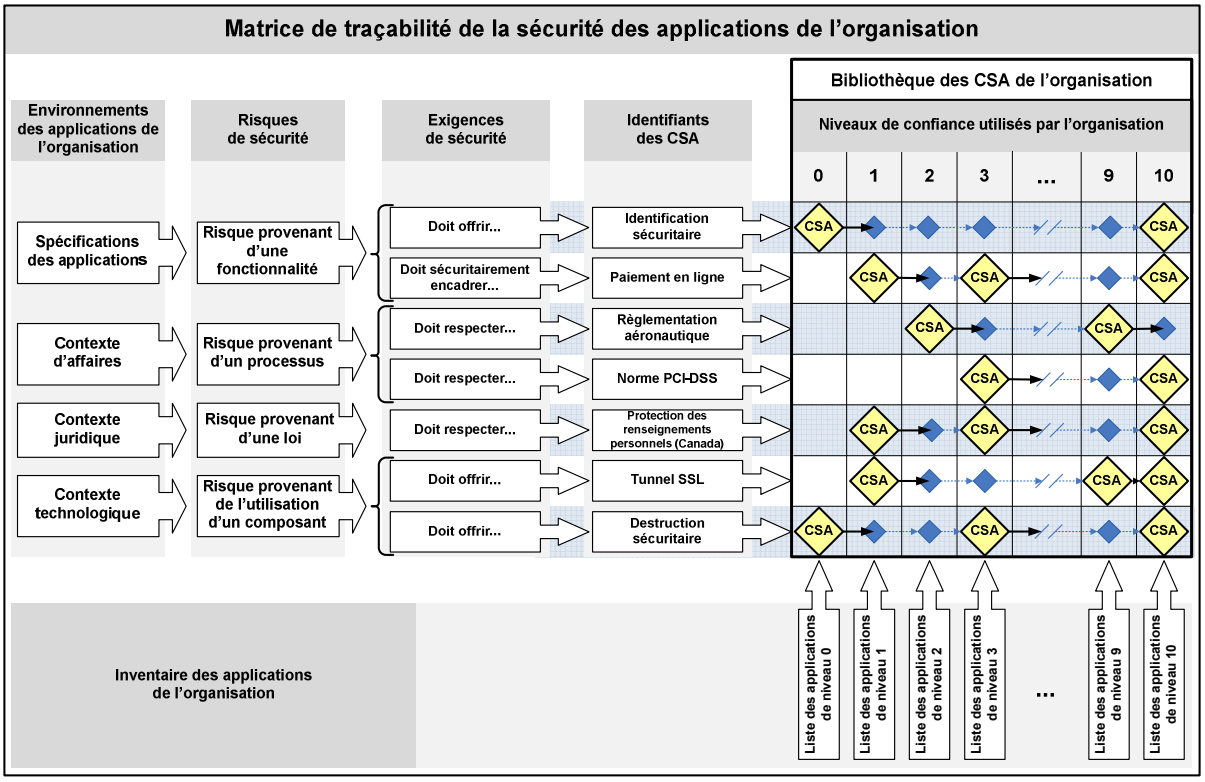


Figure-A XIII-5 Matrice de traçabilité de la SA de l'organisation

La matrice de traçabilité peut être représentée comme un tableau contenant cinq groupes d'informations interreliés, 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 de 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 de CSA.

XIII.12 Modèle de référence du cycle de vie de la sécurité d'une application (MRCVSA)

Une organisation qui est impliquée dans le développement, l'impartition, l'acquisition ou l'utilisation d'applications utilise généralement un cadre de processus pour gérer par phase les activités reliées à ses applications. Regroupant les processus et activités d'acquisition jusqu'aux activités de disposition, ce cadre représente un modèle de cycle de vie. Ce modèle n'est pas un nouveau concept. L'ouvrage *Software Maintenance Management* définit ce type de modèle comme étant : « Un cadre contenant les processus, les activités et les tâches impliquées dans le développement, l'exploitation et la maintenance d'un produit logiciel, couvrant la durée de vie du système de la définition de ses exigences à la fin de son utilisation. » (April et Abran, 2008, p. 255). Ce concept est aussi présenté dans plusieurs normes internationales dont notamment les normes ISO 12207 (ISO/IEC, 2008e, p. 12) et ISO 15288 (ISO/IEC, 2007g, p. 10). Les activités réalisées au cours des phases du cycle de vie d'un logiciel ou du système font partie des processus de l'organisation et devraient répondre aux exigences normatives fournies par ces deux normes.

Dans des projets d'application, un modèle de cycle de vie du logiciel est généralement utilisé pour définir des approches de développement. Qu'il s'agisse d'une approche de développement *waterfall*, en spirale, itérative ou agile, ce modèle est plus court et ne contient généralement que les phases du cycle de vie du développement de logiciel, soit notamment : la définition des exigences, l'analyse, la conception, l'implémentation et la vérification (Booch, Jacobson et Rumbaugh, 1999, p. 101). Ce cadre de processus est généralement développé et adapté aux besoins de l'organisation qui l'utilise, et est amélioré au fil du temps selon leurs domaines d'affaires et le type d'applications qu'elle développe.

Il n'est pas rare que des organisations utilisent simultanément différents modèles de cycle de vie de logiciel en fonction du type de logiciels qu'elles développent. Par exemple, il peut

s’agir d’applications locales, d’applications mobiles, d’applications Web, etc. Certains de ces modèles sont développés par l’organisation pour ses propres besoins de développement. Par conséquent, il est inutile d’essayer de répertorier et de faire référence à tous ces modèles, ou d’en privilégier certains par rapport à d’autres.

La solution à ces problèmes n’est pas d’imposer ni de recommander des changements dans les modèles de cycle de vie des applications actuellement en place dans les organisations. Au contraire, le modèle SA propose d’intégrer des CSA aux activités existantes dans les organisations, et ce, en utilisant un modèle de référence du cycle de vie de la sécurité des applications (MRCVSA) comme outil d’arrimage et de communication.

Non seulement le cycle de vie de l’application est plus large que celui du logiciel, mais plus encore, le cycle de vie de la SA se doit d’identifier un plus grand nombre de processus, d’activités et d’acteurs que ceux généralement identifiés dans le cycle de vie de l’application. Le MRCVSA n'est donc pas limité aux activités de développement de logiciel, mais il inclut aussi les activités réalisées par d'autres domaines d’interventions tels que la gouvernance, la gestion de l'infrastructure TI ainsi que des activités d’audit et de vérification.

Le modèle de référence du cycle de vie de la sécurité d’une application (MRCVSA), est un composant décrivant les quatre couches (une couche par domaine d'interventions), les phases (réalisation et opérations) et des groupes d'activités. 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. Tel que présenté à l'annexe XIII.9.2, ce modèle de référence 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.

XIII.12.1 Objectif visés par le MRCVSA

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. Cette situation amène le risque de sécurité qu'un CSA puisse être inefficace s'il est réalisé ou vérifié au mauvais moment. Il faut aussi voir que le travail à réaliser pour adapter un CSA à tous les modèles de cycle de vie rendrait la communication et la portabilité de CSA, entre les organisations et les projets utilisant différents modèles de cycle de vie, beaucoup plus difficile et onéreuse. Pour réaliser cet arrimage, la personne devra bien connaitre le modèle de cycle de vie sur lequel le CSA a été arrimé, ainsi que le modèle de cycle de vie dans lequel il veut l'importer.

Les objectifs visés par la mise en place du MRCVSA sont d'aider une organisation :

1) À identifier et à valider les activités et les rôles absents de ses façons de faire, en lui présentant les activités et les acteurs clés qui sont impliqués dans la sécurité des applications, pour lesquels il pourrait être important qu'ils soient intégrés à ses processus en vue d'améliorer la sécurité de ses applications;
2) À associer, de manière non ambigüe, des CSA aux activités et rôles présentés par le modèle de référence;
3) À s'assurer et à pouvoir démontrer que les risques et les exigences de sécurité sont correctement répondus à toutes les phases du cycle de vie de ses applications;
4) À minimiser le coût et l'impact de l'intégration de CSA dans ses projets d'application via l'arrimage du MRCVSA avec ses modèles de cycle de vie;
5) À communiquer ses CSA à ses équipes de projet d'application, ou à d'autres organisations, indépendamment des modèles de cycles de vie utilisés par chacune d'elles.

Pour atteindre ces objectifs, le MRCVSA devra :

1) Inclure les principales activités d'acquisition, d'impartition, d'opération et de mise à la retraite afin de pouvoir présenter les activités à réaliser aux organisations qui opèrent une application. Il faut se rappeler que le modèle SA ne s'adresse pas seulement aux organisations qui désirent développer des applications sécuritaires, mais aussi à toutes celles qui désirent les utiliser et les opérer de manière sécuritaire.
2) Être polyvalent et pouvoir être aligné à toutes les méthodes de développement, de maintenance et d'opération d'applications afin de ne pas obliger une organisation à changer ses rôles et façons de faire;
3) Préciser les principaux rôles et activités qui peuvent survenir dans toutes les phases du cycle de vie de la sécurité d'une application, incluant autant les activités de développement que celles de maintenance, d'opération, d'archivages et de destruction;
4) Préciser les principaux groupes et rôles, afin de tenir compte des différents acteurs œuvrant dans les quatre domaines de connaissance impliqués notamment dans la réalisation et la vérification des activités de sécurité des applications.

XIII.12.2 Contenu du MRCVSA

Afin d'atteindre l'objectif de cette recherche qui vise à s'assurer que ce modèle permettre d'intégrer des contrôles de sécurité durant tout le cycle de vie d'une application, le MRCVSA devra se positionner de manière à offrir une vision plus globale de l'ensemble des activités et des acteurs impliqués dans la sécurité des applications.

L'organisation doit définir et maintenir un alignement entre les phases et les activités prévues dans le MRCVSA et celles présentes dans chacun des modèles de cycle de vie que ses équipes utilisent. Étant donné que les CSA pointent sur les activités du modèle, cet alignement facilitera l'arrimage des CSA, puis l'évaluation et la réalisation de leur mise en œuvre lors de la réalisation des activités des équipes concernées.

C'est le comité du CNO qui est responsable de la gestion de l'alignement des différents modèles de cycle de vie en force dans l'organisation avec le MRCVSA, ainsi que de la validation de l'arrimage des CSA de l'organisation dans chacun d'eux. Cet arrimage permet à l'organisation de s'assurer que les CSA requis pour l'atteinte d'un niveau de confiance ciblé pour une application soient mis en place et vérifiés au moment prévu, durant tout le cycle de vie d'une application, quel que soit le modèle de cycle de vie utilisé.

La Figure-A XIII-6 présente une représentation graphique générale du MRCVSA proposé par le modèle.

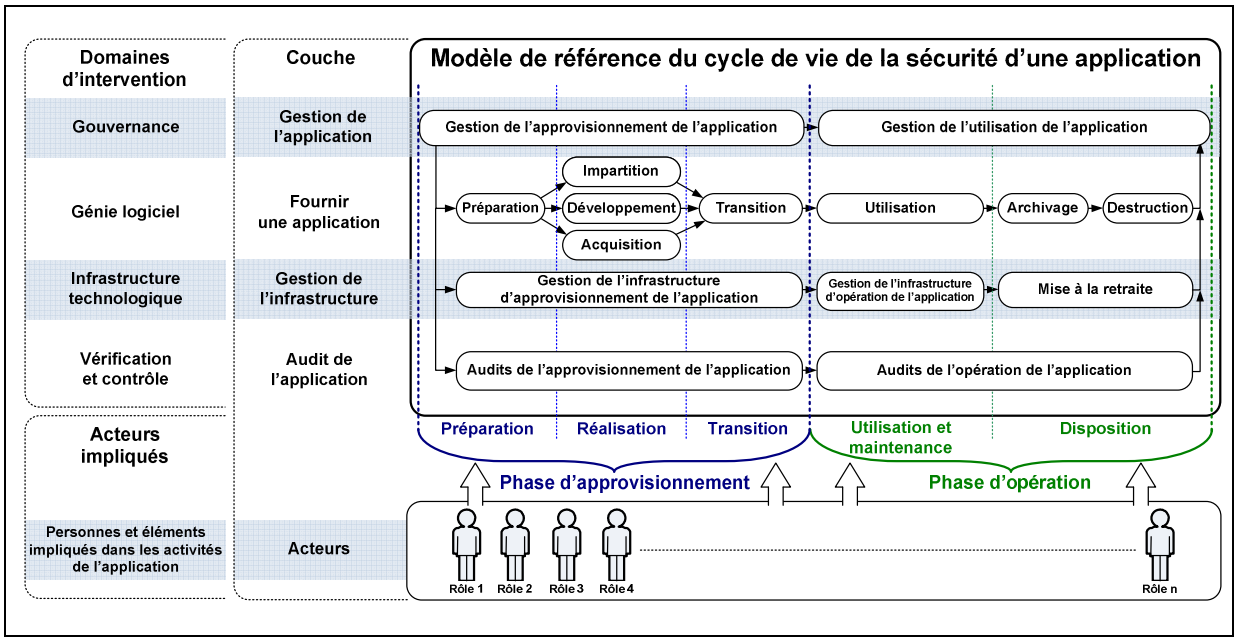


Figure-A XIII-6 Vue générale du modèle de référence du cycle de vie de la sécurité d'une application
Traduite et adaptée de (ISO/IEC, 2011d)

Le MRCVSA se divise horizontalement en phases, et verticalement en couches.

Horizontalement, il se divise en deux phases principales, soit :

1) La phase d'approvisionnement, au cours de laquelle sont réalisées les activités de préparation, de réalisation et de transitions de l'application; et

2) La phase d'opération, au cours de laquelle sont réalisées les activités d'utilisation, de maintenance et de disposition de l'application.

Verticalement, il se divise en cinq couches, soit :

1) La couche de gestion de l'application, alignée au domaine d'intervention de la gouvernance, comprend les activités du domaine de la gouvernance, telles que la gestion de projet et la gestion de l'exploitation de l'application. Ces activités sont généralement effectuées dans les processus définis dans le SGSI de l'organisation;
2) La couche « fournir une application » concerne la production et l'opération de l'application. Alignée au domaine d'intervention du génie logiciel, cette couche comprend les activités liées à l'approvisionnement et à l'utilisation de l'application elle-même. Ces activités sont généralement effectuées via les processus recommandés par des normes telles que les normes ISO 15288, ISO 12207, ISO 21827 et la série de normes ISO 15026;
3) La couche de gestion des infrastructures TI, alignée au domaine d'intervention de l'infrastructure technologique, comprend les activités liées à la gestion des services TI qui supportent les applications de l'organisation. Ces activités sont généralement effectuées via les processus recommandés par des normes telles que ISO 20000 et ITIL;
4) La couche d'audit de l'application, alignée au domaine d'intervention de vérification et de contrôle, qui comprend les activités en matière d'audit, de vérification et de contrôle. Ces activités sont généralement effectuées dans les procédés recommandés par des normes telles que ISO 15288, ISO 12207 et des documents sur les pratiques de l'industrie, tels que COBIT; et
5) La couche des acteurs impliqués par l'application, alignée sur une liste des rôles clés impliqués dans les activités de l'application, qui représentent toutes les personnes et processus automatiques intervenants dans les activités pouvant survenir durant les phases des différentes couches du modèle, tels que les chefs de projet, développeurs, administrateurs système, administrateurs de bases de données, gestionnaires de l'utilisateur, propriétaires d'applications, vérificateurs, utilisateurs finaux, techniciens de soutien, administrateurs réseau, etc.

Les activités effectuées dans les phases du MRCVSA sont décrites comme suit.

XIII.12.2.1 Couche : gestion de l'application

Cette couche comprend les secteurs d'activités qui sont habituellement réalisées par les responsables de projet et les gestionnaires, via le cadre des processus de l'organisation. Il s'agit notamment des processus de gestion de projet concernant le cycle de vie de projet et de systèmes, tel que décrit par la norme ISO 15288 (ISO/IEC, 2007g) et par les bonnes pratiques décrites par le PMBOOK (PMI, 2008) du *Project Management Institute* (PMI).

Ces activités se divisent en deux secteurs distincts, soit :

1) **Gestion de l'approvisionnement de l'application**
   Ce secteur comprend la liste des activités de gestion qui sont habituellement réalisées, durant la phase d'approvisionnement des applications telles que les processus de gestion des ressources humaines, de planification, d'évaluation et de contrôle de projet, et de gestion des décisions.
2) **Gestion des opérations de l'application**
   Ce secteur comprend la liste des activités de gestion du fonctionnement, de l'utilisation et de la maintenance de l'application, qui sont habituellement réalisées durant la phase d'utilisation et de maintenance, telle que les processus de gestion des décisions et de traitement de l'information.

XIII.12.2.2 Couche : fournir une application

Cette couche comprend les secteurs d'activités qui sont habituellement réalisées par l'équipe d'approvisionnement via le cadre des processus d'ingénierie de logiciel et d'ingénierie de systèmes TI de l'organisation, concernant autant l'approvisionnement que l'opération des applications. Il s'agit notamment des processus d'ingénierie logicielle tels que décrits par les normes ISO 12207 (ISO/IEC, 2008e) et ISO 15288 (ISO/IEC, 2007g), ou encore par des

méthodes de développement de logiciels telles que le *Rapid Application Development* (RAD) et l'*Open Unified Process* (OpenUP).

Cette couche se divise en huit secteurs d'activités distincts, soit :

1) **Activités de préparation**

   Ce secteur d'activités comprend les activités qui sont habituellement réalisées pendant la phase de préparation d'un projet d'application. Ces activités sont effectuées via les processus de l'organisation qui incluent notamment la gestion de l'information, la définition des exigences des intervenants, l'analyse des exigences de l'application et la gestion des risques du projet.

2) **Activités d'impartition**

   Ce secteur d'activités comprend les activités qui sont habituellement accomplies pendant la phase de réalisation par la voie de la sous-traitance que les activités liées à l'impartition à la sous-traitance. Ces activités sont réalisées via les processus de l'organisation tel que les processus d'acquisition, de gestion de la documentation, de gestion de la configuration logicielle et de gestion des risques.

3) **Activités de développement**

   Ce secteur d'activités comprend les activités liées à l'implémentation du logiciel qui sont notamment réalisées via les processus de gestion des risques, de conception de l'architecture du système, de conception de l'architecture du logiciel, de conception détaillée, de développement du logiciel, de gestion de la documentation, de gestion de la configuration et de la gestion des tests.

4) **Activités d'acquisition**

   Ce secteur d'activités comprend les activités liées à l'acquisition dans le but d'obtenir, ou d'acheter d'un fournisseur, un produit ou un service qui répond aux besoins de l'organisation. Les activités de ce secteur incluent notamment les processus d'acquisition,

de gestion de la documentation du logiciel, de gestion de la configuration, de gestion des risques et des processus de mise en œuvre.

5) Activités de transition

Ce secteur d'activités comprend les activités liées à la phase de transition, qui incluent notamment les activités de préparation d'une livraison, de gestion de la configuration, de tests et de déploiement de l'application dans l'environnement d'exploitation ciblé définies par l'organisation. Ces activités sont généralement effectuées via les processus de l'organisation qui incluent notamment les processus de gestion de configuration, d'intégration de systèmes, de tests et de qualification.

6) Activités d'utilisation

Ce secteur d'activités comprend les activités réalisées par tous les utilisateurs de l'application dont, notamment, les opérateurs, les gestionnaires d'accès et les utilisateurs finaux, pendant la phase d'utilisation et de maintenance. Ces activités sont liées à la formation, à l'utilisation, au support et à la maintenance de l'application dans son environnement d'opération réelle. Ces activités comprennent la gestion des accès des utilisateurs, la journalisation, la surveillance, les formations en sécurité, etc.

Certaines activités de maintenance et de gestion du changement font aussi partie de ce secteur qui inclut la mise à jour de logiciels, afin de répondre à l'évolution des exigences, comme l'ajout de nouvelles fonctionnalités et l'évolution des formats de données. Elles comprennent également la correction des bogues et l'adaptation de l'application aux nouveaux composants et périphériques utilisés par l'application.

7) Activités d'archivage

Ce secteur d'activités comprend les activités à réaliser lorsqu'il n'est plus nécessaire de maintenir en opération certaines informations ou composants de l'application. Il s'agit notamment des activités de désinstallation, de copie et d'archivage des informations et composants de l'application incluant les procédures de gestion des archives et de gestion

des copies de sauvegarde des composants et des documents reliés à l'application. Ces activités permettent de continuer à assurer la protection de l'information de l'application, même si cette information n'est plus dans l'environnement d'exploitation. Ces activités sont généralement effectuées via les processus de l'organisation qui englobent notamment les processus d'élimination du logiciel.

8) **Activités de destruction**

Ce secteur d'activités concerne la destruction sécuritaire de l'information et des composants de l'application, incluant notamment les données utilisateurs, les informations organisation, les journaux utilisateur et les paramètres d'application. Ces activités sont généralement effectuées via les processus de l'organisation qui incluent notamment les processus d'élimination du logiciel.

XIII.12.2.3 Couche : gestion de l'infrastructure

Cette couche comprend les secteurs d'activités qui sont habituellement réalisées par les équipes TI via le cadre des processus de l'organisation. Il s'agit notamment des processus de gestion de la qualité de services TI liés aux applications de l'organisation, tels que décrits par les normes ISO 15288 (ISO/IEC, 2007g), ISO 20000 (ISO/IEC, 2005e; 2005h) et les bonnes pratiques ITIL (ITIMF, 2013).

Ces activités se divisent en trois secteurs d'activités distincts, soit :

1) **Gestion de l'infrastructure d'approvisionnement de l'application**

Ce secteur d'activités comprend les activités qui sont habituellement réalisées pendant les phases de préparation, de réalisation et de transition du cycle de vie d'un projet d'application. Ces activités impliquent la fourniture et le maintien d'une infrastructure technologique sécurisée en soutien aux activités de l'équipe d'approvisionnement. Cela inclut la mise en place, le support et la maintenance des composants des divers services TI nécessaires aux divers environnements de développement, de tests différents et de déploiement. Ces activités sont effectuées via les processus de l'organisation qui

comportent notamment les processus d'installation, de maintenance, de contingence, ainsi que les processus de gestion de configuration des applications présents dans l'environnement d'approvisionnement de l'application.

2) **Gestion de l'infrastructure d'opération de l'application**

Ce secteur d'activités comprend les activités qui sont habituellement réalisées pendant la phase « utilisation et maintenance » du cycle de vie d'un projet d'application. Ces activités impliquent la fourniture et le maintien d'une infrastructure technologique sécurisée en soutien aux activités des équipes d'opération. Ces activités sont effectuées via les processus de l'organisation qui incluent notamment les processus d'installation, de maintenance, de support aux utilisateurs, de sauvegarde et de contingence, ainsi que les processus de gestion de configuration des applications présentes dans l'environnement opérationnel de l'application. Ces activités sont généralement effectuées via les processus de l'organisation qui comportent notamment les processus de fonctionnement et de maintenance.

3) **Mise à la retraite**

Ce secteur d'activités comprend les activités qui sont habituellement réalisées pendant les phases de disposition du cycle de vie d'un projet d'application. Ces activités concernent l'élimination et le recyclage des composants technologiques des divers services et systèmes utilisés par une application pour y conserver son information, afin de fournir l'assurance que toutes ces informations ont adéquatement été détruites et que ces composants peuvent être réutilisés sans risque de perte de confidentialité. Ces activités sont généralement effectuées via les processus de l'organisation qui comportent notamment le processus d'élimination.

XIII.12.2.4 Couche : audit de l'application

Cette couche comprend les secteurs d'activités qui sont habituellement réalisées par les équipes d'audits et de vérifications internes et externes, via le cadre des processus de

l'organisation. Ces activités de vérifications et d'audits peuvent être effectuées sur des acteurs, des processus, des composants technologiques utilisés par l'application, ou des artefacts produits durant le cycle de vie de l'application. Ces activités ont pour but de fournir au propriétaire de l'application les preuves et l'assurance que les exigences de sécurité requises pour l'application sont toujours respectées. Il est à noter que ces activités peuvent être réalisées périodiquement ou déclenchées suite à l'apparition d'un événement spécifique. Il s'agit notamment des processus de vérifications et d'audits de projets, tels que décrits par les normes ISO 12207 (ISO/IEC, 2008e) et ISO 15288 (ISO/IEC, 2007g), ou encore dans le recueil de bonnes pratiques COBIT (ITGI, 2007).

Ces activités se divisent en deux secteurs d'activités distincts, soit :

1) **Audits de l'approvisionnement de l'application**

   Ce secteur comprend la liste des activités de gestion qui sont habituellement réalisées, durant la phase d'approvisionnement d'applications telles que les processus de vérification du logiciel. Les activités de vérification réalisées au cours de cette phase sont généralement différentes de celles réalisées au cours de la phase d'opération d'une application. Les organisations qui opèrent uniquement les applications acquises pourraient ne jamais avoir besoin de réaliser de vérification dans la phase d'approvisionnement. Pour cette raison, la sécurité de vie des applications de référence modèle du cycle présente une zone spécifique pour les activités de vérification effectuées au cours des étapes d'opération.

   Les organisations de développement, mais pas des applications d'exploitation (telles que les éditeurs de logiciels) n'auront peut-être jamais besoin de vérification des applications dans les stades d'opération. Pour cette raison, la sécurité de vie des applications de référence modèle du cycle présente une zone spécifique pour les activités de vérification effectuées au cours des étapes d'approvisionnement.

2) **Audits de l'opération de l'application**

   Ce secteur comprend la liste des activités de gestion qui sont habituellement réalisées durant la phase d'opération de l'application. Ces activités sont effectuées via les processus de l'organisation qui incluent notamment le processus de vérification de la gestion de la configuration et de la gestion des accès.

XIII.12.2.5 Couche : acteurs impliqués par l'application

Cette couche comprend les groupes d'acteurs et les rôles qui sont habituellement impliqués dans la réalisation ou la vérification des différents processus et activités présents dans le cycle de vie des applications de l'organisation. Il s'agit notamment de groupes et de rôles identifiés par les normes ISO 12207, ISO 27001, SCRUM, OpenUP, ainsi que par les bonnes pratiques COBIT , Square et MS SDL (ISO/IEC, 2010c, p. A1) (*Voir* l'appendice B).

1) Les groupes d'intervenants impliqués dans les activités du MRCVSA, soit : le comité du CNO, la direction de l'organisation, l'équipe de projet, l'équipe de développement, l'équipe de l'infrastructure TI, l'équipe de vérification, l'équipe des opérations et les utilisateurs.

2) Les rôles des intervenants impliqués dans les activités du MRCVSA, soit :
   a) acheteur;
   b) architecte d'application;
   c) architecte de sécurité;
   d) architecte technologique;
   e) vérificateur / auditeur;
   f) chef de la sécurité;
   g) chef de projet;
   h) détenteur / propriétaire de l'application;
   i) développeur;
   j) équipe de l'infrastructure TI;

k) expert des lois et règlements;
l) expert du domaine;
m) formateur;
n) fournisseur;
o) gestionnaire;
p) opérateur d'application;
q) testeur;
r) utilisateur.

XIII.12.3 Schéma XML du CSA, et modèle de référence du cycle de vie de la sécurité d'une application

Un schéma XML a été développé pour préciser de manière formelle le CSA ainsi que le MRCVSA, soit tous les éléments définis dans les annexess XIII.9.2 et XIII.12.2, décrivant les contenus du CSA et du MRCVSA. Ce schéma sert à faciliter la communication et à valider l'intégrité de tous les documents XML décrivant les CSA échangés entre les parties.

Note : le schéma XML décrivant la structure formelle du CSA, ainsi que celui du MRCVSA, a été présenté au comité d'experts du SC27 d'ISO lors de la réalisation des cycles Delphi de cette recherche, et sont inclus dans le projet ISO 27034 *Application security – Part 5-1: Protocols and application security controls data structure – XML Schemas* (ISO/IEC, 2013a; 2015) qui est en cours de rédaction. Une version préliminaire des XML Schémas est disponible pour consultation (*Voir* l'appendice C).

XIII.13 Modèle du cycle de vie de la sécurité d'une application

Il existe différentes méthodes de développement, basées sur différents modèles de cycle de vie. Il est pratique courante dans les organisations de choisir une méthode proposant des processus, des activités et un cycle de vie, selon ce qui parait le plus approprié au type d'application ou aux approches et technologies utilisées pour la développer, la maintenir ou l'opérer. 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 SA ne propose pas d'imposer une méthode ou un cycle de vie normalisé à des organisations ou des équipes de développement d'applications, mais demande aux organisations d'aligner si nécessaire et d'arrimer les méthodes d'elles utilisent au MRCVSA.

Un modèle de cycle de vie de sécurité de l'application est basé sur un modèle de cycle de vie de l'application, mais est utilisé pour gérer les activités de sécurité des applications. Il présente des couches, des étapes et des activités en vigueur dans l'organisation, qui ont été arrimées aux phases et activités MRCVSA. (*Voir 2.4*)

XIII.13.1 Objectifs du modèle du cycle de vie de la sécurité d'une application

Les objectifs visés par la mise en place d'un modèle du cycle de vie de la sécurité d'une application sont de :

1) aider une organisation à découvrir et décrire formellement le ou les modèles du cycle de vie de sécurité d'application que ses équipes de projets utilisent;
2) aider l'organisation à compléter les modèles en place à l'aide du MRCVSA, en lui proposant un proposant une référence présentant des couches, des étapes, des activités et des acteurs qui pourraient être nécessaires à la sécurité de leurs applications et absent de leurs modèles;
3) faciliter la communication des CSA aux équipes de projets d'applications; et
4) de faciliter l'intégration de CSA aux activités existantes dans les processus des modèles utilisés par les équipes de projets d'applications.

XIII.13.2 Contenu du modèle du cycle de vie de la sécurité d'une application

Ce composant du CNO contient les phases, processus, activités et acteurs des différents modèles de cycles de vie en place dans l'organisation et fournit un arrimage entre ces modèles et le MRCVSA.

XIII.14 Cadre normatif de l'application (CNA)

Le cadre normatif de l'application (CNA) est un sous-ensemble du CNO. Il ne contient que les composants, les processus et les informations concernant une application spécifique. Cela permet de communiquer et de vérifier l'atteinte du niveau de confiance ciblé par son propriétaire. Le CNA d'une application est créé ou mis à jour, puis approuvé à la fin du processus « Créer et maintenir le cadre normatif de l'application » faisant partie du processus global de gestion de la sécurité d'une application. *(Voir l'annexe XIV.3.2 pour plus d'information sur ce processus).*

Pour chaque projet d'application de l'organisation, le CNA créé est conservé dans le CNO. Le contenu d'un CNA évoluera dans le temps, tout au long du cycle de vie de la sécurité de l'application, notamment en fonction de l'évolution de l'environnement. Par exemple, le contexte juridique ou est utilisé l'application peut changer, ou encore le propriétaire de l'application pourrait informer l'équipe de projet de sa décision d'élever le niveau de confiance ciblé pour une de ses applications. Dans dles deux situations, des éléments pourraient être ajoutés ou retirés du CNA.

Sachant que toute modification apportée au CNA a un impact direct sur l'évaluation de la sécurité d'une l'application, ces changements doivent recevoir les autorisations préalables du propriétaire de l'application.

XIII.14.1 Objectif visés par l'utilisation du CNA

Tout comme le CNO à l'échelle de l'organisation, la mise en place d'un CNA permet ainsi d'éviter les imbroglios, les recherches inutiles et les improvisations dans la réalisation d'activités ou dans la mise en place de CSA requis pour assurer l'atteinte du niveau de confiance ciblé.

Sachant que le modèle SA définit notamment la SA selon son environnement, il est important de noter que lorsqu'une même application est déployée dans deux environnements différents, les deux instances de cette application seront ici considérées comme deux applications spécifiques, différentes et indépendantes.

Les objectifs visés par la mise en place d'un cadre normatif formel d'une application sont de fournir un outil dont le contenu a été approuvé, afin de faciliter la communication entre les divers intervenants, en ramenant à l'essentiel la liste des processus, des composants et de l'information concernant la sécurité d'une application.

Plus précisément, les objectifs visés par la sélection et l'importation dans le CNA des éléments requis du CNO (composants, processus, rôles et responsabilités, etc.) sont de :

1) Donner aux intervenants, une vision claire et précise du cadre normatif qui s'applique à la SA spécifique;
2) Simplifier la liste des éléments de sécurité qui devront être mis en œuvre pour assurer et démontrer la sécurité de cette application;
3) Faciliter la communication et la maintenance de ces éléments en les conservant dans un dépôt spécifique au projet, accessible par les personnes concernées, et qui sera considéré comme la source autoritaire des éléments exigés par l'organisation pour cette application;
4) Conserver et d'assurer l'intégrité dans une source autoritaire des composants et des processus qui s'appliquent à la sécurité de cette application ainsi que l'information produite durant le cycle de vie de l'application; et
5) Réduire au minimum l'impact du coût de la SA sur le projet en maximisant la réutilisation des éléments du CNO qui ont déjà été validés et approuvés, évitant ainsi des improvisations et des initiatives malheureuses.

XIII.14.2 Contenu du CNA

Le cadre normatif d'une application est la source autoritaire des éléments et informations concernant la sécurité d'une application. Il contient notamment une copie des éléments du

CNO qui concernent la sécurité d'une instance spécifique d'une application ainsi que l'ensemble des documents et rapports qui auront été produits durant le cycle de vie de l'application. Par exemple, une organisation qui utilise deux instances de la même application, soit pour répondre aux besoins d'affaires de deux clients différents, soit pour répondre à des contraintes géographiques de deux régions différentes, peut avoir pour chacune un CNA décrivant le contexte d'affaires et juridique qui leur sont spécifiques.

La Figure-A XIII-7 présente une vue sommaire des composants et processus contenus dans le CNA d'une application.

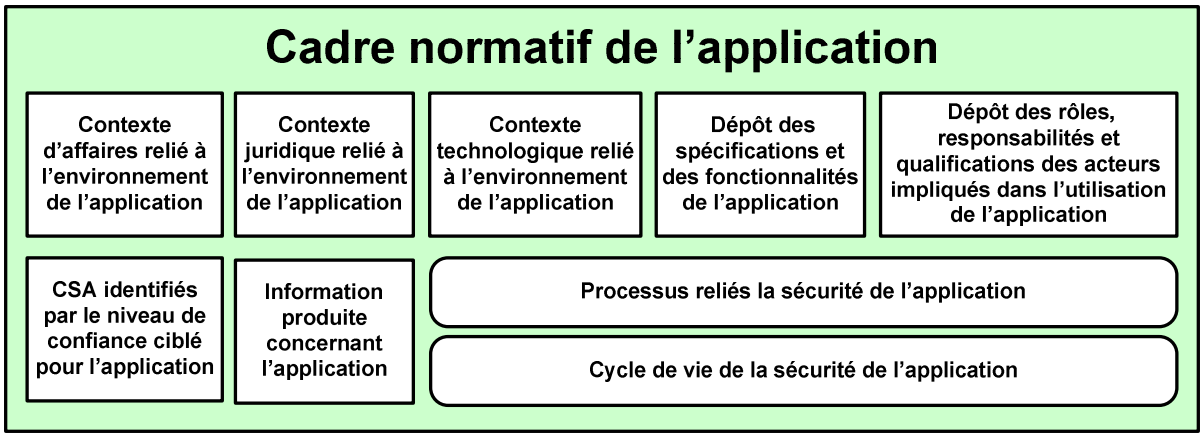


Figure-A XIII-7 Représentation sommaire du cadre normatif d'une application
Traduite et adaptée de (ISO/IEC, 2011d)

Un CNA est créé et tenu à jour pour chaque application, durant tout son cycle de vie. L'organisation y consolide les éléments pertinents du CNO et l'information produite lors de la mise en œuvre des divers processus, composants et CSA identifiés par le niveau de confiance qui lui aura été assigné au préalable. Un CNA contiendra non seulement les contextes technologiques, juridiques et d'affaires de l'application, mais aussi tous les documents, données et rapports produits durant son cycle de vie, notamment : les risques de sécurité, les exigences de sécurité, le niveau de confiance, l'inventaire de l'information catégorisée, les rapports de tests de vulnérabilité et les documents d'approbation.

Afin de pouvoir répondre correctement aux préoccupations de SA spécifique, le CNA de celle-ci contiendra tous les éléments pertinents liés à la définition, la gestion et la vérification de la sécurité d'une application.

Plus précisément, le CNA devrait notamment contenir les éléments suivants :

1) Les composants, soit :
   a) le contexte d'affaires relié à l'environnement de l'application :
      ce contexte ne contiendra que les processus d'affaires, les méthodes, les normes et les acteurs impliqués dans le projet d'application, incluant notamment les processus de gestion de l'environnement de l'application (*Voir* XIII.3);

   b) le contexte juridique relié à l'environnement de l'application :
      ce contexte ne contiendra que les exigences légales et réglementaires applicables à l'emplacement où l'application est développée, déployée et utilisée, qui ont été importées du contexte juridique du CNO (*Voir* XIII.4);

   c) le contexte technologique relié à l'environnement de l'application :
      ce contexte ne contiendra que l'information concernant des composants technologiques requis par l'application, tels que les composants d'architecture, les composants d'infrastructures TI, les protocoles, les langues et les paramètres qui ont été importés du contexte technologique du CNO (*Voir* XIII.5);

   d) le dépôt des spécifications et des fonctionnalités de l'application :
      ce dépôt ne contiendra que les spécifications de l'application, généralement présentées sous la forme d'exigences fonctionnelles, non fonctionnelles et de sécurité provenant du CNO (*Voir* XIII.6). Il contiendra aussi la liste des groupes d'informations catégorisés utilisés, entreposés, calculés et communiqués par l'application. Ces groupes d'informations incluent notamment toutes les données relatives à l'organisation et aux utilisateurs, des données de configuration, des paramètres et d'autres données utilisées par l'application (*Voir* Figure-A XII-4);

e) le dépôt des rôles, responsabilités et qualifications des acteurs impliqués dans les activités liées à l'application :

tous les rôles des acteurs qui interagiront avec l'application durant son cycle de vie doivent être identifiés. Ces rôles sont notamment l'officier de sécurité, le propriétaire de l'application, les vérificateurs, les architectes, les développeurs, les administrateurs de bases de données, des techniciens et les utilisateurs finaux;

f) les CSA identifiés par le niveau de confiance ciblé pour l'application :

les CSA s'appliquant à une application sont sélectionnés et importés de la bibliothèque de CSA de l'organisation vers le CNA, selon les exigences de sécurité de l'organisation pour l'application et selon le niveau de confiance ciblé pour l'application (*Voir* Figure-A XIII-4). Ainsi, tous les CSA associés au niveau de confiance ciblé pour l'application qui correspondent à une des exigences de sécurité devant être satisfaite pour l'application, seront identifiés et importés dans le CNA. Dès lors, les développeurs n'ont plus à concevoir des contrôles de sécurité pour chaque nouveau projet d'application, mais simplement à mettre en œuvre les CSA importés. La réutilisation des CSA du CNO assure une approche constante dans les réponses aux exigences de sécurité, pour toutes les applications où ceux-ci seront utilisés. La liste des CSA sélectionnés doit minimalement inclure tous les CSA associés au niveau de confiance minimal (*Voir* Figure-A XIII-4, niveau « zéro »);

g) le cycle de vie de la sécurité de l'application :

le composant « cycle de vie de l'application » identifie les phases et les activités que l'organisation a décidé d'inclure et d'exclure dans un projet d'application. Par exemple, une organisation qui fera l'acquisition d'une application pourra décider de ne pas inclure des groupes d'activités « développement » et « impartition ». Ce cycle de vie d'une application est un sous-ensemble du MRCVSA sélectionné en fonction des besoins d'affaires de l'organisation pour son application. Même si certaines équipes de projet d'application utilisent une nomenclature ou des noms de processus différents, le MRCVSA doit être arrimé au cycle de vie de la sécurité de l'application.

C'est grâce à cet arrimage que les activités de sécurité et de vérification définies par les CSA pourront être intégrées et réalisées durant l'exécution des différents processus du cycle de vie de l'application avec lesquels les équipes de projet et de vérification sont déjà familiers. C'est via ce mécanisme d'arrimage que les CSA, qui réfèrent à des activités du MRCVSA, pourront facilement être intégrés aux divers processus existants dans l'organisation (*Voir 2.4*), plutôt que d'être introduits via des processus de sécurité supplémentaires distincts.

2) L'information produite concernant l'application, soit :
   a) le niveau de confiance;
   b) les divers documents et rapports produits durant la réalisation, l'opération, le support et la maintenance jusqu'à la mise à la retraite de l'application.

3) Les processus de gestion reliés à la sécurité de l'application, soit :
   tous les processus du CNO reliés à la définition, la gestion et la vérification de la sécurité de l'application concernée doivent être importés du CNO vers le CNA. Ces processus sont notamment :
   a) le processus de gestion du CNA;
   b) le processus de gestion des risques de la sécurité de l'application;
   c) le processus de gestion de la sécurité de l'application; ainsi que
   d) les processus présents dans le cycle de vie de l'application.

Ces processus sont présentés dans le chapitre 7.

ANNEXE XIV

LE MODÈLE SA : PROCESSUS

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

1) acquérir, déployer, utiliser et vérifier des applications dans lesquelles ces dernières 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.

Le modèle SA propose également un processus additionnel utilisé par les équipes de vérifications internes et externes à l'organisation qui permet d'encadrer les travaux de vérification, d'audit et de certification des personnes, des applications et des organisations.

La Figure-A XIV-1 présente les deux niveaux d'opération où devraient-être utilisés les quatre processus clés du modèle pour pouvoir mettre en œuvre et vérifier la SA d'une organisation, soit au niveau de l'organisation elle-même et au niveau de ses projets d'applications. Il est à noter que même s'ils sont tous dérivés du CNO, les CNA des divers projets d'applications d'une organisation ne seront pas nécessairement identiques, chacune des d'applications ayant son propre niveau de confiance cible (NdC) à atteindre.

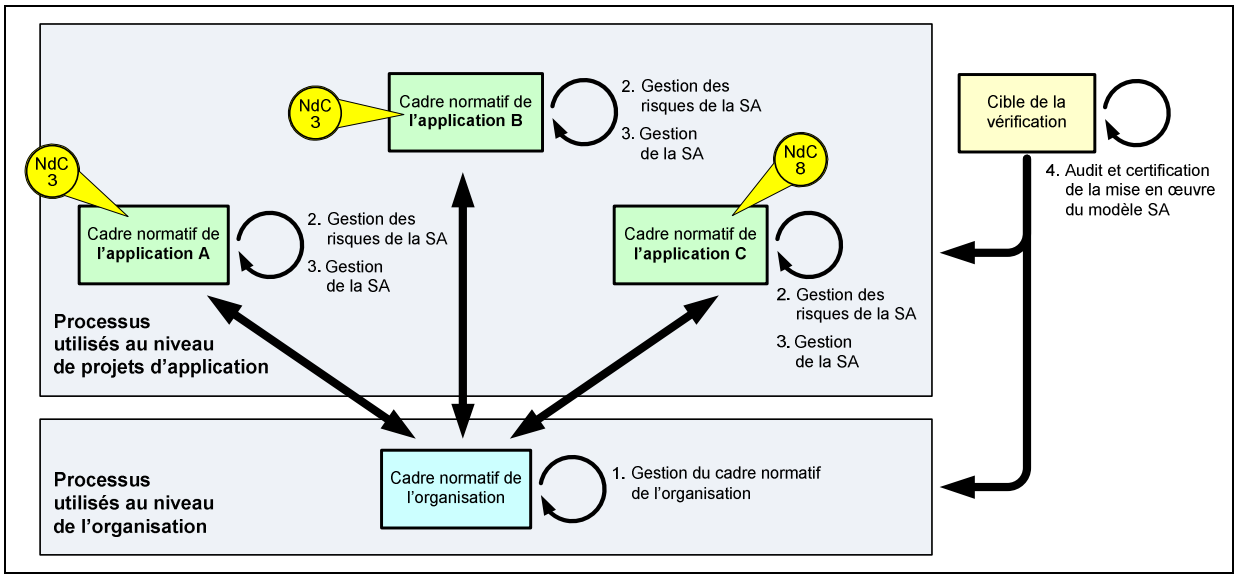


Figure-A XIV-1 Les quatre processus clés du modèle SA et leurs niveaux d'utilisation versus leurs niveaux d'opération

Cet annexe présente les quatre processus clés du modèle SA, soit :

1) Gestion du CNO (XIV.1);

   Utilisé par le comité de gestion du CNO pour mettre en place les éléments et processus du modèle SA afin qu'elle puisse développer et de gérer son CNO en fonction de ses besoins, de ses priorités et de ses ressources.

2) Gestion des risques de la sécurité d'une application (XIV.2);

   Mis en place et approuvé par le comité de gestion du CNO, il est utilisé par les équipes de projet d'applications afin de les guider dans la gestion des risques de sécurité amenés à par l'organisation par l'approvisionnement et l'utilisation d'une application.

3) Gestion de la SA (XIV.3);

   Utilisé par l'équipe de projet d'une application, pour les guider dans l'intégration des éléments de la SA dans leurs projets.

4) Audit et certification de la mise en œuvre du modèle SA (XIV.4);
   Utilisé 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.

XIV.1 Gestion du CNO

Le processus de gestion du cadre normatif de l'organisation (CNO) favorise la mise en place des éléments et des dispositifs du modèle SA permettant de développer et de gérer le CNO de l'organisation en fonction de ses besoins, de ses priorités et de ses ressources. Le modèle SA fournit un processus qui permet la gestion d'un CNO de manière à structurer et à harmoniser la SA pour l'ensemble de l'organisation. Ce processus est applicable à la gestion de tous ses éléments, incluant la priorisation et l'identification du moment où un élément sera intégré au CNO. Il permet aussi de gérer la conception, l'implémentation, la maintenance et la révision des éléments du CNO qui ont été préalablement priorisés par l'organisation. Mais plus important, il sert à formaliser le CNO, soit : à mettre en place le comité du CNO qui sera responsable de prioriser, d'implémenter, de surveiller, d'améliorer et de faire auditer le CNO et les éléments de la SA qu'il contient.

La Figure-A XIV-2 présente sommairement le processus de gestion du CNO ainsi que les principaux éléments qu'il utilise pour produire le CNO.

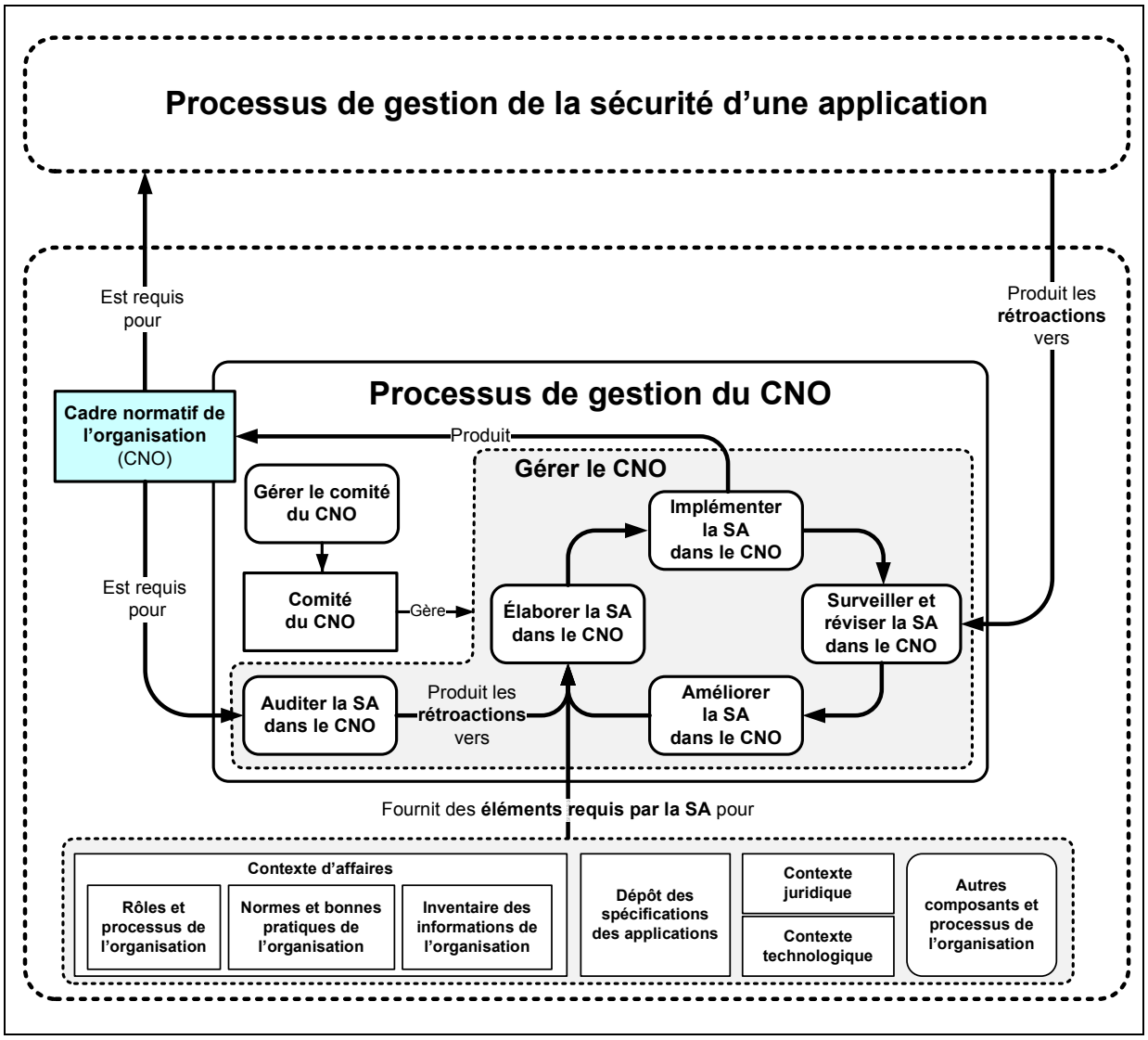


Figure-A XIV-2 Composants et processus reliés à la gestion du cadre normatif de l'organisation
Traduite et adaptée de (ISO/IEC, 2011d)

Le processus de gestion du CNO (Figure-A XIV-2) est composé de six sous-processus dont quatre d'entre eux ont été adaptés du processus « *Plan*, *Do*, *Check*, *Act* », utilisé dans la définition d'un processus de mise en place et de maintenance d'un système de gestion de la sécurité de l'information (SGSI) d'une organisation (ISO/IEC, 2005d, p. vi), afin de les spécialiser dans le développement et la gestion d'éléments de la SA de l'organisation. Ensemble, ces six sous-processus permettent à l'organisation de maintenir son CNO à jour, en fonction de ses besoins et des changements qui surviennent dans son environnement.

Le Tableau-A XIV-1 montre comment les sous-processus de gestion du CNO s'arriment avec les quatre étapes du processus de gestion d'un SGSI.

Tableau-A XIV-1 Arrimage des quatre processus de gestion d'un SGSI à ceux de gestion du CNO

Étapes du processus du SGSI	**Sous-processus de gestion du CNO**
Plan	Élaborer la SA dans le CNO
Do	Implémenter la SA dans le CNO
Check	Surveiller et réviser la SA dans le CNO
Act	Améliorer continuellement la SA

Les composants et sous-processus reliés à la gestion de la SA qui permettent de produire le CNO, sont des processus permanents de l'organisation. Ils sont réalisés et gérés par le comité du CNO, parallèlement aux processus de projets d'application de l'organisation.

L'élaboration et la maintenance de la SA dans le CNO sont réalisées en utilisant quatre sources d'éléments d'information (*Voir* Figure-A XIV-3), soit :

1) Les éléments externes à l'organisation;
   a) les normes, guides et méthodes présentant des contrôles, des principes, des méthodes et des processus qui ont été présentés à la section 6.6 de ce document;
   b) l'ensemble des éléments, regroupés selon les trois contextes, pouvant être intégrés aux environnements des applications;
   c) les pratiques recommandées sur la mise en place de fonctionnalités d'application.
2) Les éléments répertoriés dans l'organisation;
   a) l'information, existante dans l'organisation, qui a été répertoriée et regroupée selon les trois contextes;
   b) les spécifications des applications de l'organisation.

3) Les contrôles de SA de l'organisation;
   a) l'information concernant les contrôles de SA déjà en place dans l'organisation, incluant aussi ceux qui ne sont pas définis sous la forme de CSA.
4) Les rétroactions produites par les projets d'application.
   a) l'information produite par les différentes équipes d'application, telle que les demandes de changements, les rapports d'anomalies, des demandes de dérogations, etc.

La Figure-A XIV-3 présentent les principaux éléments de SA impliquées dans le processus d'amélioration continue du CNO.

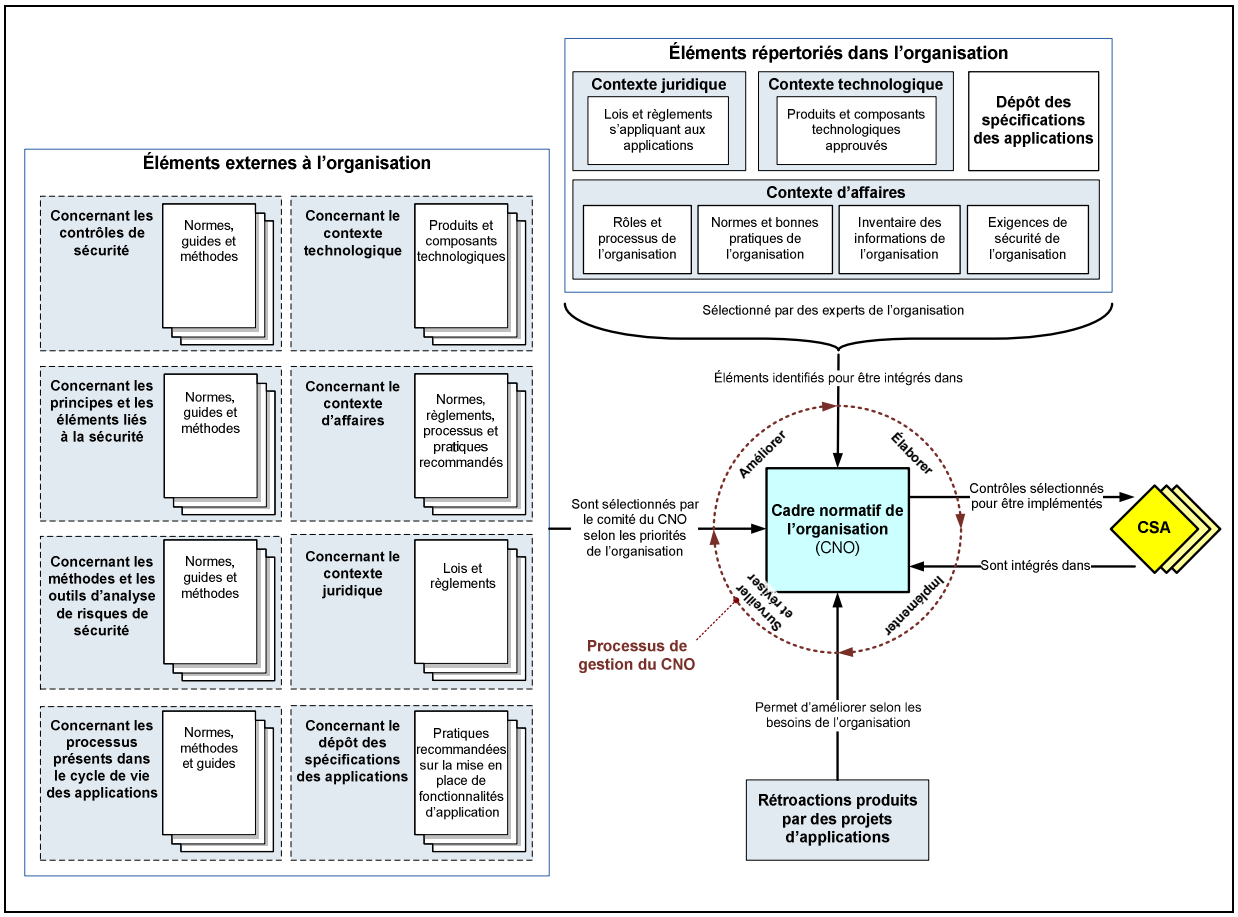


Figure-A XIV-3 Représentation sommaire des principaux éléments de SA impliquées dans le processus d'amélioration continue du cadre normatif de l'organisation
Traduite et adaptée de (ISO/IEC, 2011d)

C’est en surveillant et en utilisant les éléments d’information de ces quatre groupes reliés aux besoins de sécurité de l’organisation que sera développé et maintenu le CNO.

Le CNO contient notamment tous les composants et processus impliqués dans la sécurité des applications, tels que les règlements, les lois, les meilleures pratiques, les processus, les rôles et les responsabilités acceptés par l'organisation. Il définit les contextes de l’organisation, La bibliothèque de CSA, et devient le référentiel unique pour la SA au sein de l'organisation *(Voir* XIII.2).

Ce même processus est aussi utilisé à la gestion des éléments du CNO, soit à l’identification, la validation, l’acquisition, la vérification, l’intégration, la maintenance et la communication aux personnes concernées, d’un composant ou d’un processus dans le CNO requis par l'organisation. C’est le comité du CNO qui est responsable de la mise en place et du bon fonctionnement de ce processus.

XIV.1.1 Objectifs de la mise en place du processus de gestion du CNO

Le modèle SA spécifie qu'une organisation devrait utiliser un processus de gestion du cadre normatif de l'organisation (CNO) afin d'établir, de mettre en place, de maintenir, de constamment améliorer, de communiquer et de vérifier que les différents aspects et les éléments liés à la SA (Figure-A XIII-1) sont bien utilisés dans les projets de l'organisation.

Le SGSI d’une organisation permet notamment d’identifier les actifs informationnels sensibles d’une organisation qui devraient être protégés. (ISO/IEC, 2005d) L’utilisation d’une application par une organisation implique généralement le regroupement, le stockage, le transfert et même parfois l’archivage d’un ensemble d’informations. C’est pourquoi toute application est considérée par le SGSI comme étant un des types d’actifs informationnels qu’une organisation devrait protéger.

La Figure-A XIV-4 présente l'arrimage entre le processus de gestion du CNO et le SGSI d'une organisation.

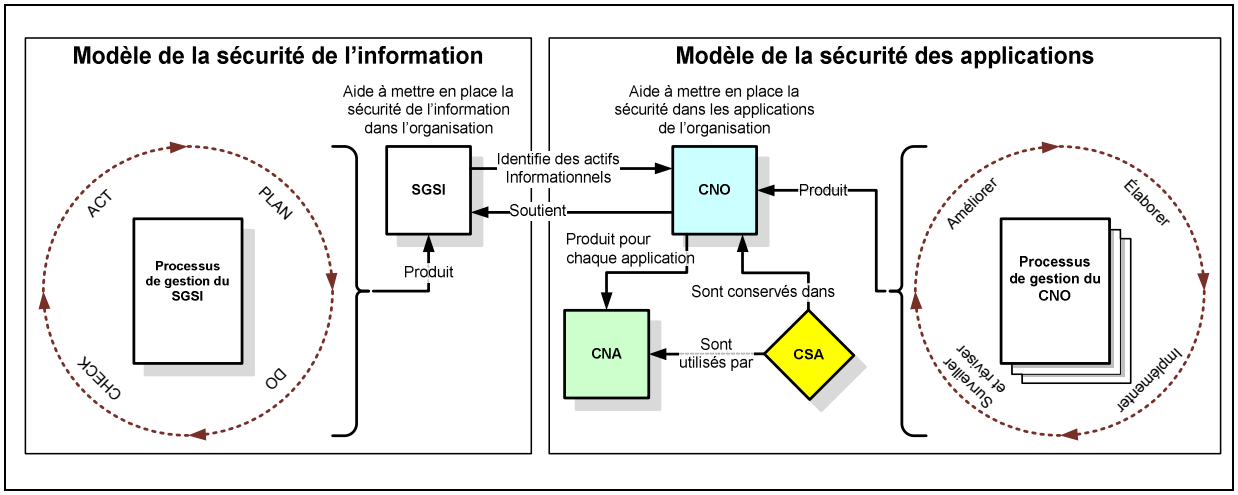


Figure-A XIV-4 Représentation sommaire de l'arrimage entre le processus de gestion du CNO et le SGSI d'une organisation

Même s'il n'est pas nécessaire à une organisation d'avoir mis en place un SGSI pour mettre en place le processus de gestion du CNO, un des objectifs de ce processus est de soutenir le SGSI de l'organisation. Ce soutien consiste à apporter aux gestionnaires du SGSI les preuves démontrant que les applications, qui ont été identifiées comme étant des actifs informationnels sensibles, possèdent toutes un cadre normatif de l'application (CNA). Ce CNA définit notamment les CSA requis à l'atteinte du niveau de confiance ciblé, qui fourniront les preuves requises démontrant que ces applications ont été adéquatement protégées et que les risques de sécurité les concertant ont tous été ramenés à un niveau acceptable définies par l'organisation (Figure-A XIV-4).

De par sa qualité de « processus continu », le processus de gestion du CNO sert aussi à s'assurer que la gestion des risques reliés à l'utilisation des applications de l'organisation s'arrime aux processus de gestion des risques de sécurité de l'information du SGSI de l'organisation, tout en tenant compte des changements continuels des environnements opérationnels des applications de l'organisation.

Le modèle SA n'oblige pas une organisation à suivre un plan de mise en œuvre précis de son CNO. De fait, il donne toute la flexibilité à l'organisation qui désire mettre en place son processus de gestion du CNO afin qu'elle puisse y intégrer progressivement les éléments reliés à la sécurité de ses applications, selon ses priorités et dans le respect de ses capacités. Le but de cette approche est de faciliter, pour des organisations grandes ou petites, la mise en place d'un CNO permettant d'obtenir des gains de sécurité rapides tout en réduisant les impacts sur l'organisation. Ceci, en laissant l'organisation identifier, pour chaque itération du processus de gestion du CNO, la priorité aux éléments de SA qui sont les plus importants pour elle ou dont le retour sur l'investissement sera le plus rentable.

Les objectifs de la mise en œuvre d'un processus de gestion du CNO sont notamment d'aider l'organisation à :

1) faciliter l'acquisition ou la conception, la validation, la mise en place, la maintenance et l'approbation des éléments du CNO, soit à :
    a) mettre en place un référentiel d'informations qui agira en tant que source autoritaire pour la consolidation et la communication des éléments du CNO;
    b) s'assurer que les résultats produits par les composants et processus intégrés au CNO auront préalablement été approuvés par l'organisation et seront en mesure de fournir au besoin, des preuves valides supportant les affirmations désirées;
    c) veiller à ce que le CNO soit aligné avec le SGSI, l'architecture de sécurité, l'architecture de l'information et l'architecture d'entreprise de l'organisation.
2) Acquérir, gérer et valider la conception d'éléments du CNO, soit à :
    a) gérer la mise en place des éléments liés à la SA en fonction des priorités de l'organisation et des ressources disponibles;
    b) attribuer les responsabilités et les ressources suffisantes pour la conception des éléments requis par les priorités de l'organisation;
    c) s'assurer que les besoins de SA de l'organisation, les niveaux de confiance de la bibliothèque de CSA, ainsi que les CSA qu'elle contient, répondent adéquatement aux besoins d'affaires de l'organisation;

d) s'assurer que les éléments de SA du CNO sont révisés et actualisés pour refléter les changements d'environnement de l'organisation. Par exemple, un changement à la Loi de la protection des renseignements personnels peut entraîner à des modifications au contexte juridique de l'organisation définie dans le CNO.

3) Établir des mécanismes de communication et de rétroaction (interne, externe, interfaces avec les projets d'application, etc.) permettant de :
   a) faciliter la communication des éléments du CNO à toutes les équipes de l'organisation;
   b) s'assurer de la bonne utilisation des éléments du CNO, soit en :
      i) veillant à ce que l'organisation soit en mesure d'offrir la formation adéquate pour que les personnes puissent assumer correctement leurs responsabilités;
      ii) s'assurant que les personnes possèdent les outils, les connaissances et les qualifications requises pour pouvoir assumer les responsabilités associées au rôle qui leur a été attribué.
   c) veiller à ce que les CSA approuvés soient correctement et uniformément appliqués à l'échelle de l'organisation;
   d) voir à ce que les résultats des activités de SA soient communiqués à toutes les parties concernées.
4) Donner à l'organisation la capacité d'améliorer la maturité des processus et des éléments du CNO liés à la sécurité de ses applications, soit en :
   a) fournissant des mécanismes de veille et de rétroaction qui favoriseront l'intégration de nouvelles connaissances, des suggestions d'améliorations de CSA et de nouvelles pratiques acquises au cours d'un projet d'application au CNO.

XIV.1.2 Gérer du comité du CNO

Le processus de gestion du comité du CNO est utilisé par l'organisation pour mettre en place un comité du CNO et lui donner la légitimité et l'espace de manœuvre essentielle à une gestion homogène de la SA dans toute l'organisation, et ce, en respect avec les priorités et les capacités de cette dernière. L'organisation allouera donc à ce comité l'autorité et les

ressources nécessaires à la mise en place des éléments de la SA dans le CNO, démontrant ainsi son engagement et l'importance qu'elle accorde à la sécurité de ses applications dans ses opérations quotidiennes.

XIV.1.2.1 Objectifs

Les objectifs visés par la mise en place de ce processus de gestion du comité du CNO sont notamment de :

1) Mettre en place un comité du CNO avec l'autorité et les ressources nécessaires pour le développement, la mise en œuvre et l'évolution du CNO;
2) Démontrer l'engagement approprié de la direction responsable.

XIV.1.2.2 Activités

Afin d'atteindre les objectifs visés, les activités suivantes devront être réalisées :

1) Nommer les membres du comité du CNO et assigner des responsabilités à chacun d'entre eux;
2) Déléguer la responsabilité opérationnelle de la SA de l'organisation au comité du CNO soit, notamment, autoriser les membres du comité à :
   a) gérer le CNO soit diriger, superviser et contrôler l'élaboration, l'implémentation, la révision, l'amélioration et la vérification du CNO;
   b) diriger l'intégration des éléments du CNO dans les processus de l'organisation;
   c) Établir la définition et diriger l'encadrement des qualifications des différents acteurs impliqués dans la SA de l'organisation.
3) Approuver les priorités, la stratégie et les ressources de l'organisation allouées à la SA de l'organisation.

XIV.1.2.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Nomination des membres du comité du CNO ainsi que l'assignation de leurs responsabilités respectives;
2) Démonstration de l'engagement de la haute direction concernant la reconnaissance de l'importance de la SA à l'intérieur de l'organisation;
3) Définition et gestion des priorités, des ressources et des orientations de l'organisation concernant la sécurité de ses applications;
4) Approbation de l'organisation sur les approches proposées afin de répondre aux exigences amenées par la mise en place du modèle dans l'organisation, notamment dans la mise en place d'une politique de gestion de la SA et des éléments requis dans le CNO;
5) Supervision et mise en place des mesures nécessaires à l'intégration des éléments du CNO dans les processus d'affaires de l'organisation;
6) Identification et mise en place d'un dépôt central qui sera considéré comme la source autoritaire des processus et des composants de la SA en vigueur dans l'organisation.

XIV.1.3 Élaborer la sécurité des applications dans le CNO

Premier des cinq sous-processus utilisés pour gérer le CNO, l'élaboration de la SA dans le CNO consiste à déterminer quels éléments requis par la SA doivent être mis en place dans l'itération courante du CNO, puis de les concevoir (Figure-A XIV-2). Ces éléments comprennent notamment le processus de gestion de la SA dans des projets d'applications, la bibliothèque de CSA ainsi que tous les processus connexes requis pour la mise en place de la SA de l'organisation.

XIV.1.3.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont de gérer l'évolution du CNO, en définissant et en mettant en place les éléments de la SA requis à l'atteinte des objectifs de sécurité de l'organisation, soit notamment de :

1) veiller à ce que les politiques de SA du CNO soient conformes aux politiques de sécurité de l'organisation;

2) s’assurer de la conformité juridique et réglementaire des applications de l’organisation;
3) voir à ce que les objectifs de gestion des risques du CNO soient alignés avec les objectifs et les stratégies de l'organisation;
4) veiller à ce que les indicateurs de performance de gestion du risque de SA, inclus au CNO, soient alignés avec les autres indicateurs de performance utilisés dans l'organisation.

XIV.1.3.2 Activités

Afin d’atteindre les objectifs visés, les activités suivantes devront être réalisées :

1) Sélectionner à partir des éléments d’information externes à l’organisation, ceux qui répondent aux priorités de l’organisation et qui devront être intégrés au CNO, soit :
   a) préciser et documenter les contextes possibles (d'affaires, juridique et technologique) dans lesquels les applications de l'organisation seront utilisées.
2) Créer, documenter et maintenir le dépôt des spécifications et des fonctionnalités des applications de l’organisation, soit :
   a) analyser les spécifications et les fonctionnalités de chaque nouvelle application lors de sa phase d’approvisionnement (Figure-A XIII-6);
   b) revoir et réviser, s’il y a lieu, les spécifications et les fonctionnalités des applications existantes dans l'organisation;
   c) identifier les groupes d’informations et les acteurs impliqués par les spécifications et les fonctionnalités identifiées, et noter les relations existantes entre l’information, les spécifications, les fonctionnalités et les acteurs.
3) Spécifier les acteurs et les processus, soit :
   a) analyser et documenter les personnes et les processus sensibles impliqués dans le cycle de vie des applications;
   b) identifier les groupes d’informations impliquées par les processus qui ont été documentés et noter les relations existant entre l’information, le processus et les acteurs;

   c) spécifier et approuver une méthode d'analyse de risques de SA formelle répondant aux critères énoncés par la norme ISO 27005.
4) Identifier les processus et les CSA à mettre en place :
   a) en fonction des risques et des exigences de sécurité priorisées par l'organisation;
   b) en fonction des processus et des contrôles de SA déjà en place, et qui devraient être convertis en CSA; et
   c) en fonction des rétroactions provenant des équipes de projets d'application.
5) Définir et valider la mise en place de La bibliothèque de CSA de l'organisation, soit :
   a) définir les niveaux de confiance en vigueur dans l'organisation;
   b) réviser, valider, vérifier et approuver tous les éléments intégrés à la bibliothèque, incluant notamment les processus et CSA adaptés d'éléments existants et de la rétroaction des projets d'application.
6) Définir et valider la mise en place de la matrice de traçabilité des risques de SA de l'organisation.

XIV.1.3.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Identification de la stratégie de l'organisation concernant la sécurité de ses applications;
2) Liste des éléments et processus du CNO requis par l'organisation;
3) Liste des applications sensibles de l'organisation;
4) Liste consolidée des risques de sécurité de l'organisation concernant ses applications;
5) Liste des priorités de l'organisation.

XIV.1.4 Implémenter la sécurité des applications dans le CNO

Ce sous-processus sert à la mise en œuvre et à la communication des éléments du CNO qui ont été conçues dans l'itération courante du processus de gestion du CNO. Il est utilisé pour identifier, valider et fournir des solutions de sécurité des applications, telles que des

composants et des processus, des directives de sécurité des applications, des services ou des pratiques obligatoires, et de les distribuer afin qu'elles soient utilisées dans tous les projets d'application de l'organisation.

XIV.1.4.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont de concevoir, valider, tester, vérifier et mettre en place les éléments de SA requis par l'organisation.

XIV.1.4.2 Activités

Afin d'atteindre les objectifs visés, les activités suivantes devront être réalisées :

1) Analyser les pratiques recommandées et les normes internationales liées à l'environnement de l'organisation et à ses besoins, puis à partir des résultats et priorités identifiés par cette analyse, développer ou compléter les processus, directives et règlements en SA en fonction des besoins de l'organisation;
2) Implémenter dans le CNO les CSA requis par l'organisation, soit par :
   a) l'acquisition, le développement ou la mise à jour des CSA;

      Lorsque requis par l'organisation, un CSA peut être développé ou mis à jour pour répondre à des exigences de sécurité spécifiques. Des experts du domaine devraient définir l'activité de sécurité et l'activité de vérification, tel que défini à l'annexe XIII.9. Par exemple, un CSA requis pour assurer la révision de code Java devrait avoir été développé par un programmeur sénior compétent, dans ce langage.
   b) la vérification et l'intégration des CSA à la bibliothèque de CSA de l'organisation;

      Une équipe de vérification composée de gestionnaires, de développeurs, de responsables d'infrastructure TI et de vérificateurs, tous experts séniors dans leur domaine d'expertise respectif, devraient être responsable de la validation des CSA liés à leur domaine de connaissances respectif, afin de s'assurer que les CSA proposés pour être intégrés à La bibliothèque de CSA, soient clairs et qu'ils fourniront des instructions précises à ceux qui les utiliseront. L'équipe de vérification doit aussi

valider que les CSA réduisent effectivement chacun des risques de sécurité identifiés au niveau acceptable, tel que défini par l'organisation. L'équipe devra également préciser pour quels niveaux de confiance ces CSA seront nécessaires. C'est au comité du CNO que revient l'approbation finale des CSA, des processus et de La bibliothèque de CSA de l'organisation.

3) Analyser et comparer les activités définies dans le modèle de référence du cycle de vie de la SA avec les activités existantes dans les méthodes et les processus de l'organisation;
4) Aligner les activités du modèle de référence avec celles de l'organisation;
5) Voir à ce que les activités proposées par le modèle de référence soient toutes incluses dans les processus et les méthodes de l'organisation, afin de pouvoir assurer un arrimage complet des éléments de la SA aux activités requises par l'organisation;
6) Communiquer aux personnes concernées l'information sur les éléments du CNO, et en promouvoir l'utilisation.

XIV.1.4.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Mise en place de processus, directives et règlements en SA en fonction des besoins de l'organisation;
2) Intégration des CSA dans la bibliothèque;
3) Préparation de la documentation sur la révision et l'arrimage des méthodes et des processus de l'organisation concernant la SA avec le MRCVSA;
4) Réalisation d'un plan de communication et de formation en SA arrimé aux éléments du CNO.

XIV.1.5 Surveiller et réviser la sécurité des applications dans l'organisation

Ce sous-processus consiste à examiner et à ajuster les composants et processus du CNO afin de s'assurer qu'ils diminuent toujours adéquatement les risques pour lesquels ils ont été

conçus, puis mis en place, et qu'ils sont utilisés en conformité avec la politique de la SA de l'organisation.

XIV.1.5.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont notamment de veiller à ce que les projets d'applications utilisent correctement les composants de SA du CNO qui sont à jour, et à recueillir les commentaires des projets.

XIV.1.5.2 Activités

Afin d'atteindre les objectifs visés, les activités suivantes devront être réalisées :

1) S'assurer que toutes les applications identifiées comme sensibles et utilisées par l'organisation, possèdent au niveau de confiance cible et un niveau de confiance actuel;
2) Utiliser et mettre à jour la matrice de traçabilité des risques de SA pour s'assurer que tout changement concernant :
   a) les risques de sécurité détectés entraîneront les changements requis aux exigences, aux processus de SA et aux CSA qui les concernent;
   b) les processus et CSA modifiés entraîneront les changements requis et l'application des nouveaux processus et CSA aux applications concernées.
3) S'assurer que la matrice de traçabilité des risques de SA est complète, et qu'elle décrit notamment les liens entre tous les groupes d'informations, les risques de SA, les exigences de sécurité qui ont été identifiés, ainsi que les CSA de l'organisation. *(Voir* XIII.3.2 pour plus de détails sur le contenu de cet élément.)
4) Consigner et conserver les résultats d'une évaluation périodique des risques de sécurité pour toutes les applications utilisées par l'organisation, afin de valider l'existence ou d'identifier tout changement dans la liste ou l'évaluation des risques de sécurité identifiés;
5) Récupérer de façon formelle et présenter au comité du CNO des idées, des propositions de nouvelles solutions et des commentaires émis par les équipes de projets d'applications

concernant le développement ou l'amélioration des CSA ou des processus de sécurité des applications.

XIV.1.5.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Production des différents rapports attendus sur les analyses de risques de sécurité des applications;
2) Atteinte du niveau de confiance assigné à chaque application sensible de l'organisation;
3) Mise à jour d'une matrice de traçabilité;
4) Élaboration d'une liste de propositions des prochaines actions à prendre concernant la SA de l'organisation.

XIV.1.6 Amélioration continue de la sécurité des applications dans l'organisation

L'amélioration continue de la SA dans l'organisation consiste à l'ajout, au maintien et à l'amélioration de tous les éléments du CNO, en réalisant une revue périodique des différents contextes de l'organisation, des rôles et des responsabilités de ses divers intervenants, ainsi que des processus et des technologies utilisés par les applications de l'organisation.

XIV.1.6.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont notamment :

1) D'améliorer l'efficacité, l'efficience, la convivialité et la pertinence des éléments du CNO;
2) De maintenir le CNO aligné avec le SGSI et les priorités de l'organisation.

XIV.1.6.2 Activités

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) Identifier tout changement pouvant requérir l'évaluation d'un nouveau risque de SA que l'organisation doit gérer ou demander la réévaluation d'un risque existant;
2) Identifier tout changement dans les priorités, les stratégies et les besoins de l'organisation concernant la SA;
3) Assurer la prise en compte de ces changements et de l'intégration des réponses de l'organisation les concernant dans le CNO;
4) Voir à ce que la matrice de traçabilité des risques de SA soit intègre, complète et à jour;
5) Prendre les mesures appropriées pour que les impacts de ces changements soient aussi pris en compte par le processus de gestion de projets d'applications de l'organisation et que les ressources nécessaires aient été évaluées et soient disponibles pour leur mise en place;
6) Gérer les changements requis dans le CNO.

XIV.1.6.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Identification et approbation des changements requis par l'organisation aux éléments de la SA;
2) Réponse attendue des éléments du CNO aux besoins et priorités de l'organisation;
3) Connaissance, approbation et disponibilités des ressources requises pour la mise en place et la maintenance des éléments du CNO, ainsi que pour la formation des différents acteurs;
4) Intégration dans les processus de l'organisation des éléments de la SA.

XIV.1.7 Auditer la sécurité des applications dans le CNO

Cinquième des sous-processus utilisés pour gérer le CNO, ce dernier est utilisé pour vérifier et s'assurer que tous les éléments concernant la SA, prévus pour l'intégration au CNO, soient présents, qu'ils aient été validés vérifiés et approuvés par les autorités adéquates, qu'ils soient fonctionnels et disponibles à l'utilisation par les projets des applications de l'organisation.

Pour plus d'information, voir l'annexe XIV.4 – Audit et certification de la mise en œuvre du modèle SA.

XIV.1.7.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont de s'assurer :

1) De la conformité du CNO aux priorités et aux exigences de SA de l'organisation;
2) Que les applications sensibles de l'organisation auront été identifiées et qu'elles sont sécuritaires.

XIV.1.7.2 Activités

Afin d'atteindre les objectifs visés, les activités suivantes devront être réalisées :

1) Prendre connaissance des priorités et des exigences de SA de l'organisation et de l'organisation mère qui la dirige, lorsque requise par cette dernière;
2) Auditer les éléments d'un CNO afin d'en évaluer la conformité aux priorités et aux exigences de SA identifiées.

Note : ces activités de vérification et d'audits pourront être réalisées soit par une équipe de vérification interne, soit par une équipe de vérification externe, selon les objectifs visés par le demandeur de l'audit. Dans tous les cas, les résultats d'un audit d'un CNO devraient donner les mêmes résultats.

XIV.1.7.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Identification de la liste des priorités et des exigences de SA de l'organisation;
2) Les éléments requis par les exigences identifiées :
    a) répondent adéquatement à celles-ci;
    b) sont en place dans le CNO;
    c) sont intégrés aux processus de l'organisation;
    d) les ressources nécessaires à leur gestion, leur maintenance et leur utilisation sont disponibles.

XIV.2 Gestion des risques de la sécurité d'une application

Ce processus est mis en place et approuvé par le comité de gestion du CNO. Il est utilisé 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. La gestion des risques est un concept clé en sécurité de l'information et elle « … peut être appliquée à l'ensemble de l'organisation, à l'une de ses parties (un département, un emplacement physique, un service), à tout système d'information existant ou planifié, ou à un processus particulier de contrôle (processus de planification de la continuité de l'entreprise). » (ISO/IEC, 2010d, p. 7). « La gestion des risques est un processus qui consiste à diriger et à contrôler un organisme en matière de risque » (ISO/IEC, 2010d, p. 5).

Selon ISO 27005, ce processus comprend les cinq étapes suivantes :

1) Établir le contexte;
2) Évaluer les risques de sécurité de l'information en :
    a) Identifiant les risques;
    b) Analysant les risques;
    c) Évaluant la portée des risques.

3) Traiter les risques de sécurité de l'information et accepter les risques résiduels;
4) Communiquer l'information sur les risques;
5) Surveiller et revoir les risques et leur ampleur.

La gestion des risques de SA est le processus qui permet de maintenir les risques de sécurité, lors de l'utilisation d'une application, à des niveaux acceptables. Cette gestion est réalisée en appliquant des contrôles aux risques qui sont jugés inacceptables, et ce, par la mise en œuvre des CSA pour chacun d'eux.

XIV.2.1 Objectifs de la mise en place du processus de gestion des risques de la sécurité des applications

Un processus de gestion des risques de SA doit utiliser ces mêmes étapes, mais en ajustant la portée et la granularité de chacune d'elles à l'application. Les objectifs visés par ce processus consistent à diriger et à contrôler :

1) La sélection, la validation, l'intégration et la maintenance des CSA dans le CNO, et
2) Leur mise en place dans le cycle de vie des applications de l'organisation afin de diminuer, à des niveaux acceptables, les risques qui les menacent.

Afin d'atteindre ces deux objectifs, les étapes de la gestion des risques de sécurité de l'information amenées par ISO 27005 ont été intégrées aux deux principaux processus du modèle soit :

1) Au processus de gestion du CNO de l'organisation (PGCNO) (*Voir* XIV.1); ainsi qu'
2) Au processus de gestion de la sécurité d'une application (PGSA) (*Voir* XIV.3).

En reprenant les cinq étapes de la norme ISO 27005, cette intégration se présente comme suit :

1) Établir le contexte
   a) cette activité est réalisée au niveau de l'organisation (PGCNO) lors de l'identification et de la consolidation dans le CNO des différentes exigences, des différents

environnements, spécifications et groupes d'informations catégorisés des applications;

b) cette activité est réalisée à l'étape 1 du PGSA – Identifier les besoins et l'environnement de l'application (*Voir XIV.3.3*), lors de l'établissement du contexte de l'application, soit son environnement, ses spécifications et lorsque sont identifiés et classifiés les groupes d'informations impliqués par l'application.

2) Évaluer les risques de sécurité de l'information

a) cette activité, qui consiste à identifier, analyser et à évaluer les risques de sécurité, est réalisée au niveau de l'organisation (PGCNO) lors de l'identification des applications sensibles qui devraient être sécurisées, étant donné qu'un bris de sécurité produirait un impact inacceptable pour l'organisation;

b) cette activité est réalisée à deux endroits durant le processus de PGCSA, soit :

i) à l'étape 2 – Évaluer les risques de sécurité amenés par l'application (*Voir XIV.3.4*). C'est à cette étape que :

(1) sont évalués les principaux risques d'utiliser l'application. L'évaluation des risques de SA détermine la valeur des groupes d'informations impliqués par l'application, identifie les menaces et les vulnérabilités qui existent (ou pourrait exister), identifie les CSA existants et leur effet sur le risque identifié, détermine les conséquences potentielles et, enfin, priorise les risques résiduels et les classe en fonction de l'environnement de l'application concernée et des critères d'évaluation définis par l'organisation;

(2) le niveau de confiance cible est assigné à l'application;

ii) à l'étape 4 – Réaliser et opérer l'application (*Voir XIV.3.6*). C'est à cette étape que :

(1) l'évaluation détaillée des risques de sécurité amenés par l'application est réalisée;

(2) le niveau de confiance cible assigné à l'application est validé et approuvé.

3) Traiter les risques de sécurité de l'information et accepter les risques résiduels

a) cette activité est réalisée au niveau de l'organisation (PGCNO) lors de la conception, de la validation, du développement et de la vérification des CSA;

b) cette activité est réalisée à deux endroits durant le processus de PGCSA, soit :
   i) à l'étape 3 – Créer et maintenir le cadre normatif de l'application (*Voir XIV.3.5*), lorsque sont identifiés les CSA qui devront être mis en place pour diminuer tous les risques de sécurité à des niveaux acceptables;
   ii) à l'étape 4 – Réaliser et opérer l'application (*Voir XIV.3.6*), lorsque les CSA sont mis en place et testés pour une application.

4) Communiquer les risques

La communication des risques et les consultations, entre les décideurs et les différents intervenants, doivent être réalisées tout au long du processus de gestion des risques de sécurité (ISO/IEC, 2010d, p. 9) :

a) cette activité est réalisée au niveau de l'organisation (PGCNO) à la suite :
   i) de la détection de tout changement pouvant avoir un impact sur les risques de sécurité provenant des trois contextes de l'organisation;
   ii) de la mise à jour de la matrice de traçabilité de la SA de l'organisation;
   iii) de tout changement apporté à la bibliothèque de CSA ou aux CSA.
b) cette activité est réalisée à deux endroits durant le processus de PGCSA, soit :
   i) à l'étape 2 – Évaluer les risques de sécurité amenés par l'application, à la suite de l'analyse de risque de haut niveau de la sécurité de l'application; et
   ii) à l'étape 4 – Réaliser et opérer l'application, à la suite de l'analyse de risque détaillée de la sécurité de l'application.

5) Surveiller et réviser les risques

a) cette activité est réalisée au niveau de l'organisation (PGCNO) lors de la veille visant la détection :
   i) de tout changement pouvant avoir un impact sur les risques de sécurité provenant des trois contextes de l'organisation;
   ii) de tout changement pouvant améliorer l'implémentation d'un contrôle, par exemple, pour remplacer un CSA jugé mois efficace.
b) cette activité est réalisée à l'étape 3 du PGSA – Créer et maintenir le cadre normatif de l'application (*Voir XIV.3.5*), lors de la modification du CNA pouvant survenir,

notamment, à la suite d'une demande de changement de l'application ou d'un changement d'un des processus concernant l'application.

6) Vérifier la sécurité de l'application

   Cette étape n'est pas présente dans le processus de gestion du risque proposé par ISO 27005. Elle a été ajoutée par le modèle pour s'assurer de l'implémentation et du suivi du bon fonctionnement des CSA tout au long du cycle de vie de l'application. Elle concerne la collecte et la vérification de preuves permettant de confirmer l'atteinte et la maintenance du niveau de confiance ciblé pour l'application. Cette activité est réalisée à l'étape 5 du PGSA – Vérifier la sécurité de l'application (*Voir XIV.3.7*).

XIV.2.2 Analyse de risques de sécurité d'une application

Selon ISO 27005 (ISO/IEC, 2010d, p. 21), « L'évaluation des risques utilise la compréhension du risque obtenu par l'analyse de risques pour prendre les décisions sur les actions à réaliser. Ces décisions devraient inclure :

1) si une activité doit être entreprise; et
2) les priorités de traitement des risques considérant les niveaux de risques estimés. »

Contrairement au vocabulaire utilisé par la norme ISO 27005 sur la gestion des risques de sécurité de l'information, l'industrie appelle « méthode d'analyse de risque » l'outil utilisé pour identifier, comprendre et prendre les décisions sur les actions à poser pour diminuer les risques.

Il est ici important de noter que des méthodes d'analyse des risques de sécurité telles que MÉHARI, OCTAVE ou EBIOS ont été conçues pour évaluer des risques de sécurité organisationnelle. 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 propose la méthode d'analyse de

risques de la sécurité d'une application « ASIA » (*Voir* XIV.2.3) qui ne présente pas ces lacunes.

L'analyse de risques de sécurité d'une application est réalisée sommairement à la deuxième étape du PGSA, puis de manière plus détaillée à la cinquième étape. C'est un processus qui permet de comprendre l'origine et la nature des risques, et de déterminer leurs niveaux d'acceptabilité. Il constitue la base de l'évaluation des risques et des décisions concernant leur traitement.

Cette analyse est réalisée au niveau de l'application. Elle permettra d'identifier les groupes d'informations impliqués par l'application, d'en déterminer leur valeur pour l'organisation, puis d'identifier les menaces et les vulnérabilités qui les concernent.

Les risques de SA proviennent principalement :

1) des menaces ciblant les informations sensibles impliquées dans l'acquisition et l'utilisation d'une application;
2) des vulnérabilités de l'application l'empêchant de protéger correctement ces informations; et
3) de l'impact d'un événement concernant une vulnérabilité.

Dans l'éventualité où l'organisation n'aurait pas encore intégré une méthode d'analyse de risques de SA dans son CNO, il revient alors au propriétaire de l'application de s'assurer que les résultats de l'analyse qu'il obtiendra auront été produits à l'aide d'une méthode permettant de réaliser une analyse de risques de sécurité au niveau de l'application.

Finalement, la La méthode d'analyse de risques de la sécurité d'une application : ASIA est présenté dans ce chapitre afin d'assister une organisation dans le développement ou la validation d'une méthode d'analyse de risques de SA à intégrer dans son CNO.

XIV.2.2.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont :

1) d'identifier les risques découlant de l'acquisition et l'utilisation d'une application dans un environnement spécifique; et
2) de produire une liste d'exigences de sécurité permettant de ramener ces risques à un niveau acceptable pour l'organisation.

XIV.2.2.2 Activités

Afin d'atteindre les objectifs visés, les activités suivantes devront être réalisées (*Voir* ANNEXE XVII, Figure-A XVII-1) :

1) **Valider le contexte de l'analyse des risques de la sécurité d'une application**

   Réaliser un processus d'analyse de sécurité qui identifiera tous les risques menaçant les groupes d'informations est un processus qui peut être long et ardu. Il n'est possible d'identifier tous les risques de sécurité amenés par une application que lorsque, notamment, toutes ses spécifications ont été précisées, que les éléments présents dans l'environnement de l'application aient été identifiés, et tous les groupes d'informations impliqués par celle-ci ont été identifiés et catégorisés (*Voir* ANNEXE XVII, Figure-A XVII-1, section : *ISO 27005 – 7. Context establishment*).

   L'objectif ici, étant d'assigner un niveau de confiance cible à l'application et d'identifier les CSA à mettre en œuvre pour la sécuriser au niveau attendu.

2) **Analyse des risques de sécurité de l'application**

   Selon la méthode de développement ou de réalisation utilisée par l'organisation, certains de ces éléments nécessaires pour compléter l'activité précédente sont généralement précisés lors du processus de conception de l'application. Ce qui est habituellement beaucoup trop tard au goût des gestionnaires de projets.

Deux niveaux d'analyse de sécurité sont donc proposés par le modèle. Le premier, de niveau sommaire, permet d'identifier rapidement les principaux risques de SA à partir d'informations préliminaires d'un projet d'application. Le deuxième, de niveau détaillé, permet d'identifier les risques de SA de manière plus détaillée.

La première approche consiste à procéder à une analyse sommaire (a), dont l'objectif principal est de donner, en début de projet, une idée générale des principaux risques de sécurité pouvant menacer une application. La deuxième approche d'analyse est plus détaillée (b); elle sera réalisée une fois que les éléments de l'environnement de l'application auront été suffisamment précisés. L'objectif ici, étant de valider le niveau de confiance ciblé pour l'application et d'identifier les CSA à mettre en œuvre.

Pour les deux approches, il s'agit du même processus d'analyse de risques de sécurité qui est appliqué. Seul le niveau de détail des éléments de l'application qui y sont analysés diffère (*Voir* ANNEXE XVII, Figure-A XVII-1, sections : *ISO 27005 – 8. Information security risk assessment* et *9. Information security risk treatment*).

a) Analyse sommaire des risques de sécurité de l'application

L'analyse sommaire des risques de sécurité est réalisée pendant la phase de préparation du cycle de vie de l'application, soit à l'étape 2 du PGCSA, lorsque l'organisation a une bonne idée du futur environnement de l'application et du pourquoi elle veut utiliser cette application, mais où toutes les réponses techniques et les spécifications la concernant n'ont pas encore toutes été précisées.

Cette analyse a pour but d'identifier et d'évaluer les principaux risques à acquérir et à utiliser l'application. Réalisée à partir des résultats de l'étape 1 du PGCSA, soit de l'environnement et des groupes d'informations identifiés, des spécifications sommaires attendues de l'application, ainsi que des résultats d'analyses de risques de sécurité précédentes d'applications possédant des caractéristiques semblables, elle

identifie selon une simple « règle du pouce », le niveau de confiance ciblé pour une application.

b) Analyse détaillée des risques de sécurité de l'application

Cette analyse peut être réalisée plusieurs fois, au cours de l'étape 4 – Réaliser et opérer l'application du PGSA, soit durant les phases « Réalisation », « Transitions », « Utilisation et maintenance » et « Disposition » du cycle de vie de l'application (*Voir* Figure-A XIII-6).

C'est notamment à partir des informations décrivant l'environnement de l'application, soit les contextes d'affaires, juridiques et technologiques où elle sera assemblée et utilisée, ses spécifications, ainsi que les processus, les acteurs et les groupes d'informations impliqués par l'application, qui ont tous été intégrés au CNA, que cette analyse de risques de sécurité permettra d'identifier plus précisément les risques liés à l'acquisition et à l'utilisation de l'application. L'objectif ici est de préciser le plus clairement possible les risques de sécurité amenés par cette application, puis de spécifier les exigences de sécurité, de sélectionner les CSA qui devraient être mis en place et de présenter les risques résiduels qui devront être acceptés.

XIV.2.2.3 Résultats

C'est à partir de la sensibilité des groupes d'informations impliqués par l'application, de l'environnement de l'application concernée et des critères d'évaluation définis par l'organisation, que cette analyse permettra d'identifier les risques de sécurité qui concernent l'application, soit :

1) Identifier les menaces et les vulnérabilités applicables qui existent (ou pourrait exister), évaluer leurs probabilités et les impacts si celles-ci survenaient;
2) Identifier les exigences de sécurité et les CSA correspondants en fonction de leur effet d'atténuation sur le risque identifié;

3) Identifier le niveau de confiance contenant minimalement, les CSA identifiés à l'étape précédente;
4) Déterminer les conséquences potentielles sur le projet d'application;
5) Identifier les risques résiduels qui devront être acceptés par l'organisation.

De plus, les activités servant à l'identification, au suivi, au stockage, à la mesure ainsi qu'à rapporter les risques de sécurité pouvant cibler les informations sensibles d'une application sont de la plus grande importance.

À la suite de la réception des résultats de cette analyse, le propriétaire de l'application doit accepter et approuver ou rejeter le niveau de confiance ciblé. De plus, il peut en tout temps, décider de changer le niveau de confiance de l'application pour le projet d'application soit, par exemple, parce qu'il considère que les coûts de sécurité sont trop importants, ou encore parce qu'il considère que cette application nécessiterait une protection plus importante.

Le niveau de confiance cible assigné à l'application est ainsi validé et approuvé.

Un changement de niveau de confiance cible modifiera la liste des CSA sélectionnée pour le projet, ce qui pourra amener des changements sur la liste et les qualifications des acteurs requis pour le projet, ainsi que l'estimation du coût pour y intégrer la sécurité. Cependant, ces effets sont plus facilement prévisibles, car l'information concernant les rôles des acteurs, les qualifications professionnelles requises et le coût approximatif pour la mise en place d'un CSA est déjà incluse dans sa description.

XIV.2.3 La méthode d'analyse de risques de la sécurité d'une application : ASIA

Les risques de SA sont en fait les risques auxquels une organisation s'expose lorsqu'elle décide d'acquérir et d'utiliser une application spécifique pour soutenir un de ses processus d'affaires. La méthodologie d'analyse des risques de sécurité des applications ASIA (*Application Security Issues Analysis*) 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* 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.

XIV.2.3.1 Objectifs

Les objectifs visés par le développement de la méthode d'analyse de risques de SA ASIA sont de proposer aux organisations une méthode leur permettant :

1) De compléter les évaluations de risques réalisées par les méthodes d'analyse de risques de sécurité de niveau organisationnel en proposant aux organisations un processus (méthode) adapté à la gestion des risques de sécurité des applications;
2) D'offrir un niveau de granularité permettant d'identifier les flots d'informations à l'intérieur des processus de l'application, d'évaluer des risques de sécurité qui les concernent, d'identifier les exigences et de mettre en place des CSA;
3) De fournir des outils et un processus d'analyse reproductible afin d'assister l'organisation dans :
    a) l'identification et l'évaluation des risques de sécurité existant dans le cycle de vie d'une application;
    b) la mise en place de contrôles pour réduire ces risques à des niveaux acceptables.
4) De s'assurer que tous les projets d'applications d'une organisation évalueront et traiteront les risques de sécurité de la même manière.

XIV.2.3.2 Activités

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) Établir le contexte

(*Voir* Figure-A XVII-1, section : *ISO 27005 – 7. Context establishment*).

a) Identification des critères d'évaluation :
   i) les critères de classification;
   ii) les critères d'impact;
   iii) les critères d'évaluation de risque;
   iv) les critères d'acceptation de risque.

b) À partir des besoins d'affaires de l'organisation, on identifie :
   i) les exigences qui sont hors portée;
   ii) les exigences qui font partie de la portée de l'application. Ces dernières sont notamment composées :
      (1) des exigences de système;
      (2) des exigences fonctionnelles;
      (3) des règles d'affaires;
      (4) des interfaces externes;
      (5) des exigences utilisateurs;
      (6) des exigences d'infrastructure;
      (7) des attributs de qualité;
      (8) des contraintes.
   iii) Les exigences de l'application sont utilisées pour identifier :
      (1) L'environnement de l'application qui est composé :
         (a) du contexte d'affaires;
         (b) du contexte juridique;
         (c) du contexte technologique de l'application.
      (2) Les éléments présents dans le cycle de vie de l'application, soit :
         (a) l'information concernant l'application
            (i) l'identification des groupes d'informations concernant l'application;

(ii) la catégorisation de la sensibilité de l'information identifiée;

(iii) l'identification des informations sensibles;

(iv) l'identification des événements pouvant menacer l'information sensible.

(b) les processus de l'application, soit :

(i) l'identification des processus concernant l'application;

(ii) la catégorisation de la sensibilité des processus identifiés en fonction de l'information qu'ils manipulent;

(iii) l'identification des processus sensibles;

(iv) l'identification des événements pouvant menacer l'information sensible via ces processus.

(c) les spécifications de l'application, soit :

(i) l'identification des spécifications de l'application;

(ii) la catégorisation de la sensibilité des spécifications identifiées en fonction de l'information qu'ils manipulent;

(iii) l'identification des spécifications sensibles;

(iv) l'identification des événements pouvant menacer l'information sensible via ces spécifications.

(d) les acteurs impliqués par l'application, soit :

(i) l'identification des rôles impliqués dans les spécifications et processus présents dans le cycle de vie de l'application;

(ii) la catégorisation de la sensibilité des acteurs identifiés en fonction de l'information qu'ils manipulent;

(iii) l'identification des rôles sensibles;

(iv) l'identification des événements pouvant menacer l'information sensible via ces rôles.

c) les menaces sont identifiées à partir :

i) de l'environnement de l'application;

ii) des spécifications, des processus et des acteurs sensibles;

iii) de l'information ciblée par une menace.

d) les vulnérabilités sont identifiées à partir :
    i) du contexte technologique de l'application;
    ii) des rôles sensibles;
    iii) des processus sensibles;
    iv) des spécifications sensibles de l'application.
e) les impacts sont évalués à partir :
    i) de la valeur de l'information sensible de l'application pour l'organisation;
    ii) des critères définissant un impact acceptable d'un impact inacceptable, soit :
        (1) les critères d'un impact inacceptable;
        (2) les critères d'un impact acceptable et des risques résiduels.
f) l'identification, l'évaluation et la gestion des risques sont réalisées en considérant les événements qui génèrent un impact en violant une information sensible, soit :
    i) les menaces;
    ii) les vulnérabilités;
    iii) les impacts;
    iv) les risques résiduels;
    v) les critères d'évaluation de risque;
    vi) les critères d'acceptation de risque.
g) l'identification, l'évaluation et la gestion des risques permettent d'identifier :
    i) les risques actuels acceptables;
    ii) les risques actuels inacceptables qui vont permettre de définir :
        (1) les exigences de sécurité qui vont permettre de définir :
            (a) un CSA qui, une fois implémenté, va fournir les résultats attendus démontrant la diminution du risque.
h) les processus de validation, de vérification et d'audit des résultats produits par les CSA serviront pour :
    i) identifier les risques résiduels;
    ii) confirmer l'atteinte du niveau de confiance de l'application.

Note : la méthode ASIA recommande l'adaptation d'une banque de connaissances, présentée sous la forme d'un questionnaire fourni par la méthode, qui regroupe des questions afin de guider l'organisation dans la couverture de l'identification des groupes d'informations, des contextes, des processus, des spécifications et des rôles impliqués par l'acquisition et l'utilisation de l'application dans l'organisation.

2) Évaluer les risques de sécurité de l'information

(*Voir* Figure-A XVII-1, section : *ISO 27005 – 8. Information security risk assessment*)

a) à partir des menaces, vulnérabilités et des impacts identifiés, est réalisée l'identification, l'estimation et l'évaluation des risques de sécurité de l'application en tenant compte des critères d'évaluation et d'acceptation des risques de l'organisation (définie à l'étape 1);
   i) L'identification des risques résiduels acceptables;
   ii) L'identification des risques inacceptables.

3) Traiter les risques de sécurité de l'information et accepter les risques résiduels

(*Voir* Figure-A XVII-1, section : *ISO 27005 – 9. Information security risk treatment*).

Les réponses aux questions proposées par la méthode ASIA guideront l'organisation dans la sélection ou la définition de ses exigences de sécurité, du niveau de confiance ciblé et dans la sélection des CSA devant être mis en place dans l'application. Il s'agit :

a) d'identifier, d'évaluer, de prioriser et de planifier les ressources requises pour réaliser les travaux requis;
b) de gérer les changements détectés et d'adapter les éléments du CNO dont, notamment, la bibliothèque et les CSA qu'elle contient, et ce, de manière à ramener ou à conserver les risques identifiés à des niveaux acceptables.

4) Communiquer les risques

La méthode ASIA recommande d'utiliser le composant « matrice de traçabilité » en guise de dépôt central pour y conserver les risques de sécurité qui ont été identifiés par les processus de gestion des risques des différents projets d'applications de l'organisation.

Tout risque de sécurité identifié lors de la réalisation d'une analyse de risques devra y être consigné et communiqué.

5) Surveiller et réviser les risques

a) Au niveau organisationnel :

i) le comité du CNO doit mettre en place un processus qui lui permettra :

(1) de surveiller l'évolution des trois contextes inclus dans la CNO pour y déceler tout changement et nouveaux risques qui pourraient survenir dans l'un d'eux;

(2) de réaliser une évaluation des risques de sécurité détaillée afin d'identifier les impacts de ces changements pour l'organisation;

(3) d'identifier et de communiquer, à l'aide de la matrice de traçabilité, les CSA et les applications touchés par cette nouvelle évaluation;

b) Au niveau d'un projet d'application :

i) dès la réception d'une demande de changement ou dès la réception du résultat d'une évaluation de risques de sécurité concernant une application qui lui appartient, le détenteur doit minimalement initier une analyse sommaire des risques de sécurité afin :

(1) d'évaluer l'impact de ces changements sur la sécurité de son application;

(2) d'accepter les risques résiduels;

(3) de s'assurer de la réalisation des travaux, lorsque nécessaire.

XIV.2.3.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Liste catégorisée des groupes d'informations couverte par cette analyse;
2) Liste catégorisée des processus et des acteurs impliqués par l'application;
3) Liste des risques de sécurité, incluant la probabilité, la menace sur un groupe d'informations et l'impact;
4) Liste des exigences de sécurité concernant les risques identifiés;

5) La liste des risques de sécurité acceptables;
6) Le niveau de confiance répondant à au moins toutes les exigences identifiées.

XIV.3 Gestion de la SA

Ce processus est utilisé par les équipes de projets d'application pour les guider dans l'intégration des éléments de la SA dans leurs projets.

En fait, le modèle SA fournit deux processus (Figure-A XIV-5) :
a) le processus de gestion de la sécurité d'une application (PGSA); et
b) le processus de gestion du CNO (PGCNO).

Ces deux processus sont utilisés à différents niveaux et ont des portées différentes. Le PGCNO est un processus continu de gouvernance qui est de niveau organisationnel, tandis que le PGSA est utilisé pour gérer la sécurité sur les projets d'application spécifiques.

La présente section traite de ce deuxième processus.

XIV.3.1 Objectifs de la mise en place du processus de gestion de la sécurité d'une application

Le processus de gestion de la sécurité d'une application (PGSA) est le processus de gestion s'appliquant à la sécurité de chaque application utilisée par une organisation. Ce processus est un des composants du CNO qui doit être appliqué à toutes les applications de l'organisation.

XIV.3.2 Processus de gestion de la sécurité d'une application

La section XIV.2 a présenté comment le PGSA intègre les éléments de gestion de risques. Maintenant, voyons comment les éléments du modèle sont intégrés dans les activités de projets de réalisation, de maintenance et d'utilisation d'applications spécifiques. Une

application est habituellement sous la responsabilité de son propriétaire qui peut choisir de partager ou de déléguer une partie de cette responsabilité avec d'autres acteurs tels que les gestionnaires des utilisateurs.

La Figure-A XIV-5 présente sommairement le processus de gestion de la SA ainsi que les principaux éléments d'information requis ou produits par celui-ci.

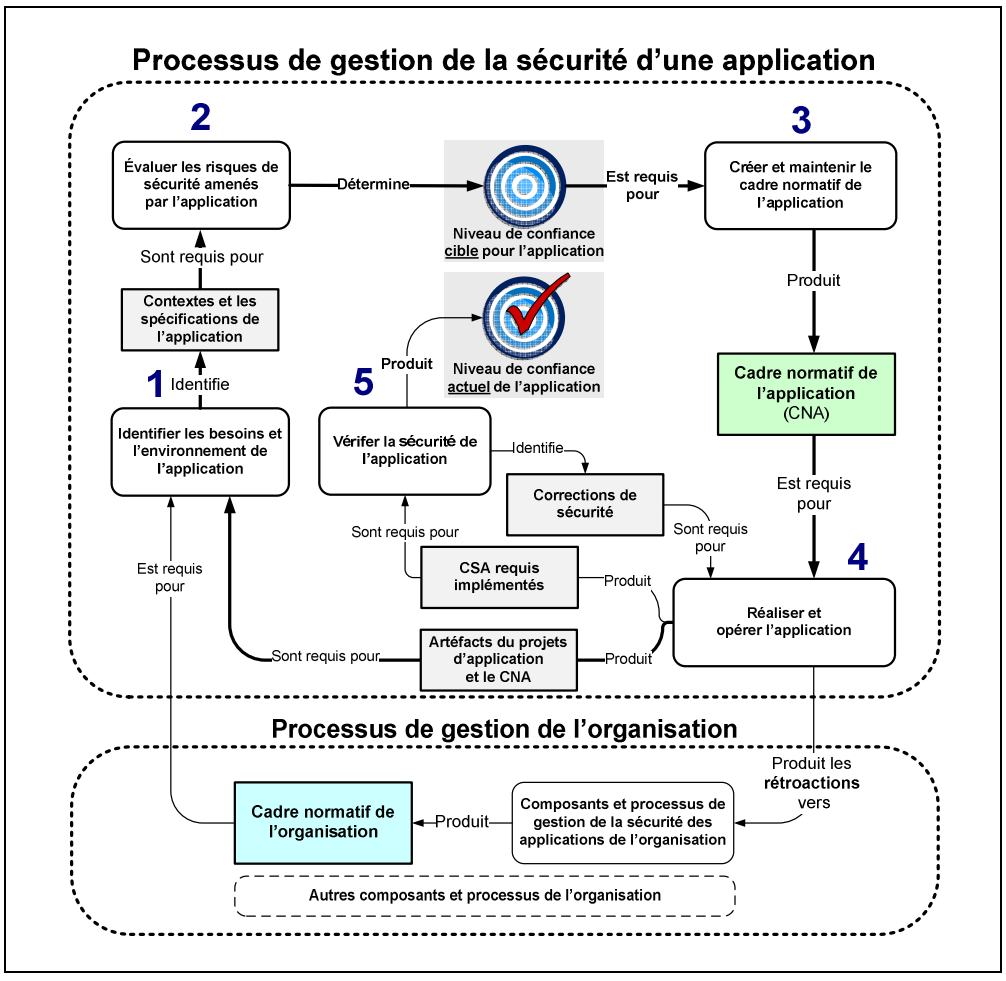


Figure-A XIV-5 Processus de gestion de la SA
Traduite et adaptée de (ISO/IEC, 2011d)

Le processus de gestion de la SA est réalisé en cinq étapes :

1) Identifier les besoins et l'environnement de l'application;
2) Évaluer les risques de sécurité amenés par l'application;

3) Créer et maintenir le cadre normatif de l'application;
4) Réaliser et opérer l'application; et
5) Vérifier la sécurité de l'application.

C’est en utilisant ces cinq processus que le propriétaire de l'application sera en mesure de fournir au SGSI de l'organisation, les preuves nécessaires que la sécurité de son application est bien gérée.

XIV.3.2.1 L’impact du modèle sur un projet d’application

Un projet d'application typique (avant la mise en œuvre de ce modèle) est dirigé par une équipe de projet, est soutenu par des processus, des outils, dans le but de réaliser un produit, soit une application fonctionnelle (Booch, Jacobson et Rumbaugh, 1999). Habituellement, l'équipe d'assurance de la qualité suit un plan de test pour vérifier les fonctionnalités de l'application en fonction des exigences fonctionnelles qui ont préalablement été acceptées.

La technologie elle-même, la méthodologie de développement utilisée par l'équipe du projet, la maturité de processus, la qualité des objets fabriqués et les qualifications des acteurs impliqués dans le projet sont rarement vérifiées, et ces processus de vérification, s’ils sont effectués, ne sont généralement pas formellement définis.

Utilisant la représentation des 4 « P » en développement de logiciel présenté par (Booch, Jacobson et Rumbaugh, 1999) la Figure-A XIV-6 démontre comment le CNO et le CNA s'intègrent dans ce processus.

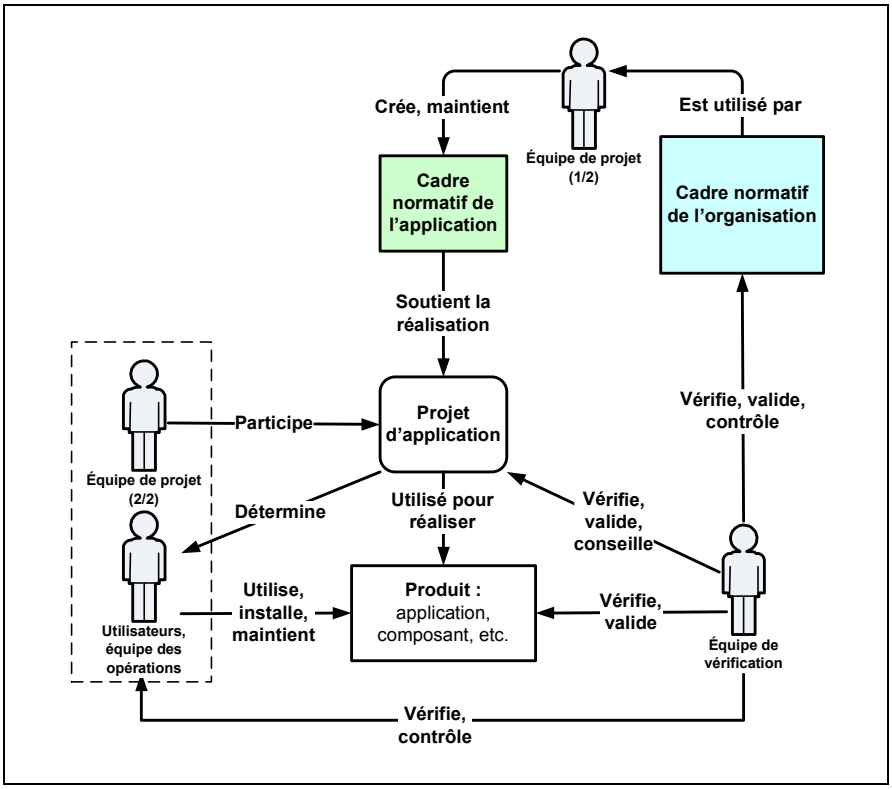


Figure-A XIV-6 Impact de la SA sur les rôles et activités de sécurité de l'organisation
Traduite de (ISO/IEC, 2011d)

XIV.3.3 Identifier les besoins et l'environnement de l'application

L'identification de l'environnement de l'application permet de préciser les trois contextes où évoluera l'application, ses principales spécifications, ses acteurs et processus, ainsi que les groupes d'informations impliqués par son acquisition et son utilisation.

Cette première étape du PGSA correspond à l'étape « établissement du contexte » définie dans le processus de gestion des risques proposé par la norme ISO 27005.

XIV.3.3.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont :

1) Identifier le détenteur de l'application;
2) Identifier, répertorier et consolider dans le CNA les informations nécessaires à la réalisation de l'analyse sommaire de risques de sécurité de l'application.

XIV.3.3.2 Activités

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) L'identification du détenteur

Un des acteurs importants à identifier est le propriétaire de l'application qui a la responsabilité d'accepter les risques résiduels associés à une application spécifique.

Le propriétaire de l'application effectue cette acceptation de deux façons :

a) en approuvant le niveau de confiance ciblé de l'application identifié à l'étape 2 et validé à l'étape 4 du PGSA; et
b) en approuvant les résultats de l'audit de sécurité d'application dans l'étape 5 du PGSA, dans laquelle le niveau de confiance actuel de l'application est mesuré et comparé au niveau de confiance ciblé. Cette étape peut être requise à tout moment par le propriétaire de l'application. Pour une validation supplémentaire, le propriétaire peut exiger de cette étape soit aussi exécutée par une équipe de vérification externe.

Une fois que le propriétaire a effectué cette acceptation, il revient à l'équipe du projet de réaliser les actions nécessaires pour l'atteinte du niveau de confiance ciblé, en mettant en œuvre tout au long du cycle de vie de l'application, les CSA associés au niveau identifié.

2) Identification des informations nécessaires à la réalisation de l'analyse sommaire de risques de sécurité de l'application

Comme présentée à la Figure-A XIV-7 cette étape consiste principalement à identifier et à extraire, des contextes de l'organisation stockée dans le CNO, l'information concernant

spécifiquement l'application, puis à la compléter à l'aide des recherches requises. Une fois terminée, cette étape fournira les informations nécessaires à la réalisation de l'évaluation des risques de sécurité.

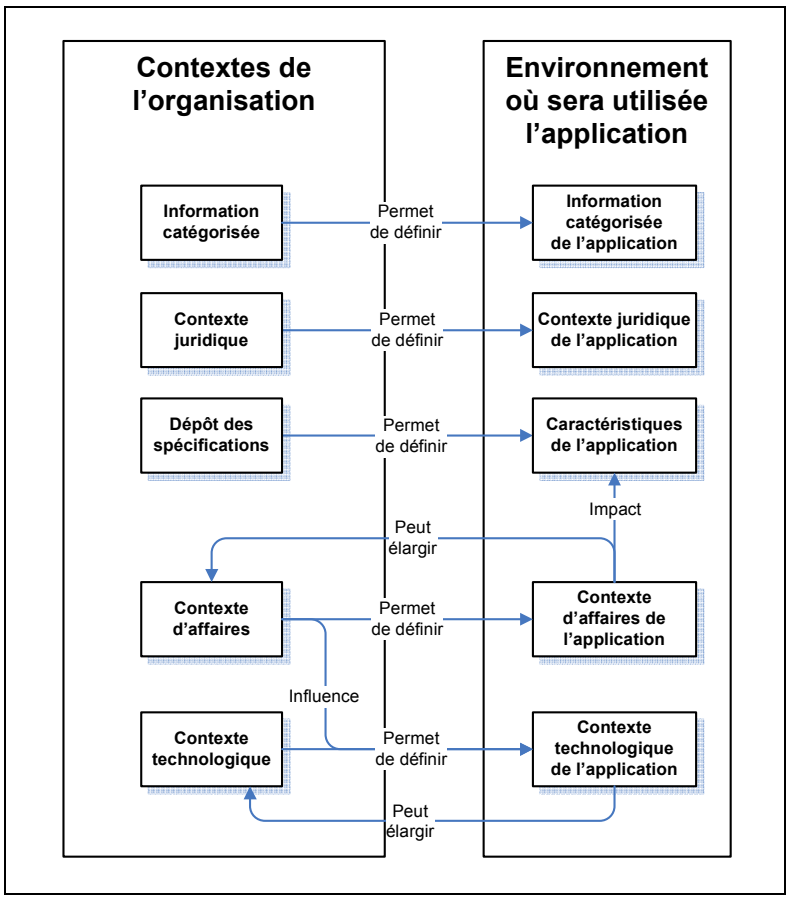


Figure-A XIV-7 Identification de l'environnement de l'application

Cette activité sera réalisée à l'aide des étapes suivantes :

a) identification du détenteur de l'application;

b) identification des besoins de l'organisation menant aux caractéristiques de l'application :

   i) identifier et préciser les exigences de l'application, soit :

      (1) identification des exigences fonctionnelles et non fonctionnelles de l'organisation pour cette application;

      (2) identification des caractéristiques de l'application;

c) identification des spécifications de l'application, soit l'ensemble des exigences auxquelles l'application devra répondre;
d) identification et classification des groupes d'informations impliqués par l'application (*Voir* Figure-A XII-4);
e) identification de l'environnement de l'application, soit :
    i) son contexte d'affaires, incluant les processus, les acteurs et les exigences d'affaires nécessitant ou concernées par la mise en place et l'utilisation de l'application;
    ii) son contexte juridique, identifiant les lois et règlements s'appliquant à l'application; et
    iii) son contexte technologique, identifiant les composants requis par celui-ci.

3) Création d'un CNA

a) Validation, vérification et intégration des résultats de cette activité au CNA de l'application.

XIV.3.3.3 Résultats

Lors de la réalisation de cette étape :

1) Une personne est officiellement désignée comme détenteur de l'application;
2) Un CNA contenant les descriptions sommaires des contextes, des spécifications de l'application ainsi que des groupes d'informations impliqués par l'acquisition et l'utilisation de l'application.

XIV.3.4 Évaluer les risques de sécurité amenés par l'application

L'évaluation des risques de SA diffère d'une évaluation des risques de sécurité organisationnelle par le niveau de granularité ainsi que la portée limitée de l'analyse adaptée à un projet d'application.

Cette étape correspond à la partie « Sélection des options de traitement des risques » de l'étape « de traitement des risques » du processus de gestion des risques proposé par la norme ISO 27005.

NOTE Une méthodologie d'analyse des risques de sécurité organisationnelle pourrait ne pas permettre d'identifier les risques et les contrôles de sécurité requis pour l'utilisation sécuritaire de l'application. Il est recommandé d'utiliser une méthode d'analyse de risques de sécurité spécifiquement développée ou adaptée pour tenir compte des spécificités d'une application et de son environnement.

XIV.3.4.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont :

1) Objectifs de projet : identifier les risques de sécurité, les exigences qui en découlent, le niveau de confiance cible et les CSA requis pour sécuriser une application;
2) Objectif de l'organisation : tenir à jour l'information contenue dans la matrice de traçabilité de l'organisation.

XIV.3.4.2 Activités

La Figure-A XIV-8 donne une vision générale du flot des principaux groupes d'informations impliqués dans ce processus. C'est lors de la réalisation du processus de gestion des risques de sécurité que l'information concernant l'environnement de l'application est récupéré du CNA et qu'elle est utilisée par le processus d'évaluation des risques de sécurité afin de définir les exigences de sécurité requises par l'organisation. Ces exigences permettront d'identifier le niveau de confiance cible et de sélectionner les CSA nécessaires à la sécurisation de l'application.

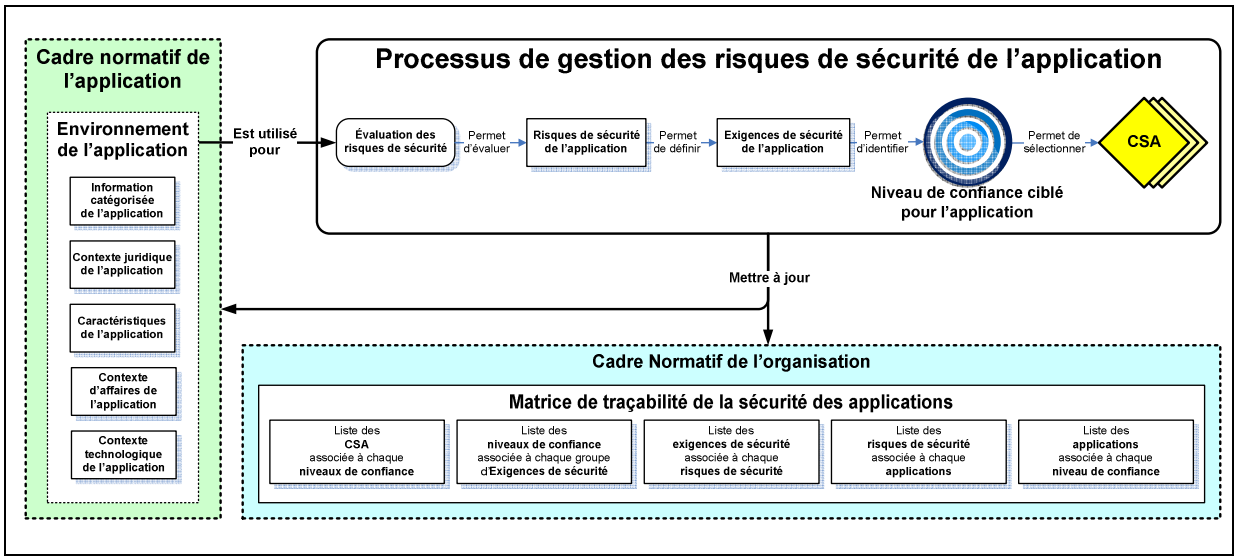


Figure-A XIV-8 Flot d'informations impliquées par le processus de gestion des risques de sécurité de l'application
Traduite et adaptée de (ISO/IEC, 2011d)

Afin d'atteindre les objectifs visés, deux groupes d'activités devront être réalisés :

1) Évaluation sommaire des risques de sécurité de l'application

L'évaluation sommaire des risques de sécurité de l'application consiste, à partir de l'environnement de l'application identifié à l'étape 1, à évaluer sommairement les risques de sécurité amenés par l'application, d'en définir les exigences de sécurité et de cibler le niveau de confiance qui proposera les CSA répondant aux exigences formulées.

Ce processus d'évaluation sommaire des risques de sécurité consiste à :

a) identifier et évaluer des risques de sécurité amenés par l'application;
b) identifier des exigences de sécurité, présentant les objectifs de sécurité minimaux requis pour l'application;
c) déterminer le niveau de confiance cible pour l'application, répondant à toutes les exigences de sécurité identifiées (*Voir* XII.2.12);
d) faire valider et approuver le niveau de confiance cible par le propriétaire de l'application;
e) mettre à jour les données du CNA.

2) **Gestion de la matrice de traçabilité de la SA de l'organisation**

Ce processus utilise les informations produites par les différentes analyses de risques de sécurité que l'organisation aura réalisées pour la tenue du contenu de la matrice de traçabilité à jour.

Ce processus de gestion de la matrice de traçabilité de la SA consiste à :

a) récupérer l'information produite lors de la réalisation d'une analyse de risques de sécurité, incluant notamment le nom de la ou des applications concernées et leurs niveaux de confiances ciblés, la liste des risques évalués et leurs sources respectives, les exigences définies;
b) mettre à jour le contenu de la matrice de traçabilité de l'organisation;
c) rendre l'information accessible aux personnes concernées.

XIV.3.4.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Une version préliminaire du CNA aura été produite et contiendra l'information concernant l'environnement de l'application ainsi que l'information produite par ce processus;
2) Le contenu de la matrice de traçabilité de la SA de l'organisation sera à jour.

XIV.3.5 Créer et maintenir le cadre normatif de l'application

La troisième étape du PGSA permet de sélectionner tous les éléments du CNO qui s'appliquent à un projet d'application spécifique et de compléter le cadre normatif de cette application (CNA). Selon le modèle, le processus de création du CNA pour une application spécifique est indispensable.

Cette étape correspond à la « Préparation et mise en œuvre des plans de traitement des risques » de l'étape « traitement des risques » proposée dans le processus de gestion des risques de la norme ISO 27005.

XIV.3.5.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont :

1) de consolider et tenir à jour les informations produites aux différentes étapes du PGSA dans le CNA;
2) d'importer du CNO, les éléments requis par le projet, incluant les CSA identifiés par le niveau de confiance ciblé;
3) de gérer le contenu du CNA durant tout le cycle de vie de l'application.

XIV.3.5.2 Activités

L'organisation devrait avoir défini et documenté les processus de création, l'approbation et la mise à jour d'un CNA. Ce processus transforme l'information générique contenue dans le CNO et conserve l'information requise pour sécuriser une application spécifique dans son CNA. Les rôles, les responsabilités et les qualifications professionnelles requises des acteurs impliqués dans le CNA devraient aussi avoir été spécifiés.

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) identification et sélection des processus et principales activités qui seront intégrées au cycle de vie de cette application. Ce cycle de vie contiendra uniquement les activités nécessaires pour ce projet d'application, par exemple, un projet développé entièrement à l'interne ne contiendra pas d'activités d'acquisition, ni d'activités d'impartition;
2) vérification de l'alignement des activités sélectionnées aux phases et activités du MRCVSA. Alors que dans la CNO, les activités contenues dans un CSA pointent sur des phases ou des activités listées dans le MRCVSA, les CSA importés dans le CNA pointent

alors, suite à cet alignement, aux phases et activités du modèle du cycle de vie spécifique à cette application;

3) importation dans le CNA des CSA identifiés par le niveau de confiance de l'application;
4) mise à jour et communication du CNA aux personnes concernées.

XIV.3.5.3 Résultats

Un CNA complet, à jour et communiqué, contenant l'ensemble des éléments nécessaires à la sécurisation de l'application.

XIV.3.6 Réaliser et opérer l'application

La quatrième étape du PGSA consiste notamment à utiliser tous les CSA qui ont été importés dans le CNA et à les intégrer aux activités du cycle de vie de l'application.

Cette étape du PGSA correspond à la partie « Préparation et mise en œuvre des plans de traitement des risques » de l'étape « de traitement des risques » définie par processus de gestion des risques de la norme ISO 27005.

XIV.3.6.1 Objectifs

L'objectif visé par ce processus est de mettre en place les éléments du CNA qui sont pertinents pour les étapes, les phases et les activités couvertes par le projet.

XIV.3.6.2 Activités

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) **Réaliser des analyses détaillées des risques de sécurité de l'application** (*Voir* XIV.2.2)
   Avant d'envisager la mise en place des CSA, une analyse détaillée de risques de sécurité doit être réalisée afin de confirmer le niveau de confiance cible de l'application qui a été

identifiée préalablement lors de l'analyse de risque sommaire, réalisée à l'étape 2 du PGSA.

Une analyse détaillée de risques de sécurité de l'application peut être demandée à tout moment, plusieurs fois par projet, lorsque jugée nécessaire par le propriétaire de l'application concernée, par l'équipe de projet ou par l'organisation. L'information requise par ce type d'analyse est généralement rassemblée à la fin des activités d'architecture qui ont lieu durant la phase de conception de l'application, une fois que les exigences de tous les niveaux ont été précisées (*Voir* Figure-A XII-6). Connaissant ainsi plus clairement l'environnement et les exigences de l'application, cette analyse permet d'identifier plus précisément les risques spécifiques de sécurité liés à l'application.
En conséquence, suite aux résultats de cette analyse de risques détaillée, le propriétaire de l'application peut, s'il le juge opportun, modifier le niveau de confiance cible de l'application. Cette modification amènera des changements à la liste des CSA sélectionnés pour le projet, ce qui aura un impact sur les acteurs impliqués et l'estimation du coût pour la mise en place de la sécurité pour le projet. Toutefois, ces impacts seront facilement prévisibles, car les informations requises telles que les acteurs, les qualifications professionnelles et l'estimation quantitative des coûts font déjà partie intégrante de chaque CSA inclus dans la bibliothèque de CSA de l'organisation.

2) Mettre en place les CSA

L'équipe du projet met ainsi en œuvre chaque CSA, en deux étapes, soit :

a) lors de la réalisation de l'activité de sécurité du CSA; et
b) lors de la réalisation de l'activité de vérification de la mesure du CSA (*Voir* XIV.3.7).

Lorsque spécifié dans la description d'une activité d'un CSA, une personne devra préalablement posséder les qualifications requises avant d'être autorisée à la réaliser. Le modèle SA identifie trois groupes de personnes qui peuvent avoir à mettre en place un CSA, soit un membre d'une équipe de projet, un membre de l'équipe des opérations ou un utilisateur (*Voir* Figure-A XIV-9).

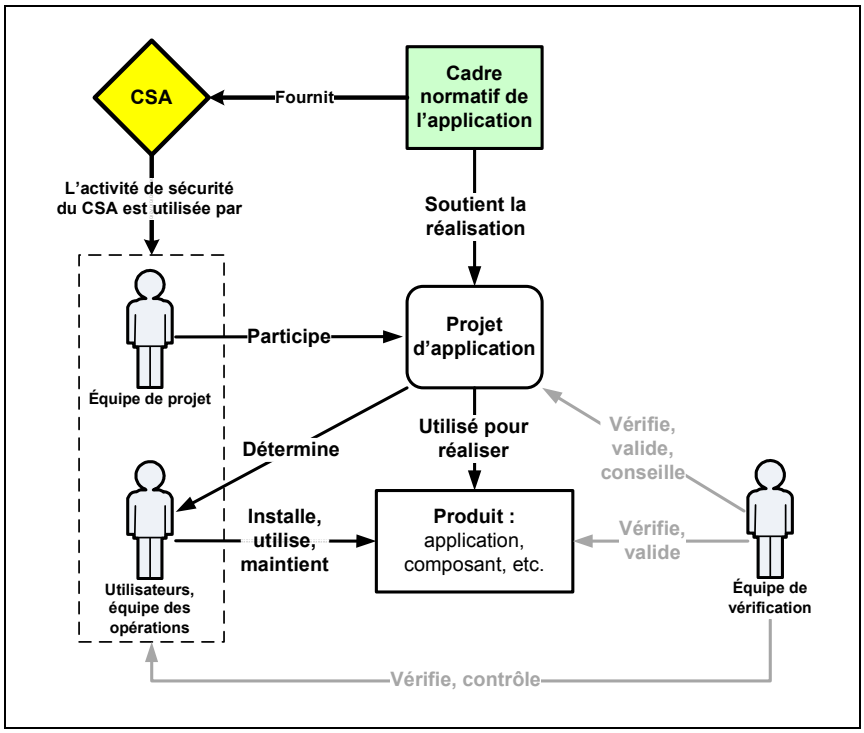


Figure-A XIV-9 Utilisation d'un CSA dans la réalisation des activités de sécurité à l'intérieur d'un projet d'application
Traduite et adaptée de (ISO/IEC, 2011d)

Par exemple, un membre de l'équipe de projet pourrait avoir à mettre en place un CSA alors qu'il participe à la réalisation d'un des processus du projet. Cette activité pourrait être de développer un composant logiciel de vérification et de l'intégrer à l'intérieur de l'application pour assurer l'intégrité de données sauvegardées. De la même manière, un membre de l'équipe des opérations pourrait avoir à réaliser une activité de sécurité décrite par un CSA, alors qu'il exécute une procédure d'installation ou de maintenance d'un composant de l'application. Dans le même ordre d'idée, un utilisateur d'application pourrait avoir à réaliser l'activité d'un CSA lors du changement d'un des paramètres de son profil.

Ayant été préalablement validés et approuvés par l'organisation avant leur déploiement dans la bibliothèque, personne n'est autorisé à mettre en place, sans approbation préalable, un CSA qu'il aurait modifié.

3) **Communiquer les rétroactions du projet au comité du CNO**

Tel que présenté par la Figure-A XIV-2, le PGCNO peut recevoir des rétroactions, produites par le PGSA qui est effectué pour chaque projet d'application dans l'organisation. Ce processus d'amélioration continue, intégré au modèle SA, permet l'évolution du CNO en fonction des besoins de l'organisation.

Cette évolution est notamment réalisée par le biais des rétroactions des projets d'application qui permettent :

a) l'intégration de nouvelles connaissances, de suggestions d'amélioration de CSA ainsi que de nouvelles pratiques acquises par une équipe dans le cadre de l'acquisition et de l'opération d'une application;
b) de recevoir, de valider, de vérifier, d'améliorer au besoin et d'approuver l'activité proposée afin de l'intégrer dans le CNO comme un nouveau CSA ou une nouvelle façon de faire qui devra être adoptée à l'avenir. Dans l'éventualité où aucun élément du CNO n'est disponible pour régler un problème de sécurité spécifique, l'organisation peut alors décider de laisser la liberté à l'équipe de projet d'analyser et de prendre action puis, d'utiliser le processus rétroaction du projet vers le PGCNO pour récupérer ce nouvel élément afin de le valider, de l'ajuster si nécessaire et de le vérifier avant de l'intégrer au CNO (*Voir* XIV.1.5).

XIV.3.6.3 Résultats

La réalisation de l'activité de sécurité du CSA produit :

1) une liste des CSA implémentés ainsi que les résultats obtenus suite à leurs implémentations;
2) les artéfacts du projet d'application incluant la mise à jour du CNA;
3) les rétroactions communiquées au comité du CNO via le PGCNO; et
4) une application qui atteint et maintient le niveau de confiance ciblé.

XIV.3.7 Vérifier la sécurité de l'application

La cinquième et dernière étape du PGSA est la vérification de la sécurité de l'application. Cette vérification consiste à réaliser les activités de vérification de mesures des CSA qui doivent être mis en place dans l'application. Les résultats produits par ces activités permettent de fournir les preuves vérifiables que les CSA devant être en place au moment de la vérification ont bien été implémentés et qu'ils fonctionnent tous, tel que prévu.

Ce processus permet de mesurer le niveau de confiance actuel de l'application et de démontrer l'atteinte du niveau de confiance cible en les comparant entre eux. L'application sera jugée sécuritaire lorsque le niveau de confiance cible approuvé par le propriétaire de l'application sera égal au niveau de confiance actuel, identifié par ce processus.

Ce processus peut aussi être utilisé par les processus d'audit et de certification d'une application et correspond à la l'étape « surveillance et examen » du processus de gestion des risques proposé par la norme ISO 27005.

Notons ici que ce procesus peut être réalisé aussi bien par des équipes de vérifications internes qu'externes, selon les circonstances et les besoins de l'organisation.

XIV.3.7.1 Objectifs

Les objectifs visés par la mise en place de ce processus de gestion du comité du CNO sont notamment de :

1) S'assurer que tous les CSA associés au niveau de confiance ciblé, ont été importés dans le CNA;
2) S'assurer que les activités de vérification des mesures de tous les CSA présents dans le CNA ont été réalisées et que les résultats attendus ont été vérifiés et obtenus;
3) Mesurer le niveau de confiance actuel de l'application afin de pouvoir affirmer qu'une application est considérée sécuritaire à l'intérieur de son environnement.

XIV.3.7.2 Activités

Afin d'atteindre les objectifs visés, les activités suivantes devront être réalisées :

1) **Vérification des CSA d'une application**

L'équipe de vérification réalise les activités de vérification des mesures des CSA afin de confirmer la mise en place et de vérifier le bon fonctionnement de ces derniers. Cette équipe peut aussi conseiller l'équipe de projet dans la mise en place des CSA qui y sont définis.

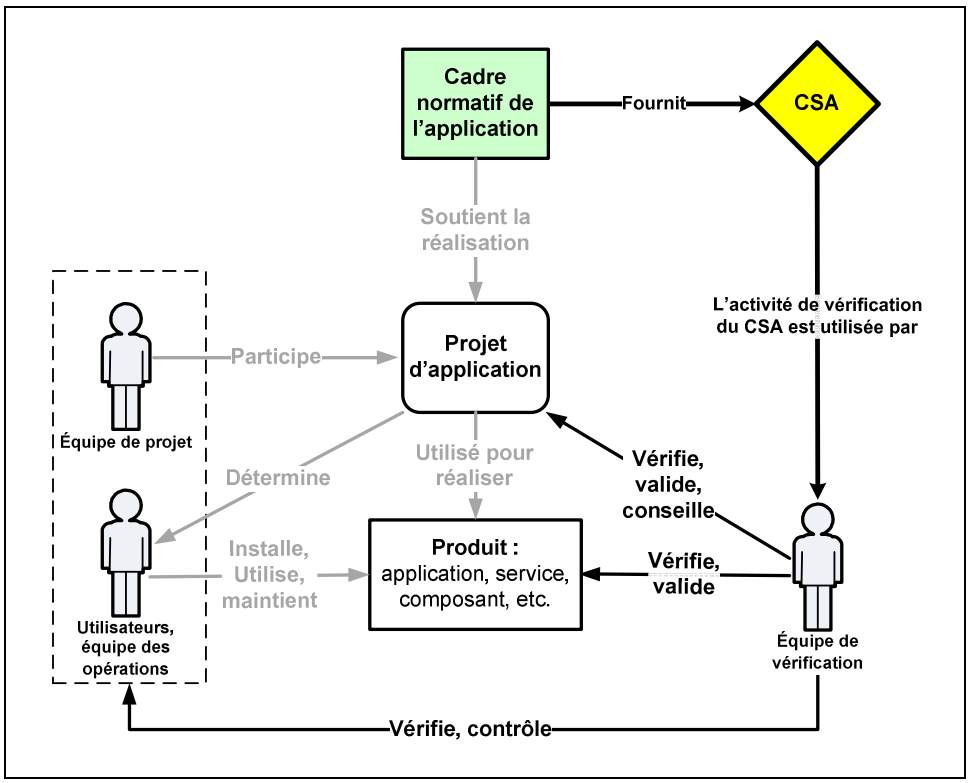


Figure-A XIV-10 Utilisation des CSA dans la vérification et la validation des activités de sécurité à l'intérieur d'un projet d'application
Traduite et adaptée de (ISO/IEC, 2011d)

Tel que présenté dans la Figure-A XIV-10, l'activité de vérification de la mesure d'un CSA peut autant concerner la vérification d'un processus que la vérification d'un composant du produit ou la vérification des qualifications d'une personne ayant un rôle jugé sensible dans le projet.

a) un contrôle de sécurité de l'application (CSA), devrait contenir ou référer à l'information sur les éléments nécessaires à la réalisation de l'activité de vérification et pouvoir fournir des preuves attendues, vérifiables et répétables confirmant son bon fonctionnement. Les CSA ont la capacité d'identifier et de décrire les activités, les acteurs et les artéfacts requis à un processus de certification, tel que les activités de sécurité, de vérification et de mesure.

XIV.3.7.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Le rapport et les résultats de la vérification de chaque CSA d'une application incluant notamment la portée de la vérification, le statut de chaque CSA, les manquements et les pistes de solutions pour y remédier;
2) Le niveau de confiance actuel de l'application.

XIV.4 Audit et certification de la mise en œuvre du modèle SA

Un processus d'audit est une démarche systématique, indépendante et documentée qui permet d'évaluer et d'obtenir des preuves de manière objective pour déterminer si les critères d'audit sont satisfaits (ISO/IEC, 2007g, p. 3). Un processus de certification est une démarche qui confirme qu'un système ou un composant est conforme aux exigences spécifiées et est acceptable pour une utilisation opérationnelle (ISO/IEC, 2010g, p. 48).

Le modèle SA n'impose ni ne priorise l'implémentation d'éléments ou de processus amenés par le modèle. Par contre, le modèle demande à l'organisation :

1) De définir la portée, les éléments et les processus qu'elle désire implémenter afin d'avoir une vision claire de ses priorités et de ses objectifs de sécurité concernant la protection de ses applications;

2) De définir, en fonction de leurs environnements et spécifications respectifs, le niveau de confiance cible de ses applications et de mettre en place les CSA qui permettront de l'atteindre.

Le modèle SA propose trois processus d'audit et de certification pour vérifier ou certifier la bonne mise en place de la SA, soit :

1) Auditer et certifier les éléments de SA du CNO;
2) Auditer et certifier la sécurité d'une application;
3) Auditer et certifier un expert en sécurité des applications.

Les processus d'audits et de certifications proposés par le modèle SA devraient être réalisés en suivant les pratiques recommandées par le document ISO : Guide 60 : Évaluation de la conformité – Code de bonnes pratiques.

Tout comme le processus de vérification de la SA, les processus d'audit et de certifications de la SA peuvent être réalisés aussi bien par des équipes d'audit internes qu'externes, selon les circonstances et les besoins de l'organisation.

XIV.4.1 Auditer et certifier les éléments de SA du CNO

Le processus Auditer et certifier les éléments de SA du CNO est utilisé pour vérifier et s'assurer que tous les éléments concernant la SA qui doivent avoir été intégrés au CNO sont présents, qu'ils ont été validés, vérifiés puis approuvés par les autorités adéquates, qu'ils sont fonctionnels, qu'ils sont en mesure de produire les résultats attendus et qu'ils sont disponibles pour être utilisés par les projets des applications de l'organisation. Il s'agit du processus de validation de la conformité du cadre normatif de l'organisation au présent modèle et il peut aussi être utilisé pour réaliser la certification de la SA d'une organisation.

Ce processus peut être particulièrement utile aux organisations qui sont divisées en groupes d'affaires ou en petites organisations indépendantes, tel que de grandes entreprises possédant

des directions régionales, des chaînes d'entreprises ou des gouvernements possédant des régies et des ministères. Toutes ces organisations peuvent vouloir s'assurer que les CNO de leurs différentes organisations satellites sont non seulement conformes et bien adaptées à leurs priorités et à leurs besoins particuliers en sécurité des applications, mais aussi qu'elles sont conformes aux attentes de SA de l'organisation mère qui les dirige.

La mise en place de ce processus d'audit devrait respecter les exigences de la norme ISO 19011 – Lignes directrices pour l'audit des systèmes de management.

XIV.4.1.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus est de produire un rapport de conformité crédible et vérifiable, permettant de confirmer l'atteinte de la cible de vérification exigée par une autorité en SA, tels que :

1) Le comité du CNO est en place et est opérationnel;
2) Les éléments du CNO :
    a) soient approuvés, disponibles, communiqués et accessibles;
    b) répondent aux objectifs et priorités de sécurité de l'organisation et, si requis, à ceux de l'organisation mère;
    c) soient soutenus par le PGCNO.
3) Des CSA sont associés à chaque niveau de confiance ciblé pour les applications de l'organisation;
4) Le niveau de confiance actuel des applications identifiées comme sensibles a été mesuré et qu'il est conforme ou surpasse le niveau de confiance qui a été ciblé par l'organisation pour ces applications;
5) Chacun des projets d'application sensible implémente correctement les processus et composants de SA présents dans le CNO.

XIV.4.1.2 Activités

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) Identification par une autorité en SA de la cible de vérification (portée de l'audit et critères à satisfaire);
2) Vérification de mise en place et de la gestion du comité du CNO :
    a) vérifier l'alignement des objectifs et priorités de l'organisation concernant la sécurité de ses applications avec les :
        i) objectifs et priorités de SA de l'organisation mère, lorsque requis;
        ii) besoins exprimés par le SGSI de l'organisation, lorsque requis;
        iii) éléments du CNO devant être mis en place.
3) Vérification de la mise en place et la gestion des divers éléments du CNO :
    a) vérifier que les éléments requis par l'organisation existent bel et bien dans le CNO;
        i) directives, politiques, règlements, processus, bibliothèque des CSA, CSA, etc.
    b) vérifier que ces éléments sont à jour, qu'ils sont intégrés aux processus de l'organisation, qu'ils ont été communiqués et qu'ils sont accessibles aux rôles concernés;
    c) vérifier que pour chacun des éléments du CNO, les processus d'élaboration, d'implémentation, de surveillance et d'amélioration sont en place et sont fonctionnels;
    d) vérifier que les processus de soutien et de formation requis existent et sont disponibles.

XIV.4.1.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Rapport d'audit présentant :
    a) la portée et la conclusion de l'audit du CNO de l'organisation;
    b) les points rencontrés; ainsi que
    c) les non-conformités.

XIV.4.2 Auditer et certifier la sécurité d'une application

Le processus « Auditer et certifier la sécurité d'une application » est utilisé pour vérifier et s'assurer qu'une application est sécuritaire, soit que son niveau de confiance actuel est égal ou supérieur à son niveau de confiance cible.

Dans le contexte de la sécurité d'une application, ce processus consiste à vérifier que tous les CSA spécifiés par le niveau de confiance ciblé pour l'application ont été mis en place, qu'ils ont tous été vérifiés et que ces vérifications ont produit les résultats attendus.

La mise en place de ce processus d'audit devrait respecter les exigences de la norme ISO 17067 – Évaluation de la conformité – Éléments fondamentaux de la certification de produits et lignes directrices pour les programmes de certification de produits.

XIV.4.2.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus est de produire un rapport de conformité crédible et vérifiable, permettant de confirmer l'atteinte de la cible de vérification exigée par une autorité en SA, tels que :

1) Le niveau de confiance actuel, mesuré pour l'application identifiée, soit conforme ou surpasse le niveau de confiance qui a été ciblée par l'organisation pour celle-ci;
2) Les processus nécessaires au maintien et à la réévaluation du niveau de confiance de l'application sont en place et sont utilisés.

La certification de SA est une démonstration formelle qu'un système ou qu'un composant est conforme aux exigences spécifiées, et qu'il est acceptable pour une utilisation opérationnelle (ISO/IEC, 2010g). Dans le contexte de la sécurité d'une application, il s'agit de réaliser le processus d'audit de sécurité d'une application en validant et en utilisant comme critères, les éléments contenus dans le CNA tels que le niveau de confiance ciblé et la liste des CSA sélectionnés (*Voir l'annexe* XIV.3.7.2 - 1).

Le modèle SA définit une application comme sécuritaire lorsque son niveau de confiance ciblé est égal au niveau de confiance actuel (mesuré).

XIV.4.2.2 Activités

Si l'on exclut l'identification par une autorité en SA de la cible de vérification (portée de l'audit et critères à rencontrer), qui doit être réalisée au début de tout audit, le processus d'audit et de certification d'une application peut se résumer en deux grandes étapes de vérifications, soit : (A) la vérification de la gestion du CNA, et (B) la vérification de la SA. (*Voir* Figure-A XIV-11)

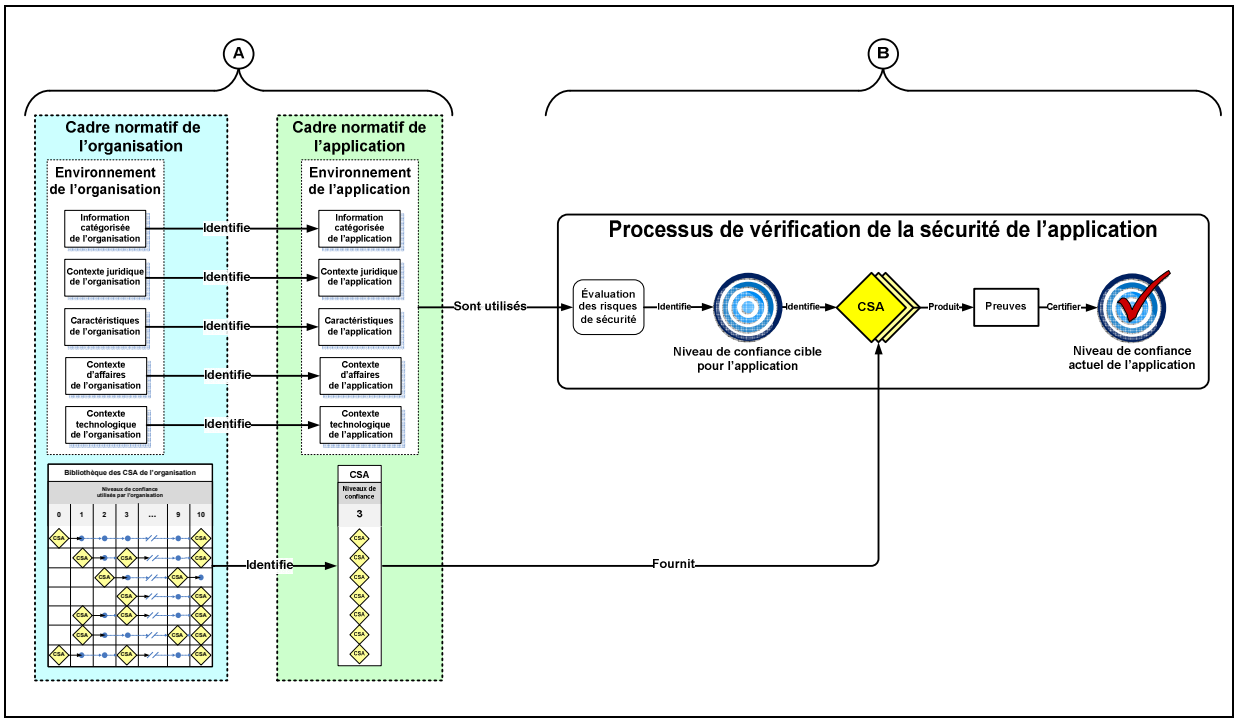


Figure-A XIV-11 Représentation sommaire du processus d'audit de la sécurité d'une application
Traduite et adaptée de (ISO/IEC, 2011d)

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) Identification de la portée de l'audit;

2) Vérification de la gestion du CNA :
    a) vérification du processus d'assignation des rôles dans le projet;
    b) vérification de la gestion des ressources assignées au projet d'application;
    c) vérification du PGSA :
        i) vérification de l'identification les besoins et l'environnement de l'application;
        ii) vérification de l'évaluation les risques de sécurité amenés par l'application;
        iii) vérification de la création et de la maintenance du cadre normatif d'application;
        iv) vérification de la réalisation et de l'opération de l'application;
        v) vérification du processus de rétroaction des résultats du projet;
3) Vérification de la SA :
    a) validation du niveau de confiance cible;
    b) vérification du contenu du CNA;
    c) validation de la mise en place et de la vérification des CSA;
    d) validation que tous les CSA ont correctement produit les résultats attendus;
    e) réalisation du processus de vérification de certains CSA et comparaison des résultats obtenus avec ceux attendus.

XIV.4.2.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

1) Rapport d'audit présentant :
    a) la conclusion de l'audit de l'application;
    b) les points rencontrés; ainsi que
    c) les non-conformités.
2) L'émission d'un rapport confirmant la portée et la justesse des éléments contenus dans le CNA de l'application et certifiant que celle-ci a atteint, au moment de l'audit, le niveau de confiance qui y est spécifié.

XIV.4.3 Auditer et certifier un expert en sécurité des applications

Le processus Auditer et certifier un expert en sécurité des applications est utilisé pour vérifier et s'assurer du niveau de connaissances, de compétences et d'expérience du professionnel en sécurité des applications, selon le schéma de certification proposé par le modèle SA.

La mise en place de ce processus d'audit devrait respecter les recommandations présentées dans le chapitre 4 de la norme ISO 24773 : Ingénierie du logiciel – Certification des professionnels de l'ingénierie du logiciel – Cadre comparatif.

XIV.4.3.1 Objectifs

Les objectifs visés par la mise en place de ce sous-processus sont :

1) Déterminer si une personne connaît, comprend, sait mettre en place et utiliser les concepts, principes et autres éléments du modèle SA pour aider une organisation à protéger ses applications;
2) S'assurer que chacune des personnes, impliquées dans une des activités de la SA, possède les qualifications requises à sa responsabilité;
3) S'assurer qu'une personne responsable de la mise en place du modèle SA à l'intérieur d'une organisation possède les connaissances et les qualifications requises pour assumer cette responsabilité.

XIV.4.3.2 Activités

Afin d'atteindre l'objectif visé, les activités suivantes devront être réalisées :

1) Vérification des qualifications requises;
2) Évaluation des connaissances et de la compréhension de la personne :
   a) sur la portée, les concepts, les principes et les définitions amenés par le modèle SA;
   b) des processus du modèle SA et de leurs implémentations;
   c) des composants du modèle SA et leurs implémentations;

d) des stratégies de gestion et de mise en place des éléments du modèle SA en fonction de l'environnement, des besoins et des ressources de l'organisation;
e) de l'utilisation du modèle SA en support à un SGSI.

XIV.4.3.3 Résultats

Au cours de la réalisation des activités de ce processus, les résultats suivants seront notamment obtenus :

L'émission d'une certification professionnelle reconnaissant que la personne auditée connaît, comprend et sait utiliser le modèle pour aider une organisation à protéger ses applications.

ANNEXE XV

EXEMPLE DE GROUPES D'INFORMATIONS PRÉSENTS DANS LA PORTÉE DE LA SÉCURITÉ D'UNE APPLICATION – DIAGRAMME DÉTAILLÉ

Figure-A XV-1 Exemple des groupes d'informations présents dans la portée de la sécurité des informations d'une application

ANNEXE XVI

EXEMPLE DE PROCESSUS D'INGÉNIERIE DES EXIGENCES DE SÉCURITÉ D'UNE APPLICATION

Voici deux exemples d'adaptation d'activités de processus d'ingénierie des exigences de sécurité d'une application. Finalement, des exemples d'exigence de sécurité seront présentés en conclusion à ces exemples.

XVI.1 Adaptation du processus *Stakeholder Requirements Definition* (6.4.1) de la norme ISO 15288

Une fois un risque de sécurité inacceptable identifié, on doit réaliser les activités suivantes :

1) Le processus de création, de validation et de vérification des exigences de sécurité; et
2) le processus d'analyse des exigences de sécurité.

XVI.2 Processus de création, de validaton et de vérification des exigences de sécurité

1) Objectif

   L'objectif de ce processus de création, de validation et de vérification des exigences de sécurité de l'organisation pour une application est similaire au but du processus permettant la création, la validation et la vérification des exigences d'un système d'information, soit : de s'assurer de définir les exigences d'un système (application) qui peuvent fournir les services requis par les utilisateurs et autres intervenants, pour un environnement défini. (ISO/IEC, 2007g, p. 37) Afin de faciliter la description de ce processus, des éléments de précision seront apportés au processus décrit à la section 6.4.1 – *Stakeholder Requirements Definition process*, de la norme ISO 15288 afin d'en ajuster la portée à la définition des exigences de sécurité des applications.

   Pour créer des exigences de sécurité, seules la portée et les informations qui seront prises en entrée à ce processus diffèrent. Tandis que les besoins des utilisateurs et autres

personnes intéressées par un système d'information sont les informations prises en entrées par ce processus de création, ce sont les besoins d'atténuer les risques de sécurité inacceptables pour l'organisation qui seront pris en entrés pour créer les exigences de sécurité. Ce changement de portée, des besoins fonctionnels et non fonctionnels d'utilisation et d'opération du système (ISO/IEC, 2007g, p. 37) vers des besoins de sécurité fonctionnels et non fonctionnels de l'application est le principal changement dans l'utilisation de ce processus et devra être appliqué à toutes ses activités.

La Figure-A XII-5 Vision sommaire des principaux éléments requis par l'analyse de sécurité d'une application présente sommairement les principaux éléments qui devront être pris en compte afin d'identifier, à partir des besoins d'affaires de l'organisation, les exigences de sécurité d'une application qui permettront à celle-ci de se procurer et de mettre en place des contrôles de sécurité de l'application (CSA).

En modifiant la portée des informations en entrée, les éléments produits par le processus seront quelque peu différents.

2) Résultats attendus

Les résultats attendus d'une implémentation d'un processus réussie de définition d'exigences de sécurité de l'organisation pour une application, sont :

a) les caractéristiques et le contexte d'utilisation et opérationnel des services de l'application sont spécifiés, incluant les contextes d'affaires, juridiques et technologiques, ainsi que les acteurs, les processus et les spécifications de l'application qui interagissent avec les informations liées à l'application;
b) les contraintes de sécurité de la solution du système sont définies;
c) la traçabilité des exigences de sécurité en fonction de ces besoins de l'organisation est atteinte;
d) les exigences de sécurité de l'organisation sont définies;
e) les exigences de validation sont identifiées.

3) Activités et tâches
   a) Ébaucher les exigences de sécurité de l'organisation
      i) Identifier les sources des exigences de sécurité possibles (risques inacceptables)
      ii) Ébaucher les exigences de sécurité de l'organisation pour cette application
   b) Définir les exigences de sécurité de l'organisation
      i) Définir les contraintes pour qu'une solution soit jugée sécuritaire, qui tiendra compte des conséquences des aspects juridiques, d'affaires et techniques où sera utilisée l'application
      ii) Définir une séquence d'activités représentatives requises par le contrôle de sécurité qui correspondent au scénario opérationnel et de support pour l'environnement anticipé.
      iii) Identifier les interactions entre les intervenants et l'application
      iv) Spécifier les besoins de santé, sureté, environnementale, et toutes autres exigences reliées à des qualités critiques de l'application.
   c) Analyse et maintenance des besoins des intervenants
      i) Analyser l'ensemble des exigences énoncées
      ii) Résoudre les problèmes amenés par ces exigences
      iii) Retourner l'analyse aux intervenants concernés afin de s'assurer que les besoins de sécurité et la diminution des risques attendus ont été correctement compris et exprimés;
      iv) Établir que les exigences ont été correctement exprimées avec les intervenants
      v) Enregistrer l'exigence de sécurité de l'intervenant dans une forme facilitant la gestion des exigences à travers le cycle de vie de l'application et au-delà
      vi) Maintenir la traçabilité des exigences de sécurité avec les sources des besoins de sécurité des intervenants

XVI.2.1 Le processus d'analyse des exigences de sécurité

1) Objectif

   L'objectif de ce processus est de transformer la vision de l'intervenant envers une exigence de sécurité devant diminuer un ou plusieurs risques de sécurité en une vision de description d'un contrôle de sécurité plus technique qui, sans spécifier aucune implémentation technique, permettra d'identifier les résultats attendus, qui seront considérés comme suffisant pour diminuer le ou les risques concernés à un niveau acceptable. (ISO/IEC, 2007g, p. 39) Afin de faciliter la description de ce processus, des éléments de précision seront apportés au processus décrit à la section 6.4.2 – *Requirements Analysis Process*, de la norme ISO 15288 afin d'en ajuster la portée à la l'analyse des exigences de sécurité des applications.

   L'analyse exigences de sécurité aidera à spécifier et concevoir des contrôles de sécurité qui pourront être associés aux acteurs, intégrés aux processus et activités impliqués dans le cycle de vie de l'application, intégrés à l'application elle-même ou dans son environnement d'opération.

   Elle aidera aussi à mettre en place les éléments et requis par le processus de traçabilité des exigences.

2) Résultats attendus
   a) Les caractéristiques, attributs, fonctionnalités et performances requis pour le contrôle de sécurité spécifié
   b) Les contraintes qui affecteront la conception et l'architecture de l'application et les objectifs de réalisations tels que spécifiés;
   c) L'intégrité et la traçabilité entre les exigences de sécurité de l'application et des intervenants
   d) La définition d'une base de vérification permettant d'affirmer l'atteinte des exigences de sécurité.

3) Activités et tâches
    a) Définition des exigences de sécurité de l'application
        i) Définition des frontières fonctionnelles du contrôle de sécurité en termes de comportements et de propriétés à fournir
        ii) Définition de chacun des contrôles de sécurité requis par l'application
        iii) Définition des contraintes d'implémentation introduites par les exigences des intervenants ou qui sont des limitations incontournables
        iv) Définition des mesures de qualités et d'utilisation techniques qui serviront à mesurer l'atteinte de l'objectif visé par l'implémentation du contrôle
        v) Spécifier les exigences des contrôles de sécurité, tel que justifiés par les l'identification des risques du projet de l'application sur la santé, la sureté la sécurité, la fiabilité, la disponibilité et la maintenance.
    b) Analyse et maintenance des exigences de l'application
        i) Analyser l'intégrité des exigences de sécurité de l'application afin de garantir que chaque exigence, groupe d'exigences est intègres dans son ensemble
        ii) Retourner l'information aux intervenants concernés afin de s'assurer que les exigences de sécurité spécifiées répond adéquatement à leurs besoins et attentes.
        iii) Démontrer la traçabilité entre les exigences de sécurité de l'application et les exigences de sécurité des intervenants
        iv) Maintenir, tout au long du cycle de vie de l'application, l'association entre la cible de sécurité visée, les décisions et les hypothèses de sécurités énoncées *(Voir* XII.2.12 – Niveau de confiance d'une application).

XVI.3 Processus de définition d'exigence adapté à la sécurité des applications

Une fois un risque de sécurité inacceptable identifié, on doit réaliser les activités suivantes :

1) Conception
    a) Identifie les risques inacceptables
    b) Examine les options
2) Génération

a) Définis les exigences
b) Produis les spécifications des exigences

3) Analyse et conception
   a) Identifier les impacts
   b) Déterminer l'acceptabilité
   c) Déterminer l'implémentation et la testabilité
4) Inspection
   a) Discussion sur les exigences proposées
   b) Discussion des scénarios opérationnels
   c) Identification des solutions acceptables et des erreurs
5) Acceptation
   a) Évaluer les risques et les bénéfices
   b) Décision des ressources qui seront allouées
   c) Établissement des exigences obligatoires (*base lines*)

XVI.4 Exemples d'exigences de sécurité

1) Exigence de sécurité d'affaires (ESA.1) – L'organisation (qui) doit pouvoir démontrer l'intégrité (comment) des composants du système (quoi) placés sur l'infrastructure en nuage (où) en tout temps (quand).
2) Exigence de sécurité utilisateur (ESU.1) – Lors de sont authentification (quand) à un terminal de l'application (ou), l'utilisateur (qui) devra pouvoir soumettre (comment) un mot de passe verbal (quoi).
3) Exigence de sécurité de système (ESS.1) – Une fois démarrée (quand), l'application (qui) devra transmettre à un service de journalisation sécurisé (comment) situé à l'extérieur du complexe (où) les événements et transactions de tous ses utilisateurs et administrateurs (quoi).

4) Exigence de sécurité de fonction (ESF.1) – Un service (qui) doit surveiller les composants critiques de l'application (quoi) sauvegardés sur les serveurs (où) et reporter immédiatement toutes pertes d'intégrité ou de disponibilité par courriel ou par SMS aux personnes désignées (comment).
5) Exigence de sécurité d'infrastructure (ESI.1) – Afin de pouvoir offrir une disponibilité continue 24/7 (pourquoi), l'infrastructure (qui) devra permettre le déploiement et l'opération continus (comment) de l'application et de ses dépôts de données (quoi) sur trois sites d'exploitation situés à plus de 1 000 km les uns des autres (où).
6) Contrainte de sécurité (CS.1) – L'intégrité (comment) des données sensibles de l'application (quoi) doit être garantie à 100% (comment).

ANNEXE XVII

ASIA : MÉTHODE DE GESTION DES RISQUES DE SÉCURITÉ D'UNE APPLICATION

Les deux figures présentées dans cette annexe :

1) La Figure-A XVII-1 Processus de gestion des risques de SA proposé par la méthode ASIA, qui présentent les grandes étapes de la méthode;
2) La Figure-A XVII-2 Représentation du modèle de mesure de l'information de la méthode ASIA, qui présente les indicateurs et les critères qui ont été vérifiés pour valider la méthode.

NOTE Ces deux figures suivantes nécessitent l'utilisation de papier de format 11 x 17 pour pouvoir s'imprimer correctement.

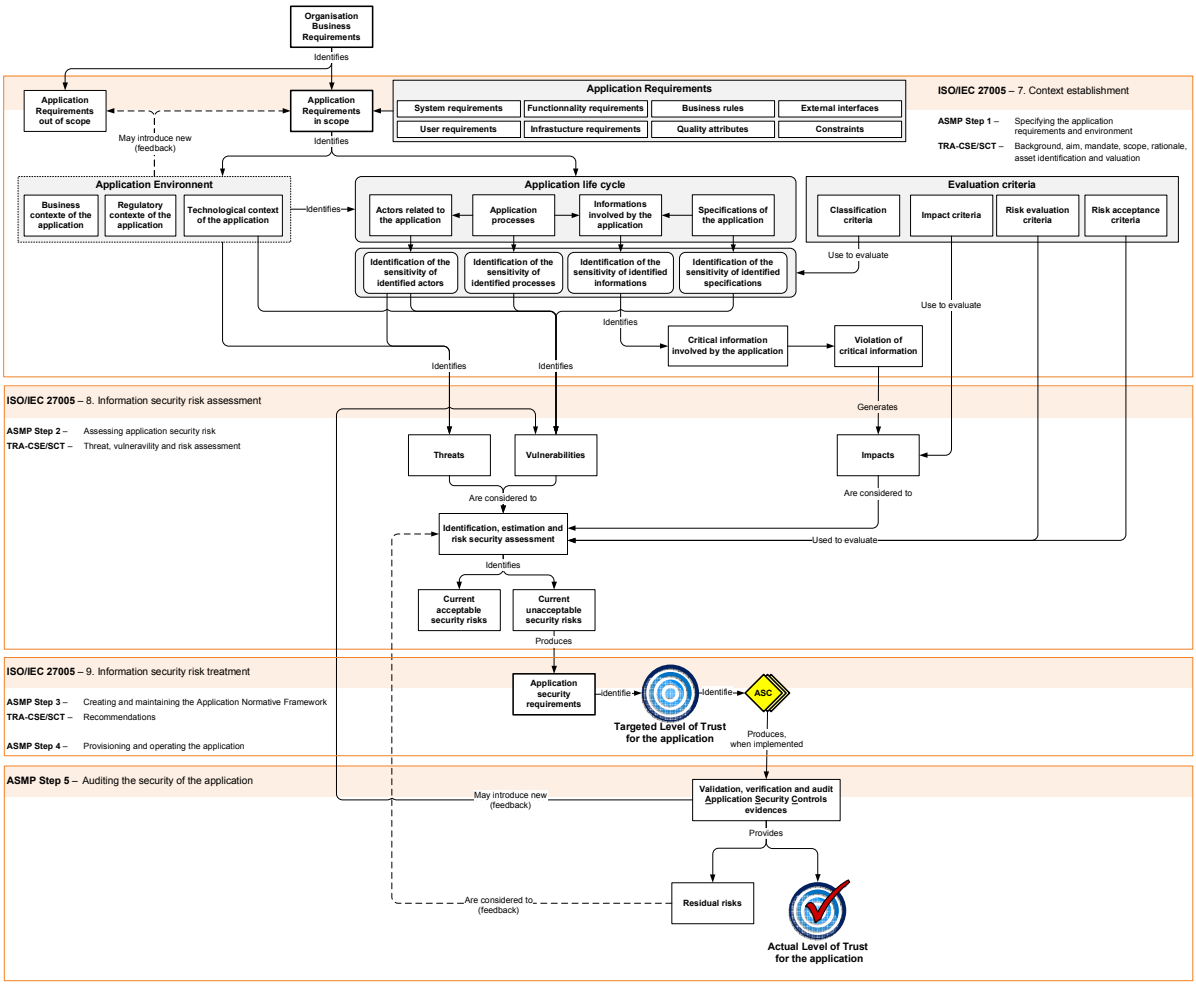


Figure-A XVII-1 Processus de gestion des risques de SA proposé par la méthode ASIA

(Insérez ici la Figure-A XVII-1 en format 11 x 17)

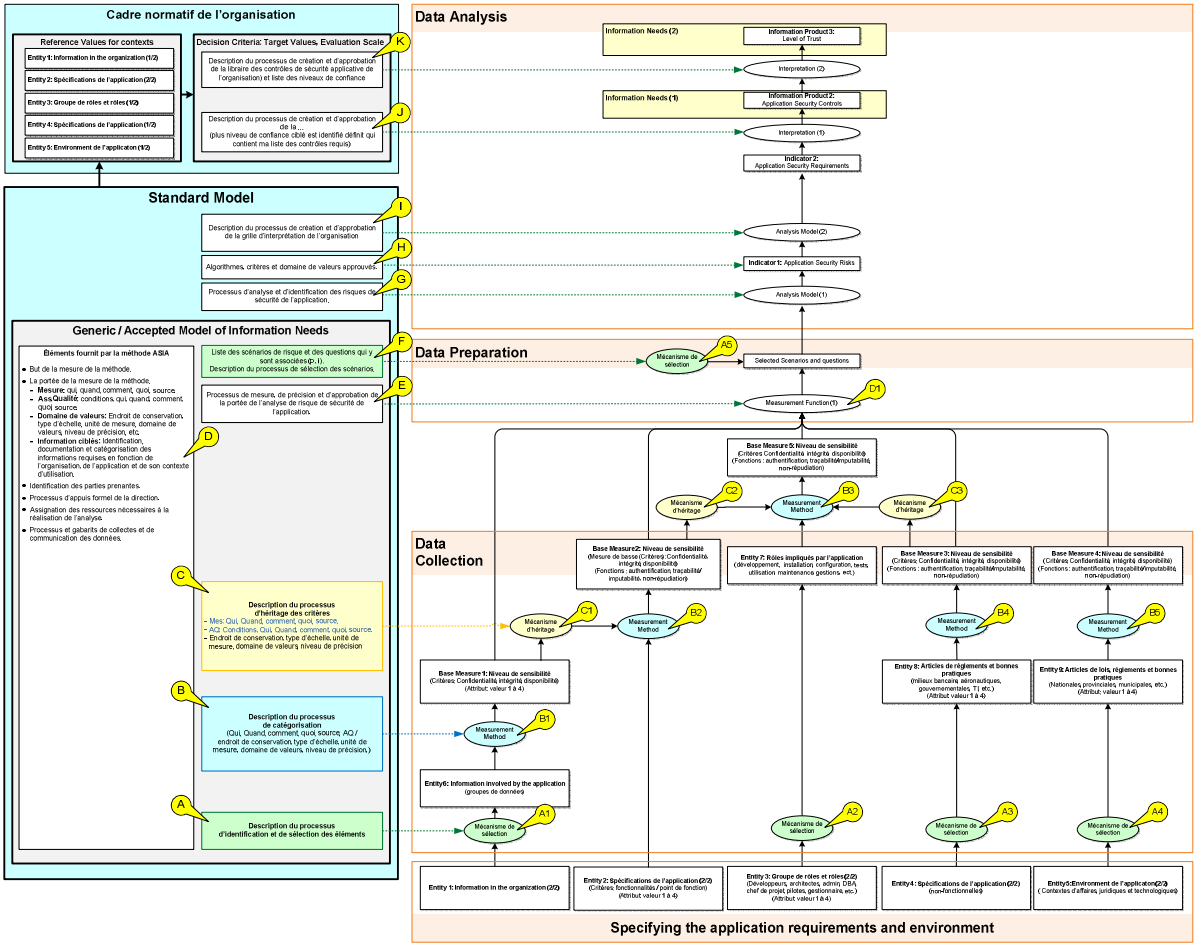


Figure-A XVII-2 Représentation du modèle de mesure de l'information de la méthode ASIA

(Insérez ici la Figure-A XVII-2 en format 11 x 17)

ANNEXE XVIII

VISION GLOBALE SOMMAIRE DES LIENS QUI RELIENT LES ÉLÉMENTS DU MODÈLE SA

La Figure-A XVIII-1 présentée dans cette annexe présente une vision globale sommaire des liens qui relient les éléments clés du modèle SA.

NOTE Cette figure nécessite l'utilisation de papier de format 11 x 17 pour pouvoir s'imprimer correctement.

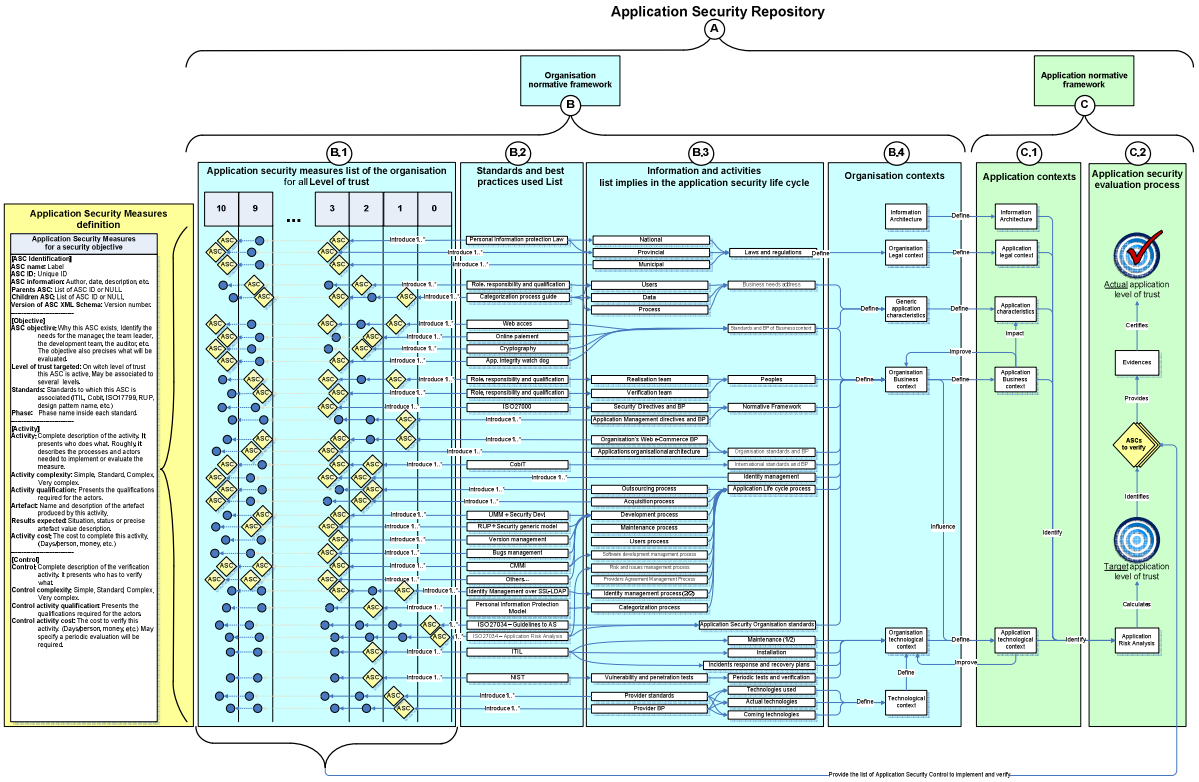


Figure-A XVIII-1 Vision globale sommaire des liens qui relient les éléments clés du modèle SA

(Insérez ici la Figure-A XVIII-1 en format 11 x 17))

ANNEXE XIX

VALIDATION ET AMÉLIORATION DU MODÈLE SA : MÉTHODE DELPHI ARRIMÉE AU PROCESSUS ISO

Cette annexe présente la validation et l'amélioration du modèle SA qui ont été réalisées à l'aide de la méthode de recherche Delphi, via le processus de gestion d'un projet d'ISO.

XIX.1 Rappel du processus de gestion de projet d'ISO

Les commentaires et contributions des experts vérificateurs délégués par chacun des pays participants, concernant la version publiée du document, sont envoyés aux éditeurs deux semaines avant la rencontre internationale pour être discutés en atelier de révision. Les commentaires reçus sont généralement présentés par le représentant du pays qui l'a soumis. Tous les commentaires sont discutés en comité, puis une décision est prise pour le traitement de chacun d'eux. Une fois de retour, les éditeurs appliquent le traitement des changements demandés et produisent la nouvelle version du document. C'est à cette étape que les processus de conception, de développement et d'amélioration des éléments du modèle SA sont réalisés. Suite à ces ajustements et à l'intégration des nouveaux éléments du modèle, la nouvelle version du document du projet de la norme est complétée, puis distribuée à chacun des pays. Ces derniers demandent alors à leurs experts respectifs d'en vérifier le contenu, ceci afin de pouvoir produire de nouveaux commentaires sur les éléments du modèle modifiés ou intégrés à cette nouvelle version.

L'acceptation du SC27 d'ISO de démarrer un projet de normes à partir des éléments proposés par notre projet de recherche marque le début du processus de validation du modèle SA. La section suivante présente les faits saillants de la réalisation des différents stades du projet lors du cycle des phases 2 et 3. Elle reprend les stades du processus de réalisation d'un projet ISO (Figure-A IX-1) et présente les événements importants survenus pendant les travaux de recherche, ainsi que les principaux éléments réalisés pendant ces stades.

XIX.2 Réalisation de la validation et de l'amélioration du modèle SA via la méthode Delphi intégrée au processus ISO

Le processus de rédaction d'ISO, à partir de l'ouverture de la période d'étude jusqu'à l'approbation de publication de la norme ISO 27034 – *Application Security*, a nécessité plus de six ans de travail. Pendant cette période, des cycles de validation et d'évolution se sont succédé tous les six mois.

Au début de chaque cycle Delphi, un document de travail présentant les éléments du modèle SA a été distribué aux représentants des pays participants, pour validation et commentaires.

Le Tableau-A XIX-1 propose une vision synthèse des commentaires, contributions et autres documents reçus ou produits par 17 des 45 pays qui ont participé aux travaux de validation du modèle durant les sept stades de ce projet d'édition d'ISO, tel qu'introduit précédemment à la Figure-A IX-1.

NOTE Ce tableau nécessite l'utilisation de papier de format 11 x 17 pour pouvoir s'imprimer correctement.

Tableau-A XIX-1 Synthèse par cycles Delphi, des commentaires et contributions reçus des organisations et pays participants

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 application 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 Limassol, (Cypre) Octobre 2008	20.3 Document, version de travail 3 Beijin, (Chine) Mai 2009	30.1 - Stade de comité Document, version de comité 1 Redmond, (US) Novembre 2009	30.2 Document, version de comité 2 Malaka, (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, (Singapour) Avril 2011	50. - Stade d'approbation Document, version finale avant publication Secrétariats SC27: DIN, Berlin, (Allemagne) Octobre 2011	60. - Stade de publication Standard international ISO/IEC 27034 - Application Security, part 1 Secrétariat ISO: Genève (Suisse) Novembre 2011	Nombre de commentaires traités
Document de travail ou norme ISO distribué pour commentaire		(ISO/IEC, 2007a)	(ISO/IEC, 2007d)	(ISO/IEC, 2007c)	(ISO/IEC, 2008b)	(ISO/IEC, 2008a)	(ISO/IEC, 2009a)	(ISO/IEC, 2009b)	(ISO/IEC, 2010b)	(ISO/IEC, 2010a)	(ISO/IEC, 2011c)	(ISO/IEC, 2011b)	(ISO/IEC, 2011a)	
Demandes de liaison envoyées		(SC27/WG4, 2006a) (SC27/WG4, 2006b) (SC27/WG4, 2006c)	(SC27/WG4, 2007a) (SC27/WG4, 2007c) (SC27/WG4, 2007d)	(SC27/WG4, 2007b) (SC27/WG4, 2007e) (SC27/WG4, 2007f)	(SC27/WG4, 2008a) (SC27/WG4, 2008b) (SC27/WG4, 2008c)	-	-	-	-	-	-	-	-	
Commentaires et contributions reçus des pays participants		(N/A)	(ISO/IEC, 2007e)	(ISO/IEC, 2007b)	(ISO/IEC, 2008c)	(ISO/IEC, 2008d)	(ISO/IEC, 2009f)	(ISO/IEC, 2009g)	(ISO/IEC, 2010d)	(ISO/IEC, 2011d)	(ISO/IEC, 2011e)	(ISO/IEC, 2011a)	-	
États-Unis (US)	**Nombre de commentaires émis**	-	-	58	275	75	9	49	7	30	5	-	-	508
	Contributions proposées			(DHS, 2007) (Microsoft, 2007) (Goertzel et al., 2007)			(ISO/IEC, 2009f, pp. 53-70)	(Ladd, 2009)						
Afrique du Sud (ZA)	**Nombre de commentaires émis**	-	-	8	68	-	106	60	-	35	-	-	-	277
	Contributions proposées				(Amsanga, 2008)									
Australie (AU)	**Nombre de commentaires émis**	-	1	2	14	75	9	12	-	14	-	-	-	127
	Contributions proposées					(ISO/IEC, 2008d, p. 15)								
Japon (JP)	**Nombre de commentaires émis**	-	3	-	4	16	7	35	22	4	8	2	-	101
	Contributions proposées	(Nakao, 2006a) (Nakao, 2006b)					(ISO/IEC, 2009f, pp. 10-17)	(Takebe, 2009)						
ISO/SC7 (WG7)	**Nombre de commentaires émis**	-	-	-	-	-	-	59	-	-	-	-	-	59
	Contributions proposées							(SC7, 2003)						
Brésil (BR)	**Nombre de commentaires émis**	-	-	-	23	-	-	-	-	-	-	-	-	23
	Contributions proposées													
Malaysie (MY)	**Nombre de commentaires émis**	-	-	7	-	-	2	-	-	-	2	-	-	11
	Contributions proposées													
France (FR)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	7	5	-	-	12
	Contributions proposées													
Autriche (AT)	**Nombre de commentaires émis**	-	-	-	-	8	-	-	-	-	-	-	-	8
	Contributions proposées													
Royaume Uni (UK)	**Nombre de commentaires émis**	-	5	3	-	-	-	-	-	-	-	-	-	8
	Contributions proposées													
Canada (CA)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	4	-	-	-	4
	Contributions proposées	(Poulin, 2006)	(Poulin, 2007a) (Poulin, 2007b) (Poulin, 2007c) (Poulin et Rousselle, 2007)	(Poulin, 2007d)	(Poulin, 2008a) (Poulin, 2008b) (Poulin et Guay, 2008) (Poulin, Rousselle et Amsenga, 2008)		(Poulin, 2009a) (Poulin, 2009b) (Poulin, 2009c) (Poulin, 2009d)	(Poulin, 2010)						
Danemark (DK)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	-	-	1	-	1
	Contributions proposées													
Indonésie (IN)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	1	-	-	-	1
	Contributions proposées													
Italie (IT)	**Nombre de commentaires émis**	-	-	-	-	-	-	1	-	-	-	-	-	1
	Contributions proposées													
Pays-Bas (NL)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	-	1	-	-	1
	Contributions proposées													
Norvège (NO)	**Nombre de commentaires émis**	-	-	1	-	-	-	-	-	-	-	-	-	1
	Contributions proposées			(ISO/IEC 2008c, p6)										
Hong Kong (HK)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	-	-	-	-	0
	Contributions proposées	(Ma, 2006)												
Suède (SW)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	-	-	-	-	0
	Contributions proposées	(Carlstedl, 2006)												
Allemagne (GE)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	-	-	-	-	0
	Contributions proposées					(BSI, 2005a) (BSI, 2005b) (BSI, 2005c)								
ITU-T (SCG27)	**Nombre de commentaires émis**	-	-	-	-	-	-	-	-	-	-	-	-	0
	Contributions proposées		(ITU-T, 2007b)	(ITU-T, 2007a)										
Total de commentaires reçus par cycle :		0	9	79	384	174	133	216	29	95	21	3	-	
Total de commentaires reçus par stade :		0	9				770		245		116	3	-	
Nombre total de commentaires reçus pour le projet :														1143

(Insérez-ici le Tableau-A XIX-1 en format 11 x 17)

La majorité des commentaires reçus des experts des pays et organisations impliqués dans la validation du modèle SA concernaient principalement l'amélioration du texte et la correction d'inconsistances décrivant les différents éléments et processus amenés par le modèle.

Les annexes XIX.3 à XIX.8 présentent les événements clés provenant du traitement des commentaires et des contributions reçus durant les cycles Delphi de ce travail de recherche. Seuls les événements qui concernent une amélioration ou une réorientation du modèle SA, suite à la réception et au traitement d'un commentaire ou par l'ajout d'une contribution provenant des experts valideurs des pays participants, sont présentés ici. Ces sections présentent aussi les principaux documents qui ont été produits durant chacun des stades de ce projet. Afin d'alléger le contenu, les commentaires des experts vérificateurs de type éditorial, qui concernaient les erreurs de grammaire, d'orthographe ou de structure de phrase, n'y ont pas été intégrés.

Tel que mentionné précédemment, un stade du processus d'édition de norme ISO est composé d'un ou de plusieurs cycles de 6 mois. Chaque cycle de six mois du processus ISO se divise en quatre étapes. C'est durant la réalisation de deux des quatre étapes de chacun des cycles que nous avons présenté le modèle SA ainsi que les éléments qui le composent, soit :

1) **Durant l'étape de conception et d'amélioration**

   Parmi l'ensemble des activités requises pour mener à bien cette recherche, les plus importantes sont notamment :

   a) recherche exploratoire, appuyée par des questionnements et l'élaboration de prototypes de solutions;
   b) recherche de normes et de bonnes pratiques dans le domaine de la sécurité des applications;
   c) définition d'un modèle général de la sécurité des applications;
   d) participation active à plusieurs groupes de travail;
   e) édition et rédaction de la norme ISO 27034 *Application Security*;

f) proposition de solutions pratiques permettant la mise en place des éléments et des processus du modèle;

a) utilisation de solutions pratiques pour des contextes d'applications en industrie.

2) Durant l'étape de validation

Une fois que les experts délégués par les différents pays ont vérifié les différents éléments du modèle, et nous ont proposé leurs commentaires et contributions, nous avons réalisé les activités suivantes :

a) réception et traitement des commentaires des représentants nationaux ;

b) obtention de consensus sur le traitement des commentaires reçus;

c) rétroaction de l'industrie sur les solutions pratiques proposées : liaisons formelles et informelles avec les experts d'organisations et de sous-comités ISO, dont notamment ceux d'IT-UT, du SC27, du SC7, du SC22 (*Voir* 5), Figure-A XIX-1);

d) validations et recommandations des différents éléments du modèle par les experts internationaux du domaine;

e) approbation des pays participants.

La Figure-A XIX-1 présente les comités, sous-comités et groupes de travail auxquels ont été distribués des demandes de liaisons, ainsi qu'un suivi du progrès de nos travaux.

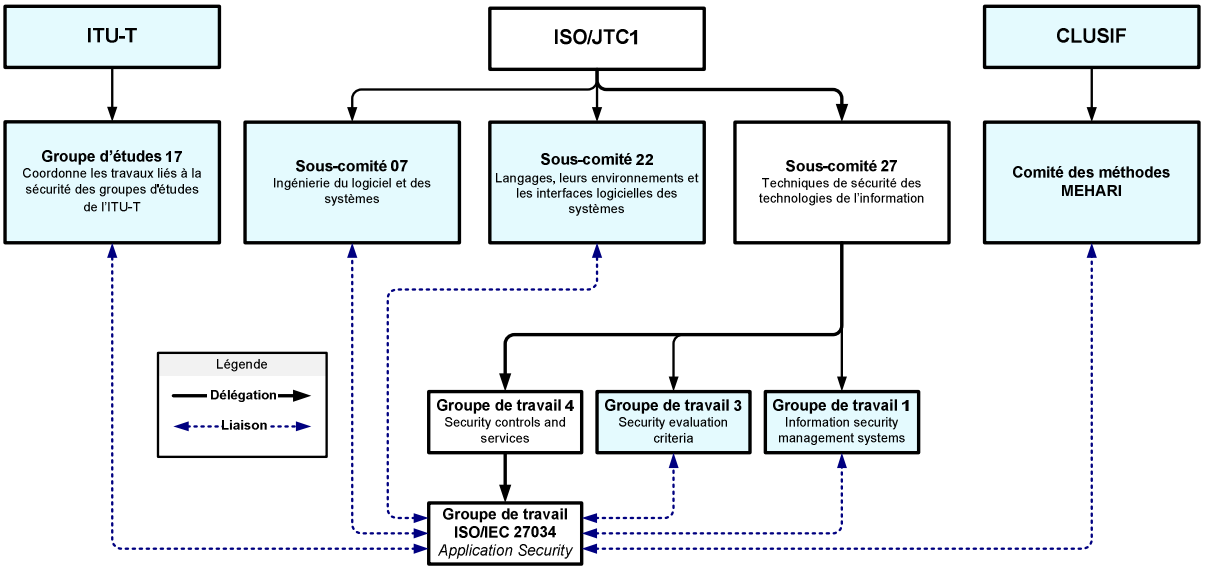


Figure-A XIX-1 Liaisons entre le projet ISO 27034 et les comités externes

Le groupe d'études 17 d'ITU-T coordonne les travaux liés à la sécurité technique des TI. Le sous-comité 7 d'ISO, avec la collaboration de l'IEEE, coordonne et encadre les recherches ainsi que la rédaction de normes en génie logiciel. Le sous-comité 22 d'ISO coordonne et encadre les recherches et la rédaction de normes concernant les langages de programmation, leur environnement, ainsi que les interfaces des systèmes. À l'intérieur du sous-comité 27, les groupes de travail 1 et 3, travaillant respectivement sur la gouvernance de la sécurité de l'information et sur la gestion de la sécurité au niveau des systèmes d'information, ont également été informés lors de séances d'information internes qui ont eu lieu lors de certaines rencontres internationales bisannuelles.

Voici une présentation sommaire des principaux événements qui se sont produits durant les différents stades et processus ISO, qui ont eu lieu lors des phases 2 et 3 de ce projet de recherche.

XIX.3 Stade préliminaire (00)

XIX.3.1 Étude et validation d'une demande de l'industrie ou d'un organisme.

Présentation et validation des principaux concepts et de l'idée générale du modèle SA produits lors de la revue de littérature et des travaux d'analyse complémentaires.

Période : 6 mois, de novembre 2006 à mai 2007 – 1 cycle Delphi.

XIX.3.2 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur l'orientation du modèle

Quatre contributions ont été présentées par les experts des pays suivants :

1) deux par le Japon (Nakao, 2006a), (Nakao, 2006b) qui, sommairement, présentait les concepts suivant :
   a) le danger des logiciels malicieux (*malwares*) et les cyberattaques;
   b) la gestion du risque dans l'identification des contrôles de protection des données des applications et des systèmes d'information à mettre en place;
   c) le besoin d'une approche permettant la mise en place de technologies de conception de système sécuritaire et l'arrimage de cette approche à la norme ISO 27001.
2) une par Hong Kong (Ma, 2006) qui, sommairement, présentait ses projets de recherche actuels, dont ceux concernant :
   a) l'importance de la protection des infrastructures réseau contre notamment les attaques des réseaux sans fil, et
   b) l'arrimage entre les différentes normes de sécurité de l'information de cette ville.
3) une par la Suède (Carlstedl, 2006) qui, sommairement, présentait son approche en sécurité de l'information et l'importance de s'arrimer à des normes internationales en matière de sécurité de l'information, dont celle de la série ISO 27000.

Même si le modèle amené par le chercheur incluait déjà plusieurs éléments proposés par les experts des divers pays, ces présentations confirmaient l'importance de tenir en compte trois orientations clés concernant la sécurité des applications, soit :

1) l'alignement du modèle avec la famille de normes ISO 27000 qui concerne la gestion de la sécurité des informations dans une organisation;
2) l'intégration du principe de « gestion du risque » dans le modèle pour guider l'identification des contrôles de sécurité à mettre en place dans une application;
3) la protection de l'infrastructure technologique requise par une application dans la portée de sa sécurité.

XIX.3.3 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur un des éléments du modèle

Aucun commentaire ou contribution proposés par les représentants nationaux n'a eu un impact sur un des éléments du modèle.

XIX.3.4 Résolutions et documents de liaison produits durant ce stade

Suite à sa présentation du modèle SA, le chercheur a été nommé au poste de responsable de la rédaction d'une nouvelle proposition de projet ISO. Sa fonction consistait à prendre en charge le démarrage du projet et de rédiger les divers documents requis aux fins de distribution aux experts des pays participants, soit :

1) Proposition de projet, qui a été présentée et approuvée par les représentants des pays présents.
2) Demandes de liaison qui ont été transmises aux trois groupes et comités JTC1/SC7 (SC27/WG4, 2006b), JTC1/SC22 (SC27/WG4, 2006c) et ITU-T/SG17 (SC27/WG4, 2006a) afin de les informer du démarrage du projet et de solliciter leur participation.
3) Rapport d'avancement de projet, produit à la fin de ce stade (SC27/WG4, 2006d).

Durant ce stade, aucun commentaire ne fut présenté par les pays participants. De tous les pays qui ont voté à ce stade, 100 % ont soutenu le passage du projet au stade suivant.

XIX.4 Stade de proposition (10)

Définition de la portée du projet et consolidation des contributions reçues.
Présentation et validation du modèle initial de la sécurité des applications.
Période : 6 mois, de mai à octobre 2007 – 1 cycle Delphi.

XIX.4.1 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur un des éléments du modèle

Aucun commentaire ou contribution proposés par les représentants nationaux n'a eu un impact sur un des éléments du modèle. Une contribution complémentaire du chercheur, soit une figure représentant le cycle de vie de la SA selon la couche de production d'une application, avait été présentée en appui au modèle.

XIX.4.2 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur l'orientation du modèle

Les commentaires et contributions reçus des pays participants ne proposaient aucun contenu précis, mais plutôt des orientations que le modèle devait prendre en compte. Par exemple :

1) Les commentaires présentés par l'Australie soulignaient que le modèle doive tenir en compte des activités d'impartition dans le cycle de développement d'une application. Il ont aussi exprimé le besoin que le modèle doive pouvoir servir de guide à une entreprise désirant développer une application sécuritaire (ISO/IEC, 2007f, p. 2).
2) Les commentaires du Japon ont notamment exprimé l'importance que le modèle tienne compte de la gestion des menaces et des risques de sécurité. Ces commentaires, qui étaient déjà adressés dans le modèle proposé par le chercheur (Poulin, 2007b, p. 22 et 42), confirmaient l'importance des orientations données au modèle, soit de gérer les activités de sécurité via la gestion du risque de sécurité.
3) Le Royaume-Uni a souligné l'importance que le modèle SA puisse soutenir le SGSI amené par la norme ISO 27001 (ISO/IEC, 2007f, p. 4). Cette préoccupation, qui était implicitement présente vu que le modèle s'appuyait sur un mécanisme de gestion du risque, a été explicitement intégrée au modèle.

4) La réponse du ITU-T/SG 17 à la demande de liaison du projet qui lui avait été envoyée, proposait sept documents, dont le contenu pouvait être arrimé avec le modèle (ITU-T, 2007b). Le sujet proposé portait principalement sur les exigences et les critères concernant des implémentations spécifiques de contrôles de sécurité d'application, tels que le document « X.1141 – *Security Assertion Markup Language* (SAML 2.0) » qui présente un langage basé sur le XML pour l'échange d'information en matière de sécurité, ou le document « X.sap-1 – *Guideline on secure password-based authentication protocol with key exchange »,* qui présente un guide pour l'implémentation d'un protocole d'authentification. Ces contributions ne s'appliquaient pas directement au modèle, mais elles pourraient toujours être utilisées par celui-ci lorsque nécessaires.

XIX.4.3 Résolutions et documents de liaison produits durant ce stade

À la suite de ce stade, le chercheur a commencé à réaliser un travail d'harmonisation du vocabulaire du modèle au vocabulaire du SC27. C'est aussi suite aux discussions, et aux commentaires traités durant ce stade, qu'a démarré une discussion sur la définition d'une application et la différence entre une application et la portée de sa sécurité.

Pour donner suite à ces discussions, le chercheur a rédigé les documents suivants pour distribution :

1) Un plan de travail a été proposé en début de rencontre de projet pour réaliser ce stade (Poulin, Kuiper et Kang, 2007);
2) La production du rapport du traitement des neuf commentaires, représentant le consensus des décisions prises par le comité de validation du projet (ISO/IEC, 2007f);
3) L'envoi de trois demandes de liaison aux groupes et comités JTC1/SC7 (SC27/WG4, 2007c), ITU-T/SG17 (SC27/WG4, 2007a) et NESSI (SC27/WG4, 2007d), pour les inviter contribuer ou à commenter nos travaux.

Durant ce stade, les neuf commentaires qui ont été présentés par l'Australie, le Japon et le Royaume-Uni ont été traités par consensus. Des pays participants qui ont voté à la fin de ce stade, 87 % ont soutenu le passage du projet au stade suivant.

XIX.5 Stade de préparation (20)

Rédaction de la norme et validations périodiques de son contenu par l'équipe de projet durant quatre cycles.

Période : 25 mois, d'octobre 2007 à novembre 2009 – 4 cycles Delphi.

Outre ceux concernant l'amélioration du texte, les commentaires reçus pendant ce stade concernaient principalement l'arrimage du vocabulaire et des concepts présentés dans la norme au vocabulaire et au processus des normes du sous-comité 7 soit, notamment, les normes ISO 12207 – *Software Life Cycle Processes*, et ISO 15288 – *System life cycle processes*. Tous les commentaires permettant d'améliorer la clarté des diagrammes et d'exprimer plus clairement les concepts présentés dans le document ont été approuvés.

XIX.5.1 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur un des éléments du modèle

Durant ces quatre rencontres, des discussions ont eu lieu concernant :

1) La structure du document;
2) L'arrimage du vocabulaire provenant des domaines de la gouvernance, du génie logiciel, des infrastructures TI et de la vérification;
3) Les concepts et principes introduits par le modèle.

Des consensus préliminaires ont été obtenus sur une définition du terme « application », du concept de la SA et du concept de niveau de confiance.

Parmi les événements clés qui ont eu lieu, il est pertinent de mentionner les éléments suivants :

1) Mise à jour du document énumérant les normes et pratiques recommandées pouvant être utilisées pour le développement du modèle (Poulin, Rouselle et Amsenga, 2008), en y intégrant de nouvelles références proposées par une contribution des experts de l'Afrique du sud (Amsanga, 2008), (ISO/IEC, 2008c, p. 41) dont, notamment, les normes suivantes :
   a) ISO 10007:2003, *Quality management systems – Guidelines for configuration management*;
   b) ISO/IEC 12207:2008, *Systems and Software Engineering – Software Life Cycle Processes;*
   c) ISO/IEC 15288:2008, *Systems Engineering – System life cycle processes;* et
   d) ISO/IEC 15443-1 *Information technology – Security techniques – A framework for IT security assurance*.
2) Des commentaires, provenant de l'Australie et des États-Unis, concernaient l'usage du terme « contrôle » qui était incompatible avec le concept de contrôle utilisé dans les documents ISO 27001 et 27002. Pour faire suite aux discussions et traiter ce commentaire, l'objet qui était initialement nommé « Mesure de Sécurité des Applications » fut renommé « Contrôle de Sécurité des Applications » (CSA). De plus, l'activité de vérification incluse dans ce contrôle fut renommée « mesure de vérification » (ISO/IEC, 2008c, pp. 2, 5 et 59);
3) Une contribution du Japon illustrant des exemples de CSA construits à partir de contrôles de sécurité de la norme ITU-T SP800-53 (ISO/IEC, 2009i, pp. 10-17). Celle-ci fut acceptée et placée en annexe;
4) Une contribution des États-Unis illustrant comment un processus de développement de logiciels axé sur la sécurité (Microsoft SDL) se compare au modèle de sécurité proposé (ISO/IEC, 2009i, pp. 53-70). Celle-ci fut acceptée et placée en annexe.

XIX.5.2 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur l'orientation modèle

Événements clés :

1) Des commentaires, provenant de l'Afrique du Sud concernaient l'ajout des deux principes suivant : « la sécurité est une exigence » et « la sécurité est dépendante du contexte » (ISO/IEC, 2008c, p. 23). Ceux-ci étaient implicitement inclus dans le modèle, mais n'avaient pas été clairement identifiés. Ils ont donc été ajoutés à la section « Principes » de la deuxième version du document de travail (ISO/IEC, 2008a, p. v);
2) Des commentaires provenant du Brésil confirmaient l'orientation du modèle dans l'identification des résultats de vérification attendus, lors de la définition de contrôles de sécurité (ISO/IEC, 2008c, p. 10). L'ensemble de ces commentaires a été pris en compte dans la suite des travaux;
3) Des commentaires provenant du Japon soulignaient la nécessité d'identifier des processus organisationnels, pour gérer les éléments du CNO de manière à soutenir le SGSI (ISO/IEC, 2008c, p. 14). Ces commentaires ont été pris en compte et les processus ont été définis et introduits à la deuxième version comité du document (ISO/IEC, 2008a, p. 36);
4) Des commentaires provenant du Royaume-Uni concernaient principalement leurs préoccupations sur les éléments suivants :
   a) l'alignement du modèle avec les normes ISO de la série 27000. Ces commentaires furent pris en compte par le chercheur dès ce stage, pour l'orientation des ajustements du modèle (ISO/IEC, 2007b, p. 8 et 20); et
   b) la clarification du terme « application » qui fut à ce moment défini comme étant une « application d'affaires », soit une application qui aide une organisation à automatiser un processus ou une fonction d'affaires. Un processus d'affaires inclut les personnes et la technologie (ISO/IEC, 2007b, p. 7).
5) Une contribution a été réalisée par le Japon. Elle présentait un exemple de conversion d'un contrôle de sécurité, provenant de la norme NIST 800-53 – *Recommended Security Controls for Federal Information Systems*, vers la structure d'un CSA proposé par le modèle (ISO/IEC, 2009i, p. 10). Cette contribution a été placée à l'annexe B de la première version comité de la norme ISO 27034 (ISO/IEC, 2009b, p. 62);

6) Une contribution, provenant des experts des États-Unis, présente l'arrimage entre le cycle de développement sécuritaire (SDL) de Microsoft[58] avec le modèle, afin de démontrer la possibilité, pour une organisation, de mettre en place le modèle SA sans changer ni ses processus ni son cycle de développement (ISO/IEC, 2009i, p. 53). Cette contribution a été placée à l'annexe A de la norme ISO 27034 (ISO/IEC, 2009b, p. 46);
7) Trois autres contributions ont été émisses par les experts des États-Unis :
   a) une première, provenant du département « Homeland Security », illustrant un processus de développement de logiciel sécuritaire (DHS, 2007);
   b) une deuxième, provenant conjointement des organisations « Information Assurance », ITAC et DACS, présentant l'assurance de sécurité dans le logiciel (Goertzel et al., 2007); et
   c) une dernière, provenant de Microsoft, présentant une introduction de leur « Software Development Lifecycle » (Microsoft, 2007).

   Ne s'appliquant pas directement au modèle, ces contributions ont été utilisées comme guides en fonction de leurs champs spécifiques de connaissances.

8) Une réponse à notre demande de liaison nous est parvenue d'ITU-T (ITU-T, 2007a), présentant des projets qui pourraient influencer nos travaux ainsi que leur vif intérêt à une collaboration entre nos groupes de travail;
9) Trois contributions, provenant des experts de l'Allemagne (BSI, 2005c), (BSI, 2005b), (BSI, 2005a), présentaient trois parties de la norme BSI 100, soit : la partie 1 : le SGSI, la partie 2 : une méthode de protection de base des TI, et la partie 3 : une approche de gestion du risque pour les TI. Concernant plutôt l'organisation, ces trois normes ne s'appliquaient pas directement à la sécurité des applications, mais il était entendu que le modèle devrait tenir compte de leurs équivalents chez le SC27, soit des normes appartenant à la série ISO 27000;

---

[58] Microsoft Security Lifecycle Development.

10) Deux contributions, provenant des experts de l'Australie (ISO/IEC, 2008d, p. 15), proposaient du texte pour remplacer celui de l'introduction ainsi qu'une structure pour le chapitre 7 du document de travail de la norme. La section du texte proposé, précisant que « les protections technologiques de sécurité étant insuffisantes » fût intégrée au texte de l'introduction (ISO/IEC, 2008d, p. 1). Par contre, la proposition de structure pour le chapitre 7 fut rejetée par consensus (ISO/IEC, 2008d, p. 10).

XIX.5.3 Résolutions et documents de liaison produits durant ce stade

Rédaction par le chercheur des documents suivants pour distribution :

1) Envois de six demandes de liaison aux groupes et comités JTC1/SC7 (SC27/WG4, 2007e), (SC27/WG4, 2008b), JTC1/SC22 (SC27/WG4, 2007f), (SC27/WG4, 2008c) et ITU-T/SG17 (SC27/WG4, 2007b), (SC27/WG4, 2008a), pour les inviter à contribuer ou à commenter nos travaux.
2) Un rapport d'avancement de projet a été produit à la fin de chacune de ces rencontres (SC27/WG4, 2007g), (SC27/WG4, 2008d), (SC27/WG4, 2008e) et (SC27/WG4, 2009a, pp. 6-7).

Durant ce stade, les 770 commentaires présentés par les représentants nationaux des États-Unis, de l'Afrique du Sud, de l'Australie, du Japon, du Brésil, de la Malaisie, de l'Autriche, du Royaume-Uni et de la Norvège ont été traités par consensus. Des pays participants qui ont voté à la fin de ce stade, 86 % ont soutenu le passage du projet au stade de comité (30), acceptant l'ensemble des concepts et éléments de SA intégrés à la norme. Le résultat de ce vote confirme aussi que les pays croyaient que le document était prêt pour être soumis à un plus grand nombre d'experts vérificateurs.

XIX.6 Stade de comité (30)

Bonification de la norme et validation périodique de son contenu par les membres d'un comité élargi de vérificateurs experts délégués par les pays participants.

Période : 11 mois, de novembre 2009 à octobre 2010 – 2 cycles Delphi.

Non seulement les experts vérificateurs nationaux participants aux travaux du SC27 ont continué à commenter le document du projet, mais ce dernier a aussi été distribué, par les pays participants, à des groupes d'experts vérificateurs œuvrant dans des organisations et des entreprises des nations concernées.

Outre ceux concernant l'amélioration du texte, les commentaires reçus pendant ce stade des États-Unis, de l'Afrique du Sud, de l'Australie, du Japon, du SC7 et de l'Italie concernaient principalement l'arrimage du vocabulaire et des concepts présentés dans la norme aux vocabulaires et aux processus des normes « ISO 31000 – Management du risque » et « ISO 27005 – Gestion des risques » liés à la sécurité de l'information. Tous les commentaires permettant d'améliorer la clarté des diagrammes et d'exprimer plus clairement les concepts présentés dans le document ont été approuvés.

XIX.6.1 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur un des éléments du modèle

Événements clés : Aucun.

XIX.6.2 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur l'orientation du modèle

Événements clés :

1) Les commentaires de l'Australie concernaient principalement l'alignement de la terminologie et du ou des processus du modèle avec les normes ISO 31000 et ISO 27005 concernant la gestion du risque de sécurité (ISO/IEC, 2009h, p. 6). Cet alignement était déjà en cours, mais une attention particulière a été portée pour satisfaire à ces demandes spécifiques;
2) Les commentaires de l'Afrique du Sud concernaient principalement l'alignement de la terminologie et processus du modèle avec les normes ISO 15288 et ISO 12207

concernant les processus présents dans le cycle de vie d'un système et d'un logiciel (ISO/IEC, 2009h, pp. 23-37). Cet alignement était déjà en cours;

3) Les commentaires du Japon concernaient principalement des demandes de clarification permettant de mieux préciser la portée de certains éléments, tels que le contexte d'affaires, le contexte juridique et les CSA (ISO/IEC, 2009h, pp. 2-14). Ces précisions furent apportées durant de stade;
4) Finalement, des discussions ont eu lieu à propos du concept de « niveau de confiance » (NdC) et ce qu'il apportait de plus par rapport au concept de « niveau d'assurance » défini par la norme « ISO 15443-1 Un canevas pour l'assurance de la sécurité dans les technologies de l'information – Partie 1 : Vue d'ensemble et canevas » (ISO/IEC, 2005f). Nous avons démontré que le NdC s'appuyait sur la définition de niveau d'assurance pour apporter des preuves vérifiables de ses prétentions. Cependant, il appert que dans les faits, il était surtout utilisé comme outil de communication, servant à identifier clairement les différents contrôles de sécurité à mettre en place et à vérifier lorsqu'un NdC était assigné à une application. Le concept du NdC amené par le modèle est une spécialisation du concept de « Base informatique de confiance » (*Trusted Computing Base)* proposée par Charles P. Pfleeger et Shari Lawrence Pfleeger dans leur ouvrage *Security in computing (Pfleeger et Pfleeger, 2008, p. 337)*.

XIX.6.3 Résolutions et documents de liaison produits durant ce stade

Aucune demande de liaison n'a été envoyée ni n'a été reçue durant ce stade.

Un rapport d'avancement de projet a été produit par le chercheur à la fin de chacune de ces deux rencontres (SC27/WG4, 2009b) et (SC27/WG4, 2010b).

Après douze mois de travail, le comité a approuvé le traitement des commentaires et a proposé le passage du document à la version de comité finale (FCD), lors de sa prochaine distribution. Des pays participants qui ont voté à la fin de ce stade, 70 % ont soutenu le

passage du projet au stade d'enquête (40), acceptant l'ensemble des concepts et éléments de SA intégrés à la norme.

XIX.7 Stade d'enquête (40)

Dernières validations avant que le document de travail de la norme soit soumis au vote d'approbation des pays membres du SC27.

Période : octobre 2011 à novembre 2011 – aucun cycle Delphi.

Un des défis de ce projet était de concilier le vocabulaire de quatre secteurs d'interventions en sécurité de l'information. Celui-ci a été présent tout au long de l'étape de validation, et s'est finalement conclu à la fin de ce stade.

XIX.7.1 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur un des éléments du modèle

Événements clés :

1) Un des commentaires émis par un expert du SC7 d'ISO proposait le remplacement du terme « Processus », qui décrivait des groupes d'actions dans le modèle de référence du cycle de vie de la sécurité des applications, afin d'éviter des conflits avec certains documents de ce sous-comité. Pour améliorer l'alignement du vocabulaire du modèle avec celui utilisé par le SC7, l'expression « ensemble d'activités » a été proposée et acceptée (ISO/IEC, 2011b, p. 25);
2) Un des commentaires émis par les experts du Japon demandait d'améliorer la définition d'application, afin de la clarifier (ISO/IEC, 2011f, p. 5). La définition bonifiée qui a été adoptée est : « une solution TI qui inclut le logiciel, les données et les procédures, conçue pour aider un utilisateur d'une organisation à réaliser une tâche particulière, ou à gérer un

problème TI particulier, en automatisant un processus ou une fonction d'affaires. »[59] Cette nouvelle définition a été intégrée à la version finale de la norme (ISO/IEC, 2011c, p. 2).

3) À la demande du Japon, le rôle « Fournisseur », est un des rôles qui devrait être identifié parmi les rôles de l'audience ciblée par le modèle (ISO/IEC, 2011f, p. 5). Ce rôle a été ajouté à la section 0.3 de la norme (ISO/IEC, 2011c, p. xii).

XIX.7.2 Commentaires et contributions clés proposés par les pays participants qui ont eu un impact sur l'orientation du modèle

Événement clé :

1) Deux commentaires ont été émis par les experts de la France, soit :
   a) le premier demandant une clarification de la portée relative à une application et celle se rapportant à la SA (ISO/IEC, 2011f, p. 3). Ce commentaire a été résolu par l'insertion d'une table, dans la section 6.3.1 du document, présentant les éléments reliés à la portée d'une application et ceux reliés à la portée de sa sécurité (ISO/IEC, 2011c, p. 7).
   b) Le second suggérant d'expliciter les relations entre le modèle SA et certaines normes clés de sécurité et de génie logiciel publiés par l'ISO (ISO/IEC, 2011f, p. 2). Ces précisions ont été ajoutées à la section 0.5 de la norme (ISO/IEC, 2011c, p. xiv).

XIX.7.3 Résolutions et documents de liaison produits durant ce stade

Aucun document de liaison n'a été envoyé ni reçu durant ce stade.

Un rapport d'avancement de projet a été produit par le chercheur à la fin de chacune de ces deux rencontres (SC27/WG4, 2010a) et (SC27/WG4, 2011).

---

[59] Traduction libre.

Durant ce stade, chacun des 116 commentaires, qui ont été présentés par les représentants nationaux des États-Unis, de l'Afrique du Sud, de l'Australie, du Japon, de la Malaisie, de la France, du Canada, de l'Indonésie et des Pays-Bas, a été traité et approuvé par consensus. Des pays participants qui ont voté à la fin de ce stade, 67 % ont soutenu le passage du projet au stade d'approbation (50), acceptant l'ensemble des concepts et des éléments de SA intégrés à la norme.

XIX.8 Stade d'approbation (50)

Distribution du document à tous les pays du SC27 pour être soumis à un vote d'approbation final sans réserve.

XIX.8.1 Résolutions et documents de liaison produits durant ce stade

Aucun rapport n'a été produit à la fin de ce cycle, sauf le document présentant les trois commentaires traités par le JTC1.

Le traitement de chacun des trois commentaires, qui ont été présentés par le Japon, a été réalisé par les représentants du comité joint (JTC1) d'ISO. Des pays participants qui ont voté à la fin de ce stade, 96 % ont soutenu le passage du projet au stade de publication (60), approuvant ainsi la distribution du modèle SA.

XIX.9 Stade de publication (60)

La version finale du document de la norme ISO 27034 – *Application Security – Part 1 : Overview and concepts* (ISO/IEC, 2011d) fut publiée, mise en ligne sur le site Web d'ISO et distribuée aux pays participants en début décembre 2011.

ANNEXE XX

VALIDATION ET AMÉLIORATION DU MODÈLE SA : VÉRIFICATION EMPIRIQUE PARTIELLE

XX.1 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'application 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 chez des 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 ceux qui ont eu un impact ou qui ont mené à l'intégration d'éléments du modèle dans un projet d'application.

Projet DGÉQ, janvier 2006

Présentation, développement et utilisation d'un processus d'audit technique de sécurité basé sur le modèle SA préliminaire[60] par l'équipe de vérification pour vérifier les 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 de l'organisation (4) l'organisation a exprimé sa

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

satisfaction de manière concrète en recommandant le chercheur à Élections Canada pour prendre en charge le volet de la SA dans la première phase du projet pilote de réalisation du système de votation par internet canadien.

Conférence Nurun, juin 2007

Sur invitation de la compagnie Nurun inc., présentation d'une version préliminaire du modèle SA et de son implémentation dans un projet d'audit de sécurité des SVÉ, lors d'une rencontre du groupe de la pratique Techno-Sécurité de l'entreprise hôte. (Poulin, 2007e).

- Date et lieu : 21 juin 2007, Québec
- Nombre de participants : 15
- Interprétation de la mesure : (1) intérêt de l'entreprise à avoir de l'information sur le modèle et son implémentation, (2) intérêt de l'entreprise à appliquer des éléments du modèle dans ses projets, (4) support 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.

Conférence CRIM, mai 2008

Présentation du modèle lors de la Journée de la qualité du logiciel du Centre de recherche informatique de Montréal (CRIM). Cette conférence avait pour objet d'exposer que la qualité est une alliée essentielle dans la SA et de présenter l'arrimage entre la qualité et le modèle SA (Poulin, 2008c).

- Date et lieu : Montréal, le 14 mai 2008
- Nombre de participants : 40 personnes.
- Interprétation de la mesure : (1) intérêt des entreprises et organisations à investir pour recevoir, ou faire communiquer, de l'information sur le modèle.

Conférence LGS, décembre 2008

Présentation, sur invitation, du modèle et d'une étude de cas présentant son implémentation dans un projet d'audit de sécurité des SVÉ, lors d'une rencontre du groupe de la pratique de sécurité de la compagnie Groupe LGS inc. (Poulin, 2008d).

- Date et lieu : 9 décembre 2008, Québec
- Nombre de participants : 10 personnes
- Interprétation de la mesure : (1) intérêt de l'entreprise à investir pour recevoir de l'information sur le modèle, (2) intérêt de l'entreprise à appliquer des éléments du modèle dans ses projets.

Conférence Boeing, mars 2009

À la demande du responsable des tests de SA internes de Boeing, présentation du modèle SA lors d'une rencontre de travail du comité de vérification de la certification professionnelle CSSLP d'$(ISC)^2$ (Poulin, 2009c). Cette présentation a amené Boeing à soutenir ce professionnel pour qu'il participe aux travaux du SC27, à titre d'expert délégué par les États-Unis, sur le projet de la sécurité des applications. Durant cette période, les États-Unis ont produit à eux seuls plus de 508 commentaires qui ont tous été traités à l'intérieur du processus de projet d'ISO (*Voir* Tableau-A XIX-1).

- Date et lieu : 26 mars 2009, Washington DC
- Nombre de participants : 1
- Interprétation de la mesure : (1) intérêt de l'entreprise à avoir de l'information sur le modèle, (2) intérêt de l'entreprise à appliquer des éléments du modèle dans ses projets, (4) soutien de Boeing à la délégation des États-Unis au SC27, dans le but de faire participer un de ses professionnels au projet de la norme ISO 27034.

Projet Tracsys, avril 2009

Lors d'une rencontre avec un chef de projet de la compagnie TracSys inc., la présentation du modèle SA a suscité un vif intérêt. L'entreprise était au démarrage du projet de développement de l'application C2 Trace, qui servirait éventuellement à gérer et à suivre via satellite, la cueillette, le transport et la livraison par camion de marchandises entre des entreprises œuvrant dans les provinces du Canada et dans certains états des États-Unis. Les éléments du modèle utilisés ont aidé la compagnie TracSys inc. à identifier les risques et intégrer les activités de sécurité requises durant la réalisation de la première phase de ce projet. Satisfaite des résultats obtenus, la compagnie a accepté de réaliser une présentation conjointe du modèle SA appuyée par une étude de cas démontrant comment son projet avait utilisé le modèle dans le développement de l'application C2 Trace. Cette présentation a eu lieu lors d'un des événements d'Action-TI (Poulin et Gagnon, 2009).

- Dates et lieu du projet : 8 avril 2009, Québec
- Nombre de participants : 5 personnes ont participé au projet, et 45 personnes ont assisté à la présentation
- Envergure du projet : 3 750 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 C2 Trace, (3) 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 acceptant de témoigner de son expérience avec le modèle.

Conférence ISIQ / MSG, mars 2010

Présentation du modèle lors d'un WebSeminaire offert conjointement par l'Institut de la sécurité de l'information du Québec (ISIQ) et le ministère des Services gouvernementaux du Québec (Poulin, 2010b).

- Date et lieu : 29 mars 2010, Québec
- Nombre de participants : 80 personnes
- Interprétation de la mesure : (1) intérêt des entreprises et organisations à investir pour recevoir ou faire communiquer de l'information sur le modèle.

Conférence RSI, mai 2010

Présentation du modèle lors du congrès « RSI 2010 » regroupant des professionnels de la sécurité de l'information (Poulin, 2010c).

- Date et lieu : 18 mai 2010, Montréal
- Nombre de participants : 50 personnes
- Interprétation de la mesure : (1) intérêt des entreprises et organisations à investir pour recevoir ou faire communiquer de l'information sur le modèle, (2) intérêt d'une entreprise à appliquer des éléments du modèle dans un de ses projets[61].

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

---

[61] C'est durant cet événement que le Mouvement Desjardins s'est montré intéressé à appliquer certains éléments du modèle dans ses processus de développement, de maintenance et de vérification de certaines de ses applications.

des rencontres de ce projet que le composant « Matrice de traçabilité de la sécurité des applications » à été conçu et intégré dans le modèle par le chercheur, afin de répondre à un besoin de gestion du suivie 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.

Conférence GoSec, février 2011

Présentation du modèle lors du congrès « GoSec2011 » regroupant des professionnels de la sécurité de l'information (Poulin, 2011a).

- Date et lieu : 9 février 2011, Montréal
- Nombre de participants : 50 personnes
- Interprétation de la mesure : (1) intérêt des entreprises à avoir de l'information sur le modèle.

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 d'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 buts de faire participer un de ses professionnels au projet de la norme ISO 27034.

Conférence DGÉQ Février 2013

Présentation du modèle SA et démonstration de son utilisation par Élections Canada pour prendre en charge la sécurité dans son projet de système de votation par Internet (Poulin, 2013b). Cette rencontre de travail était une des étapes d'un projet du DGÉQ visant à identifier une stratégie de sortie du moratoire sur l'utilisation ses systèmes de votation électronique au Québec.

- Date et lieu : 27 février 2013, Québec
- Nombre de participants : 12 personnes
- Interprétation de la mesure : (1) intérêt de l'entreprise à avoir de l'information sur le modèle, (2) intérêt de l'organisation à appliquer des éléments du modèle dans leur projet, (3) utilisation des éléments qui conviennent à l'atteinte des objectifs de sécurité de l'organisation, (4) l'organisation reconnaît le progrès réalisé en matière de SA dans son précédent projet, et envisage la possibilité d'utiliser le modèle à nouveau.

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.

ANNEXE XXI

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 :

5) Comme sources de contrôles de sécurité des applications, qui serviront à définir des CSA requis par l'organisation pour ses applications;
6) 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;
7) 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; et
8) 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.

La Figure-A XXI-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.

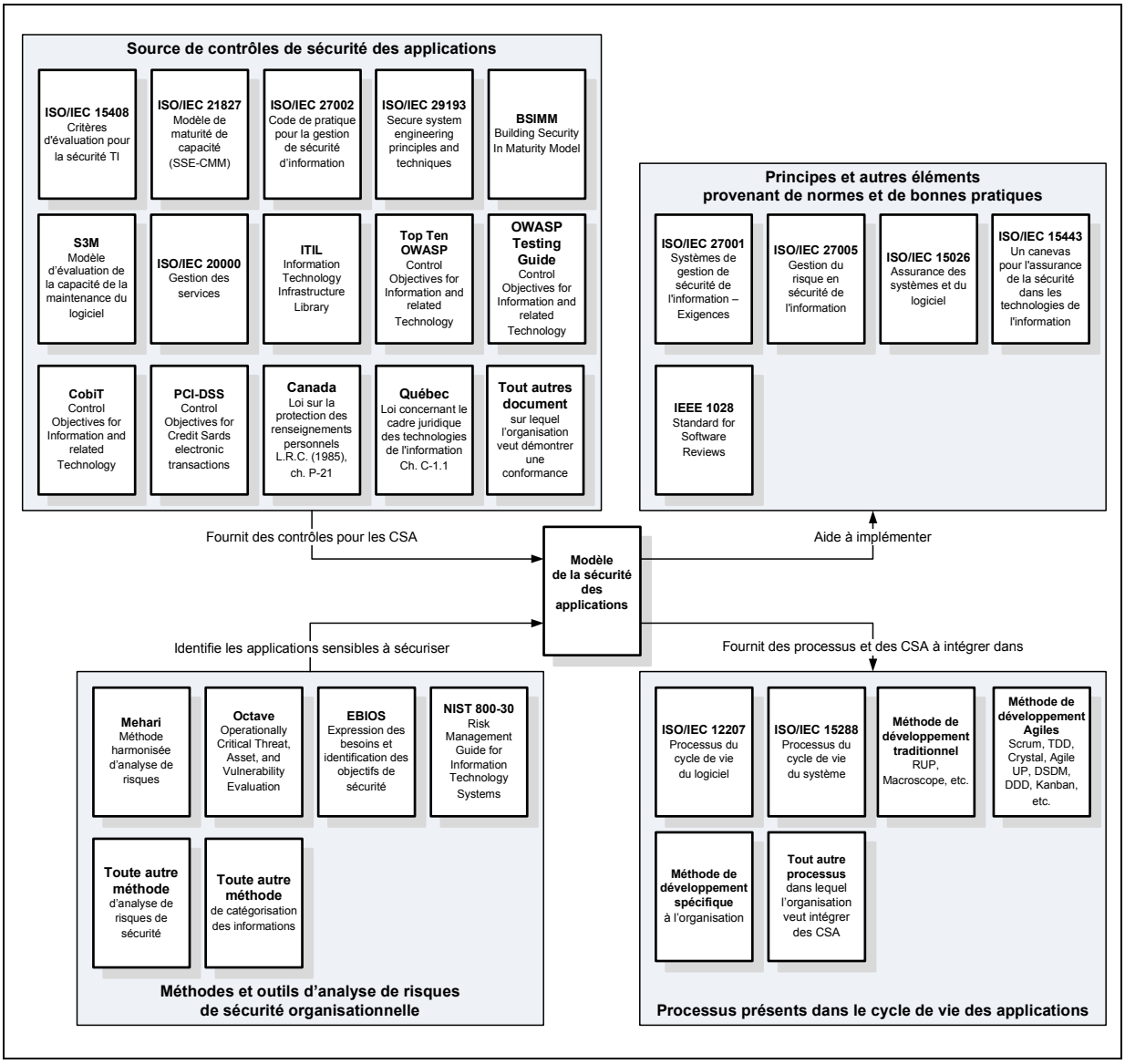


Figure-A XXI-1 Relations du modèle avec d'autres normes, méthodes, règlements et bonnes pratiques
Traduite et adaptée de (ISO/IEC, 2011d)

Il est important de noter que la liste des documents présentés dans la Figure-A XXI-1 ne représente qu'un aperçu des normes et bonnes pratiques pouvant être reliées au modèle SA, et n'est présentée que pour aider à la compréhension du positionnement du modèle. Des organisations comme l'OWASP et l'ISACA continuent à publier des documents qui peuvent être reliés au modèle via l'un des quatre groupes de documents, par exemple le Top 10 2013

des risques de sécurité des applications Web (OWASP, 2013) qui présente les nouveaux risques de sécurité des applications Web pour 2013.

XXI.1 Source de contrôles de sécurité des applications

Cette section présente une liste non exhaustive de normes, de lois, et de bonnes pratiques desquels peuvent être développés des CSA afin d'en permettre l'implémentation.

Voici quelques exemples de documents pouvant servir au développement de CSA.

1) La norme ISO 15408-3, *Information Evaluation criteria for IT security – Part 3 : Security assurance components.* Cette norme présente des exigences et des activités de sécurité que l'organisation peut mettre en œuvre au moyen de CSA (ISO/IEC, 2005b).
2) La norme ISO 27002, *Code of practice for information security management.* Cette norme présente des contrôles de sécurité qui peuvent être utilisés par une organisation pour mettre en place des CSA (ISO/IEC, 2005c).
   Les contrôles les plus appropriés à la SA proposés par la norme ISO 27002 proviennent des sections suivantes :
   a) chapitre 10 – Gestion des communications et des opérations;
   b) chapitre 11 – Contrôle d'accès; et
   c) chapitre 12 – Acquisition, développement et maintenance de systèmes d'information.
3) La norme ISO 29193, *Secure system engineering principles and techniques* (en développement). Cette norme présente des conseils pour l'ingénierie de systèmes ou de produits TI sécuritaires qui peuvent être mis en œuvre à l'aide de CSA (ISO/IEC, 2009e).
4) La norme ISO 21827, *Capability Maturity Model* (SSE CMM). Cette norme présente des pratiques d'ingénierie de sécurité qui peuvent être utilisées par une organisation pour définir des CSA. En outre, les procédés du modèle aideront à atteindre plusieurs des capacités qui définissent les niveaux de capacité dans la norme ISO 21827 (ISO/IEC, 2006a).

5) Les documents *Top Ten OWASP* et l'*OWASP Testing Guide (OWASP, 2008b)*, qui présentent des activités de sécurité et de tests identifiés pour atténuer les principaux risques de sécurité concernant les applications Web.
6) Le document *COBIT – Control objectives for information and related technology*, propose une approche, des processus et des objectifs de contrôles permettant de vérifier et d'auditer la sécurité des actifs informationnels d'une organisation (ITGI, 2007).
7) Le document *Software Maintenance Management: Evaluation and Continuous Improvement*, propose un modèle d'évaluation de la capacité à maintenir le logiciel. Ce modèle présente notamment des groupes de processus clés contenant des activités et des résultats attendus permettant d'améliorer la maturité des processus de maintenance du logiciel (April et Abran, 2008).
8) Le document *PCI-DSS – Controls objectives for credits cards electronic transactions*, propose des objectifs de contrôle permettant de certifier la sécurité des transactions électroniques pour les applications offrant un service de paiement par cartes de crédit (LLC, 2010).
9) Le document *ITIL – Information Technology Infrastructure Library*, propose des processus et des contrôles pour la gestion et la sécurisation des services d'infrastructure technologique (OGC, 2007).
10) Loi canadienne sur la protection des renseignements personnels, qui encadre le traitement la conservation et la divulgation de renseignements concernant les individus au Canada (Canada, 13 novembre 2013).

XXI.2 Sources de principes et processus pris en compte par le modèle SA

Cette section présente une liste non exhaustive de normes faisant état des bonnes pratiques de génie logiciel, d'assurance de sécurité ou de gestion de risques bénéfiques pour une organisation, qui ont été pris en compte lors de la conception du présent modèle.

1) La norme ISO 27001, *Information security management systems – Requirements (ISO/IEC, 2005d)*. Le présent modèle contribue à mettre en œuvre, avec une portée

limitée à la sécurité des applications, des recommandations de la norme ISO 27001. En particulier, les approches suivantes sont utilisées :

a) une approche systématique de la gestion de la sécurité;
b) l'approche processus « Plan, Do, Check, Act », appliquée à un processus de gestion de la sécurité de l'information; et
c) la mise en œuvre de la sécurité de l'information fondée sur la gestion des risques.

2) La norme ISO 15026-2:2011 Ingénierie du logiciel et des systèmes – Assurance du logiciel et des systèmes – Partie 2, Cas d'assurance (ISO/IEC, 2010f). L'utilisation des processus et des CSA proposés par le présent modèle dans des projets d'application fournit directement les cas d'assurance sur la sécurité de l'application. Plus précisément :
   a) les assertions et leurs justifications sont fournies par le processus de d'analyse des risques de sécurité de l'application;
   b) la preuve est fournie par les mesures de vérification intégrées dans les CSA; et
   c) la conformité à ce modèle peut être utilisée comme argument dans de nombreux cas d'assurance.
3) La norme ISO TR 15443, *Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework (ISO/IEC, 2005f), and – Part 3: Analysis of assurance methods (ISO/IEC, 2007d).* Le présent modèle permet d'appliquer et de refléter les principes d'assurance de sécurité proposés par la norme ISO 15443 partie 1, et à contribuer au cas d'assurance selon la norme ISO 15443, partie 3.
4) La norme ISO 27005, *Information Security Risk Management (ISO/IEC, 2010d)*. Le présent modèle contribue à mettre en œuvre, avec une portée limitée à la sécurité des applications, les processus de gestion des risques proposés par la norme ISO 27005.
5) La norme IEEE 1028 : *Standard for Software Reviews* (IEEE, 1997). Le présent modèle contribue à mettre en œuvre, avec une portée limitée à la sécurité des applications, les processus de révision de logiciel proposés par la norme IEEE 1028.

XXI.3 Méthodes d'analyse de risques de sécurité organisationnelle

Des méthodes d'analyse de risques de sécurité organisationnelle, telles que MÉHARI – Méthode harmonisée d'analyse de risques (CLUSIF, 2005), Octave – *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (SEI, 2001), EBIOS – Expression des besoins et identification des objectifs de sécurité (DCSSI, 2004) ainsi que la norme américaine NIST 800-30, *Risk Management Guide for Information Technology Systems* (Stoneburner, Goguen et Feringa, 2002), offrent toutes des processus d'analyse de risques de sécurité de l'information permettant aux organisations d'évaluer les risques de sécurité amenés par les systèmes, les applications et autres actifs informationnels en leur possession.

Les résultats de ces analyses de risques de sécurité organisationnelle permettent notamment d'identifier les actifs informationnels les plus sensibles de l'organisation, dont les applications qui devront être protégées.

XXI.4 Processus présents dans le cycle de vie des applications

Lors de son implémentation, le modèle SA permet de concevoir des activités de sécurité et des CSA qu'une organisation peut intégrer à ses processus existants, tels que ceux proposés par :

1) Les normes internationales ISO 15288, *Systems and software engineering – System life cycle processes (ISO/IEC, 2004d)*, et ISO 12207, *Systems and Software Engineering – Software life cycle process (ISO/IEC, 2008e)*. Le présent modèle fournit des processus supplémentaires ainsi que des CSA qu'une organisation peut intégrer aux processus existants du cycle de vie des systèmes et des logiciels, tels que proposés par les normes ISO 15288 et ISO 12207.
2) Les méthodes de développement traditionnelles, les méthodes de développement agiles aussi bien que les méthodes de développement propriétaires d'une organisation sont en mesure de proposer des processus dans lesquels il est possible d'intégrer des CSA.

L'approche d'intégrer directement les activités de sécurité et les activités de vérification dans les processus de la méthode de développement utilisée par les équipes de projets d'applications, facilite la gestion de la résistance aux changements des divers intervenants impliqués par ces changements, permet de diminuer leurs coûts de formation, ainsi que minimiser les coûts d'intégration de la sécurité dans lesprojets de réalisation et d’opération d'applications.

ANNEXE XXII

LISTE DES CONSTATS GÉNÉRAUX SUITE À L'ÉVALUATION DES SYSTÈMES DE VOTATIONS ÉLECTRONIQUES UTILISÉS LORS DES ÉLECTIONS MUNICIPALES QUÉBÉCOISES DE 2005

Cette annexe présente la liste des 18 constats généraux (CG) du DGÉQ suite à l'évaluation des systèmes de votations électroniques (SVÉ) utilisés lors des élections municipales québécoises de novembre 2005 (Poulin, 2006c, pp. 10-25, 113-114).

CG1 : Aucun fournisseur ne possède une documentation claire et détaillée concernant les rôles, responsabilités et qualifications requises des membres de son équipe de projet, tant en ce qui a trait au développement, aux tests qu'au soutien technique.

CG2 : Aucun fournisseur n'a pu nous fournir une documentation précisant les rôles, les responsabilités et les qualifications requises des personnes impliquées dans leur projet notamment, celles qui ont participé à la réalisation du développement du logiciel du système de votation électronique et celles qui ont décidé de l'infrastructure technologique à mettre en place.

CG3 : Après avoir pris connaissance des documents reçus des fournisseurs, on ne peut ni mesurer ni garantir la compétence des formateurs, le degré de compréhension des personnes formées et la compétence des techniciens qui auraient suivi la formation.

CG4 : À l'exception de l'entreprise TM Technologies Élections qui possédait certains résultats de test, aucun fournisseur ne nous a fourni des preuves que des validations formelles des mesures de sécurité mises en place aient été réalisées.

Cette validation aurait permis de vérifier l'efficacité de chacune des mesures et de prouver qu'elles répondaient aux attentes.

CG5 : Aucun fournisseur ne nous a remis de document nous prouvant que l'impact de l'adaptation des divers processus inclus dans le processus de votation traditionnel a été analysé, de manière à permettre la distribution, le stockage et l'utilisation sécuritaire de leur système de votation électronique.

CG6 : Aucun fournisseur ne nous a remis de document nous prouvant que des mesures ont été mises en place pour limiter l'accès au matériel de votation aux seules personnes autorisées.

CG7 : Tous les systèmes de votation électronique proposés conservent le processus traditionnel d'authentification d'un électeur.

L'utilisation ou non d'une LÉI (liste électorale informatisée) n'a aucun impact sur ce processus et n'y introduit aucun nouveau risque.

CG8 : Aucun fournisseur n'a produit de documents démontrant que la sécurité a été assurée en ce qui a trait à l'infrastructure technologique utilisée par leur système de votation électronique.

CG9 : Aucun fournisseur n'a réalisé d'analyse de risque formelle de leur système.

CG10 : Aucun mécanisme de vérification des fonctionnalités, de l'intégrité et des paramètres du logiciel contenu dans les appareils n'existait sur les systèmes proposés par les fournisseurs.

Il faut noter que le comportement d'un système peut être modifié dès que survient un changement dans la programmation ou dans les paramètres utilisés.

CG11 : À l'exception de TM Technologies Élections, aucun fournisseur n'a mis en place ni n'a vérifié la présence de mesure de protection du bulletin de vote électronique qui était conservé dans la mémoire du système de votation qu'il proposait.

CG12 : Aucune preuve ne nous a été fournie que les systèmes de votation électronique, tels que programmés et utilisés lors de l'élection municipale 2005 possédaient de dépôt des votes électroniques sécuritaire officiel ayant pu permettre une vérification des votes enregistrés.

Les seules preuves que nous avons reçues concernent le fait que ces systèmes conservent en mémoire le résultat des votes pour chacun des candidats.

CG13 : Aucun système de votation électronique ne possède des mesures de protection et de vérification des résultats de vote qu'il aurait enregistrés.

CG14 : Aucun des systèmes de votation audités ne possède de mécanisme identifiant les types de vote.

Ceci n'avait aucun impact sur la protection des votes contenus dans les systèmes utilisés en novembre 2005.

CG15 : Aucun des systèmes de votation audité ne confirme de façon claire et précise, la lecture, l'interprétation et la sauvegarde du vote de l'électeur.

CG16 : Aucun des systèmes de votation audités ne présente de preuve suffisante nous permettant de garantir qu'il est impossible d'associer un électeur à son vote.

CG17 : Aucun des systèmes de votation audités ne garantit l'intégrité de chacun des votes reçus et du résultat de la consolidation qui en découle, le cas échéant.

CG18 : À la lumière de l'ensemble des constats précédents, force est de constater que les fournisseurs, à l'exception de TMTé, ne connaissaient pas le fonctionnement détaillé de leurs systèmes de votation électronique.

De plus, l'ensemble de la documentation (exemple : documentation de développement, de tests, des instructions aux utilisateurs, etc.) était incomplète chez l'ensemble des fournisseurs.

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

Le Tableau-A XXIII-1 présente, pour les différents SVÉ, les constats de l'évaluation de l'atténuation des risques de sécurité (niveau acceptable ou non acceptable) selon les constats généraux de sécurité identifiés lors l'audit de sécurité du projet DGÉQ 2006. Il présente aussi l'atténuation de ces mêmes risques, via des éléments intégrés au modèle SA.

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
3.1.1	**Les processus**									
3.1.1.1	**Les rôles, les responsabilités et les qualifications requises**									
	1. Validation des rôles, des responsabilités et des qualifications requises de tous les intervenants (incluant le fournisseur) devant interagir avec le système	CG1, CG2	Réalisation	Non	Non	Non	Non	Non	Oui	Oui
	a. Équipe de projet		Réalisation	Non	Non	Non	Non	Non	Oui	Oui
	b. Équipe de support et de formation	CG3	Opération	Non	Non	Non	Non	Non	Oui	Oui
	c. Personnel électoral		Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
3.1.1.2	**Les processus touchés par l'introduction d'un système de votation électronique** • Aucun fournisseur n'a fourni des preuves que des validations formelles des mesures de sécurité mises en place aient été réalisées	CG4	Opération	Non	Non	Non	Non	Oui	Oui	Oui
	• Aucun fournisseur n'a remis de document nous prouvant que l'impact de l'adaptation des divers processus inclus dans le processus de votation traditionnel a été analysé, de manière à permettre la distribution, le stockage et l'utilisation sécuritaire de leur système de votation électronique	CG5	Opération	Non	Non	Non	Non	Non	Oui	Oui
	• Aucun fournisseur n'a remis de document nous prouvant que des mesures ont été mises en place pour limiter l'accès au matériel de votation aux seules personnes autorisées	CG6	Opération	Non	Non	Non	Non	Non	Oui	Oui
	1. Validation du processus d'authentification de l'électeur.	CG7	Opération	Non applicable	Non applicable	Non applicable	Non applicable	Non applicable	Oui	Oui
	2. Validation du processus de votation.		Opération	Partielle	Partielle	Partielle	Partielle	Partielle	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
	3. Identification des processus de réception, de stockage, de validation et d'intégrité des votes.		Opération	Non	Non	Non	Non	Oui	Oui	Oui
	4. Validation des processus de fin d'une séance de vote et de fermeture du scrutin (BVO).		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**									
	1. Validation du diagramme et des spécifications physiques de l'endroit de votation		Opération	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	2. Vérification des mesures prouvant que l'aménagement des lieux assure la confidentialité du vote		Opération	Non	Non	Non	Non	Non	Oui	Oui
	3. Vérification des mesures prouvant que le système et l'aménagement utilisé assurent aux clientèles particulières		Opération	Oui	Oui	Oui	Oui	Oui	Oui	Oui
3.1.2.2	**Les spécifications techniques et électriques**									
	1. Validation des spécifications techniques et électriques de l'endroit de votation		Opération	Partielle	Partielle	Partielle	Partielle	Partielle	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
	2. Vérification des mesures prouvant que le lieu permet l'utilisation adéquate du système de votation		Opération	Non	Non	Non	Non	Non	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.**									
	1. Vérification que la documentation du système comprend une section décrivant les objectifs, la portée, les limitations, les fonctionnalités et les interfaces du système	CG8	Réalisation	Non	Non	Non	Non	Non	Oui	Oui
	2. Validation de l'infrastructure technologique utilisée incluant, notamment, les composants essentiels (matériel et logiciel) ainsi que l'infrastructure de télécommunication	CG8	Opération	Non	Non	Non	Non	Non	Oui	Oui
	3. Validation de la qualité de service ciblée		Opération	Non	Non	Non	Non	Non	Oui	Oui
	4. Traitement des erreurs		Opération	Non	Non	Non	Non	Non	Oui	Oui
	5. Validation du processus concernant le soutien technique du système de votation		Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
	6. Validation des mesures limitant les accès au système de votation (intrusion, lien non autorisé, etc.)		Opération	Non	Non	Non	Non	Non	Oui	Oui
	7. Validation du processus d'installation et d'initialisation du système de votation		Opération	Non	Non	Non	Non	Non	Oui	Oui
	8. Vérification des mesures prouvant la disponibilité fonctionnelle du système		Opération	Non	Non	Non	Non	Oui	Oui	Oui
	9. Validation des éléments de configuration et des processus de gestion de la configuration		Opération	Non	Non	Non	Non	Oui	Oui	Oui
	10. Validation du processus de vérification du système et de ses applications		Opération	Non	Non	Non	Non	Non	Oui	Oui
	11. Vérification des moyens offerts à l'utilisateur permettant de constater facilement le bon fonctionnement du système		Opération	Non	Non	Non	Non	Non	Oui	Oui
	12. Validation des plans, des composants de relève et de réaction aux incidents		Opération	Oui	Non	Non	Non	Oui	Oui	Oui
	13. Validation des plans de récupération du système		Opération	Non	Non	Non	Non	Non	Oui	Oui
	14. Validation des processus d'archivage		Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
	15. Validation du processus de désinstallation et de destruction des données du système de votation		Opération	Non	Non	Non	Non	Non	Oui	Oui
	16. Validation des infrastructures de réception des résultats n'assure la protection des données		Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.3.2	**Le logiciel utilisé par le système de votation**									
	1. Validation de la couverture des risques et des mécanismes de sécurité identifiés	CG9	Opération	Non	Non	Non	Non	Non	Oui	Oui
	2. Vérification que le code source du système ne contient pas d'erreur : valider l'existence, la couverture et les résultats de tests unitaires, fonctionnels et intégrés du système de votation	CG10	Réalisation	Non	Non	Non	Non	Non	Oui	Oui
	3. Vérification qu'une revue de code a été effectuée et qu'aucun code malicieux n'a été détecté	CG10	Réalisation	Non	Non	Non	Non	Non	Oui	Oui
	4. Vérification des mesures prouvant que le code vérifié est bien celui qui est exécuté par le système de votation	CG10	Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
3.1.3.3	**Le bulletin de vote (papier ou électronique)**									
	1. Vérification des mesures assurant la distribution et la disponibilité du bulletin de vote, papier ou électronique	CG11	Opération	Non	Non	Non	Non	Oui	Oui	Oui
	2. Vérification des mesures prouvant l'intégrité du 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**									
	1. Vérification des mesures prouvant la provenance d'un dépôt des votes	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	2. Validation de la protection du dépôt des votes durant la période de votation	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	3. Vérification des mesures prouvant qu'une personne ne peut voter plusieurs fois.	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	4. Vérification des mesures prouvant la sauvegarde et l'intégrité d'un dépôt des votes conservés dans les appareils de votation et les urnes	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
	5. Vérification des mesures prouvant la disponibilité et l'intégrité des votes conservés dans un dépôt des votes	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	6. Validation des processus de transmission des votes ou des résultats du dépouillement des votes	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	7. Vérification des mesures prouvant la destruction des données des appareils de votation utilisés au terme du processus électoral	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	8. Vérification des mesures prouvant que personne ne peut ajouter frauduleusement un vote	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui
	9. Vérification des mesures prouvant que personne ne peut retirer un vote	CG12	Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
3.1.4.2	**L'intégrité du résultat du dépouillement des votes** 1. Vérification des mesures prouvant : l'intégrité des données affichées, l'intégrité des données calculées, l'intégrité des données imprimées et l'intégrité des données conservées dans le dépôt des votes	CG13	Opération	Non	Non	Non	Non	Non	Oui	Oui
	2. Vérification des mesures prouvant l'intégrité des résultats.	CG13	Opération	Non	Non	Non	Non	Non	Oui	Oui
	3. Vérification des mesures prouvant la possibilité d'un processus de recomptage judiciaire approuvé	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** 1. Vérification des mesures permettant d'identifier les votes réalisés : en situation normale; en situation de réaction à un incident; en tout temps	CG14	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.5.2	**Le choix de l'électeur** 1. Valider que le vote de l'électeur est bien sauvegardé	CG15	Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
	2. Vérification des mesures confirmant à l'électeur la prise en compte de son vote : message de confirmation clair, exprimé à l'électeur; message clair d'erreur si l'opération a échoué; la documentation comprend une procédure de vérification du vote d'un électeur	CG15	Opération	Non	Non	Non	Non	Non	Oui	Oui
	3. Valider la concordance entre le choix exprimé de l'électeur sur son vote et conservé dans le dépôt des votes	CG15	Opération	Non	Non	Non	Non	Non	Oui	Oui
	4. Valider l'intégrité du vote imprimé, lorsqu'imprimé	CG15	Opération	Non	Non	Non	Non	Non	Oui	Oui
3.1.5.3	**La protection d'un vote**									
	1. Vérification des mesures prouvant l'intégrité du vote, soit que personne ne peut modifier un vote dans le système, sans laisser de trace	CG17	Opération	Non	Non	Non	Non	Non	Oui	Oui
	2. Vérification des mesures prouvant le secret du vote	CG16	Opération	Non	Non	Non	Non	Non	Oui	Oui
	3. Vérification des mesures prouvant la disponibilité de l'ensemble des votes originaux	CG17	Opération	Non	Non	Non	Non	Non	Oui	Oui

Tableau-A XXIII-1 Atténuation des risques de sécurité identifiés par les constats généraux de l'audit de sécurité du projet DGÉQ 2006 (suite)

				Risques de sécurité atténués à un niveau acceptable						
				Tabulatrice			Terminal de votation			Inclus dans le
#	**Titre de la section du rapport**	**Constats Généraux #**	Env.	**Accu-Vote ES 2000**	**Perfas-Tab**	**Perfas-Tab 2 (DVS)**	**Perfas-MV**	**Votex**	**SVI d'ÉC**	**Modèle SA**
3.1.6	**Conclusion des constats généraux**									
	1. Évaluaton du niveau de confiance envers le SVÉ	CG18	Réalisation & opération	Faible	Faible	Faible	Faible	Faible	Équivalent à l'actuel	Oui[62]

[62] L'évaluation du niveau de confiance envers le SVÉ sera possible.

ANNEXE XXIV

ARTICLE PUBLIÉ PAR LE CHERCHEUR

Revue : GÉNIE LOGICIEL / INGÉNIERIE SYSTÈME – SEPTEMBRE 2010, NO 110
LE MAGAZINE DE L'INGÉNIERIE DU LOGICIEL ET DES SYSTÈMES

ISSN : 1265-1397

GÉNIE LOGICIEL / INGÉNIERIE SYSTÈME – SEPTEMBRE 2010, N^{O} 110
LE MAGAZINE DE L'INGÉNIERIE DU LOGICIEL ET DES SYSTÈMES

L'évolution du modèle de la sécurité des applications

Le modèle SA 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
Luc.Poulin@Cogentas.ca

[b] Département de génie logiciel et des TI
École de technologie supérieure – Université du Québec
1100, rue Notre-Dame Ouest,
Montréal (Québec) Canada
Alain.Abran@ets-mtl.ca, Alain.April@ets-mtl.ca

Résumé

Bien que nombre 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 reproductibles, 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, ainsi que de 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

1 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 contrôles.

Bien que nombre de processus, de méthodes et d'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 a 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 apportées 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 de 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 écoulées 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 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 sécurité des applications.

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.

Ce qui suit 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.

2 LES FONDEMENTS DE SÉCURITÉ DES APPLICATIONS

2-1 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.

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

2-2 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 celle publiée, tout en ayant la même portée.*
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'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.*
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.*
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.*
Information sensible	information qui, par décision d'une autorité compétente, doit être protégée car sa divulgation, sa modification, sa destruction non autorisées ou sa perte, provoquerait un dommage notable aux biens ou aux personnes [9].
Niveau de confiance (NdC)	Étiquette identifiant une liste de CSA *NOTE : Le niveau de confiance dans la sécurité d'une application est considéré atteint lorsque les CSA identifiés par une liste ont tous été mis en place et ont été vérifiés.*
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.
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.
Sécurité d'une application (SA)	Protéger les informations impliquées par l'utilisation d'une application. *NOTE : Ce terme n'est pas défini dans le modèle SA initial. La protection des informations sensibles impliquées par l'utilisation d'une application est l'objectif de sécurité ultime d'une organisation pour une application.*

2-3 Principes

Toutes les applications acquièrent, traitent, communiquent ou conservent de l'information. Parmi cette information, certains éléments ou groupes d'information sont plus sensibles que d'autres. La sécurité d'une application entend la mise en place des contrôles de sécurité permettant de diminuer les risques que ces informations sensibles soient compromissent.

Le modèle SA repose sur les principes suivants :

1- La sécurité d'une application doit être gérée

La sécurité des applications 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 :

Le contexte d'affaires : Ce contexte 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 quartier 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 cette dernière dispose.

Le contexte juridique : Une application utilisée dans une province ou une région de n'importe quel 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 réglementaire et non pas le contexte juridique. Il apparaît aujourd'hui plus pratique de regrouper dans ce contexte l'identification des lois et règlements en vigueur dans 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.

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 ces derniers utilisaient tous 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'elles déclareront qu'une application est sécuritaire, que ce soit une personne ou une organisation, elles devront être en mesure de fournir des preuves tangibles et reproductibles qui soutiendront ses déclarations.

2-4 Concepts

2.4.1 Environnement de l'application

La Figure 1 illustre le fait 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.

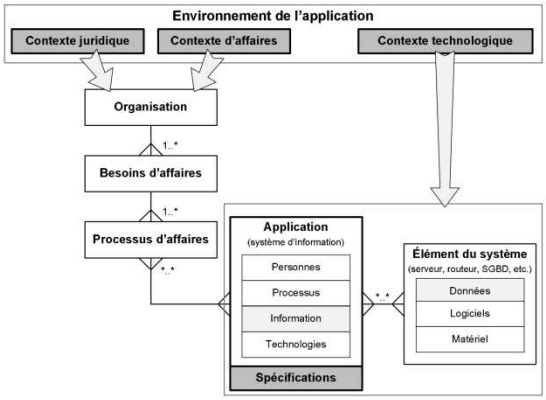


Figure 1 : L'environnement de l'application

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, exécuter 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.

2.4.2 Portée de la sécurité d'une application

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

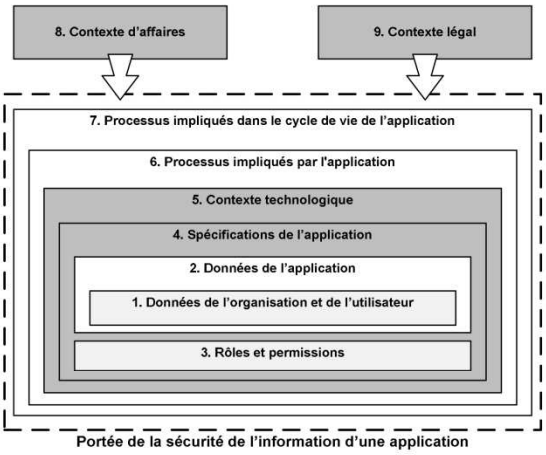


Figure 2 : Portée de la sécurité de l'information d'une application *(traduit et adapté d'ISO 27034)*[2]

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 son 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.

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.

2.4.3 Quatre secteurs d'intervention en sécurité d'applications

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 suivre et de maintenir tous les composants de l'infrastructure TI, incluant les environnements de développement, de test et d'exploitation.

3- L'équipe de développement, qui a besoin d'utiliser des outils pour développer, corriger, maintenir et assister 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 sécurité d'applications doivent être satisfaits par le modèle SA.

[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 recherche.

2.4.4 Source des risques de la sécurité des applications

Les sources des risques relatifs à la sécurité d'une application sont multiples. Les risques 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 altérés 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 attaquée via l'Internet.

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

2.4.5 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.

La protection d'une application est principalement assurée par la mise en place de CSA, soit dans l'application elle-même, soit dans les processus impliqués par cette dernière. Les techniques qui seront utilisées pour diminuer les risques ciblés par ces CSA dépendront du contexte ou ces risques existent et de la stratégie adoptée pour les ramener à un niveau acceptable.

Une organisation qui développe des applications pourra notamment intégrer des CSA dans ses processus existants de développement, de déploiement et de test sans avoir à changer complètement ses façons de faire. De la même manière, une organisation qui a acquis une application pourra de son côté intégrer des CSA dans ses processus de gestion, de support, de contingence ou d'archivage. 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 assigné à son application, ont été mis en œuvre, ont été vérifiés et qu'ils fonctionnent tous tel que prévu.

3 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.

3.1 Les composants du modèle SA

Cette section présente les six composants clés du modèle SA.

3.1.1 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. Ce modèle 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.

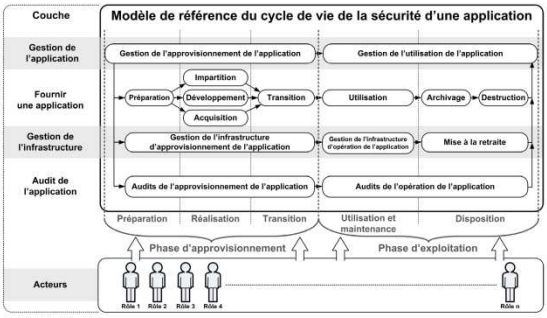


Figure 3 : Représentation simplifiée du modèle de référence du cycle de vie de la SA
(traduit et adapté d'ISO 27034)

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.

3.1.2 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).

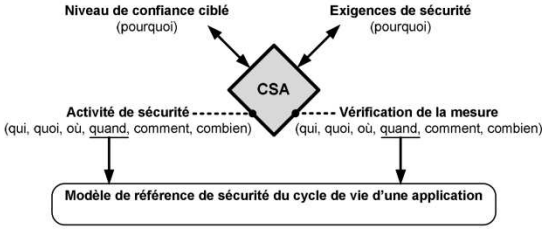


Figure 4 : Le contrôle de la sécurité des applications
(traduit et adapté d'ISO 27034)

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

3.1.3 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.

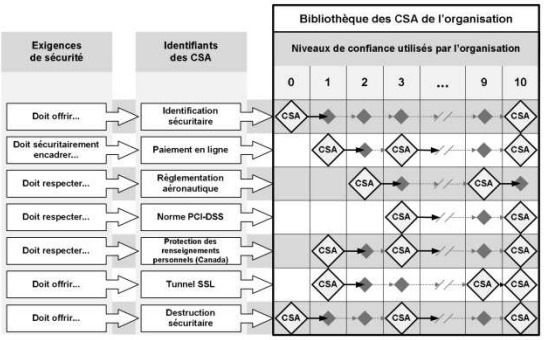


Figure 5 : La bibliothèque CSA
(traduit et adapté d'ISO 27034)

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. Chaque losange du tableau représente un CSA. Un losange grisé représente la répétition du CSA de la colonne précédente à ce niveau.

La sélection d'un niveau de confiance par une organisation, soit la liste de CSA à mettre en œuvre, prend notamment en compte leurs coûts d'implémentation et de vérification en regard de 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 » requises par une application ainsi que les « Identifiants des CSA » associés à celles-ci. Les deux éléments d'information retirés de cette figure, qui de fait représentaient les sources des risques relatifs à la sécurité pouvant menacer une application, ont été inclus dans un nouveau composant du modèle : la matrice de traçabilité de la SA de l'organisation.

3.1.4 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 à tout changement de risques de SA les concernant. Ces changements au niveau des risques de sécurité viendront inévitablement des contextes d'affaires, juridique ou technologique.

La Figure 6 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.

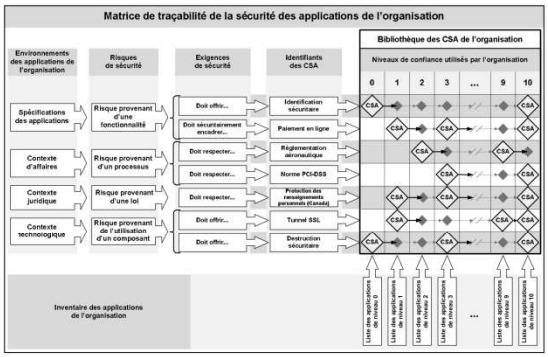


Figure 6 : Matrice de traçabilité de la SA de l'organisation

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 à été assigné un niveau de confiance de la bibliothèque des CSA.

3.1.5 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.

3.1.6 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.

3.2 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.

3.2.1 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.

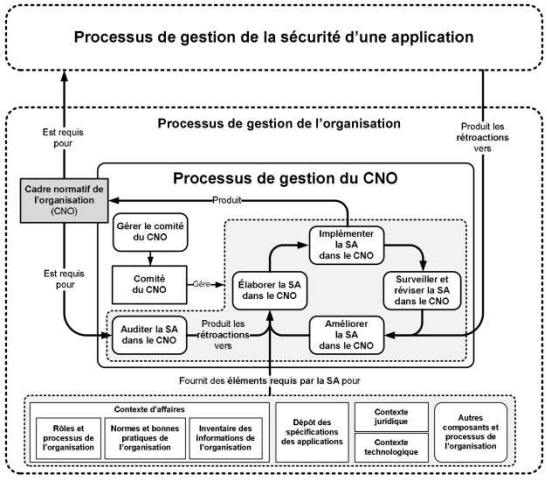


Figure 7 : Le processus de gestion du CNO
(traduit et adapté d'ISO 27034)

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 – qui décrit les activités qui devraient être mis en place pour gérer la nomination, l'allocation des ressources et les objectifs de ce comité.
2. élaborer la SA dans le CNO – qui décrit les activités permettant d'identifier et de valider la cible de SA dans le respect des ressources alloués par l'organisation, soit les priorités, les stratégies et les éléments qui devront être mis en place dans le CNO ;
3. implémenter la SA dans le CNO – qui décrit les activités permettant la mise en place, la vérification et la communication des éléments de l'ONF identifié par l'organisation ;
4. surveiller et réviser la SA dans le CNO – qui décrit les activités permettant d'examiner et d'ajuster les composants et processus du CNO afin de s'assurer qu'ils diminuent toujours adéquatement les risques pour lesquels ils ont été conçus et mis en place, et qu'ils sont utilisés en conformité avec la politique de la SA de l'organisation ;
5. améliorer la SA dans le CNO – qui décrit les activités permettant l'ajout, le maintien et l'amélioration de tous les éléments du CNO, en réalisant une revue périodique des différents contextes de l'organisation, des rôles et des responsabilités de ses divers intervenants, ainsi que des processus et des technologies utilisés par les applications de l'organisation; et
6. auditer la SA dans le CNO – qui décrit les activités permettant de vérifier et d'auditer le CNO pour en valider la conformité avec les objectifs et éléments de sécurité ciblés par l'organisation.

NOTE : La représentation du processus de gestion du CNO donnée 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.

3.2.2 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.** Qui consiste à préciser les trois contextes où évoluera l'application, ses principales spécifications, ses acteurs et processus, ainsi que les groupes d'informations impliqués par son acquisition et son utilisation.
2. **Évaluer les risques de sécurité amenés par l'application**, et déterminer le niveau de confiance nécessaire pour cette application. Qui consiste à identifier pour une application un niveau de confiance cible en fonction des risques de sécurité qui s'y rattache. L'identification de ces risques se fera notamment en suivant les flots d'information jugé sensible à l'intérieur de l'application afin d'identifier les éléments à protéger et de définir les exigences de SA requis pour diminuer les risques de sécurité concernant ces composants, ces processus ou ces acteurs.
3. **Créer et maintenir le cadre normatif de l'application.** Qui consiste à consolider dans le CNA les documents et les rapports produits lors des deux étapes précédentes du PGSA, avec les éléments extrait du CNO qui sont requis pour mettre en place le niveau de confiance ciblé, approuvé par le détenteur.
4. **Réaliser et exploiter l'application.** Qui consiste notamment à utiliser tous les CSA qui ont été importés dans le CNA et à les intégrer aux activités du cycle de vie de l'application.
5. **Vérifier la sécurité de l'application.** Qui consiste à réaliser les activités de vérification de mesures des CSA qui doivent être mis en place dans l'application. Les résultats produits par ces activités permettent de fournir les preuves vérifiables que les CSA devant être en place au moment de la vérification ont bien été implémentés et qu'ils fonctionnent tous, tel que prévu.

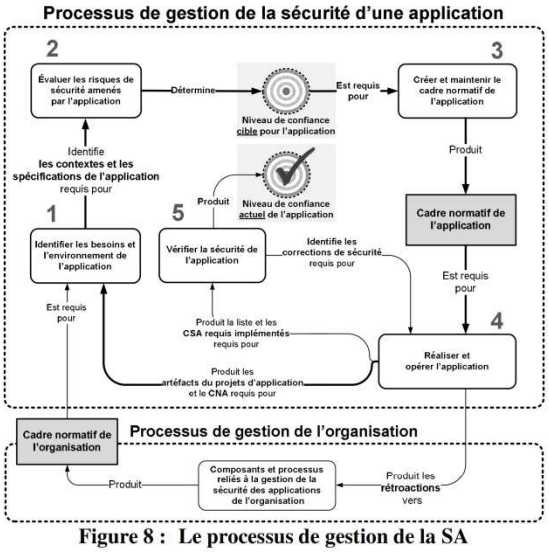


Figure 8 : Le processus de gestion de la SA
(traduit et adapté d'ISO 27034)

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 été légèrement 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 ».

4 CONCLUSION

Peu d'approches et de modèles permettent de déclarer une application sécuritaire et d'appuyer cette déclaration sur 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 répondre 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 comme 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 facilitée par l'ajout, dans le modèle SA, de la matrice de traçabilité de la SA de l'organisation.

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 consulter 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.

[9] ISO/IEC, Information technology - Vocabulary - Part 8: Security. 1998, ISO/IEC: Genève, Suisse. p. 38.