UNIVERSITÉ DU QUÉBEC À MONTRÉAL

ÉVALUATION DE L'APPLICATION DES ACTIVITÉS DE SÉCURITÉ, PROPOSÉES PAR LES MÉTHODES DE GESTION DES RISQUES DE SÉCURITÉ POUR LES SYSTÈMES D'INFORMATION, DANS UN CONTEXTE DE CYCLE DE DÉVELOPPEMENT DU LOGICIEL

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN INFORMATIQUE

PAR

PATRICK MAROIS

DÉCEMBRE 2009

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

ASD	Adaptive software development
AUP	Agile Unified Process
BUP	Basic Unified Process
CEI	Commission électrotechnique internationale
CERT	Computer Emergency Response Team
CLASP	Comprehensive, Lightweight Application Security Process
CLUSIF	Club de la sécurité de l'information français
DCSSI	Direction centrale de la sécurité des systèmes d'information
DIC	Disponibilité, intégrité et confidentialité
DREAD	Damage potential, Reproducibility, Exploitability, Affected users, Discoverability
DSDM	Dynamic systems development method
EBIOS	Expression des Besoins et Identification des objectifs de sécurité
EssUP	Essential Unified Process
EUP	Enterprise Unified Process
FDD	Feature driven development
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
MARION	Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux
MEHARI	Méthode Harmonisée d'Analyse des Risques
MELISA	Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information
RAD	Rapid Application Development

RUP	Rational Unified Process
SEI	Software Engineering Institute
SDL	Security Development Lifecycle
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege
OCTAVE	The Operationally Critical Threat, Asset, and Vulnerability Evaluation
OpenUP	Open Unified Process
OWASP	The Open Web Application Security Project
PCI-DSS	Payment Card Industry Data Security Standard
TSP-SECURE	Team Software Process for Secure Software Development
XP	Extreme programming

LE RÉSUMÉ

Ce mémoire concerne la sécurité informatique appliquée dans le domaine du logiciel informatique. En fait, il s'agit de l'intégration des concepts de la gestion des risques de sécurité pour les systèmes d'information dans un contexte du cycle de développement du logiciel. Après la présentation générale de ces sujets, la recherche aborde la problématique de la présence des vulnérabilités de sécurité dans les logiciels mis en opération. La solution proposée pour restreindre leur présence est fondée sur l'hypothèse qu'il est possible d'intégrer des activités reliées à la gestion des risques de sécurité aux étapes du cycle de développement du logiciel afin que ses bénéfices permettent de diminuer la présence de vulnérabilités de sécurité dans les logiciels produits.

La recherche présentée dans ce mémoire prend ses appuis sur des concepts éprouvés dans les différents domaines étudiés. Le *Processus Unifié* est utilisé à titre de référence pour le cycle de développement du logiciel, tandis que les méthodes *EBIOS*, *MEHARI* et *OCTAVE* ont été employées pour la gestion des risques de sécurité.

La démarche analytique entreprise dans cette recherche commence d'abord par l'étude des méthodes de gestion des risques pour en extraire une liste généralisée d'activités de sécurité. Elle présente ensuite des détails sur les activités effectuées dans chacune des étapes du *Processus Unifié*. En dernier lieu, elle intègre une à une les activités générales de la gestion des risques dans les étapes du cycle de développement logiciel. Les résultats ont démontré qu'un petit nombre d'activités générales de la gestion des risques avait un lien direct avec le cycle de développement du logiciel, alors que les autres pouvaient être intégrées et réalisées en fonction de leurs interdépendances avec les activités concernées.

En démontrant que certaines activités avaient un ancrage réel avec une activité de projet réalisée lors d'une étape du cycle de développement logiciel, et qu'il existe de fortes interdépendances entre les activités de gestion des risques, il est alors possible de croire que les activités de gestion des risques peuvent être réalisées conjointement aux activités de projet dans un cycle de développement du logiciel. Puisque la gestion des risques de sécurité vise à diminuer les vulnérabilités de sécurité et qu'elle se retrouve ainsi intégrée au développement logiciel, l'hypothèse fut confirmée.

Mots clés : méthode de gestion des risques de sécurité, sécurité des systèmes d'information, cycle de développement du logiciel, sécurité informatique, vulnérabilités de sécurité dans les logiciels, EBIOS, MEHARI, OCTAVE, Processus Unifié.

INTRODUCTION

Élaborés pour répondre à une multitude de nos besoins, les logiciels informatiques sont aujourd'hui des outils nécessaires à notre style de vie. Le domaine du logiciel a pris tout un essor durant les dernières années au même titre que les technologies en général. Dans une société de plus en plus informatisée et ouverte sur le monde, les logiciels utilisés sont exposés à toutes sortes de situations parfois bonnes, parfois mauvaises. Afin d'éviter des événements malencontreux, le domaine de la sécurité informatique progresse et tente de suivre le rythme effréné de leur évolution technologique. La nécessité d'une plus grande présence de la sécurité informatique dans le domaine du logiciel est d'actualité et constitue l'élément motivateur de la présente recherche.

Dans un contexte se rapprochant plus particulièrement à celui des entreprises, quels sont les enjeux d'utiliser des logiciels dont la sécurité informatique est inadéquate ? Les logiciels utilisés jouent-ils un rôle important dans les processus d'affaires de l'entreprise ? Les informations manipulées par les logiciels sont-elles confidentielles ? Servent-elles à prendre des décisions importantes ? Les réponses à toutes ces questions sont probablement affirmatives. Toutefois, il faut également se demander si les actions nécessaires pour assurer la sécurité informatique des logiciels et des données manipulées sont effectuées correctement et si elles répondent aux besoins les plus prioritaires de l'entreprise.

L'importance de la sécurité informatique pour le domaine du logiciel n'est pas un nouveau sujet. Pourtant, la problématique relative à la présence des vulnérabilités de sécurité dans les logiciels en opération est encore bien existante. La présente recherche vise à contribuer à la résolution de cette problématique en présentant une solution dont l'approche principale est la gestion des risques de sécurité. Considérant l'importance de s'attaquer à la source même du problème, la solution prend en charge la sécurité dès le développement même du logiciel. Par l'utilisation de concepts reconnus dans le domaine de la gestion des risques, la solution vise à démontrer leur intégration au cycle de développement du logiciel afin d'en retirer les bénéfices de leur réalisation.

Pour résoudre la problématique énoncée, la solution passe inévitablement par une plus grande considération de la sécurité dans les activités de développement du logiciel. Des projets de recherche et des publications abordent la résolution de cette problématique, mais la situation perdure. Est-ce que les solutions proposées sont inadaptées ou est-ce la problématique qui ne cesse de se complexifier ? Le but de la présente recherche n'est pas de remettre en question les autres efforts prodigués pour solutionner la problématique, mais se veut plutôt complémentaire aux différentes solutions déjà proposées.

L'apport de la présente recherche au domaine du développement logiciel est celui d'amener une solution d'approche face à la problématique énoncée, et ce, en établissant le lien entre des concepts éprouvés du domaine du développement logiciel et ceux de la gestion des risques de sécurité. Depuis une quinzaine d'années, l'expertise du domaine de la gestion des risques de sécurité pour les systèmes d'information, incluant les logiciels, s'est développée et des méthodes structurées sur le sujet ont été élaborées. C'est justement à partir de cette expertise que la recherche se fonde en tentant d'intégrer les bonnes pratiques de la gestion des risques de sécurité à travers les étapes d'un projet de développement logiciel.

Pour ce faire, les sujets importants qui sont à la base de la recherche doivent être présentés pour en faire ressortir leurs caractéristiques respectives. Ensuite, ces mêmes sujets seront mis en relation dans une démarche analytique où une approche déductive sera utilisée pour démontrer qu'il est possible de les réaliser conjointement pour atteindre les objectifs visés par la recherche. Basée sur des sujets dont les concepts sont éprouvés, la recherche vise donc à démontrer leurs bienfaits pour réduire les vulnérabilités de sécurité présentes dans les logiciels mis en opération.

Ce document présente la recherche effectuée et comporte cinq parties principales. Les deux premières parties établissent la mise en contexte des sujets importants. La troisième établit les bases en présentant les caractéristiques de la recherche. La quatrième élabore la réalisation des travaux de la recherche et, finalement, la cinquième partie conclut en produisant le sommaire des résultats obtenus. Brièvement, voici les éléments abordés dans chacun des cinq chapitres de ce document :

Le premier chapitre traite du développement logiciel et de ses liens avec la sécurité informatique.

Le second chapitre concerne la gestion des risques pour la sécurité des systèmes d'information.

Le troisième chapitre dicte les motifs et les caractéristiques de la recherche.

Le quatrième chapitre présente la démarche analytique de la recherche.

Le cinquième chapitre synthétise les résultats obtenus et valide la solution proposée.

CHAPITRE I

QUAND LE DÉVELOPPEMENT LOGICIEL RENCONTRE LA SÉCURITÉ INFORMATIQUE

L'informatique fait maintenant partie intégrante de nos activités quotidiennes. Omniprésente dans les milieux de travail, les domiciles et les endroits publics, elle est utilisée à différentes fins dont la communication, la gestion d'informations et le divertissement personnel. En plus d'être très avantageuse aux endroits où elle permet un rendement plus efficace des tâches à réaliser, l'informatique occupe une place primordiale dans les activités de certains secteurs stratégiques de notre société comme les centres hospitaliers, les agences de transport et les centrales d'énergie pour ne citer que ceux-là.

Derrière toute cette technologie existe un grand nombre de logiciels qui interagissent entre eux afin de satisfaire les besoins des utilisateurs en la matière. Avec l'augmentation de la demande et des besoins toujours plus complexes à traiter, la production de ces logiciels devient par le fait même une activité de création importante à considérer. Le développement d'un logiciel est un projet qui implique plusieurs personnes, comprend diverses étapes à réaliser et comporte de nombreux facteurs pouvant influencer sa réussite. L'un de ces facteurs, devenu nécessaire au courant des dernières années, est celui de la sécurité informatique. Les logiciels sont maintenant devenus une cible de choix pour les attaques informatiques, et ce, en raison des informations convoitées qu'ils manipulent et de leur importance pour le bon fonctionnement de divers services. Pour le développement logiciel, l'application des concepts de la sécurité informatique s'avère donc un sujet d'actualité et d'importance pour le futur des activités de ce domaine.

Le but de ce chapitre consiste à présenter une vue d'ensemble de la situation actuelle en ce qui a trait à la considération de la sécurité informatique dans le contexte de développement logiciel. La première section fait un tour d'horizon des concepts de base du développement logiciel. Quant à la seconde, elle introduit ceux de la sécurité informatique pour ensuite poursuivre plus spécifiquement sur son application dans le domaine du développement logiciel.

Dans l'ensemble de ce document, le rôle de ce chapitre est de contribuer à la mise en place du contexte de la recherche en y présentant des sujets qui seront maintes fois cités dans les chapitres suivants.

1.1 Le développement logiciel

Cette section aborde des notions de base du domaine du développement logiciel qui seront utiles tout au long de la recherche. La première section définit le concept de développement logiciel et y présente sommairement les grandes étapes. Ensuite, la deuxième section traite des modèles de base qui ont été définis dans le but de structurer les activités à réaliser pour produire un logiciel. La troisième et dernière section mentionne des facteurs pouvant influencer la réussite d'un projet de développement logiciel.

1.1.1 Le déroulement d'un projet de développement logiciel

Tout d'abord, il est essentiel de comprendre le sens du terme « développement logiciel » avant de l'aborder concrètement. Celui-ci peut être défini comme étant un processus de création d'un produit logiciel qui sera conçu selon des spécifications établies et par une série d'étapes à réaliser. La mise en œuvre d'une activité de développement logiciel fait référence à plusieurs termes semblables dans la littérature traitant de ce sujet et ils représentent essentiellement les mêmes concepts. Parmi les termes « cycle de vie logiciel », « cycle de développement », « cycle de développement logiciel, « cycle de développement du logiciel », « cycle de développement d'application », « processus de développement » et « conception logicielle », celui qui sera utilisé dans le cadre de ce document est « cycle de développement du logiciel » tel que défini par l'Office québécois de la langue française.

Le cycle de développement du logiciel se divise en plusieurs étapes jouant chacune un rôle bien différent dans le processus de création du logiciel. L'orchestration de ces étapes représente un défi énorme. Les opinions divergent quant à savoir quelles sont exactement les étapes à suivre, comment elles doivent être gérées, quels sont les travaux à réaliser durant chacune d'elles et quelle est l'importance relative des unes par rapport aux autres. Malgré toutes ses interrogations, il est possible d'en identifier les plus communes :

a) **La définition des besoins** permet l'obtention des besoins fonctionnels et non fonctionnels du client;
b) **La conception** permet l'analyse des besoins exprimés et des contraintes identifiées pour les traduire en spécifications logicielles;

c) **L'implémentation** permet la programmation des spécifications logicielles;
d) **L'intégration** permet l'assemblage des travaux de programmation en un logiciel fonctionnel;
e) **La validation** permet la vérification du logiciel à l'égard des besoins exprimés;
f) **La maintenance** permet la modification du logiciel à des fins de correction et d'évolution.

Plusieurs projets de recherche se consacrent précisément sur différentes façons de faire afin de produire des logiciels de qualité, à faibles coûts et dans les meilleurs délais possible. Avec les années, ces travaux ont permis la formalisation de méthodes favorisant ainsi un déroulement structuré et documenté des étapes d'un projet de développement logiciel. La prochaine section présente quelques résultats de ces projets.

1.1.2 Les modèles de cycle de développement du logiciel

En raison d'une demande en pleine croissance pour des logiciels de nature variée, les spécialistes du domaine ont travaillé à rendre le développement logiciel plus efficace en standardisant les activités à réaliser pour accomplir la tâche. Ainsi, des modèles de base ont été établis au fil des années et ont évolué selon les résultats obtenus par leurs utilisations dans des projets réels ou à la suite de nouvelles idées proposées. Cette section en présente quelques-uns des plus connus. Les numéros apparaissant dans les figures indiquent l'ordre chronologique des étapes réalisées dans le modèle en question. Voici ces modèles :

a. **Le modèle en cascade** : Ce modèle est considéré comme étant le tout premier modèle établi. Son approche consiste à effectuer les étapes de développement de manière séquentielle durant un seul et unique cycle. Cela veut dire que les éléments à produire lors d'une étape spécifique doivent être terminés et validés avant que le travail de l'étape suivante puisse débuter. Après des années d'expérimentation, quelques améliorations ont été apportées à ce modèle afin de diminuer sa rigidité et, plus précisément, permettre le retour en arrière afin de rendre possible la modification du travail réalisé dans les étapes précédentes.

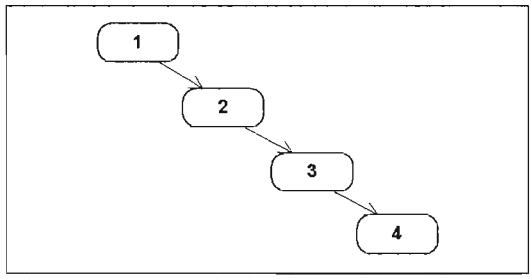

Figure 1.1 Exemple des étapes du modèle en cascade.

b. **Le modèle en V :** Ce modèle est présenté comme une évolution du modèle en cascade. Il se distingue par le fait que pour chacune des étapes de développement à réaliser, une étape de validation des résultats produits devra également être accomplie. Même si ces étapes sont effectuées plus tard dans le cycle, elles sont toutefois définies lors de la réalisation de l'étape de développement qui leur est associée. Une attention particulière est donc portée sur la vérification des résultats attendus suite à la réalisation des étapes de développement.

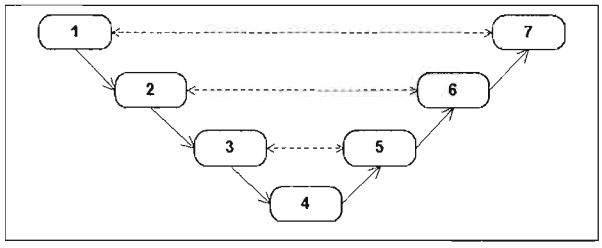

Figure 1.2 Exemple des étapes du modèle en V.

c. **Le modèle en spirale :** Ce modèle met l'accent sur une priorisation des tâches en fonction des résultats obtenus suite à une analyse de risques effectuée à chaque cycle de développement. Cette analyse porte sur les objectifs établis en tout début de cycle et les risques énoncés font référence à différents aspects du projet dont les ressources humaines, l'organisation du travail, les éléments techniques, l'assurance qualité, etc. Un cycle complet est composé de quatre étapes distinctes :

1. Déterminer les objectifs, les alternatives et les contraintes;
2. Analyser les risques et évaluer les alternatives;
3. Développer et vérifier la solution retenue;
4. Revoir les résultats et planifier le cycle suivant.

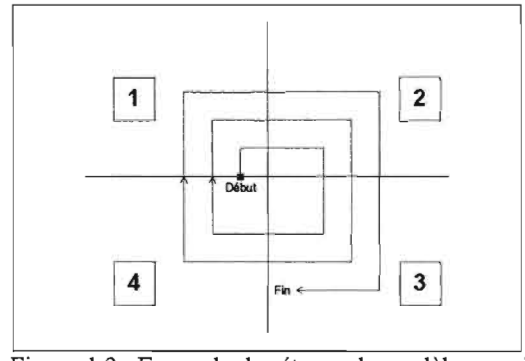

Figure 1.3 Exemple des étapes du modèle en spirale.

Les quatre étapes sont effectuées, cycle après cycle, pour bâtir graduellement la solution désirée. Quant à la gravité des risques identifiés, elle devient de moins en moins importante après chaque cycle réalisé.

d. **Le modèle par incrément :** Ce modèle se caractérise tout d'abord par la réalisation d'une première série d'étapes séquentielles afin de produire les composants logiciels de base qui formeront le noyau du logiciel. Une fois ceux-ci fonctionnels et réunis, les autres composants peuvent alors être développés en parallèle et intégrés au noyau. Le logiciel est alors bâti de manière incrémentale par l'ajout successif de chacun des composants au noyau (incluant les composants de base et les autres composants déjà intégrés). Cette technique favorise le développement du logiciel par parties opérationnelles, ce qui rend disponible une version fonctionnelle du logiciel après chaque ajout d'incrément.

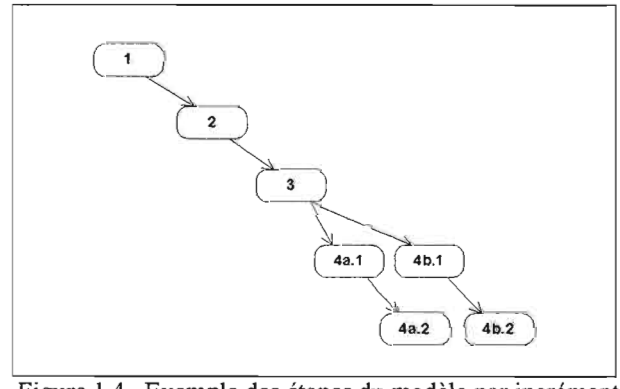

Figure 1.4 Exemple des étapes du modèle par incrément.

e. **Le modèle par itération :** Ce modèle s'apparente à celui en cascade à la différence que le cycle n'est pas effectué qu'une seule fois pour réaliser l'ensemble du travail, mais bien plusieurs fois sur des parties réduites du travail. Pour chacun de ces cycles, les grandes étapes de développement sont exécutées séquentiellement sur la petite portée concernée. Chaque itération résulte d'une partie opérationnelle et contribue ainsi à bâtir graduellement le logiciel. Celui-ci peut alors être soumis régulièrement au client entre deux cycles pour ajuster conséquemment le développement qui reste à faire selon les commentaires obtenus.

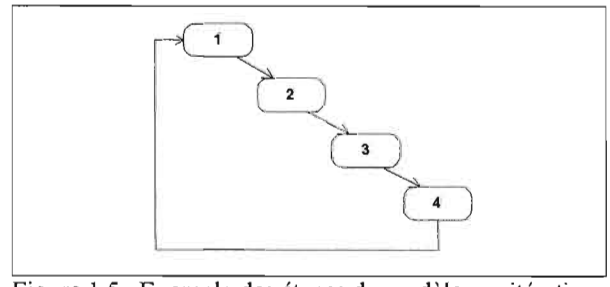

Figure 1.5 Exemple des étapes du modèle par itération.

f. **Les méthodes agiles :** Les méthodes dites « agiles » sont connues plus formellement depuis une dizaine d'années et leur adoption sur le marché ne cesse de s'accroître à en juger par la présence de sites Web et d'offres de formation les concernant. Elles visent à réduire le formalisme du cycle de développement du logiciel de façon à pouvoir s'adapter rapidement à toutes sortes d'éventualités et à produire les logiciels dans les plus courts délais possible. Les concepts prônés dans ces méthodes sont l'interaction élevée entre les personnes impliquées, la diminution de la documentation formelle, l'utilisation du processus par itération, l'ouverture aux changements durant le processus et l'importance des tests continus pour la validation. Basées sur des concepts communs, plusieurs méthodes agiles existent et les plus connues sont les suivantes : Rapid Application Development (RAD), Extreme programming (XP), Scrum, Crystal clear, Adaptive software development (ASD), Dynamic systems development method (DSDM) et Feature driven development (FDD).

Par surcroît, il existe différentes variantes de ces modèles de base et d'autres types d'approches possibles, mais en dresser la liste complète nécessiterait un travail énorme. De plus, ils sont souvent adaptés par les entreprises afin de répondre plus précisément à leurs besoins et leurs

façons de faire pour développer des logiciels. Pour la présente recherche, il s'agit plutôt de démontrer l'existence de façons de faire définies et structurées pour le domaine du développement logiciel.

Malgré la disponibilité de ces modèles, le constat actuel démontre qu'il est encore répandu de faire fi d'un modèle structuré pour développer des logiciels. En conséquence, il est difficile de répondre adéquatement à la complexité des besoins qui sont formulés aujourd'hui. Cette complexité n'est pas étrangère au fait que plusieurs facteurs peuvent influencer la réalisation des activités durant un projet de développement logiciel. Sans l'utilisation d'une certaine démarche structurée, il est plus ardu de gérer adéquatement ces différents facteurs.

1.1.3 Les facteurs influençant un projet de développement logiciel

Un projet de développement logiciel n'est pas simple à gérer dû au fait que plusieurs décisions, qui influenceront le résultat final, doivent être prises tout au long du processus. Les modèles présentés dans la section précédente offrent des solutions pour structurer les activités à réaliser et pour aider à la prise de décisions. Parmi celles-ci, certaines sont largement influencées par des facteurs, prévisibles ou non, qui peuvent s'avérer un gage de succès ou d'échec pour le projet. Il y a notamment le niveau de qualité et de finition attendu, les délais et les coûts de production, la disponibilité des ressources matérielles et humaines, l'expertise des intervenants dans le projet, la complexité du sujet traité, la performance informatique, la complexité et l'évolution des technologies utilisées, la sécurité informatique, la valeur des informations traitées, les changements apportés aux spécifications durant le projet, etc.

Ces exemples démontrent à quel point le processus de développement logiciel est complexe à gérer et qu'il est essentiel qu'il puisse s'adapter facilement à toutes sortes de situations pour éviter de mettre en péril les objectifs du projet. Parmi les facteurs énumérés, l'attention sera maintenant portée sur l'un d'entre eux : la sécurité informatique. Tout comme le concept de développement logiciel, la sécurité informatique est un sujet important dans le contexte de la présente recherche et sera présentée plus en détail dans la prochaine section.

1.2 La sécurité informatique

Cette section introduit le domaine de la sécurité informatique pour en comprendre globalement sa raison d'être et ses implications dans le cadre d'un projet de développement logiciel. La première section traite de la sécurité informatique dans son ensemble afin de comprendre en quoi elle est nécessaire dans les différents domaines de l'informatique. La seconde section aborde, quant à

elle, des points justifiant la pertinence de la sécurité informatique dans le domaine du développement logiciel en présentant ses objectifs, son importance et, sommairement, quelques projets de recherche en cours à ce sujet. L'objectif visé est de démontrer que la sécurité informatique s'applique dans plusieurs domaines de l'informatique dont celui du développement logiciel.

1.2.1 La sécurité informatique en bref

L'Office québécois de la langue française définit la sécurité informatique comme étant un « ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service ». Dans cette définition, les objectifs de la sécurité informatique sont clairement établis, mais pourquoi protéger nos biens informatiques, la confidentialité des données et la continuité de service ? Comme mentionné en tout début de chapitre, l'informatique est devenue un élément important dans notre société. Dans un contexte d'entreprise, le terme « important » s'apparente énormément à celui de « valeur ». La sécurité informatique vise donc à protéger les éléments de valeur contre d'éventuels incidents qui pourraient mettre en péril les processus d'affaires de l'entreprise. Que l'incident soit le résultat d'une attaque planifiée ou d'une erreur involontaire, des mesures de sécurité doivent être mises en œuvre pour tenter d'éviter que cela se produise. Qu'il s'agisse de la manière dont les accès physiques et logiques aux équipements informatiques sont contrôlés, du chiffrement des communications sur le réseau informatique ou de la sensibilisation auprès des utilisateurs sur la confidentialité des informations manipulées avec les logiciels, ces mesures sont toutes liées à la sécurité informatique et doivent être conséquentes aux besoins de l'entreprise en la matière. Du fait que chaque domaine de l'informatique peut nécessiter des mesures de sécurité bien différentes, l'attention sera maintenant portée plus spécifiquement sur celui du développement logiciel.

1.2.2 La sécurité pour le domaine du développement logiciel

Par le passé, moins d'importance était attribuée à la sécurité informatique de sorte que cette situation s'est également reflétée dans les différents modèles de cycle de développement du logiciel proposés par les spécialistes. L'adoption de plus en plus forte de ces modèles explique en partie les difficultés actuelles à changer les façons de faire afin que la sécurité informatique soit prise en charge convenablement dans les projets de développement logiciel. Toutefois, les personnes provenant de différents corps de métier et ayant un intérêt pour le sujet ont commencé à réaliser l'importance de ce facteur. Suite à cela, les spécialistes ont donc commencé à chercher des solutions possibles à ces difficultés rencontrées.

Dans le domaine du développement logiciel, la sécurité informatique se traduit par la prise en compte des besoins de sécurité durant la conception même du logiciel pour éviter que celui-ci contienne des vulnérabilités de cette nature une fois mis en opération. Les besoins de sécurité peuvent être très variables pour chacun des logiciels, car ils dépendent énormément de son contexte d'utilisation, de la nature des données traitées et de son exposition à des menaces potentielles. Pour en revenir à la définition de la sécurité informatique, un logiciel sécuritaire est un logiciel qui est en mesure de se protéger contre une utilisation malveillante de lui-même, de protéger les informations qu'il manipule et d'assurer qu'il est disponible en temps et lieu pour supporter le processus d'affaires pour lequel il est utilisé. L'expression des besoins de sécurité sera abordée plus en détail dans le deuxième chapitre de ce document.

1.2.3 L'importance de la sécurité pour le domaine du développement logiciel

Comme abordé précédemment, les entreprises doivent mettre les efforts nécessaires pour sécuriser les logiciels qu'ils produisent et utilisent, puisqu'ils représentent des outils de valeur pour le bon fonctionnement de leurs processus d'affaires. Subir les désagréments d'un incident de sécurité informatique sur un logiciel peut engendrer plusieurs problèmes et, du même coup, provoquer une série de conséquences ayant des degrés d'importance bien différents. À titre d'exemples, une telle situation peut occasionner une perte de confiance envers les personnes utilisant le logiciel, une dégradation de l'image de l'entreprise, une perte d'informations stratégiques ou une indisponibilité du logiciel à un moment inopportun pour ne nommer que ceux-là.

Que ces logiciels soient développés par une équipe interne à l'entreprise ou par un producteur externe, les utilisateurs ont de bonnes raisons d'exiger des logiciels sécuritaires avec tous les enjeux actuels entourant la sécurité informatique. Les exigences reliées à celle-ci sont maintenant plus élevées et ne proviennent pas uniquement des clients. Les domaines de l'informatique sont aujourd'hui assujettis à se conformer à certains standards et diverses législations pour certains secteurs d'activités comme la santé et les finances (norme PCI-DSS, loi C-198, loi sur la protection des renseignements personnels, etc.). La prise en compte de ces incitatifs externes et la sécurité comme facteur de qualité d'un logiciel démontrent rapidement des bénéfices concrets de l'intégration de la sécurité dans le développement logiciel.

1.2.4 Les difficultés à intégrer la sécurité dans le développement logiciel

Après avoir élaboré sur son importance, qu'en est-il de la faisabilité à conjuguer ensemble ces deux domaines ? Malheureusement, des difficultés surviennent lorsqu'il est temps de bien vouloir

considérer la sécurité informatique durant le développement logiciel. L'une des plus importantes vient du fait que les actions effectuées durant un projet de développement logiciel le sont sur une cible mouvante. Des imprévus peuvent survenir durant le projet et nécessiter le changement des objectifs, des intervenants, des technologies utilisées, etc. Parmi ces imprévus, certains affectent directement les mesures mises en place pour assurer la sécurité informatique. Voici quelques-unes des difficultés possibles :

- **La sensibilisation** : les intervenants du projet de développement logiciel doivent être sensibilisés à l'importance de la sécurité pour être en mesure de contribuer adéquatement à son application.
- **Une démarche encore plus complexe à réaliser** : l'application d'une démarche structurée pour le développement logiciel est complexe en soi et l'intégration de nouveaux concepts de sécurité informatique amplifie cette situation.
- **L'évolution constante des technologiques** : les technologies matérielles et logicielles utilisées pour concevoir et faire fonctionner les logiciels continuent à évoluer. Cette réalité inclut également les technologies utilisées pour commettre des attaques informatiques sur les logiciels. Du fait de cette constante évolution, certains besoins de sécurité peuvent ne pas avoir été prévus et, ainsi, provoquer la présence de vulnérabilités de sécurité dans le logiciel.
- **Le niveau de connaissance en sécurité informatique** : les intervenants du projet de développement logiciel doivent avoir une connaissance suffisante de la sécurité informatique selon leurs rôles et leurs responsabilités.
- **Le changement des besoins du client** : les spécifications logicielles, qui nécessitent peut-être des besoins bien précis en matière de sécurité informatique, peuvent devoir être modifiées durant le projet.
- **Le caractère unique de chaque logiciel** : malgré l'existence de modèles de base pour uniformiser les activités du cycle de développement du logiciel, chaque logiciel est unique en soi par ses besoins et ses caractéristiques (fonctionnalités, technologies utilisées, etc.).
- **Aucun consensus sur les meilleurs concepts** : il n'y a pas de consensus sur les meilleurs concepts de sécurité à appliquer dans un projet de développement logiciel.
- **Le moment où prendre en compte la sécurité** : la sécurité informatique ne peut pas être réalisée d'un seul coup dans le cadre d'un projet de développement logiciel. En raison de tous les facteurs influençant un tel projet, elle doit être prise en considération durant tout le cycle de développement du logiciel.

- **L'identification des besoins de sécurité** : les besoins de sécurité semblent plus difficiles à décrire par les clients, étant donné leur nature moins tangible que les besoins fonctionnels par exemple.

Longtemps jugée comme un mal nécessaire, la sécurité informatique représente maintenant une valeur ajoutée pour le développement logiciel. Due à l'importance que cela représente, différents projets de recherche ont débuté pour tenter de remédier aux difficultés rencontrées. La prochaine section fait état de quelques-uns d'entre eux.

1.2.5 Quelques projets de recherche

Au fil du temps, des solutions ont été proposées afin de favoriser et de faciliter l'intégration de la sécurité dans le développement logiciel. L'envergure des projets qui suggèrent ces solutions, en termes de grosseur et de portée, peut s'avérer très variable d'un projet à l'autre. L'un peut cibler l'amélioration d'une étape du cycle de développement du logiciel ou une activité de sécurité spécifique, tandis qu'un autre peut viser l'amélioration de l'ensemble du cycle de développement du logiciel. Pour les besoins de la présente recherche, cette section présente des projets de recherche qui concernent l'amélioration globale de la sécurité informatique et qui visent l'ensemble du cycle de développement du logiciel. Voici quelques-uns des plus connus :

a. **CLASP** (OWASP) : **C**omprehensive, **L**ightweight **A**pplication **S**ecurity **P**rocess [1]

Produit par la compagnie Secure Software Inc. et maintenant sous la tutelle de OWASP, *The Open Web Application Security Project*, le projet CLASP propose une série d'activités de sécurité à intégrer dans le cycle de développement du logiciel et dénote un certains nombres de rôles liés à la sécurité que doivent avoir les intervenants d'un projet. L'objectif principal de CLASP est d'aider les équipes de développement logiciel à introduire la sécurité dans leurs projets, que ceux-ci soient nouveaux ou existants. Indépendant d'un modèle de cycle de développement du logiciel particulier, CLASP propose une série de bonnes pratiques par l'entremise de plusieurs activités de sécurité à réaliser durant les étapes du développement logiciel. Les activités sont également liées aux rôles de sécurité attribués aux différents intervenants du projet.

b. **NIST SP 800-64** (NIST) : **N**ational **I**nstitute of **S**tandards and **T**echnology [2]

Le SP 800-64 (Security Considerations in the Information System Development Life Cycle) fait partie de la série de documents 800-* du NIST qui ont pour but de décrire les politiques et procédures en matière de sécurité informatique aux États-Unis. Plus précisément, le SP 800-64 aide à comprendre les exigences de sécurité informatique à considérer dans les différentes étapes du cycle de développement du logiciel pour les systèmes d'information et la mise en œuvre de mesures de sécurité adéquates. Il sera question plus précisément du concept de « système d'information » lors du deuxième chapitre. Sur la base d'un cycle de développement du logiciel générique, chacune des phases est énoncée avec une série d'activités de sécurité à réaliser minimalement pour incorporer efficacement la sécurité.

c. **SDL** (Microsoft) : **S**ecurity **D**evelopment **L**ifecycle [3]

Le Cycle de Développement Sécurité, termes francisés du Secure Development Lifecycle (SDL), consiste à ajouter une série d'activités de sécurité dans chacune_des phases du cycle de développement du logiciel telle que définie par Microsoft, leader mondial du marché du logiciel. Les objectifs visés par cette approche sont les suivants : augmenter la qualité de l'application, réduire le nombre de vulnérabilités existantes, détecter et supprimer les failles le plus rapidement possible dans le cycle de développement de l'application, minimiser les coûts des mises à jour et modifier la perception de l'utilisateur. La compagnie Microsoft offre différentes ressources informatiques pour aider les entreprises à implémenter la démarche et, du même coup, leur permettre de créer des logiciels plus sécurisés.

d. **Security in the software lifecycle** (Department of Homeland Security) [4]

Le document intitulé « Security in the software lifecycle: Making Software Development Processes – and Software Produced by Them – More secure » présente les principaux enjeux de la sécurité des logiciels durant leur cycle de développement. Vis-à-vis ces enjeux, le référentiel élabore sur des modèles d'amélioration de processus, des concepts sur la gestion des risques, des méthodes de développement logiciel, des bonnes pratiques, des outils informatiques aidant à la résolution des vulnérabilités, etc. Le projet aborde donc la question en présentant une gamme très vaste de solutions possibles dont

le but est de prendre en charge la sécurité informatique durant le développement logiciel.

e. **TSP-Secure** (SEI) : **T**eam **S**oftware **P**rocess for **Secure** Software Development [5]

Issu de la famille du modèle TSP provenant du Software Engineering Institute de l'Université Carnegie Mellon University, qui se spécialise dans la production de logiciels de qualité en se concentrant sur l'élimination des défauts de conception, TSP-Secure vise plus précisément les orientations de haut niveau en matière de sécurité informatique des logiciels pour les équipes de développement. La méthode vise plus précisément la planification de la sécurité, l'utilisation de bonnes pratiques, l'aide pour la gestion de la qualité tout au long du cycle de développement du logiciel et la formation des développeurs en matière de sécurité informatique.

Ces projets de recherche présentent des solutions pour améliorer la sécurité informatique du développement logiciel en insérant différentes activités de sécurité dans le cycle de développement du logiciel. Dans un tout autre ordre d'idées, il faut également souligner que des initiatives sont en cours pour modifier directement les modèles de cycle de développement du logiciel afin qu'ils soient réellement adaptés à la sécurité informatique. Quelles que soient l'ampleur, l'approche ou la nature des solutions proposées, le point à retenir est qu'elles sont toutes des initiatives positives vers un même objectif commun.

En résumé, le développement logiciel et la sécurité informatique sont des domaines complexes en soi, et le fait de vouloir les réunir comporte certaines difficultés à surmonter. Après avoir énoncé brièvement certains concepts de base du développement logiciel et de la sécurité informatique, l'attention fut ensuite portée vers l'intégration de la sécurité dans un contexte de développement logiciel. Cette mise en contexte s'avère importante puisqu'elle représente l'un des sujets importants de la recherche présentée dans ce document et dont il sera de nouveau question lors du troisième chapitre.

Ce premier chapitre visait à présenter globalement le développement logiciel et sa relation possible et nécessaire avec la sécurité informatique. Le prochain chapitre poursuit la mise en contexte des sujets importants de la recherche en abordant la gestion des risques de sécurité pour la protection des systèmes d'information.

CHAPITRE II

LA GESTION DES RISQUES POUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

D'un point de vue général, le terme « gestion » est défini comme étant l'ensemble des activités de planification, de direction et de contrôle nécessaires pour que l'entité atteigne ses objectifs. Là où son utilité prend tout son sens dans un contexte d'entreprise, c'est lorsque ses principes sont appliqués dans un secteur d'activités en particulier tels les ressources humaines, les finances ou le marketing. Parmi ces secteurs, celui de l'informatique nécessite également l'usage de bonnes pratiques de gestion afin de répondre adéquatement aux besoins de l'entreprise. Parmi ces bonnes pratiques, il y a notamment celles reliées à la gestion de la sécurité informatique. Elles visent l'ensemble des activités de planification, d'organisation et de contrôle de la sécurité informatique sur les ressources matérielles et logicielles de l'entreprise.

Dans la même continuité que les sujets présentés dans le chapitre précédent, ce deuxième chapitre aborde plus précisément la sécurité informatique appliquée au domaine du logiciel. Remplacés ici par le concept de « systèmes d'information » qui sera introduit et expliqué dans la première section, les logiciels représentent des enjeux importants pour les entreprises qui en font l'usage dans leurs processus d'affaires. Une entreprise peut posséder plusieurs de ces systèmes d'information, d'où l'importance d'avoir une stratégie globale et structurée pour gérer adéquatement leur sécurité informatique.

Le but de ce chapitre est tout d'abord de présenter la sécurité des systèmes d'information de manière générale, mais ensuite de l'aborder via une approche méthodologique existante. La première section introduit donc la sécurité des systèmes informatiques dont les concepts d'expression des besoins de sécurité et d'identification des mesures de sécurité. Ensuite, la seconde section vise plus précisément la manière d'implanter la sécurité des systèmes d'information en présentant l'approche par la gestion des risques de sécurité.

Dans l'ensemble de ce document, le rôle de ce chapitre consiste à conclure la mise en contexte de la recherche débutée au premier chapitre et qui consiste à présenter les sujets importants pour sa démarche. Il est à noter que la présentation des notions de gestion des risques dans ce chapitre est confrontée à une difficulté du fait qu'il n'existe pas de vocabulaire commun dans ce domaine. Pour les besoins de la présente recherche, il faut toutefois établir et définir les termes qui seront utilisés dans la démarche pour en favoriser sa compréhension.

2.1 La sécurité des systèmes d'information

Dans un contexte où la technologie est maintenant devenue un outil quasi essentiel en entreprise, la complexité des logiciels informatiques continue de croître et les informations qu'ils manipulent sont de plus en plus vitales pour le bon fonctionnement de leurs processus d'affaires. Dans ce deuxième chapitre, le terme « système d'information » sera maintenant utilisé en remplacement du terme « logiciel » puisqu'il donne un sens plus large au concept de logiciel, en incluant également tout ce qui se retrouve dans son contexte d'utilisation pour traiter les informations. Plus précisément, un système d'information est un ensemble d'entités (organisation, site, personnel, matériel, réseau, logiciel ou système) organisé pour accomplir des fonctions de traitement d'information. Tout dépendant de la valeur que possèdent les systèmes d'information pour une entreprise, la sécurité à appliquer doit être minimalement de la même envergure. Bien entendu, la valeur est étroitement liée à la nature même des activités de l'entreprise.

Malgré tous les efforts possibles, l'obtention d'une sécurité informatique parfaite est pratiquement impossible à atteindre, puisque la cible à protéger est en continuel changement et les solutions de sécurité nécessitent de nombreux efforts à implanter et à maintenir à jour. Il ne faut pas non plus négliger que l'application de la sécurité informatique représente des coûts financiers non négligeables pour une entreprise. Toutefois, gérer et contrôler adéquatement cette sécurité représentent un objectif possible et réalisable. Dans cette perspective, différentes raisons poussent les entreprises à investir du temps et de l'argent pour protéger leurs systèmes d'information. En plus de vouloir éviter les conséquences d'un incident de sécurité, certaines règles gouvernementales ou normes en sécurité informatique peuvent leur être imposées selon la nature de leurs activités. Les entreprises peuvent également devoir donner un certain niveau de confiance envers leurs clientèles et leurs partenaires sur la gestion effectuée quant à la sécurité des systèmes d'information. Tout d'abord confrontées à ces incitatifs, les entreprises peuvent maintenant voir la sécurité informatique comme une valeur ajoutée en terme d'assurance qualité lorsqu'elle est appliquée adéquatement.

Pour mettre en œuvre cette sécurité des systèmes d'information dans une entreprise, il faut tout d'abord bien comprendre ce qu'elle représente. Il s'agit des moyens techniques, organisationnels, juridiques et humains pour garantir la sécurité de l'information qui transigent entre les entités du système d'information. Dans cette définition, la sécurité de l'information précise la sécurité informatique nécessaire pour protéger adéquatement toute information quel que soit son support. L'information représente la matière brute qui est exploitée par les systèmes d'information et il est possible, via l'utilisation de critères de sécurité, de leur attribuer des valeurs exprimant ainsi leurs besoins de sécurité. Même s'il est souvent dit que les systèmes d'information ont de la valeur pour une entreprise, cette valeur est conséquente de celle des informations qu'ils manipulent. La sécurité des systèmes d'information représente donc la sécurité appliquée aux systèmes afin de répondre aux besoins de sécurité des informations manipulées par ces derniers.

La sensibilisation à l'égard de la sécurité des systèmes d'information ne représente que les premiers pas de la démarche. La suite génère une série de questionnements dont les trois prochaines sections de ce chapitre répondront globalement. La première s'attarde à l'expression des besoins de sécurité afin que l'entreprise puisse identifier quels sont ses besoins en matière de sécurité pour ses systèmes d'information. La seconde aborde les bonnes pratiques en la matière afin que l'entreprise puisse déterminer quelles sont les solutions possibles pour combler ses besoins de sécurité. La troisième section précise, une fois que l'entreprise sait ce dont elle a besoin et ce qui existe comme solutions de sécurité, comment faire pour choisir les solutions adéquates en fonction de ses besoins exprimés et ses priorités.

2.1.1 L'expression des besoins de sécurité

À la base même de la démarche, il faut tout d'abord connaître les besoins de l'entreprise en matière de sécurité pour les systèmes d'information. Pour ce faire, il faut parvenir à évaluer leur importance selon les informations qu'ils manipulent. Quelles seraient les conséquences sur les processus d'affaires si un système en particulier tombait en panne, rendant ainsi les informations qu'il contient inaccessibles ? Est-ce que l'entreprise possède des systèmes d'information où sont transmises des informations confidentielles ? Des décisions importantes sont-elles prises selon des résultats donnés par un système ? Ces questions restent parfois sans réponse et les enjeux qu'elles représentent peuvent s'avérer cruciaux pour l'entreprise. Pour y répondre adéquatement, le tout débute par l'expression des besoins de sécurité.

Les besoins de sécurité sont couramment exprimés à l'aide de critères de sécurité dont les plus connus sont les suivants :

- **La disponibilité** : propriété d'une information d'être accessible et utilisable en temps voulu et de la manière requise par une personne autorisée;
- **L'intégrité** : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation;
- **La confidentialité** : propriété d'une information d'être inaccessible aux personnes non autorisées.

La sécurité de l'information vise à protéger les besoins de sécurité exprimés par ces critères. Il est donc possible d'attribuer des valeurs à n'importe quelles ressources informationnelles utilisées dans un système d'information de l'entreprise. Le terme « actif informationnel » est couramment utilisé pour représenter une ressource informationnelle tels un système d'information, un matériel informatique et de télécommunication, un logiciel, un progiciel, une banque de données ou une information. L'attribution de valeurs sur les critères de sécurité pour les actifs informationnels est couramment appelée une activité de « catégorisation des actifs informationnels ». À titre d'exemple, si l'échelle de valeurs est de 1 à 4 où 4 représente la valeur la plus forte, la valeur du DIC (**D**isponibilité – **I**ntégrité – **C**onfidentialité) d'un actif pourrait donner les résultats suivants : D = 3, I = 2, C = 4. Il est ensuite possible d'en déduire que le critère le plus important pour cet actif informationnel est celui de la confidentialité, suivi de la disponibilité et de l'intégrité. Également, son niveau de confidentialité est celui de la valeur la plus élevée qu'il est possible d'attribuer, ce qui en dit énormément sur son besoin en la matière. L'objectif global est de déterminer les besoins de sécurité pour tous les actifs informationnels du système d'information ou du moins, les plus importants. Par conséquent, les actifs ayant les plus grands besoins en matière de sécurité doivent être priorisés dans une démarche de sécurité des systèmes d'information. Quoique très connu, la catégorisation des actifs informationnels est une façon parmi d'autres de réaliser l'expression des besoins de sécurité. Une fois ceux-ci exprimés, reste ensuite à déterminer la façon de les combler.

2.1.2 L'identification des mesures de sécurité

La sécurité de l'information a donc pour objectif de protéger les actifs informationnels en fonction de leurs besoins exprimés à l'aide des critères de sécurité. Pour assurer la sécurité d'un actif par des moyens concrets, des mesures de sécurité doivent être mises en place. Puisque ces mesures de nature très variée peuvent être difficiles à identifier concrètement, des projets de recherche en proposent certaines qui peuvent être considérées comme étant de bonnes pratiques pour la gestion de la sécurité de l'information. Il y a notamment la norme internationale ISO/CEI 27002 (autrefois appelée ISO/IEC 17799) [6] qui suggère un ensemble de 133 mesures recommandées réparties dans les onze catégories de sécurité suivantes :

1. Politique de sécurité;
2. Gestion des biens;
3. Sécurité liée aux ressources humaines;
4. Sécurité physique et environnementale;
5. Gestion des communications et de l'exploitation;
6. Contrôle d'accès;
7. Acquisition, développement et maintenance des systèmes d'information;
8. Gestion des incidents liés à la sécurité de l'information;
9. Gestion de la continuité d'activité;
10. Conformité légale et réglementaire.

Par son statut de norme, elle agit à titre de référence en matière de sécurité de l'information et, plus important encore, elle représente un consensus par des spécialistes du domaine. Il existe de nombreuses autres sources de référence concernant des mesures de sécurité possibles. Les méthodes utilisées pour appliquer la sécurité des systèmes d'information, comme celles présentées dans la prochaine section, contiennent également des bases de connaissance pouvant servir à déterminer des mesures de sécurité.

Reste maintenant à savoir comment mettre la sécurité des systèmes d'information en place en fonction du contexte de l'entreprise. Pour y parvenir d'une manière structurée, la prochaine section introduit l'approche par la gestion des risques de sécurité. Cette démarche fait le lien entre les besoins de l'entreprise, les mesures de sécurité recommandées dans le domaine et la priorisation à faire quant aux mesures les plus importantes à appliquer.

2.2 L'approche par une gestion des risques de sécurité

La gestion des risques est définie de la manière suivante par l'Office québécois de la langue française : « Ensemble des activités qui consistent à recenser les risques auxquels l'entité est exposée, puis à définir et à mettre en place les mesures préventives appropriées en vue de supprimer ou d'atténuer les conséquences d'un risque couru ». Prenant appui sur cette définition, il faut également ajouter que le type de risque concerné ici est celui de sécurité informatique. Cette section présente donc l'approche par une gestion des risques de sécurité. À cet égard, la première section traite de l'équation du risque qui est l'un des principes de base de cette approche. La seconde énonce une série d'étapes à réaliser pour atteindre les objectifs visés. Pour terminer, la troisième présente quelques méthodes de gestion des risques reconnues dans ce domaine.

2.2.1 L'équation du risque

Puisque les risques encourus ne sont pas les mêmes pour chacun des actifs, une des activités dans la gestion des risques est d'établir la façon avec laquelle il sera possible de les comparer. Cette valeur du niveau de risque joue un rôle déterminant dans la suite de la démarche quant à l'importance à donner au traitement du risque en question. Plus ce niveau sera critique, plus une attention particulière devra être portée envers ce risque. L'équation commune pour évaluer le niveau de risque est la suivante [7] :

Risque = menace * vulnérabilité * impact

Le niveau de risque est donc obtenu par l'évaluation de la probabilité que la menace survienne, le degré de sévérité des vulnérabilités reliées à l'actif et l'importance de l'impact sur l'entreprise si la menace se concrétise.

Sans entrer dans les détails, la manière dont ces trois variables sont ensuite calculées dépend fortement de la méthode de gestion des risques utilisée. Leur méthode d'évaluation peut adopter une approche quantitative, qualitative ou les deux combinées. Quelle que soit la manière d'évaluer les risques encourus, l'important est d'avoir les outils appropriés pour les comparer sur une base de critères égaux.

2.2.2 Les grandes étapes de la gestion des risques

Il n'est pas simple d'identifier concrètement les étapes d'une approche par la gestion des risques puisque les références qui traitent de ce sujet les présentent de différentes façons. Même si elles abordent sensiblement les mêmes notions, les différences sont nombreuses au niveau des termes utilisés, de la façon de faire les activités de sécurité, de la logique d'approche ou même du découpage des étapes. Pour la présente recherche, il est primordial d'établir une série d'étapes pour la gestion des risques puisque les travaux de la démarche analytique, présentés au quatrième chapitre, viendront s'y appuyer à titre de référence sur le sujet.

Ainsi, la gestion des risques de sécurité peut être présentée par une démarche comprenant neuf étapes distinctes. À travers leur réalisation, les informations récoltées permettront de répondre aux interrogations sur les besoins à identifier, les solutions de sécurité adéquates et l'évaluation des paramètres de l'équation des risques pour chacun des actifs informationnels considérés. Les étapes sont présentées sommairement dans ce chapitre, mais les activités qui sont réalisées dans chacune

d'entre elles feront l'objet de l'une des étapes de la démarche analytique. Voici les neuf étapes en question :

- **Organisation de la démarche** : Cette étape permet d'assurer le bon déroulement de la démarche de gestion des risques. Bien que certaines des activités soient inhérentes aux autres étapes, les activités de cette étape concernent les principales facettes de la gestion tels la planification, la communication, la préparation et le soutien à la démarche. Cette étape n'est pas numérotée, comparativement aux autres étapes, pour signifier que sa portée couvre l'ensemble de la démarche de gestion de risques.

1. **Identification et étude du contexte** : Cette étape vise à définir la portée de la démarche en analysant l'environnement de la cible choisie pour la démarche de gestion de risques. L'étude du contexte est importante pour la gestion des risques, puisqu'elle permet d'obtenir les informations relatives à tout ce qui gravite autour de la cible et qui peut possiblement l'influencer.

2. **Identification des actifs informationnels** : Cette étape permet de définir concrètement la cible de la démarche de gestion de risques. Il s'agit d'abord d'inventorier les principaux actifs informationnels de la cible. Il faut ensuite identifier ceux qui lui sont les plus importants, voire même les plus critiques. Les actifs informationnels considérés comme critiques et ceux qui les supportent seront sélectionnés pour la suite de la démarche de gestion de risques.

3. **Identification et évaluation des besoins de sécurité** : Cette étape consiste à attribuer des valeurs aux critères de sécurité choisis pour chacun des actifs informationnels à considérer dans la démarche. Cette attribution de valeurs correspond à l'expression des besoins de sécurité et doit être établie avec les personnes en charge des actifs informationnels en question.

4. **Identification et évaluation des menaces et des vulnérabilités** : Cette étape dresse un portrait des menaces auxquelles les actifs informationnels sont exposés. Après avoir identifié les menaces possibles, ses caractéristiques (éléments attaquants ou méthode d'attaque, enjeux concernés, critères de sécurité visés, etc.) et les vulnérabilités de sécurité relatives aux actifs en question, l'évaluation des menaces permet de les

comparer et de prioriser les plus probantes dans la suite de la démarche de gestion de risques.

5. **Identification et évaluation des risques** : Cette étape consolide les informations nécessaires pour identifier les risques à considérer. Les risques encourus sur les actifs informationnels sont identifiés suite à l'analyse de leurs besoins de sécurité, des menaces auxquelles ils sont exposés et des vulnérabilités qu'ils contiennent. Une fois formulé explicitement, chacun des risques peut alors être évalué avec l'équation du risque afin d'en établir leur importance relative.

6. **Identification des exigences de sécurité** : Cette étape détermine les recommandations générales de sécurité à prendre en considération pour atténuer les risques qui sont pris en charge. Un risque à traiter qui est partiellement ou pas du tout couvert par les exigences résultera en ce qui est appelé un risque résiduel. La décision de ne pas traiter un risque peut également être déterminée du fait qu'il soit toléré ou transféré vers un tiers.

7. **Sélection des mesures de sécurité** : Cette étape identifie les mesures de sécurité concrètes qu'il faut implanter afin de répondre aux exigences de sécurité établies. Par l'entremise de l'exigence de sécurité dont elle correspond, la mesure vise habituellement à atténuer l'une des variables qui compose l'équation du risque (la menace, la vulnérabilité ou l'impact).

8. **Implantation des mesures de sécurité** : Cette étape concrétise la mise en place des mesures de sécurité qui correspondent aux exigences de sécurité et, du même coup, aux risques qui ont été identifiés durant la démarche. Chacune des mesures doit être créée ou acquise, testée et ensuite implantée.

Dans les publications concernant les étapes de la gestion de risques, il est courant de les voir regroupées en deux grandes phases qui sont l'analyse de risques et la maîtrise des risques. L'analyse de risques, aussi appelée l'appréciation des risques, correspondrait dans l'ensemble aux étapes un à cinq. Pour ce qui est de la maîtrise des risques ou également appelée le traitement des risques, elle concorderait avec les étapes six à huit. Bien entendu, les étapes et la définition de ces grandes phases dépendent de la source de référence consultée.

La figure 2.1 représente les deux grandes phases et les neuf étapes de la gestion de risques telles que présentées dans cette section :

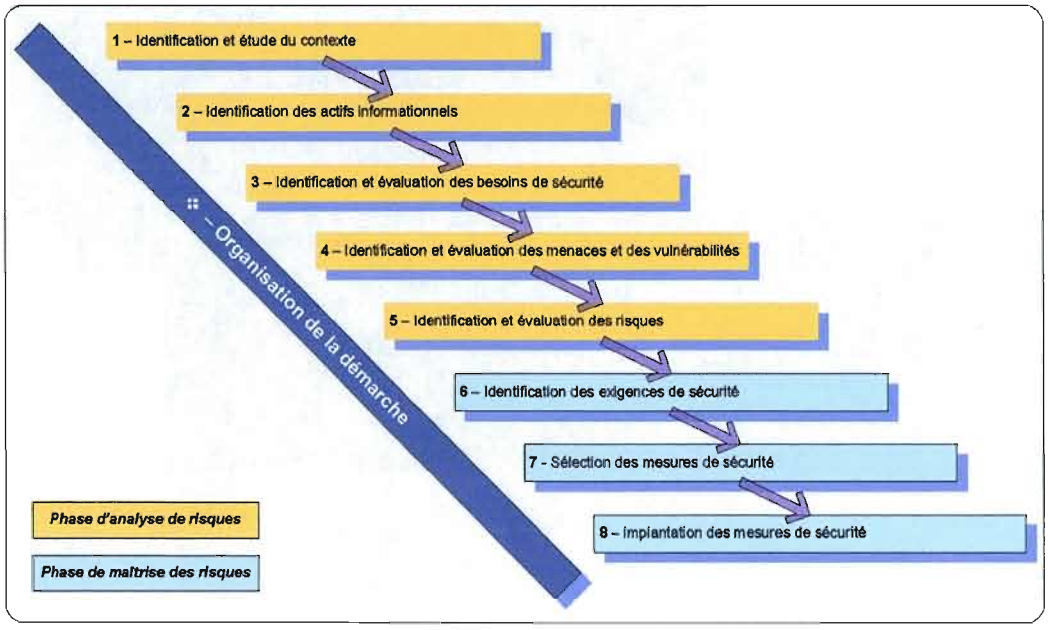

Figure 2.1 Les neuf étapes d'une démarche de gestion de risques.

Ce découpage de la démarche de gestion de risques en étapes est une façon générale de la présenter, et l'enjeu ici est d'en établir une base de référence pour la suite de la recherche. De plus, il est important de noter que cette démarche méthodologique doit être effectuée de façon cyclique dans un contexte réel, puisqu'il est impossible de traiter tous les actifs et leurs risques d'un seul coup. Il faut donc en sélectionner un certain nombre représentant les plus critiques et, par la suite, recommencer le cycle avec ceux qui sont considérés les plus critiques à ce moment-là. En effet, les risques peuvent varier au fil du temps de sorte que de nouveaux risques peuvent apparaître, comme d'anciens peuvent revenir. Le travail n'est donc jamais terminé, d'où l'importance d'intégrer la gestion des risques dans les activités de continuité de l'entreprise.

La prochaine section présente des méthodes reconnues dans le domaine de la gestion des risques. Elles font référence à la plupart des notions expliquées précédemment tout en ayant chacune des particularités qui les distinguent.

2.2.3 Quelques méthodes de gestion des risques

Quand vient le moment de choisir une méthode à utiliser, une décision importante s'impose. D'un côté, il existe des méthodes reconnues dans le domaine qui sont prêtes à être utilisées. Elles offrent l'avantage d'avoir été éprouvées et leur évolution est gérée par des gens possédant l'expertise du domaine. Les désavantages se situent au niveau de l'apprentissage et de l'adaptation de la démarche à suivre afin qu'elles correspondent aux réels besoins de l'entreprise. D'un autre côté, une méthode ad hoc peut être créée par une entreprise et utilisée dans le cadre de ses activités de gestion des risques. Elle offre l'avantage d'une démarche qui vise plus spécifiquement ses besoins en la matière. La principale difficulté se situe au niveau de la maintenance d'une telle méthode afin qu'elle s'adapte continuellement aux orientations et aux changements de l'entreprise, et du domaine de la gestion des risques de sécurité.

Quel qu'en soit le choix, l'utilisation d'une méthode reconnue ou ad hoc, elle doit contribuer à une prise de décisions éclairée en ce qui concerne la sécurité des systèmes d'information pour les besoins de sécurité identifiés. Après de nombreuses lectures, il n'est pas simple de déterminer quelles publications présentent véritablement une méthode de gestion de risques par rapport à une norme, un recueil de bonnes pratiques, une certaine partie de la démarche de gestion de risques, un référentiel général sur la gestion de la sécurité, etc. Les listes sont souvent mélangées parce que les différents ouvrages ne traitent pas uniquement d'un seul concept ou ne cadre pas parfaitement dans une approche de sécurité bien précise. Ils sont donc difficiles à classer en catégories. Malgré tout, le tableau 2.1 démontre quelques méthodes reconnues dans le domaine [8] :

Tableau 2.1
Méthodes de gestion des risques de sécurité

Noms	Provenances	Auteurs
CRAMM (CCTA Risk Analysis and Management Method)	Angleterre	L'agence britannique CCTA (Central Communication and Telecommunication Agency)
EBIOS (Expression des Besoins et Identification des objectifs de sécurité)	France	L'agence française DCSSI (Direction centrale de la sécurité des systèmes d'information)
MEHARI (Méthode Harmonisée d'Analyse de Risques Informatiques)	France	Le club professionnel CLUSIF (Club de la Sécurité de l'Information Français)

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	États-Unis	Carnegie Mellon University SEI (Software Engineering Institute)
SPRINT (Simplified Process for Risk Identification)	Internationale	L'association internationale ISF (Information Security Forum)
NIST 800-30 (Risk Management Guide for Information Technology systems)	États-Unis	L'institut NIST (National Institute for Standards and Technology)

En résumé, les informations contenues et manipulées par les systèmes informatiques représentent aujourd'hui un élément de valeur pour les entreprises. De ce fait, il est primordial d'appliquer une sécurité informatique ajustée à cette valeur. Pour les systèmes d'information, il existe une démarche qui vise à améliorer le niveau de sécurité par la réduction des risques encourus sur ses actifs informationnels importants. Pour appliquer cette démarche, il faut principalement réunir les informations nécessaires pour être en mesure d'identifier et d'évaluer les risques et, selon les résultats, mettre en œuvre les mesures de sécurité pouvant les atténuer. Les méthodes reconnues, telles qu'énoncées dans ce chapitre, présentent une démarche structurée et permettent la démonstration de résultats concrets sur l'amélioration du niveau de sécurité informatique pour les systèmes d'information.

Ce deuxième chapitre termine la mise en contexte des sujets importants de la recherche. Il visait à présenter les principes de base de la gestion des risques dans le contexte des systèmes d'information. Le prochain chapitre établira les fondements de la recherche de façon à faire le pont entre la mise en contexte établie précédemment et la démarche analytique présentée par la suite.

CHAPITRE III

LES FONDEMENTS DE LA RECHERCHE

Le premier chapitre abordait les thèmes du développement logiciel et de la sécurité informatique. Quant au second, il introduisait celui de la gestion des risques pour la sécurité des systèmes d'information. Les chapitres précédents visaient à exposer les sujets importants de la présente recherche. Le troisième chapitre a pour but d'établir les fondements de celle-ci, en établissant les liens entre ces sujets et leur utilité dans la démarche analytique, le thème principal du quatrième chapitre.

La première section introduit la problématique qui sera traitée par la recherche soit celle qui consiste à la difficulté de produire des logiciels dont les besoins en sécurité informatique ont été considérés adéquatement selon le contexte d'utilisation du logiciel en question. La deuxième section présente, par l'entremise d'une hypothèse générale, la solution pour remédier à cette problématique. La troisième section positionne la solution proposée par rapport aux autres projets de recherche similaires. La quatrième section explique les choix entourant les référentiels qui seront utilisés dans la démarche analytique et qui servent d'appui aux concepts de la solution proposée. Pour terminer, la cinquième section détaille le déroulement de la démarche analytique en décrivant chacune des étapes qui seront réalisées.

Dans l'ensemble de ce document, le rôle de ce chapitre consiste à présenter les fondements de la recherche et à positionner celle-ci par rapport aux autres solutions existantes. Du même coup, les paramètres de la démarche analytique seront alors établis, indiquant ainsi sur quelles bases devront être interprétés les résultats obtenus.

3.1 La problématique visée

La démarche pour mener à bien un projet de développement logiciel peut s'avérer complexe à entreprendre. Quel que soit le modèle de cycle de développement du logiciel utilisé, la gestion des vulnérabilités pouvant s'introduire durant les phases de développement du logiciel n'est pas une problématique facile à résoudre. En plus du temps nécessaire pour identifier ces vulnérabilités, des solutions doivent être trouvées et appliquées dans les meilleurs délais possible selon la gravité de la situation. Une vulnérabilité informatique, dans son sens large, peut être définie comme une faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent. Les vulnérabilités dont il sera question dans la présente recherche sont uniquement celles qui contribuent à la présence de failles en matière de sécurité informatique. Le terme « vulnérabilité de sécurité » sera donc utilisé dans la suite de ce document pour faire référence à ce type bien précis de vulnérabilités informatiques.

Pour en revenir aux projets de développement logiciel, les efforts déployés pour gérer les besoins de sécurité informatique sont encore très peu priorisés. Introduites malencontreusement tout au long du cycle de développement du logiciel, les vulnérabilités de sécurité sont couramment détectées et prises en considération qu'à la toute fin du cycle de développement ou lorsque le logiciel est déjà en opération. En plus des coûts financiers supplémentaires engendrés par leur résolution tardive, les conséquences peuvent être des plus dommageables si les vulnérabilités sont découvertes suite à une attaque informatique. Pour une entreprise, une telle situation pourrait engendrer différentes conséquences néfastes comme des poursuites légales, des problèmes opérationnels, une perte de marché ou d'image, etc.

Pour parer à ce type de problèmes, certaines entreprises utilisent de bonnes pratiques prônées par la sécurité informatique comme celles des domaines de la gouvernance, de l'audit informatique ou de la gestion des risques pour contrôler leurs différents secteurs d'activité. Ces vérifications incluent les systèmes d'information supportant les processus d'affaires et, du même coup, les logiciels qui y sont utilisés. Malgré l'application de ces bonnes pratiques qui contribuent à améliorer la sécurité informatique, il faut toutefois constater que le travail est effectué lorsque le système d'information est en opération et, par conséquent, potentiellement à risque pour l'entreprise.

Plusieurs facteurs peuvent expliquer la difficulté actuelle à traiter judicieusement les besoins de sécurité durant le cycle de développement du logiciel. Voici quelques-uns d'entre eux :

- La complexité grandissante des projets de développement logiciel;

- Une mauvaise connaissance du sujet due à une formation déficiente des ressources humaines;
- Une culture d'entreprise ne considérant pas l'importance de la sécurité informatique;
- Des besoins plus difficiles à définir du fait qu'ils sont moins concrets et tangibles que les besoins fonctionnels;
- La diversité des projets de développement logiciel, quant aux technologies utilisées et à la sensibilité des informations manipulées, peut générer des besoins de sécurité différents pour chaque projet.

Suite à ces différentes observations, la problématique visée par la présente recherche est donc celle de la présence élevée de vulnérabilités de sécurité dans les logiciels produits et mis en production dans les entreprises [9, 10, 11].

3.2 La solution proposée

Des projets de recherche visant à améliorer la sécurité informatique dans le domaine du développement logiciel ont été présentés lors du premier chapitre. Ces projets proposent une série d'activités de sécurité générales, dont celle de la gestion des risques de sécurité qui y est régulièrement citée. La solution proposée vise à aborder cette activité de façon plus significative et détaillée. Tel qu'énoncé dans le deuxième chapitre, l'approche par une gestion des risques est reconnue pour contribuer à l'amélioration de la sécurité des systèmes d'information. Si ces mêmes principes étaient appliqués au contexte même du développement logiciel, les bonnes pratiques seraient alors tout de suite mises en application sur le logiciel avant même sa mise en opération. Il s'agit donc de prendre en considération les mesures de sécurité adéquates au moment même où le logiciel est développé et non pas d'attendre qu'une tâche de vérification de la sécurité des systèmes d'information soit effectuée par l'entreprise sur ses systèmes d'information déjà en opération.

En appliquant les activités de sécurité proposées dans les méthodes de gestion des risques de sécurité dans une démarche de développement logiciel, il est possible de croire qu'elles contribueraient à améliorer la sécurité informatique de celui-ci avant même sa mise en opération. Pour se faire, il faut tenir pour acquis qu'il est possible d'intégrer des activités de sécurité informatique parmi celles d'une démarche de développement logiciel et que ces nouvelles activités intégrées permettent de déterminer et de prioriser les travaux de sécurité à prendre en considération durant le développement logiciel, selon les besoins et les risques de sécurité les plus importants. Cette solution est formulée de manière plus formelle par l'hypothèse principale suivante :

Les activités de sécurité véhiculées dans les méthodes de gestion des risques pour la sécurité des systèmes d'information peuvent être appliquées dans les étapes du cycle de développement du logiciel, et ce, dans le but de diminuer la présence de vulnérabilités de sécurité au moment où le logiciel sera achevé et mis en opération.

Par l'intégration des activités générales des méthodes de gestion de risques dans un contexte de développement logiciel et, ainsi, en adoptant une approche par résolution de risques, les outils seraient alors en place pour contribuer efficacement à la diminution des vulnérabilités de sécurité. C'est donc sur ces points fondamentaux que la recherche s'appuie afin de démontrer la pertinence de la solution relativement à la situation problématique identifiée.

3.3 Le positionnement de la solution proposée

La présente recherche n'est pas la seule à viser l'objectif de diminuer la présence de vulnérabilités de sécurité durant le développement logiciel ou de proposer une approche par la gestion des risques de sécurité. Cette section présente donc le positionnement de la solution proposée par rapport à ces autres projets de recherche traitant de la même problématique.

En ce qui concerne les projets de recherche visant le même objectif, les projets qui ont été présentés au premier chapitre font partie de cette catégorie. Ils visent l'amélioration de la sécurité informatique dans le développement logiciel pour une diminution des vulnérabilités de sécurité. Cependant, leur approche est beaucoup plus globale, puisqu'ils proposent un ensemble varié d'actions générales à intégrer durant le cycle de développement du logiciel dont celle de gestion des risques. La solution proposée ne vise donc pas à être de la même envergure que ces différents projets de recherche, mais plutôt à détailler plus concrètement l'activité de gestion des risques de sécurité dont ils vantent l'importance et les bénéfices.

Concernant les projets de recherche ou publications qui utilisent une approche par la gestion des risques de sécurité, il y a notamment ceux-ci qui sont relativement connus :

- Assessing Information Security Risks in the Software Development Life Cycle [12];
- NIST : SP 800-30 "Risk Management Guide for Information Technology Systems" [13];
- Microsoft STRIDE[14] & DREAD [15];
- Building Security In : Risk Analysis in Software Design [16];

Ce qui distingue la solution proposée de celles des projets comme ceux énumérés précédemment, c'est qu'elle prend sa source directement des activités de sécurité prônées par des méthodes éprouvées dans le domaine de la sécurité des systèmes d'information. Elle n'est pas basée uniquement sur les principes de base du domaine, mais bien sur les activités des approches méthodologiques concrètement effectuées en entreprise. La solution proposée présente donc une corrélation très forte avec les principes de gestion des risques de sécurité pris à même les méthodes du domaine, ce qui n'est pas le cas dans les autres projets de recherche similaires.

La figure 3.1 résume le positionnement de la solution, mais également les liens avec les autres éléments importants de la recherche tels que le cycle de développement du logiciel, le logiciel lui-même, le système d'information et les méthodes de gestion des risques.

A. Un logiciel est produit par le cycle de développement du logiciel.
B. Le logiciel est mis en opération et devient alors un des actifs informationnels d'un système d'information.
C. Les méthodes de gestion des risques sont appliquées pour sécuriser le système d'information.
D. Des projets visent à réduire les vulnérabilités de sécurité dans le développement logiciel (même objectif que la solution proposée).
E. Des projets visent à intégrer la gestion des risques dans le développement logiciel (même approche que la solution proposée).
F. La solution proposée utilise les principes des méthodes de gestion des risques en intrants et, comme les autres projets similaires, elle vise une intégration au cycle de développement du logiciel.

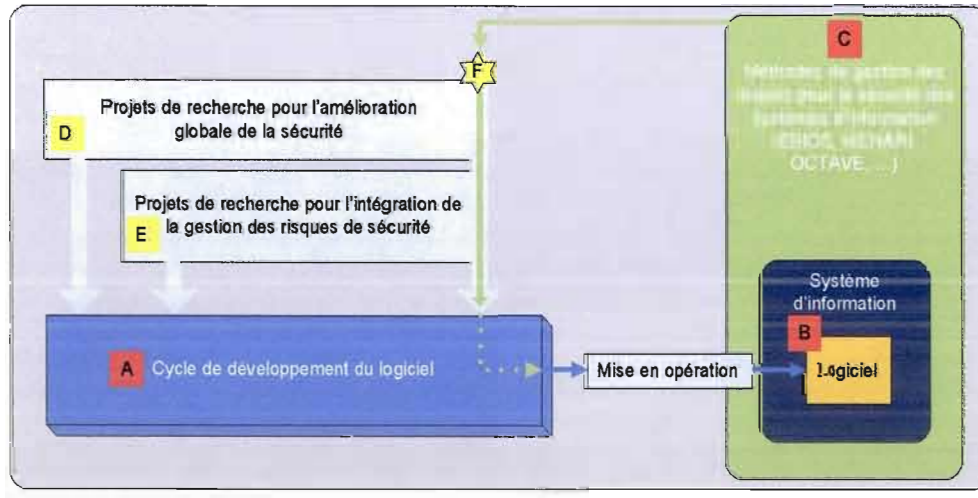

Figure 3.1 Positionnement de la solution proposée.

3.4 Les référentiels pour la démarche analytique

Étant donné l'étendue des publications reliées aux domaines de la gestion des risques de sécurité et du développement logiciel, cette section précise les référentiels qui seront utilisés pour les représenter dans le cadre de la démarche analytique et les critères qui ont favorisé leur sélection. Il est à noter que les choix entourant ces publications de référence n'ont pas fait l'objet d'une recherche exhaustive, mais qu'ils ont été effectués en considérant tout de même les options les plus connues de leur domaine respectif.

3.4.1 La sélection d'un modèle de cycle de développement du logiciel

Pour réaliser la démarche analytique, il est nécessaire de se baser sur des informations détaillées concernant les étapes effectuées dans un cycle de développement du logiciel. Par conséquent, la sélection d'un modèle de référence s'avère indispensable et vise principalement à répondre aux critères suivants :

a. Avoir une certaine notoriété dans le milieu du développement logiciel;
b. Offrir une documentation adéquate des étapes et des activités à réaliser;
c. Être encore d'actualité et être utilisable dans la plupart des projets de développement logiciel;
d. Considérer de façon importante les besoins d'affaires des clients;
e. Correspondre aux concepts de base du développement logiciel présentés dans le premier chapitre.

En considérant ces différents critères de sélection, le modèle du Processus Unifié [17] a été retenu pour les raisons suivantes :

- Il est éprouvé[a], fortement documenté[b] et reconnu dans le domaine du développement logiciel pour ses principes de base solides[a].
- Il prône un développement itératif et incrémental[e], des notions très valorisées actuellement dans le domaine[c]. Il est donc plus souple que les modèles classiques (en cascade, en V) et, de plus, il incorpore des principes véhiculés dans les méthodes AGILE[c].
- Il est piloté par les cas d'utilisation[d] et la diminution des risques de projet.
- Il donne de l'importance à la qualité ainsi qu'à la gestion des besoins[d] et des exigences.

- Il ne vise pas les besoins d'un secteur d'activité particulier ni une taille d'entreprise précise pour son utilisation[c].

La notoriété de ce modèle de développement logiciel a largement contribué à sa sélection pour le contexte de la présente recherche, parce que ses principes sont aujourd'hui très connus et ont été utilisés comme modèle de base pour plusieurs autres modèles : Rational Unified Process (RUP), Enterprise Unified Process (EUP), Agile Unified Process (AUP), Basic Unified Process (BUP), Essential Unified Process (EssUP) et Open Unified Process (OpenUP). Le Processus Unifié est complet dans le sens où il correspond bien à l'ensemble des principes véhiculés dans le domaine du développement logiciel, ce qui n'est pas nécessairement le cas pour d'autres modèles. L'utilisation d'un modèle qui serait « théoriquement » moins complet aurait amené des difficultés supplémentaires dans le cadre de cette recherche. Encore une fois, le but ici n'est pas d'établir des comparaisons entre les modèles prônés pour le développement logiciel, mais bien d'en sélectionner un répondant à l'ensemble des principes du domaine. Puisqu'une connaissance plus approfondie de ce modèle sera nécessaire pour réaliser la démarche analytique, une section complète détaille le Processus Unifié dans le quatrième chapitre.

3.4.2 La sélection des méthodes de gestion des risques

Bien qu'il existe un très grand nombre de méthodes pour la gestion des risques, le choix s'est arrêté plus précisément sur quelques-unes d'entre elles. La sélection visait à retenir trois méthodes, utilisées dans des contextes réels d'entreprise, pour représenter les concepts généraux de la gestion des risques. Le fait de combiner l'étude de trois méthodes différentes vise à donner une perspective plus générale des activités de sécurité à prendre en compte dans la gestion des risques, ce qui n'aurait pas été le cas si une seule méthode avait été considérée pour représenter cette approche. Voici les critères principaux qui ont servi à la sélection de ces trois méthodes :

a. **Leur disponibilité** : que la documentation de la méthode soit disponible facilement;
b. **Leur prix** : que l'obtention de la méthode soit gratuite;
c. **Leur langue** : que la documentation de la méthode soit écrite en langue française ou anglaise;
d. **Leur utilisation** : que la méthode soit citée comme référence en la matière dans plusieurs articles traitant du domaine.

À partir de ces exigences, les méthodes retenues pour la recherche ont été EBIOS, MEHARI et OCTAVE. Les informations relatives à chacune d'entre elles quant aux critères établis sont les suivantes :

- **EBIOS** : **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité [18]
    a. Téléchargement sur le site Web de l'agence française DCSSI
    b. Gratuite
    c. Française
    d. [7] [8] [19] [20] [21] [22]

- **MEHARI** : **M**éthode **H**armonisée d'**A**nalyse des **R**isques [23]
    a. Téléchargement sur le site Web du CLUSIF
    b. Gratuite
    c. Française
    d. [7] [8] [19] [20] [21]

- **OCTAVE** : The **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation [24]
    a. Téléchargement sur le site Web du Carnegie Mellon University's Computer Emergency Response Team (CERT)
    b. Gratuite
    c. Anglaise
    d. [7] [8] [19] [20] [21] [22] [25]

Fait à noter, les trois méthodes sont issues d'origines différentes : EBIOS du milieu gouvernemental, MEHARI d'un regroupement professionnel de sociétés et OCTAVE, d'un milieu universitaire. Tout comme dans le cas du modèle de cycle de développement du logiciel, les détails de ces méthodes sont nécessaires pour réaliser la démarche analytique et sont décrits plus précisément dans le quatrième chapitre.

3.5 Le déroulement de la démarche analytique

Cette section décrit la stratégie entreprise pour mener à bien la démarche analytique et, ensuite, permettre la réalisation d'une synthèse des résultats. Le déroulement global de la démarche analytique se découpe en trois grandes étapes que voici :

- **Étape 1** : L'identification des activités générales des méthodes de gestion des risques;
- **Étape 2** : La présentation du contexte du cycle de développement du logiciel;

- **Étape 3** : L'intégration des activités générales de la gestion des risques dans un contexte de cycle de développement du logiciel.

Les tableaux 3.1, 3.2 et 3.3 décrivent ces étapes en précisant pour chacune d'elles, l'objectif général à atteindre, les mesures concrètes visées, les intrants informationnels nécessaires, les tâches à réaliser et les extrants informationnels produits.

Tableau 3.1
Détails de l'étape 1 de la démarche analytique

Étape 1 : L'identification des activités générales des méthodes de gestion des risques	
Objectif :	Procéder à l'étude de méthodes de gestion des risques pour identifier les activités générales qu'elles véhiculent.
Mesure(s) :	✓ Identifier la liste des activités de sécurité proposées dans chacune des méthodes étudiées. ✓ Positionner chacune des méthodes par rapport aux étapes générales de la gestion des risques présentés dans le deuxième chapitre. ✓ Positionner chacune des activités de sécurité identifiées par rapport aux étapes générales de la gestion des risques présentées dans le deuxième chapitre. ✓ Dresser une liste des activités générales de la gestion des risques à partir uniquement des activités de sécurité identifiées dans les méthodes étudiées. ✓ Identifier les dépendances existantes entre les différentes activités générales de la gestion des risques.
Intrant(s) :	✓ E1.IN1 – Documents officiels sur la méthode EBIOS. ✓ E1.IN2 – Documents officiels sur la méthode MEHARI. ✓ E1.IN3 – Documents officiels sur la méthode OCTAVE.
Tâche(s) à réaliser :	

N°	Tâches	Intrants	Extrants
1	Analyser les documents relatifs à EBIOS et résumer les activités de base de la méthode.	E1.IN1	E1.EX1
2	Analyser les documents relatifs à MEHARI et résumer les activités de base de la méthode.	E1.IN2	E1.EX2
3	Analyser les documents relatifs à OCTAVE et	E1.IN3	E1.EX3

		résumer les activités de base de la méthode.		
	4	Synthétiser, par méthode, les activités de base qu'elles proposent.	E1.EX1 E1.EX2 E1.EX3	E1.EX4
	5	Produire une liste des activités générales des méthodes de gestion des risques.	E1.EX4	E1.EX5
Extrant(s) :	▪ E1.EX1 – La description des activités de base de la méthode MEHARI. ▪ E1.EX2 – La description des activités de base de la méthode EBIOS. ▪ E1.EX3 – La description des activités de base de la méthode OCTAVE. ▪ E1.EX4 – La synthèse, par méthode, de leurs activités de base. ▪ E1.EX5 – La liste des activités générales de la gestion des risques.			

Tableau 3.2
Détails de l'étape 2 de la démarche analytique

Étape 2 : La présentation du contexte du cycle de développement du logiciel				
Objectif :	Procéder à l'étude d'une méthode de cycle de développement du logiciel pour en identifier les étapes et les activités qui y sont réalisées.			
Mesure(s) :	▪ Détailler les étapes réalisées dans un cycle de développement du logiciel telles que définies par le Processus Unifié.			
Intrant(s) :	▪ E2.IN1 – Livre officiel des auteurs du Processus Unifié. ▪ E2.IN2 – Documents généraux traitant du cycle de développement du logiciel selon le Processus Unifié.			
Tâche(s) à réaliser :		**N°**	**Tâches**	**Intrants**	**Extrants**
		1	Décrire les étapes du cycle de développement du logiciel du Processus Unifié en précisant pour chacune d'elles les objectifs visés, la nature des travaux effectués et les principaux livrables produits.	E2.IN1 E2.IN2	E2.EX1
Extrant(s) :	▪ E2.EX1 – La description des étapes du Processus Unifié.			

Tableau 3.3
Détails de l'étape 3 de la démarche analytique

<table>
<tr><th colspan="2">Étape 3 : L'intégration des activités générales de la gestion des risques dans un contexte de cycle de développement du logiciel</th></tr>
<tr><td>Objectif :</td><td>Démontrer que les activités générales de la gestion des risques peuvent être intégrées dans les étapes du cycle de développement du logiciel.</td></tr>
<tr><td>Mesure(s) :</td><td>▪ Intégrer toutes les activités générales de gestion des risques dans le cycle de développement du logiciel.
▪ Identifier les activités de sécurité qui sont concrètement liées à une activité du cycle de développement du logiciel par rapport à celles qui le sont par l'intermédiaire d'une autre activité de sécurité intégrée.</td></tr>
<tr><td>Intrant(s) :</td><td>▪ E1.EX5 – La liste des activités générales de la gestion des risques.
▪ E2.EX1 – La description des étapes du Processus Unifié.</td></tr>
<tr><td>Tâche(s) à réaliser :</td><td>
<table>
<tr><th>N°</th><th>Tâches</th><th>Intrants</th><th>Extrants</th></tr>
<tr><td>1</td><td>Pour chacune des activités identifiées dans la liste des activités générales de la gestion des risques, démontrer leur intégration aux étapes du cycle de développement du logiciel en identifiant et en justifiant le point d'encrage possible (une activité du développement logiciel ou une activité de gestion des risques intégrée préalablement).</td><td>E1.EX5
E2.EX1</td><td>E3.EX1</td></tr>
</table>
</td></tr>
<tr><td>Extrant(s) :</td><td>▪ E3.EX1 - Les résultats de l'intégration des activités générales de la gestion des risques dans le Processus Unifié.</td></tr>
</table>

En conclusion, les éléments énoncés dans ce troisième chapitre servent d'indicateurs de base pour encadrer l'activité de recherche présentée dans ce document. La problématique visée et la solution proposée pour l'atténuer ont tout d'abord été énoncées. Ensuite, la solution proposée fut positionnée par rapport aux autres publications ou projets de recherche similaires. Puis, les publications de référence et les détails entourant les grandes étapes du déroulement de la démarche

analytique ont été spécifiés. Les résultats obtenus par la démarche analytique seront ensuite transportés au cinquième chapitre pour la synthèse des résultats. Son objectif sera de présenter les résultats de façon globale, de manière à pouvoir confirmer ou infirmer l'hypothèse principale émise concernant la solution proposée.

Ce troisième chapitre visait à établir les fondements de la recherche et, par le fait même, à faire le lien entre les chapitres qui ont introduit les sujets importants et ceux qui les élaboreront pour les fins de la démarche. Le prochain chapitre constitue le point central de ce document, c'est-à-dire la démarche analytique de la recherche.

CHAPITRE IV

LA DÉMARCHE ANALYTIQUE

Après avoir présenté sommairement les concepts du cycle de développement du logiciel et de la gestion des risques, le quatrième chapitre a pour but de démontrer les relations possibles entre ces deux domaines, et ce, en considérant la portée de la démarche analytique telle que définie au troisième chapitre. Les différentes sections de ce chapitre visent à atteindre cet objectif en présentant graduellement les résultats obtenus durant la démarche, permettant ainsi d'en établir les conclusions nécessaires par la suite.

La première section traite des notions de gestion des risques en détaillant tout d'abord les activités de sécurité prônées dans les méthodes de gestion des risques sélectionnées et, ensuite, les analyser afin de produire une liste intégrée des activités générales de la gestion des risques. La deuxième section présente plus en détail les étapes réalisées dans un modèle de cycle de développement du logiciel afin d'y exposer plus clairement les activités réalisées et leurs objectifs. Quant à la troisième section, elle démontre l'intégration de chacune des activités générales de la gestion des risques (les résultats de la première section) à travers les étapes du cycle de développement du logiciel (résultats de la deuxième section).

Dans l'ensemble de ce document, le rôle de ce chapitre consiste à mettre en relation, par une démarche analytique, les informations présentées dans les chapitres précédents. Le résultat global de cette démarche et les conclusions à tirer feront l'objet d'un sommaire dans le chapitre suivant.

4.1 **Étape 1 :** L'identification des activités générales des méthodes de gestion des risques

Cette première étape de la démarche analytique se divise en trois parties. La première consiste à faire l'étude des trois méthodes de gestions de risques sélectionnées pour la recherche. La deuxième vise à extraire de cette étude une liste précise des activités de sécurité réalisées dans chacune des trois démarches analysées. La troisième et dernière reprend cette liste pour en bâtir une seconde contenant les activités générales de la gestion de risques qui sera utilisée par la suite dans la démarche. Cette seconde liste représente donc le résultat final de cette première étape.

Une description plus approfondie des méthodes EBIOS, MEHARI et OCTAVE permettra de comprendre plus précisément l'application de ces méthodes afin d'en extraire les principales activités de gestion des risques. Il est à noter que le vocabulaire utilisé pour décrire les méthodes est celui employé dans les publications officielles. Ensuite, les activités de sécurité qui ont été décrites pour chacune des méthodes seront extraites et résumées sous la forme de tableaux. La dernière partie consiste à dresser une liste des activités générales de la gestion des risques. Elle sera créée d'abord en regroupant toutes les activités de sécurité en fonction des étapes de la gestion des risques présentées au deuxième chapitre, ensuite en fusionnant les activités représentant les mêmes concepts et, pour terminer, en définissant des activités générales les représentant et dont le titre et la description utiliseront des termes génériques du domaine. Cette liste des activités générales de la gestion des risques représente l'intrant de base nécessaire à la réalisation de l'étape 3 de la démarche analytique.

4.1.1 Description des méthodes de gestion des risques

La méthode EBIOS (Expression des **B**esoins et **I**dentification des **O**bjectifs de Sécurité) [18, 19, 20] :

Produite par l'agence française DCSSI (Direction centrale de la sécurité des systèmes d'information), la méthode EBIOS fut créée en 1995 et la deuxième version, la plus récente, date de 2004.

L'objectif principal de cette méthode consiste à identifier les besoins et les objectifs de sécurité au moment de l'étape de spécification des besoins d'un système. Puisque la majeure partie des efforts de spécification s'effectue au début d'un projet, la méthode convient parfaitement pour la

conception d'un nouveau système. Toutefois, elle peut également être utilisée pour un système existant.

La méthode EBIOS est compatible avec les normes de sécurité ISO/IEC 15408 (*Critères d'évaluation de la sécurité des technologies de l'information*) et ISO/IEC 27002 (*Code de bonne pratique pour la gestion de la sécurité de l'information*), ce qui lui accorde une certaine cote de crédibilité. Le support matériel est composé d'un guide divisé en cinq sections et d'un logiciel supportant l'application de la démarche.

Du point de vue méthodologique, EBIOS traite des éléments de base de la gestion des risques tels les actifs importants, les menaces, les vulnérabilités et les risques. L'importance donnée aux résultats qui découlent de la réalisation de la méthode relève de la décision des parties prenantes de l'entreprise, puisque les objectifs de celle-ci, en matière de sécurité informatique, représentent un facteur décisionnel important pour le traitement final à appliquer aux risques identifiés.

La méthode présente cinq étapes à suivre. À noter que les étapes 2 et 3 peuvent être effectuées parallèlement :

1. **L'étude du contexte**
2. **L'expression des besoins de sécurité**
3. **L'étude des menaces**
4. **L'identification des objectifs de sécurité**
5. **La détermination des exigences de sécurité**

Afin de comprendre les aspects importants de cette méthode, les nombreuses activités réalisées au cours de ces étapes sont présentées plus en détail dans cette section.

Étape 1 : Étude du contexte. La réalisation de cette étape s'effectue par l'exécution des trois activités suivantes :

Étude de l'organisme. Cette activité permet d'obtenir une vision générale de l'entreprise permettant ainsi de définir adéquatement l'environnement où le système d'information est en opération.

Pour réaliser cette activité, il est essentiel de débuter par la présentation des caractéristiques de l'entreprise : la nature de ses activités, ses valeurs, sa structure, etc. Ensuite viennent les contraintes (budgétaires, de ressources, territoriales, etc.) dont l'entreprise doit tenir compte ainsi que les références réglementaires (lois et règlements) auxquelles elle est assujettie. Pour terminer, il faut donner une description sommaire des environnements fonctionnels en lien avec celui où le système-cible est ou sera en opération.

Étude du système-cible. Cette activité permet de présenter, de manière plus détaillée, le contexte d'utilisation du système informatique ciblé par la démarche.

Pour réaliser cette activité, l'étude doit débuter par une présentation sommaire du système-cible, en énonçant sa portée, son rôle, ses relations avec les autres environnements du système d'information, etc. Par la suite, des renseignements supplémentaires, considérés importants, doivent être fournis sur ce qui est en lien avec le système-cible tels : les enjeux, les éléments essentiels (fonctions, informations et processus), les fonctions du système (traitements et informations d'entrée et de sortie), les hypothèses, les règles de sécurité (formalisées ou non), les contraintes (contrôlables ou non) et les références réglementaires.

Détermination de la cible de l'étude de sécurité. Cette activité permet de spécifier les entités qui utilisent les éléments essentiels du système-cible.

Pour réaliser cette activité, une identification et une description des différentes entités du système-cible (l'entreprise elle-même, un site, le personnel, le matériel, le réseau, un logiciel, etc.) doivent être produites, puisqu'elles sont enclines à être exploitées à cause de leurs interactions avec les éléments essentiels du système-cible. Puis, il faut documenter cette interaction en énonçant les liens spécifiques qui existent entre les entités et les éléments essentiels utilisés.

Étape 2 : Expression des besoins de sécurité. La réalisation de cette étape s'effectue par l'exécution des deux activités suivantes :

Réalisation des fiches de besoins. Cette activité permet de définir les outils nécessaires pour permettre aux utilisateurs d'exprimer et de justifier les besoins en matière de sécurité pour tous les éléments essentiels.

Pour réaliser cette activité, la première chose à faire consiste à déterminer les critères de sécurité qui seront utilisés pour exprimer les besoins. Les critères « disponibilité », « intégrité » et « confidentialité » sont couramment utilisés, mais tout autre critère peut également être choisi. Par la suite, une échelle de valeurs doit être définie pour représenter les différents degrés dans l'expression des besoins pour chacun de ces critères. Pour conclure, une liste d'impacts qui seraient significatifs pour le contexte de l'entreprise est établie. À partir de ce moment, il est possible de créer les fiches d'expression de besoins qui seront utilisées lors de l'activité suivante de la présente étape. Une fiche est remplie pour chaque élément essentiel et contient un tableau permettant d'indiquer, pour chacun des impacts identifiés et par rapport à chacun des critères de sécurité, une valeur en terme de besoin de sécurité à l'aide de l'échelle de valeurs préalablement définie.

Synthèse des besoins de sécurité. Cette activité permet de recueillir les besoins de sécurité des éléments essentiels auprès des utilisateurs par l'usage des fiches de besoins.

Pour réaliser cette activité, il faut réunir un groupe d'utilisateurs connaissant bien les tâches effectuées avec le système-cible et le guider dans l'utilisation des outils d'évaluation (critères et échelles) des besoins de sécurité. Par le biais des fiches de besoins rédigées pour chacun des éléments essentiels, les utilisateurs pourront établir le besoin de sécurité nécessaire pour chacun des critères de sécurité par rapport à chacun des impacts identifiés. Lorsque toutes les fiches sont complétées, un tableau de synthèse des besoins regroupera les valeurs les plus élevées pour chacun des critères de sécurité en lien avec chaque élément essentiel.

Étape 3 : Étude des menaces. La réalisation de cette étape s'effectue par l'exécution des trois activités suivantes :

Étude des origines des menaces. Cette activité permet d'identifier les méthodes d'attaque et leur origine (les éléments menaçants) dans le contexte où ceux-ci s'avéreraient de réelles menaces envers les entités du système-cible.

Pour réaliser cette activité, il s'agit d'identifier une liste de méthodes d'attaque pertinentes, donc plausibles, et qui peuvent générer des impacts pour le système-cible. Pour chacune de ces méthodes, il importe de préciser les critères de sécurité qui sont affectés directement et les éléments menaçants qui sont susceptibles d'entreprendre l'attaque. De

plus, les éléments menaçants doivent être documentés en spécifiant leur type, leur cause et leur potentiel d'attaque. Il convient aussi d'énumérer et de justifier les méthodes d'attaque qui pourraient générer des risques pour l'entreprise, mais qui ne seront pas retenus dans le cadre de cette étude.

Étude des vulnérabilités. Cette activité permet d'identifier les faiblesses de sécurité du système- cible qui pourraient être exploitées par une menace.

Pour réaliser cette activité, il faut établir les vulnérabilités des entités du système-cible qui pourraient être exploitées par chacune des méthodes d'attaque sélectionnées à l'activité précédente. Par la suite, une estimation du niveau de vulnérabilité, en utilisant une échelle de valeurs sur la possibilité de réalisation, doit être déterminée pour chacune des vulnérabilités sélectionnées.

Formalisation des menaces. Cette activité permet d'identifier les menaces réelles à considérer dans l'étude de sécurité.

Pour réaliser cette activité, une liste des menaces pouvant avoir des impacts sur le système-cible doit être élaborée. Une menace est déterminée en spécifiant les informations suivantes : l'élément menaçant ainsi que son potentiel d'attaque, la méthode d'attaque utilisée, les critères de sécurité affectés, les vulnérabilités exploitables avec leur niveau de possibilité de réalisation et les entités reliées à ces vulnérabilités. Chacune des menaces peut ensuite être évaluée en déterminant sa valeur d'opportunité, qui représente le degré de circonstance favorable à se réaliser, à partir des niveaux de possibilité de réalisation estimés pour les vulnérabilités qui lui sont associées. La valeur d'opportunité permettra alors d'effectuer une hiérarchisation des menaces afin d'en faire ressortir les plus importantes.

Étape 4 : Identification des objectifs de sécurité. La réalisation de cette étape s'effectue par l'exécution des trois activités suivantes :

Confrontation des menaces aux besoins. Cette activité permet d'identifier les risques de sécurité réels pour le système-cible.

Pour réaliser cette activité, les besoins de sécurité qui ont été exprimés pour chacun des éléments essentiels doivent être pris en compte et confrontés aux menaces identifiées.

Pour cela, les critères de sécurité seront utilisés pour faire cette comparaison, puisqu'ils ont été utilisés à la fois dans la description des besoins de sécurité désirés et dans la description des menaces. Un risque est alors formulé en spécifiant toutes les informations relatives au besoin de sécurité en question et en précisant la menace concernée. Ensuite, il est possible de hiérarchiser la liste des risques selon leur impact sur les éléments essentiels et l'opportunité des menaces. Donc, si des risques présentant des valeurs faibles sont écartés de l'étude, il est important de les noter et de justifier ces décisions.

Formalisation des objectifs de sécurité. Cette activité permet de définir les objectifs de sécurité nécessaires pour satisfaire tous les risques identifiés et retenus, sans toutefois élaborer sur les solutions à mettre en œuvre pour y parvenir.

Pour réaliser cette activité, une liste d'objectifs de sécurité souhaitable à entreprendre doit être établie tout en tenant compte des hypothèses, des règles de sécurité, des contraintes et des références réglementaires qui ont été identifiées lors de l'étude du système-cible. Un objectif de sécurité traite un risque en s'attaquant à l'une de ses trois composantes : l'origine de la menace (éléments menaçants et méthodes d'attaque), les vulnérabilités exploitées ou les conséquences (éléments essentiels et impacts). Ensuite, une vérification de chacun des points à traiter (les risques, les hypothèses, les règles de sécurité et les références réglementaires) est effectuée pour vérifier si chacun d'eux est couvert par les objectifs de sécurité sélectionnés. Leur niveau de couverture doit être spécifié en indiquant s'il est nul, partiel ou complet. Une seconde vérification consiste à démontrer que chacun des objectifs de sécurité sélectionnés est relié à au moins un des points à traiter. Puis, les objectifs de sécurité sélectionnés sont classés en deux catégories, soit les objectifs reliés directement au système-cible et ceux reliés à son environnement. Pour finir, si un point à traiter n'est pas couvert par un objectif de sécurité ou qu'il l'est partiellement (niveau de couverture nul ou partiel), cela doit être noté et justifié.

Détermination des niveaux de sécurité. Cette activité permet d'identifier le niveau de résistance de sécurité nécessaire à appliquer pour chacun des objectifs de sécurité ainsi que le niveau des exigences d'assurance désiré, celles-ci indiquant le degré de rigueur dans la mise en œuvre des objectifs.

Pour réaliser cette activité, il s'agit de déterminer le niveau de résistance nécessaire pour que chacun des objectifs de sécurité s'oppose adéquatement à l'élément menaçant.

Cette valeur représente un indicateur de qualité nécessaire dans la mise en œuvre de l'objectif de sécurité et est déterminée par la valeur du plus haut potentiel d'attaque des risques couverts par l'objectif en question. Dans le cas où il est décidé de mettre un niveau de résistance inférieur à ce qu'il doit être, cette décision doit être justifiée. De plus, il faut déterminer un niveau d'assurance pour le déploiement des objectifs de sécurité. Ce degré de rigueur concerne principalement les efforts à invertir dans les tests et les vérifications lors du processus de déploiement des objectifs de sécurité.

Étape 5 : Détermination des exigences de sécurité. La réalisation de cette étape s'effectue par l'exécution des deux activités suivantes :

Détermination des exigences de sécurité fonctionnelles. Cette activité permet d'identifier les exigences de sécurité fonctionnelles à effectuer pour satisfaire chacun des objectifs de sécurité déterminés à l'étape précédente.

Pour réaliser cette activité, les exigences de sécurité fonctionnelles sont tout d'abord identifiées. Il s'agit des moyens précis à implanter afin d'atteindre les objectifs de sécurité prévus. Une exigence fonctionnelle doit prendre en considération les contraintes budgétaires et techniques de l'entreprise et doit avoir comme objectif principal de traiter les risques de manière à les réduire, à les refuser, à les transférer ou à les accepter. Après, il s'agit de démontrer que tous les objectifs de sécurité sont couverts par ces exigences fonctionnelles, en spécifiant le niveau de couverture (nul, partiel ou complet) duquel le niveau de résistance fait partie. Il faut aussi démontrer que chaque exigence fonctionnelle correspond au moins à un objectif de sécurité. S'il est décidé que certains objectifs de sécurité ne seront pas couverts par une exigence fonctionnelle ou bien qu'ils le seront partiellement (niveau de couverture nul ou partiel), ces choix doivent alors être énumérés et justifiés. Ensuite, selon le même principe que les objectifs de sécurité, les exigences fonctionnelles sélectionnées sont classées en deux catégories, soit les objectifs reliés directement au système-cible et ceux reliés à son environnement. Pour terminer, il s'avère important de documenter les dépendances, si existantes, entre les exigences de sécurité fonctionnelles sélectionnées à mettre en œuvre.

Détermination des exigences de sécurité d'assurance. Cette activité permet d'identifier les exigences de sécurité d'assurance afin de satisfaire le niveau d'assurance choisi lors de l'activité de détermination des niveaux de sécurité.

Pour réaliser cette activité, il faut identifier les exigences qui sont de nature à assurer la confiance dans la conformité du déploiement des exigences fonctionnelles et dans l'efficacité de répondre réellement aux besoins de sécurité identifiés. Si les exigences n'atteignent pas le niveau requis, cela doit être noté et justifié. Ensuite, les exigences d'assurance sélectionnées sont classées en deux catégories, soit les objectifs reliés directement au système-cible et ceux reliés à son environnement. Pour finir, les dépendances qu'il pourrait y avoir entre une exigence d'assurance et toute autre exigence sont identifiées et justifiées.

Les documents tels que le schéma directeur de l'entreprise, la politique de sécurité ou les spécifications du système s'avèrent de bonnes sources d'information pour commencer une démarche EBIOS. Durant le déroulement de celle-ci et lorsqu'elle est complétée, il est possible de créer plusieurs documents relatifs à la sécurité comme : un schéma directeur ou un plan d'actions de la sécurité des systèmes d'information, une fiche d'expression rationnelle des objectifs de sécurité (un FEROS), et tout autre rapport concernant les informations cumulées durant la démarche. EBIOS permet donc de prioriser la sécurité informatique très tôt dans un projet de développement ou de vérification d'un système informatique, donnant aux entreprises la possibilité d'exprimer clairement leur volonté à considérer les risques de sécurité informatique.

L'étude de cette méthode démontre des similarités avec l'objectif principal de la présente recherche qui est d'utiliser la gestion des risques de sécurité pour le domaine du logiciel. Toutefois, la méthode EBIOS n'est pas directement adaptée aux étapes du cycle de développement du logiciel comparativement à la solution proposée dans la présente recherche. Il faut aussi noter que, comparativement aux autres méthodes étudiées, la méthode *EBIOS* met davantage l'accent sur des activités permettant une définition précise du contexte de la cible et de son environnement. En ce qui a trait aux phases et aux étapes de la gestion des risques démontrées dans le deuxième chapitre, cette méthode de gestion des risques vise principalement la phase de l'analyse de risques, mais plus particulièrement les étapes 1 à 6 comme démontré dans la figure 4.1 :

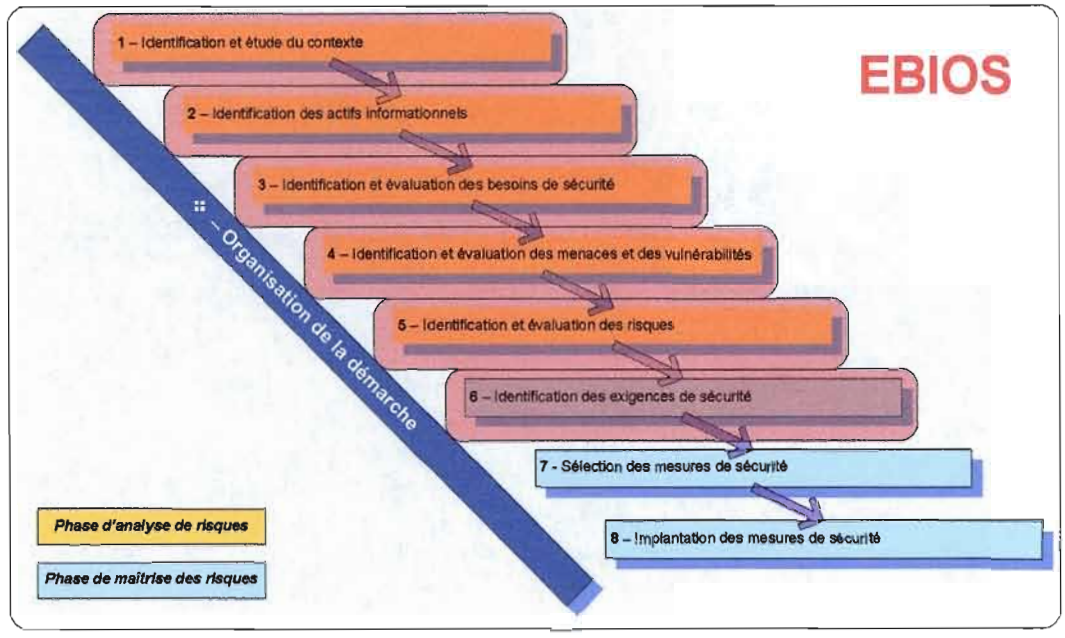

Figure 4.1 Positionnement de la méthode EBIOS par rapport aux étapes de la gestion des risques.

Les différentes activités de sécurité réalisées dans la méthode EBIOS seront positionnées par rapport aux étapes générales de la gestion des risques lorsqu'il sera question de les regrouper afin de bâtir la liste des activités générales de la gestion des risques.

La méthode MEHARI (Méthode Harmonisée d'Analyse des Risques) [19, 23] :

MEHARI est la toute dernière méthode produite par le CLUSIF (Club de la Sécurité de l'information Français). Sa réalisation découle directement de ses consœurs MARION et MELISA. MARION est une méthode d'audit visant à évaluer le niveau de sécurité informatique d'une entreprise, tandis que MELISA est une méthode d'analyse de risques en fonction de l'évaluation des vulnérabilités. La première version de MEHARI fut proposée en 1996, et la plus récente version date de 2007.

Son objectif principal est la conduite d'une démarche d'analyse de risques et la réduction de leur niveau par l'identification des contre-mesures appropriées. En plus de sa démarche d'analyse de risques reconnue sur le marché, la méthode présente plusieurs outils pour une gestion globale de la

sécurité. Ces outils permettent aux entreprises d'obtenir les indicateurs voulus en ce qui a trait à leur gestion des risques et à l'état actuel de leur sécurité informatique.

Dans les nombreuses activités de sécurité présentées par la méthode, il y a notamment l'expression des besoins de sécurité par une identification des dysfonctionnements ou une catégorisation des actifs. Il y a aussi l'audit de sécurité dont les éléments à contrôler ont une certaine concordance avec les mesures de sécurité définies dans la norme ISO/CEI 27002 – *Code de bonne pratique pour la gestion de la sécurité de l'information*. La méthode est composée de plusieurs guides, d'exemples d'utilisation et de documents représentant des bases de connaissance. Le logiciel commercial RISICARE permet de supporter la démarche et d'offrir plusieurs automatismes pour faciliter les calculs à effectuer durant son application.)

La méthode n'impose pas une démarche précise, mais plutôt une démarche composée d'actions de sécurité soutirées de trois modules. Le choix de ces actions dépendra des besoins de l'entreprise et de différents facteurs qui la caractérisent comme son contexte d'activités, sa taille, sa culture en sécurité informatique et son mode de gestion. Ainsi, il est essentiel que l'entreprise détermine bien les objectifs de sécurité qu'elle vise avant de se lancer dans une démarche MEHARI. Ses trois modules de sécurité sont les suivants :

Module 1 : L'analyse des enjeux de la sécurité et de la classification des informations et ressources
Module 2 : Le diagnostic de l'état des services de sécurité
Module 3 : L'analyse de situations de risque

Ces trois modules sont composés de différentes activités de sécurité à réaliser pour atteindre les objectifs de la méthode et sont présentées plus en détail dans cette section. Puisque la méthode MEHARI présente une démarche permettant la réalisation de ces modules de manière indépendante et non de façon globale et linéaire, une brève conclusion sera donnée à la fin de chacun de ces modules en lien avec l'utilisation possible des éléments produits. Il faut cependant noter que le module 3, celui de l'analyse de situations de risque, peut utiliser les résultats des travaux effectués dans les modules 1 et 2 durant sa propre démarche si ces deux modules ont été réalisés préalablement.

Module 1 : L'analyse des enjeux de la sécurité et de la classification des informations et ressources. Le but de ce module est d'identifier les événements redoutés et leurs

conséquences en se basant sur ce que les employés connaissent de l'entreprise et de la valeur des actifs informationnels utilisés.

Étape 1.1 : L'échelle de valeurs des dysfonctionnements. Cette étape requiert la réalisation des quatre activités suivantes :

Identification des activités majeures et de leurs finalités. Cette activité vise à identifier les activités de l'entreprise qui sont ciblées pour l'étude.

Pour mener à bien cette activité, il s'agit de répertorier les activités importantes du domaine ciblé pour l'étude et qui sont supportées par différents processus de l'entreprise. Les informations recueillies sont présentées sous la forme de fonctionnalités par une brève description ainsi que leur finalité attendue.

Identification des dysfonctionnements redoutés. Cette activité vise à déterminer les mauvais fonctionnements qui pourraient survenir dans les activités de l'entreprise.

Pour mener à bien cette activité, une recherche est effectuée pour identifier les dysfonctionnements redoutés dans les activités de l'entreprise. Les dysfonctionnements peuvent être de nature fonctionnelle ou technique. Les dysfonctionnements fonctionnels concernent principalement ce qui pourrait affecter le déroulement des processus de l'entreprise comme des tâches qui ne sont pas effectuées dans les délais prévus ou des tâches effectuées de manière non conforme à ce qui est défini. Quant aux dysfonctionnements techniques, il s'agit de ceux qui pourraient affecter la mise en œuvre des moyens nécessaires pour supporter les activités de l'entreprise comme les moyens matériels (locaux, équipements, serveurs informatiques, etc.), les moyens non matériels (données informatiques, programmes informatiques, etc.) ou les moyens en personnel (personne indispensable).

Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés. Cette activité vise à déterminer la gravité des dysfonctionnements identifiés.

Pour mener à bien cette activité, il faut déterminer les niveaux de gravité des dysfonctionnements identifiés à l'étape précédente à l'aide d'une échelle de valeurs. Cette échelle doit présenter un nombre précis de niveaux de gravité et doit également préciser les

critères de criticité et les seuils correspondants afin d'indiquer le moment où il faut passer d'un niveau à un autre. Le niveau de gravité d'un dysfonctionnement est donc déterminé à l'aide de cette échelle à partir du critère de criticité et du seuil adéquat pour le dysfonctionnement en question.

Échelle de valeurs des dysfonctionnements. Cette activité vise à synthétiser les travaux effectués à l'*Étape 1.1* par la présentation des informations entourant les événements que l'entreprise peut redouter.

Pour mener à bien cette activité, il s'agit de consolider les travaux d'analyse effectués en les présentant par activité de l'entreprise. Les niveaux de gravité établis et leurs paramètres seront énoncés pour chacune des activités de l'entreprise en fonction de chaque dysfonctionnement redouté. De plus, l'échelle de valeurs des dysfonctionnements doit nécessairement faire l'objet d'un consensus de la part des dirigeants de l'entreprise sur les valeurs qu'elle présente.

Étape 1.2 : La classification des informations et ressources du système d'information. Cette étape requiert la réalisation des trois activités suivantes :

Identification des éléments à classifier. Cette activité vise à identifier les éléments qui doivent faire l'objet d'une classification.

Pour mener à bien cette activité, les éléments à classifier peuvent être répertoriés en considérant les ressources utilisées par chaque processus ou activité de l'entreprise, par les services communs ou par l'architecture technologique partagée dans l'entreprise. Pour faciliter le travail, il est courant d'effectuer des regroupements de ressources similaires afin de ne pas avoir à traiter un trop grand nombre d'éléments.

Critères de classification. Cette activité vise à déterminer les critères de sécurité utilisés pour la classification des informations et des ressources du système d'information.

Pour mener à bien cette activité, il faut établir les critères de sécurité à utiliser dans le cadre de l'activité de classification. Ces critères font couramment référence à la disponibilité, à l'intégrité et à la confidentialité, mais d'autres critères peuvent également être considérés selon les besoins de l'entreprise.

Processus de classification. Cette activité vise à classifier chacun des éléments identifiés selon les critères de classification établis.

Pour mener à bien cette activité, l'objectif consiste à déterminer, à l'aide d'échelles de valeurs, le niveau d'impact qu'occasionnerait le non-respect de chacun des critères de sécurité sur les éléments identifiés s'il advenait que les dysfonctionnements redoutés se réalisent. Le tableau final de la classification présente donc la sensibilité de chacun de ces éléments du système d'information par rapport aux différents critères de sécurité choisis. À partir de ces différentes valeurs, il est également possible d'établir un tableau d'impact intrinsèque qui correspond à l'évaluation des conséquences d'un risque dans l'absence totale de mesures de sécurité. Les valeurs de la classification sont donc utilisées pour remplir ce tableau et les différents types de ressources pouvant être atteints par les scénarios de risques sont fournis par les bases de connaissances de la méthode MEHARI. Il est à noter que le tableau d'impact intrinsèque peut être utilisé dans le cadre des activités d'une analyse des risques (Module 3).

Étape 1.3 : L'établissement de plans d'action basés sur l'analyse des enjeux. Cette étape requiert la réalisation de l'activité suivante :

Plans d'action basés sur l'analyse des enjeux. Cette activité vise à bâtir des plans d'action à partir des informations recueillies durant l'analyse des enjeux.

Pour mener à bien cette activité, il faut établir des plans d'action selon les mesures de sécurité qui pourraient être réalisées immédiatement pour une situation d'urgence qui aurait été détectée durant la réalisation des différentes activités de l'analyse des enjeux. Les travaux effectués pour l'identification et l'évaluation des dysfonctionnements peuvent avoir fait ressortir des situations problématiques à traiter dans les plus brefs délais.

Module 2 : Le diagnostic de l'état des services de sécurité. Le but de ce module est de faire un diagnostic de la qualité des services de sécurité en place dans l'entreprise, en procédant à une analyse des vulnérabilités du système d'information.

Étape 2.1 : L'analyse des vulnérabilités du système d'information. Cette étape requiert la réalisation des trois activités suivantes :

Élaboration du schéma d'audit. Cette activité vise à identifier des domaines de solutions de sécurité à considérer pour l'analyse des vulnérabilités.

Pour mener à bien cette activité, il s'agit de faire des regroupements de services de sécurité similaires afin de limiter le nombre d'audits à effectuer. Dans une entreprise, plusieurs solutions peuvent être en place pour répondre à ces différents services de sécurité. Les auditer tous requerrait une charge de travail considérable. Le schéma d'audit est donc décomposé de manière à présenter ces différents domaines pour lesquels un audit séparé sera effectué. Le premier niveau de décomposition concerne douze domaines de responsabilité tels que défini dans la méthode (l'organisation, la sécurité physique des réseaux, la sécurité applicative, les aspects juridiques et réglementaires, etc.). Ensuite, le deuxième niveau de décomposition est effectué pour des raisons techniques, stratégiques ou pour tout autre aspect servant à faire une division logique en sous-domaines.

Évaluation des services de sécurité. Cette activité vise à procéder à l'évaluation des services de sécurité selon le schéma d'audit établi.

Pour mener à bien cette activité, l'évaluation d'un service de sécurité est effectuée à l'aide d'une échelle de valeurs décrivant des niveaux de qualité définis selon les trois caractéristiques suivantes : l'efficacité du service, sa robustesse et les moyens de contrôle de son bon fonctionnement. Il est possible de procéder à l'analyse des vulnérabilités par une évaluation directe de la qualité des services ou bien par l'utilisation de questionnaires fournis par la méthode. Il est important de noter que cette activité nécessite la coopération des employés de l'entreprise, puisque que ce sont eux qui possèdent la majeure partie des informations en lien avec les services de sécurité de l'entreprise.

Synthèse des vulnérabilités. Cette activité vise à transformer les résultats bruts de l'évaluation des services de sécurité pour en présenter une synthèse.

Pour mener à bien cette activité, il s'agit de compiler les résultats obtenus lors de l'évaluation de la qualité des services de sécurité et de les présenter de manière à ce que les informations expriment la situation actuelle. Le diagnostic peut être présenté de différentes façons comme à partir des services de sécurité, des domaines de solutions de sécurité, de façon globale, par thème de sécurité ou même en comparaison à une norme en matière de

sécurité. Il est à noter que la synthèse des vulnérabilités peut également être utilisée dans le cadre des activités d'une analyse des risques (Module 3).

Étape 2.2 : L'établissement de plans d'action basés sur l'audit des vulnérabilités. Cette étape requiert la réalisation de l'activité suivante :

Plans d'action basés sur l'audit des vulnérabilités. Cette activité vise à bâtir des plans d'action à partir des informations recueillies durant la réalisation du diagnostic de l'état des services de sécurité.

Pour mener à bien cette activité, il faut établir des plans d'action selon les mesures de sécurité à mettre en œuvre suite aux résultats de l'audit des vulnérabilités. Les mesures seront identifiées de façon à améliorer les services de sécurité qui n'ont pas un niveau de qualité suffisant selon les objectifs de l'entreprise. Pour ce faire, ces objectifs doivent être définis préalablement aux travaux effectués pour le diagnostic de l'état des services de sécurité, puisque cette étape ne fait pas partie de la démarche de ce module dans la méthode MEHARI.

Module 3 : L'analyse de situations de risque. Le but de ce module est d'évaluer les risques, caractérisés par leur potentialité et leur impact global, encourus par l'entreprise dans l'éventualité qu'ils se concrétisent.

Étape 3.1 : La recherche des situations de risque. Cette étape requiert la réalisation de l'activité suivante :

Sélection des scénarios critiques devant être pris en compte pour une analyse des risques. Cette activité vise à déterminer quels sont les scénarios de risque pertinents à traiter dans le cadre d'une analyse des risques.

Pour mener à bien cette activité, il faut procéder à la recherche des scénarios à considérer dans l'étude et sur lesquels il est important pour l'entreprise d'évaluer le risque global. La première façon de les identifier est l'approche directe par l'utilisation de l'échelle de valeurs des dysfonctionnements déterminée durant l'analyse des enjeux et de la classification des informations et ressources (Module 1). Les dysfonctionnements permettent d'identifier les conséquences redoutées pour des situations identifiées par l'entreprise. Pour

obtenir un scénario de risques à partir d'un dysfonctionnement, il faut également lui associer des informations sur les circonstances de son déclenchement (un incident involontaire, un type d'attaque précis par utilisateur à l'interne, etc.). La seconde est la recherche systématique à partir d'une base de scénarios génériques fournie par la méthode MEHARI. Cette deuxième façon est plus exhaustive parce qu'elle ne part pas directement des préoccupations identifiées par l'entreprise comme dans le cas de la première façon, mais plutôt d'une vision plus large des scénarios possibles.

Étape 3.2 : L'analyse de situations de risque et l'utilisation des automatismes de MEHARI. Cette étape requiert la réalisation des huit activités suivantes pour chacun des scénarios de risque identifiés à l'étape précédente :

Évaluation de l'exposition naturelle. Cette activité vise à déterminer s'il existe des facteurs qui accentuent l'exposition de l'entreprise au scénario de risque analysé.

Pour mener à bien cette activité, l'exposition naturelle, qui contribue à la potentialité du risque, est établie en évaluant l'exposition naturelle standard et l'exposition naturelle spécifique de l'entreprise face au scénario de risque en question. L'exposition naturelle standard est celle qui est considérée comme étant propre à tout type d'entreprise, tandis que l'exposition naturelle spécifique est déterminée en fonction des caractéristiques spécifiques à l'entreprise (emplacement physique, nature des activités, etc.).

Évaluation des facteurs de réduction de risque agissant sur la potentialité à partir d'un audit de sécurité MEHARI. Cette activité vise à évaluer l'efficacité des mesures de sécurité mises en place et pouvant limiter la potentialité du scénario de risque.

Pour mener à bien cette activité, il faut considérer les deux facteurs pouvant affecter le niveau de potentialité du risque. Le premier facteur concerne les mesures dissuasives qui font référence aux mesures qui signalent un risque personnel à l'attaquant potentiel. Le deuxième facteur a trait aux mesures de prévention qui concernent les mesures en place pour faire en sorte de rendre difficile la réalisation du scénario. Ces mesures de prévention sont aussi appelées les conditions de survenance. Si la qualité de ces mesures a été évaluée suite à un diagnostic de l'état des services de sécurité (Module 2), ces valeurs sont déjà disponibles dans la synthèse des vulnérabilités. Sinon, des audits doivent être effectués par le même procédé pour les obtenir.

Évaluation de la potentialité. Cette activité vise à mesurer la potentialité du scénario de risque en considérant les éléments qui l'influencent et qui ont été évalués.

Pour mener à bien cette activité, la valeur de la potentialité est déterminée en fonction de la plus forte valeur obtenue dans l'évaluation de l'exposition naturelle et des mesures dissuasives et préventives. Concrètement, cette valeur représente une évaluation globale d'un niveau de probabilité du scénario de risque et sera utilisée dans l'évaluation du risque global.

Évaluation de l'impact intrinsèque. Cette activité vise à déterminer les conséquences du scénario de risque en faisant abstraction de toute mesure de sécurité appliquée.

Pour mener à bien cette activité, l'impact intrinsèque contribue à l'impact du risque et est établi en évaluant la gravité maximale des conséquences du scénario de risque. Si le scénario de risque analysé a été sélectionné suite à l'analyse des enjeux (Module 1), cette valeur est déjà disponible dans l'échelle de valeurs des dysfonctionnements. Sinon, il faut procéder à l'évaluation de cette valeur par le même procédé.

Évaluation des facteurs de réduction de risque agissant sur l'impact à partir d'un audit de sécurité MEHARI. Cette activité vise à évaluer l'efficacité des mesures pouvant limiter l'impact global du scénario de risque.

Pour mener à bien cette activité, il faut considérer les trois facteurs pouvant affecter le niveau d'impact du risque. Les mesures de protection, aussi appelées de confinement, représentent le premier facteur et visent à ce que les conséquences directes du scénario ne se propagent pas dans l'espace et le temps. Le deuxième facteur concerne les mesures palliatives et traitent de la préparation et de l'anticipation face à la réalisation du scénario de risque. Le troisième facteur a trait aux mesures de récupération et concerne la possibilité de faire des recours en justice et des requêtes aux assurances. Si la qualité de ces mesures a été évaluée suite à un diagnostic de l'état des services de sécurité (Module 2), ces valeurs sont déjà disponibles dans la synthèse des vulnérabilités. Sinon, des audits doivent être effectués par le même procédé pour les obtenir.

Évaluation de la réduction d'impact. Cette activité vise à évaluer un indicateur de réduction d'impact à partir des résultats obtenus lors de l'évaluation des facteurs de réduction de risque agissant sur l'impact.

Pour mener à bien cette activité, un indicateur de réduction d'impact est déterminé à l'aide des facteurs évalués précédemment (les mesures de protection, palliatives et de récupération) et de grilles standards d'évaluation, définies dans la méthode, en fonction du type de conséquence du scénario analysé. Le type de conséquence exprime la perte obtenue au niveau d'un des critères de sécurité utilisés dans l'étude (exemple : une perte de disponibilité). Cet indicateur de réduction d'impact est utilisé dans l'évaluation de l'impact global du scénario.

Évaluation de l'impact. Cette activité vise à mesurer l'impact global du scénario de risque en considérant les éléments qui l'influencent et qui ont été évalués.

Pour mener à bien cette activité, une formule est calculée pour obtenir la valeur de l'impact réel à considérer suite à l'évaluation des éléments qui pourraient l'affecter. Appelé l'impact résiduel, il est obtenu en prenant le minimum entre les deux valeurs suivantes : l'impact intrinsèque ou la valeur maximale moins l'indicateur de réduction. Ainsi, la valeur exprimée sera l'impact réel du scénario de risque, puisque la valeur maximum de l'impact et les facteurs d'atténuation sont considérés. Cette valeur sera utilisée dans l'évaluation du risque global.

Évaluation globale du risque. Cette activité vise à évaluer la gravité du scénario de risque grâce aux valeurs exprimées par la potentialité et l'impact du scénario de risque.

Pour mener à bien cette activité, l'évaluation finale du scénario de risque est effectuée au moyen des deux paramètres principaux, la potentialité et l'impact, en plus d'une grille d'acceptabilité des risques. Avec ces différentes valeurs, il est alors possible de déterminer la gravité du scénario de risque et de planifier des actions en conséquence. La grille d'acceptabilité des risques permet de déterminer, selon un tableau ayant comme axes la potentialité et l'impact, le niveau de gravité du risque pour l'entreprise. La méthode propose l'utilisation de trois niveaux de gravité pour un scénario soit : insupportable, inadmissible ou toléré. Les deux premiers nécessitant une intervention tandis que le

troisième est habituellement accepté par l'entreprise, corrigé au besoin ou tout simplement ignoré.

Étape 3.3 : L'établissement de plans d'action basés sur l'analyse des risques. Cette étape requiert la réalisation l'activité suivante :

Plans d'action basés sur l'analyse des risques. Cette activité vise à bâtir des plans d'action à partir des informations recueillies durant la réalisation de l'analyse des risques.

Pour mener à bien cette activité, il faut établir des plans d'action selon les mesures de sécurité de haut niveau à mettre en œuvre suite à l'évaluation des scénarios de risques. Plusieurs manières peuvent être décidées pour établir les plans d'action en fonction des résultats obtenus. L'objectif est de déterminer des mesures pour mitiger les différents scénarios de risques jugés avec une gravité assez élevée pour qu'ils soient traités. Des mesures générales de sécurité n'affectant pas directement un scénario de risques peuvent également faire partie d'un plan d'actions.

Par sa grande flexibilité d'utilisation, la méthode ne définit pas une démarche précise afin de s'adapter plus facilement aux besoins spécifiques de l'entreprise. Cependant, la documentation de la méthode expose trois possibilités de démarche qui auront comme résultat final la production d'un plan de sécurité. Ce dernier peut être basé à partir d'une analyse de risques complète, d'une analyse de risques spécifique à un projet ou encore, à partir directement du diagnostic (audit) de vulnérabilités.

MEHARI offre donc de multiples possibilités pour une entreprise qui désire effectuer une démarche pour améliorer sa sécurité informatique dans un cycle continu d'activités. Sa grande flexibilité permet d'aborder les risques de plusieurs manières tout en ne perdant pas de vue le but ultime, qui est de réduire les risques à un niveau acceptable. Ce sont les plans de sécurité produits qui permettront à l'entreprise d'atteindre concrètement cet objectif.

L'étude de cette méthode s'est avérée quelque peu difficile étant donné la manière dont elle est présentée dans les documents officiels. Le découpage logique et l'ordre des sujets présentés sont différents entre les documents généraux sur la démarche et ceux qui détaillent chacun des modules. De plus, les documents détaillés font parfois référence aux documents qui résument la méthode. Il y a

donc certaines inconstances dans l'utilisation des termes employés (plan d'actions versus plan de sécurité) et dans les titres de section entre les documents (le module « L'analyse des situations de risque » présenté dans un bref résumé par rapport au document qui le détaille et qui s'intitule « Guide de l'analyse de risque » ou bien le module « Le diagnostic de l'état des services de sécurité » qui est parfois appelé « Audit des services de sécurité »).

Malgré tout, la méthode MEHARI emploie la plupart des techniques utilisées pour la gestion des risques de sécurité pour un système d'information, ce qui représente un intrant informationnel important pour la démarche analytique de la présente recherche. En ce qui a trait aux phases et aux étapes de la gestion des risques démontrées dans le deuxième chapitre, cette méthode de gestion des risques vise principalement la phase de l'analyse de risques, mais plus particulièrement les étapes 1 à 6 comme démontré dans la figure 4.2 :

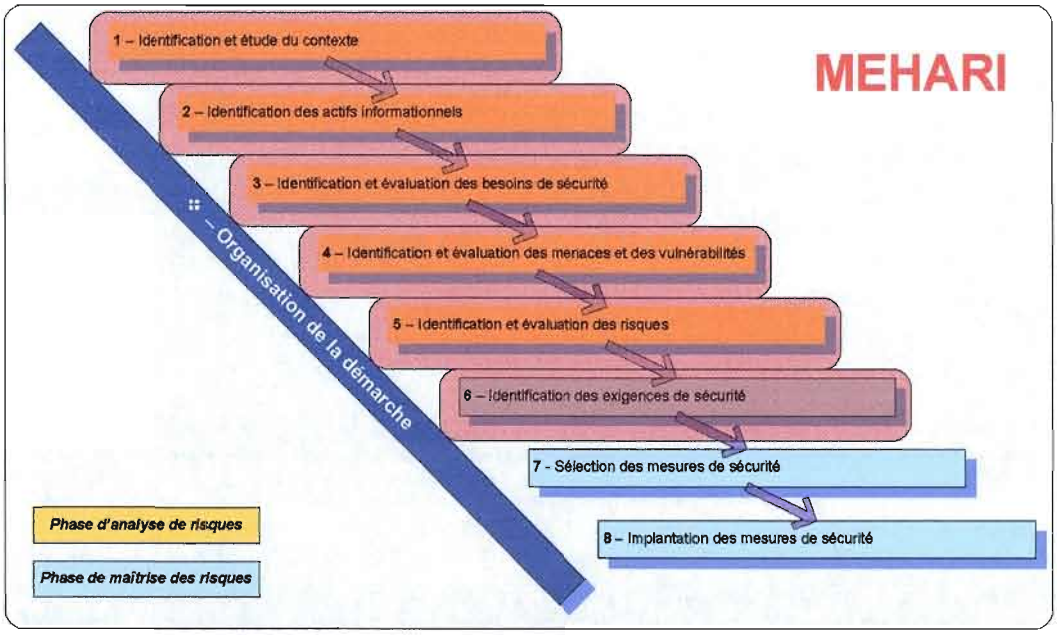

Figure 4.2 Positionnement de la méthode MEHARI par rapport aux étapes de la gestion des risques.

Les différentes activités de sécurité réalisées dans la méthode MEHARI seront positionnées par rapport aux étapes générales de la gestion des risques lorsqu'il sera question de les regrouper afin de bâtir la liste des activités générales de la gestion des risques.

La méthode OCTAVE (The **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation) [19, 22, 24] :

La méthode OCTAVE provient de l'université américaine Carnegie Mellon University. Celle-ci est réputée pour ses travaux en matière de sécurité informatique. OCTAVE fut créée en 1999 et une deuxième version parut en 2001. De plus, une version allégée nommée OCTAVE-S fut présentée en 2003. Il à noter que cette méthode n'offre pas de documentation en langue française. Par conséquent, les termes utilisés pour la décrire dans ce chapitre sont traduits de l'anglais.

OCTAVE se spécialise dans l'évaluation des vulnérabilités et des menaces sur les actifs opérationnels importants d'une entreprise. L'un des objectifs principaux des créateurs était de mettre au point une méthode pouvant être pilotée à l'interne dans l'entreprise. Pour cela, la méthode requiert qu'une équipe multidisciplinaire soit formée afin d'obtenir différents points de vue et, ainsi, définir un portrait réel de l'entreprise en matière de sécurité. Du même coup, les employés deviennent sensibilisés à la problématique des risques informatiques. OCTAVE est une méthode adaptée pour les grosses entreprises, et c'est pour cette raison que la méthode OCTAVE-S fut créée. Cette version contient des processus allégés afin d'être conduite par une équipe plus réduite et répondre ainsi aux besoins des petites et moyennes entreprises.

Le guide d'implantation de la méthode contient 18 volumes incluant un catalogue de bonnes pratiques en sécurité basé sur des référentiels tels que BS7799. Des outils gratuits et commerciaux existent pour supporter la démarche.

La méthodologie est clairement axée sur les actifs de l'entreprise. Il faut ainsi identifier lesquels sont les plus importants et centrer l'analyse de risques sur ceux-ci. Les menaces potentielles et les vulnérabilités exploitables sont considérées pour évaluer les risques et définir la stratégie de sécurité. Pour ce faire, la méthode propose une démarche en trois phases principales, mais contenant également une phase de préparation :

- **Préparation**

1. **Identifier les profils de menaces basés sur les actifs.**
2. **Identifier les vulnérabilités de l'infrastructure.**
3. **Développer la stratégie de sécurité.**

Huit processus découlent de ces trois phases principales et les activités qui sont effectuées pour les réaliser seront le thème principal de cette section. Tout d'abord, il est question de la phase de préparation.

Préparation à l'étude OCTAVE. Cette phase est composée des activités de préparation nécessaires afin de rendre possible la réalisation d'une étude de gestion de risques à l'aide de la méthode OCTAVE.

Durant cette phase, l'appui de la haute direction à l'égard de l'étude à réaliser est tout d'abord requis. Ensuite, les membres de l'équipe d'analyse sont sélectionnés et formés. La portée de l'étude sera établie en sélectionnant les secteurs opérationnels de l'entreprise à considérer ainsi que certains des employés qui y travaillent. De plus, des instructions de base leur seront remises. Pour terminer, la logistique de l'étude est organisée et elle inclut nécessairement les dates prévues pour les rencontres ainsi que le matériel nécessaire.

Phase 1 : Identifier les profils de menaces basés sur les actifs. Cette phase est composée des quatre processus suivants à réaliser :

Processus 1 : Recueillir la connaissance de la haute direction. Ce processus a pour but d'obtenir la vision de la haute direction envers les actifs de l'entreprise et la sécurité qui leur est attribuée.

Durant ce processus, une réunion avec les membres de la haute direction est convoquée afin de dialoguer sur plusieurs aspects relatifs aux actifs de l'entreprise. Tout d'abord, il s'agit d'identifier ces différents actifs et de sélectionner ceux étant jugés les plus importants. Concernant ces derniers, il faut déterminer différentes informations supplémentaires comme les préoccupations à leur égard et leurs impacts potentiels, leurs exigences de sécurité exprimées au moyen des critères de sécurité et, finalement, le ou les critères de sécurité jugés les plus importants à considérer. Ensuite, un questionnaire concernant les pratiques en place dans l'entreprise pour répondre aux exigences de sécurité est remis à chacun des participants. À l'égard des réponses qui sont fournies, des discussions s'ensuivent relativement au contexte de l'entreprise (ses pratiques courantes en termes de stratégie de protection ainsi que ses vulnérabilités). Pour conclure, il est important de valider avec les participants si les personnes sélectionnées pour le *Processus 2,* qui concerne

spécifiquement les directeurs de secteurs opérationnels, sont véritablement les ressources adéquates et d'ajuster cette liste au besoin.

Processus 2 : Recueillir la connaissance des directeurs de secteurs opérationnels. Ce processus a pour but d'obtenir la vision des directeurs de secteurs opérationnels envers les actifs de l'entreprise et la sécurité qui leur est attribuée.

Durant ce processus, une réunion avec les directeurs de secteurs opérationnels de l'entreprise, identifiés par la haute direction, est convoquée afin de dialoguer sur plusieurs aspects relatifs aux actifs de l'entreprise. Comme ce fut le cas lors du *Processus 1*, il s'agit d'identifier ces différents actifs et de sélectionner ceux étant jugés les plus importants. Concernant ces derniers, il faut déterminer différentes informations supplémentaires comme les préoccupations à leur égard et leurs impacts potentiels, leurs exigences de sécurité exprimées au moyen des critères de sécurité et, finalement, le critère de sécurité jugé le plus important à considérer. Ensuite, un questionnaire concernant les pratiques en place dans l'entreprise pour répondre aux exigences de sécurité est remis à chacun des participants. À l'égard des réponses qui sont fournies, des discussions s'ensuivent relativement au contexte de l'entreprise (ses pratiques courantes en termes de stratégie de protection ainsi que ses vulnérabilités). Puis, il est important de valider avec les participants si les personnes sélectionnées pour le *Processus 3*, qui concerne spécifiquement les membres du personnel, sont véritablement les ressources adéquates et d'ajuster cette liste au besoin. Pour finir, les résultats obtenus lors du *Processus 1* sont présentés aux participants.

Processus 3 : Recueillir la connaissance des membres du personnel. Cette activité a pour but d'obtenir la vision des membres du personnel affectés aux opérations et aux technologies de l'information envers les actifs de l'entreprise et la sécurité qui leur est attribuée.

Durant ce processus, une réunion avec les membres du personnel de l'entreprise, identifiés par les directeurs de secteurs opérationnels, est convoquée afin de dialoguer sur plusieurs aspects relatifs aux actifs de l'entreprise. Comme ce fut le cas lors du *Processus 1* et *2*, il s'agit d'identifier ces différents actifs et de sélectionner ceux étant jugés les plus importants. Concernant ces derniers, il faut déterminer différentes informations supplémentaires comme les préoccupations à leur égard et leurs impacts potentiels, leurs exigences de sécurité exprimées au moyen des critères de sécurité et, finalement, le critère de sécurité jugé le plus important à considérer. Ensuite, un questionnaire concernant les

pratiques en place dans l'entreprise pour répondre aux exigences de sécurité est remis à chacun des participants. À l'égard des réponses qui sont fournies, des discussions s'ensuivent relativement au contexte de l'entreprise (ses pratiques courantes en termes de stratégie de protection ainsi que ses vulnérabilités). Pour conclure, les résultats obtenus par la réalisation des *Processus 1* et *2* sont présentés aux participants.

Processus 4 : Créer les profils de menaces. Ce processus a pour but de regrouper les résultats obtenus lors des *Processus 1, 2* et *3* afin d'en extraire les actifs critiques, y compris leurs exigences de sécurité et les menaces qui pèsent sur eux.

Des activités de préparation doivent être effectuées pour réaliser ce processus. Il s'agit de consolider certains résultats obtenus durant les processus précédents. Ainsi, trois listes sont produites : le regroupement des actifs importants, leurs exigences de sécurité et les préoccupations à leur égard accompagnées de leurs impacts potentiels.

Durant ce processus, l'équipe d'analyse procédera à différents travaux de synthèse de la *Phase 1* soit : déterminer un petit groupe d'actifs critiques pouvant générer des impacts importants pour l'entreprise, affiner leurs exigences de sécurité et identifier les profils de menaces qui pèsent sur chacun d'eux.

Suite aux activités principales de ce processus, un livrable contenant les profils de chaque actif, ainsi que les préoccupations identifiées pour chacun d'eux, est documenté formellement.

Phase 2 : Identifier les vulnérabilités de l'infrastructure. Cette phase est composée des deux processus suivants à réaliser :

Processus 5 : Identifier les composantes clés. Ce processus a pour but d'identifier les composantes de l'infrastructure qui sont en lien avec les actifs critiques sélectionnés pour l'étude.

Durant ce processus, il faut d'abord identifier les systèmes pour lesquels les actifs critiques sont fortement dépendants et, par la suite, identifier les types de composantes (serveur, dispositif réseau, dispositif de sécurité, dispositif de sauvegarde, ordinateur de bureau ou portable, etc.) qui sont liés à ces systèmes. Ensuite, une sélection de toutes les

composantes à évaluer est effectuée incluant automatiquement les systèmes pour lesquels les actifs critiques sont dépendants. Pour terminer, l'approche préconisée et les outils pour détecter les vulnérabilités sont également choisis en préparation de l'évaluation.

Processus 6 : Évaluer les composantes sélectionnées. Ce processus a pour but d'évaluer les composantes de l'infrastructure sélectionnées lors du *Processus 5* pour détecter les vulnérabilités technologiques.

Des activités de préparation doivent être effectuées pour réaliser ce processus. Il s'agit de faire un audit de sécurité, par l'utilisation d'outils de détection de vulnérabilités, des composantes sélectionnées et de résumer les résultats en les rattachant aux différents actifs critiques en question.

Durant ce processus, il s'agit de réviser et d'analyser les vulnérabilités identifiées pour chacun des actifs critiques. Au besoin, recueillir davantage d'informations sur ces vulnérabilités afin de les connaître et de les comprendre suffisamment pour la suite de l'étude.

Phase 3 : Développer la stratégie de sécurité. Cette phase est composée des deux processus suivants à réaliser :

Processus 7 : Réaliser l'analyse de risques. Ce processus a pour but d'identifier et d'évaluer les risques au moyen des menaces et de leurs impacts sur l'entreprise.

Durant ce processus, il s'agit tout d'abord d'identifier les risques. Pour cela, il faut décrire textuellement les impacts qu'aurait la réalisation d'une menace sur chacun des actifs critiques de l'entreprise et, par le fait même, sur sa mission. Chaque impact comprend une description du résultat et est associé à un type d'impact. Les types d'impact utilisés sont les suivants : la divulgation, la modification, la perte/destruction et l'interruption. Un risque est alors déterminé par la combinaison d'une menace et d'un résultat d'impact. Ensuite, les critères d'évaluation du risque sont déterminés. Les risques identifiés n'ont pas tous le même niveau de gravité pour l'entreprise. Donc, c'est en établissant une échelle de valeurs qu'il est possible, par une évaluation, d'établir une gravité relative. Finalement, chacun des risques identifiés est évalué et une mesure d'impact (une valeur tirée de l'échelle) lui est attribuée en fonction des critères d'évaluation des risques établis.

Processus 8 : Développer la stratégie de protection. Ce processus a pour but d'élaborer la stratégie en matière de sécurité à mettre en place pour l'entreprise selon les informations recueillies lors des *Processus 1* à *7*. Le processus se divise en deux étapes :

Étape 1 – Développer la stratégie de protection. Cette étape a pour but de produire une stratégie de protection pour l'entreprise, des plans de mitigation pour les risques reliés aux actifs critiques et une liste d'actions possibles à réaliser à court terme.

Des activités de préparation doivent être effectuées pour réaliser cette étape. Il faut tout d'abord compiler les résultats des questionnaires complétés par les différents participants lors des *Processus 1, 2* et *3* concernant les pratiques actuellement en place pour sécuriser les actifs de l'entreprise. De plus, il faut consolider ces mêmes résultats avec les informations discutées suite à ce questionnaire et qui sont spécifiquement relatives au contexte de l'entreprise (ses pratiques courantes en termes de stratégie de protection ainsi que ses vulnérabilités).

Durant cette étape, chacun des membres de l'équipe d'analyse doit d'abord revoir les informations produites durant les processus précédents soit : les vulnérabilités technologiques, les pratiques de la stratégie de protection, les vulnérabilités de l'entreprise, les exigences de sécurité et les informations concernant les risques. Ensuite, l'équipe d'analyse crée la stratégie de protection qui contribuera à la gestion de la sécurité interne pour l'entreprise, les plans de mitigation qui définissent les mesures requises pour atténuer les risques qui pèsent sur les actifs critiques et, finalement, la liste d'actions contenant des mesures qui peuvent être effectuées à court terme par les gens de l'entreprise sans besoin supplémentaire (expertise ou formation précise, changements aux politiques de l'entreprise, etc.).

Étape 2 – Sélection de la stratégie de protection. Cette étape, en étroite collaboration avec la haute direction, a pour but de réviser, d'approuver et de décider comment implanter les travaux énoncés durant le *Processus 8 – Étape 1*.

Des activités de préparation doivent être effectuées pour réaliser cette étape. Il s'agit de compiler, de bonifier et de raffiner les informations produites dans les différents processus de l'étude et, plus spécifiquement, celles produites lors du *Processus 8 – Étape 1*. Elles seront présentées à la haute direction durant cette étape et incluront les points suivants :

les actifs traités, les profils de risques menaçant les actifs critiques, la stratégie de protection de l'entreprise, les plans de mitigation et la liste d'actions.

Durant cette étape, il s'agit avant tout d'impliquer la haute direction dans les résultats et la mise en œuvre des solutions. Une révision de l'information entourant les risques peut alors être effectuée et englobera les aspects suivants : les pratiques courantes et les vulnérabilités de l'entreprise, les informations sur les actifs et les profils de risques reliés aux actifs critiques. Ensuite, il faut revoir et modifier au besoin la stratégie de protection, les plans de mitigation des risques et la liste d'actions. Finalement, la haute direction doit décider comment (le quoi, le quand et le qui) s'effectueront la mise en œuvre de la stratégie de protection et les plans de mitigation.

Suite aux activités principales de ce processus, il est essentiel de documenter formellement les informations et les décisions résultantes du *Processus 8 – Partie 2* et qu'elles soient diffusées auprès des personnes concernées dans l'entreprise.

Les informations recueillies par et auprès des gens de l'entreprise durant la première phase (*Processus 1* à *4*) s'avèrent donc un intrant informationnel important pour la qualité des résultats de la démarche. Lorsque celle-ci est complétée, il est possible de produire différents documents relatifs à la sécurité tels qu'une stratégie de protection, un plan de gestion des risques pour l'infrastructure technologique et une liste d'actions à entreprendre à court terme pour l'entreprise. La manière avec laquelle la méthode OCTAVE peut être appliquée à l'interne permet aux entreprises de travailler plus directement et par elles-mêmes à l'amélioration de leur sécurité informatique, en donnant les indicateurs nécessaires pour prendre de bonnes décisions face aux risques.

L'étude de cette méthode démontre qu'en plus des différents concepts de la gestion des risques, la méthode OCTAVE donne une importance particulière aux tâches reliées à l'organisation de la démarche de gestion des risques et, plus spécialement, sur les aspects de préparation et de communication. Bien que la plupart des méthodes abordent également ces différentes tâches, la méthode OCTAVE les officialise par des activités bien précises. Il faut aussi souligner que contrairement aux méthodes *EBIOS* et *MÉHARI*, a méthode *OCTAVE* présente l'évaluation de la probabilité de la menace, dans l'équation du risque telle que présentée au deuxième chapitre, comme étant optionnelle parce qu'il n'y a pas de données actualisées et validées pour appuyer ces prédictions. En ce qui a trait aux phases et aux étapes de la gestion des risques démontrées dans le

deuxième chapitre, cette méthode de gestion des risques vise principalement la phase de l'analyse de risques, mais plus particulièrement les étapes 1 à 6 et l'étape spéciale d'organisation de la démarche comme démontrées dans la figure 4.3 :

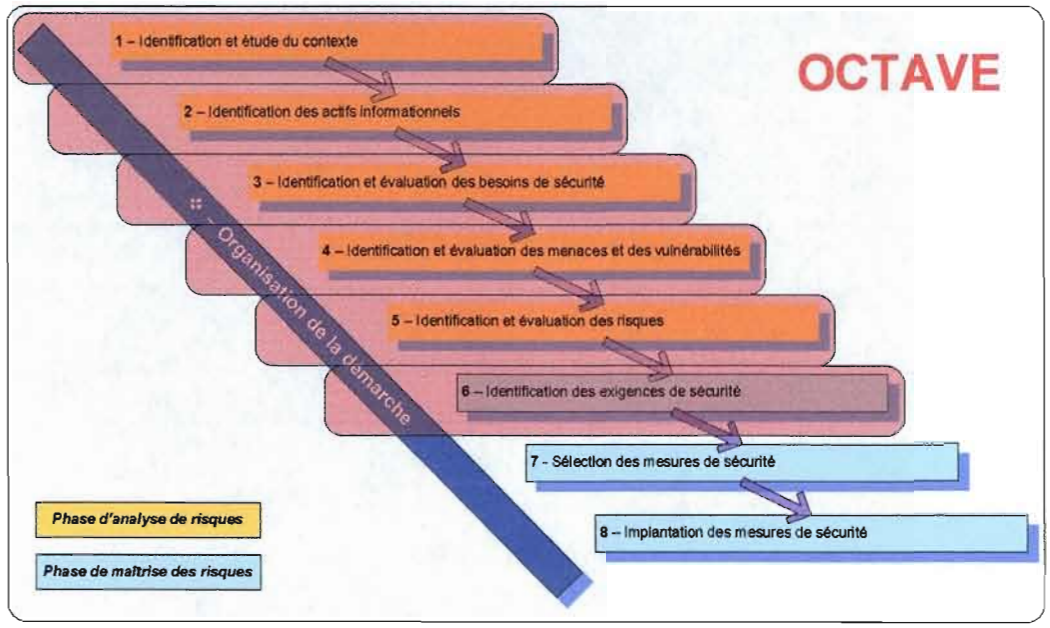

Figure 4.3 Positionnement de la méthode OCTAVE par rapport aux étapes de la gestion des risques.

Les différentes activités de sécurité réalisées dans la méthode OCTAVE seront positionnées par rapport aux étapes générales de la gestion des risques lorsqu'il sera question de les regrouper afin de bâtir la liste des activités générales de la gestion des risques.

4.1.2 Présentation de la synthèse des activités de sécurité identifiées

Suite à l'étude des méthodes EBIOS, MEHARI et OCTAVE, il fut possible d'identifier les principales activités de sécurité effectuées dans chacune des trois démarches. Les tableaux 4.1, 4.2 et 4.3 présentent un sommaire de ces activités qui sont tirées directement de la documentation officielle fournie par les organismes en charge de ces méthodes. Le dernier niveau du tableau correspond précisément aux activités de sécurité qui seront prises en considération pour la suite dans la démarche analytique. Afin d'en faciliter le repérage dans les sections suivantes, un code de référence a été attribué à chacune d'entre elles (exemple : *E-1.1.1*).

Tableau 4.1

Activités de sécurité de la méthode EBIOS

Méthode EBIOS			
1	**Étude du contexte**		
	1.1	Étude de l'organisme	
		E-1.1.1	Présenter l'organisme
		E-1.1.2	Lister les contraintes pesant sur l'organisme
		E-1.1.3	Lister les références réglementaires applicables à l'organisme
		E-1.1.4	Faire une description fonctionnelle du SI global
	1.2	Étude du système-cible	
		E-1.2.1	Présenter le système-cible
		E-1.2.2	Lister les enjeux
		E-1.2.3	Lister les éléments essentiels
		E-1.2.4	Faire une description fonctionnelle du système-cible
		E-1.2.5	Lister les hypothèses
		E-1.2.6	Lister les règles de sécurité
		E-1.2.7	Lister les contraintes pesant sur le système-cible
		E-1.2.8	Lister les références réglementaires spécifiques au système-cible
	1.3	Détermination de la cible de l'étude de sécurité	
		E-1.3.1	Lister et décrire les entités du système
		E-1.3.2	Croiser les éléments essentiels et les entités
2	**Expression des besoins de sécurité**		
	2.1	Réalisation des fiches de besoins	
		E-2.1.1	Choisir les critères de sécurité à prendre en compte
		E-2.1.2	Déterminer l'échelle de besoins
		E-2.1.3	Déterminer les impacts pertinents
	2.2	Synthèse des besoins de sécurité	
		E-2.2.1	Attribuer un besoin de sécurité par critère de sécurité (disponibilité, intégrité, confidentialité…) à chaque élément essentiel
3	**Étude des menaces**		
	3.1	Étude des origines des menaces	
		E-3.1.1	Lister les méthodes d'attaques pertinentes
		E-3.1.2	Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter
		E-3.1.3	Caractériser, pour chaque méthode d'attaque retenue, les éléments menaçants associés par leur type (naturel, humain ou environnemental) et leur cause (accidentelle ou délibérée)
		E-3.1.4	Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant
		E-3.1.5	Mettre en évidence les méthodes d'attaque non retenues avec des justifications
	3.2	Étude des vulnérabilités	
		E-3.2.1	Identifier les vulnérabilités des entités selon les méthodes d'attaque
		E-3.2.2	Estimer éventuellement le niveau des vulnérabilités
	3.3	Formalisation des menaces	
		E-3.3.1	Formuler explicitement les menaces
		E-3.3.2	Hiérarchiser éventuellement les menaces selon leur opportunité

4	**Identification des objectifs de sécurité**		
	4.1	Confrontation des menaces aux besoins	
		E-4.1.1	Déterminer les risques en confrontant menaces et besoins de sécurité
		E-4.1.2	Formuler explicitement les risques
		E-4.1.3	Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces
		E-4.1.4	Mettre en évidence les risques non retenus (risques résiduels) avec des justifications
	4.2	Formalisation des objectifs de sécurité	
		E-4.2.1	Lister les objectifs de sécurité
		E-4.2.2	Justifier la complétude de la couverture, en vérifiant la compatibilité avec les contraintes pesant sur l'organisme et le système-cible : des risques, des hypothèses (et les enjeux) et des règles de sécurité (et les références réglementaires)
		E-4.2.3	Classer éventuellement les objectifs de sécurité en deux catégories : objectifs de sécurité portant sur le système-cible et objectifs de sécurité portant sur l'environnement du système-cible
		E-4.2.4	Mettre en évidence les défauts de couverture (risques résiduels) avec des justifications
	4.3	Détermination des niveaux de sécurité	
		E-4.3.1	Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité
		E-4.3.2	Choisir le niveau des exigences d'assurance
5	**Détermination des exigences de sécurité**		
	5.1	Détermination des exigences de sécurité fonctionnelles	
		E-5.1.1	Lister les exigences de sécurité fonctionnelles
		E-5.1.2	Justifier la complétude de la couverture des objectifs de sécurité
		E-5.1.3	Mettre en évidence les éventuels défauts de couverture (risques résiduels) avec des justifications
		E-5.1.4	Classer les exigences de sécurité fonctionnelles en deux catégories : exigences de sécurité fonctionnelles portant sur le système-cible et exigences de sécurité fonctionnelles portant sur l'environnement du système-cible
		E-5.1.5	Justifier éventuellement la couverture des dépendances des exigences de sécurité fonctionnelles
	5.2	Détermination des exigences de sécurité d'assurance	
		E-5.2.1	Lister les exigences de sécurité d'assurance
		E-5.2.2	Classer éventuellement les exigences de sécurité d'assurance en deux catégories : exigences de sécurité d'assurance portant sur l'environnement du système-cible et exigences de sécurité d'assurances portant sur l'environnement du système-cible
		E-5.2.3	Justifier éventuellement la couverture des dépendances des exigences de sécurité d'assurance

Tableau 4.2

Activités de sécurité de la méthode MEHARI

Méthode MEHARI			
1	**L'analyse des enjeux de la sécurité et de la classification des informations et ressources**		
	1.1	L'échelle de valeurs des dysfonctionnements	
		M-1.1.1	Identification des activités majeures et de leurs finalités
		M-1.1.2	Identification des dysfonctionnements redoutés
		M-1.1.3	Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés
		M-1.1.4	Échelle de valeurs des dysfonctionnements
	1.2	La classification des informations et ressources du système d'information	
		M-1.2.1	Identification des éléments à classifier
		M-1.2.2	Critères de classification
		M-1.2.3	Processus de classification
	1.3	L'établissement de plans d'action basés sur l'analyse des enjeux	
		M-1.3.1	Plans d'action basés sur l'analyse des enjeux
2	**Le diagnostic de l'état des services de sécurité**		
	2.1	L'analyse des vulnérabilités du système d'information	
		M-2.1.1	Élaboration du schéma d'audit
		M-2.1.2	Évaluation des services de sécurité
		M-2.1.3	Synthèse des vulnérabilités
	2.2	L'établissement de plans d'action basés sur l'audit des vulnérabilités	
		M-2.2.1	Plans d'action basés sur l'audit des vulnérabilités
3	**L'analyse des risques**		
	3.1	La recherche des situations de risque	
		M-3.1.1	Sélection des scénarios critiques devant être pris en compte pour une analyse des risques
	3.2	L'analyse de situations de risque et l'utilisation des automatismes de MEHARI	
		M-3.2.1	Évaluation de l'exposition naturelle
		M-3.2.2	Évaluation des facteurs de réduction de risque agissant sur la potentialité à partir d'un audit de sécurité MEHARI
		M-3.2.3	Évaluation de la potentialité
		M-3.2.4	Évaluation de l'impact intrinsèque
		M-3.2.5	Évaluation des facteurs de réduction de risque agissant sur l'impact à partir d'un audit de sécurité MEHARI
		M-3.2.6	Évaluation de la réduction d'impact
		M-3.2.7	Évaluation de l'impact
		M-3.2.8	Évaluation globale du risque
	3.3	L'établissement de plans d'action basés sur l'analyse de risques	
		M-3.3.1	Plans d'action basés sur l'analyse de risques

Tableau 4.3

Activités de sécurité de la méthode OCTAVE

Méthode OCTAVE			
1	**Préparation à l'étude OCTAVE**		
	1.1	Activités pour la préparation à l'étude OCTAVE	
		O-1.1.1	Obtenir le soutien de la haute direction pour l'étude OCTAVE
		O-1.1.2	Sélectionner les membres de l'équipe d'analyse
		O-1.1.3	Former l'équipe d'analyse
		O-1.1.4	Sélectionner les secteurs opérationnels de l'entreprise qui participeront à l'étude OCTAVE
		O-1.1.5	Sélectionner les participants
		O-1.1.6	Coordonner la logistique
		O-1.1.7	Donner des instructions aux participants
2	**Phase 1 : Identifier les profils de menaces basés sur les actifs**		
	2.1	**Processus 1** : Recueillir la connaissance de la haute direction	
		O-2.1.1	Identifier et prioriser les actifs utilisés par l'entreprise selon la haute direction
		O-2.1.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon la haute direction
		O-2.1.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon la haute direction
		O-2.1.4	Obtenir la connaissance de la haute direction envers la stratégie de protection actuelle et des vulnérabilités de l'entreprise
		O-2.1.5	Choisir ou confirmer les secteurs opérationnels visés par l'évaluation ainsi que les directeurs qui participeront à l'étude
	2.2	**Processus 2** : Recueillir la connaissance des directeurs de secteurs opérationnels	
		O-2.2.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les directeurs de secteurs opérationnels
		O-2.2.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels
		O-2.2.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels
		O-2.2.4	Obtenir la connaissance des directeurs de secteurs opérationnels envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise
		O-2.2.5	Choisir ou confirmer les membres du personnel qui participeront à l'étude
		O-2.2.6	Communiquer les résultats du *Processus 1*
	2.3	**Processus 3** : Recueillir la connaissance des membres du personnel	
		O-2.3.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les membres du personnel
		O-2.3.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les membres du personnel
		O-2.3.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les membres du personnel
		O-2.3.4	Obtenir la connaissance des membres du personnel envers la stratégie de protection actuelle et des vulnérabilités présentes dans

		l'entreprise
	O-2.3.5	Communiquer les résultats des *Processus 1 et 2*
2.4	**Processus 4** : Créer les profils de menaces	
	O-2.4.1	Regrouper, par groupe consulté, les actifs identifiés
	O-2.4.2	Regrouper, par groupe consulté et par actif, les exigences de sécurité
	O-2.4.3	Regrouper, par groupe consulté et par actif, les préoccupations et leurs impacts
	O-2.4.4	Sélectionner les actifs critiques
	O-2.4.5	Raffiner les exigences de sécurité à l'égard des actifs critiques
	O-2.4.6	Identifier les menaces qui pèsent sur les actifs critiques
	O-2.4.7	Inscrire les préoccupations dans le livrable contenant les profils des actifs
3	Identifier les vulnérabilités de l'infrastructure	
3.1	**Processus 5** : Identifier les composantes clés	
	O-3.1.1	Identifier les types de composantes
	O-3.1.2	Identifier les composantes de l'infrastructure à examiner
3.2	**Processus 6** : Évaluer les composantes sélectionnées	
	O-3.2.1	Exécuter les outils d'évaluation de vulnérabilités sur les composantes de l'infrastructure sélectionnées
	O-3.2.2	Réviser les vulnérabilités technologiques et résumer les résultats
4	Développer la stratégie de sécurité	
4.1	**Processus 7** : Réaliser l'analyse de risques	
	O-4.1.1	Identifier les impacts des menaces qui pèsent sur les actifs critiques
	O-4.1.2	Créer les critères d'évaluation du risque
	O-4.1.3	Évaluer les impacts des menaces qui pèsent sur les actifs critiques
4.2	**Processus 8** : Développer la stratégie de protection	
	O-4.2.1	Compiler les résultats des questionnaires
	O-4.2.2	Consolider les informations recueillies sur la stratégie de protection
	O-4.2.3	Réviser les vulnérabilités technologiques, les pratiques de la stratégie de protection, les exigences de sécurité, les vulnérabilités de l'entreprise et les informations concernant les risques
	O-4.2.4	Créer la stratégie de protection
	O-4.2.5	Créer les plans de mitigation
	O-4.2.6	Créer la liste d'actions
	O-4.2.7	Compiler un résumé des actifs
	O-4.2.8	Compiler les profils de risques
	O-4.2.9	Compiler la stratégie de protection de l'entreprise
	O-4.2.10	Compiler les plans de mitigation
	O-4.2.11	Compiler la liste d'actions
	O-4.2.12	Réviser les informations sur les risques
	O-4.2.13	Réviser et raffiner la stratégie de protection, les plans de mitigation et la liste d'actions
	O-4.2.14	Créer les prochaines étapes
	O-4.2.15	Documenter la stratégie de protection, les plans de mitigation des risques, la liste d'actions et les prochaines étapes

Ces trois tableaux affichent donc un total de 119 activités de sécurité à considérer. La répartition des activités, par méthode, est la suivante : 45 pour EBIOS, 22 pour MEHARI et 52 pour OCTAVE. Ces différentes activités ont ensuite été utilisées comme intrants de base pour la création de la liste d'activités générales de la gestion des risques. Cette partie est décrite en détail dans la section qui suit.

4.1.3 Création de la liste des activités générales de la gestion des risques de sécurité

À partir des trois listes établies dans la section précédente, toutes les activités de sécurité qu'elles contiennent et qui proviennent des méthodes de gestion des risques doivent maintenant être considérées comme un seul et unique ensemble d'activités. À partir de cet ensemble, une liste des activités générales de la gestion des risques peut ensuite être établie. Pour ce faire, les deux étapes suivantes ont été effectuées et sont expliquées plus en détail par la suite :

1. **Associer chacune des activités de sécurité à l'une des étapes de la gestion des risques**. L'association est réalisée en déterminant à quelle étape de la gestion des risques, présentée au deuxième chapitre, l'activité en question contribue-t-elle à la réalisation de l'objectif.

2. **Dresser une liste d'activités générales à partir des différentes activités de sécurité provenant des méthodes étudiées**. À partir des regroupements d'activités obtenus à la première étape, les activités d'un même regroupement peuvent ensuite faire l'objet d'une analyse plus particulière afin d'identifier les activités présentant des concepts similaires ou différents. De ces activités découleront de nouvelles activités générales de la gestion des risques de sécurité, formulées de façon à utiliser des termes génériques pour en faciliter leur utilisation dans la suite de la démarche analytique.

La création de la liste d'activités générales représente l'objectif principal de la première étape de la démarche analytique. Pour y parvenir, les deux étapes citées ci-dessus ont engendrées différents traitements sur les informations soutirées des méthodes de gestion des risques. Le détail de ces deux étapes est donc présenté dans ce qui suit afin d'en comprendre les résultats qui ont été obtenus.

La première étape pour dresser la liste consistait à associer chacune des activités de sécurité provenant des méthodes étudiées à l'une des étapes de la gestion des risques. Durant la réalisation de cette étape, deux difficultés importantes sont survenues :

- L'association d'une activité de sécurité à une étape de la gestion des risques fut la plupart du temps assez simple à établir, puisque les trois méthodes de gestion des risques étudiées présentent les mêmes grandes notions du domaine. Cependant, certaines décisions ont dû être prises lorsque des activités pouvaient correspondre logiquement à plus d'une étape de la gestion des risques. Cette situation s'explique par le fait que les méthodes de gestion des risques proposent des activités de sécurité regroupées selon leur propre découpage méthodologique. Ainsi, en fonction du découpage des étapes de la gestion des risques dans la présente recherche, le but visé par une activité de sécurité provenant d'une méthode pouvait sembler contribuer à plus d'une étape. Toutefois, des choix ont été faits pour déterminer l'étape la plus adéquate selon l'approche globale de la gestion des risques telle qu'établie dans la présente recherche.

  Par exemple, l'activité *E-1.2.3 : Lister les éléments essentiels* est considérée avec les activités de sécurité reliées à l'établissement du contexte dans sa méthode de provenance (EBIOS). Dans le découpage méthodologique de la gestion des risques pour la présente recherche, il existe une étape équivalente pour l'étude du contexte (n° 1 – *Identification et étude du contexte*). Cependant, il existe également une étape spécifique pour l'identification des éléments essentiels (n° 2 – *Identification des actifs informationnels*). Dans cette situation, l'activité *E-1.2.3* fut donc placée dans l'étape 2 afin de correspondre plus logiquement à l'approche globale de la gestion de risques telle que présentée dans la présente recherche. Il est important de noter que ces décisions ne remettent aucunement en cause les regroupements d'activités de sécurité effectués dans les méthodes en question, mais démontrent plutôt que la présente recherche définit son propre découpage méthodologique se traduisant par des regroupements d'activités de sécurité légèrement différents.

- Deux activités de sécurité, provenant de la méthode MEHARI, ont été écartées pour la suite des traitements en rapport à la création de la liste des activités générales. La raison est que ces activités visent à recommander des mesures de sécurité à partir de travaux

qui pourraient être réalisés de manière totalement indépendante de celle d'une démarche de gestion des risques de sécurité.

Il s'agit des activités *M-1.3.1 : Plans d'action basés sur l'analyse des enjeux* et *M-2.2.1 : Plans d'action basés sur l'audit des vulnérabilités.* La première est l'activité finale d'une démarche d'expression des besoins, tandis que la deuxième est celle d'une démarche d'audit de sécurité. Ces deux démarches peuvent être effectuées de manière indépendante à celle de la gestion des risques de sécurité. Leurs résultats sont exprimés par la réalisation des deux activités en question. Dans la méthode MEHARI, il existe également une autre activité ayant le même but, mais spécifiquement pour la démarche de la gestion des risques. Il s'agit de l'activité *M-3.3.1 : Plans d'action basés sur l'analyse de risques* qui, dans ce cas-ci, a bel et bien été considérée pour la suite des traitements en rapport à la création de la liste des activités générales.

Le tableau 4.4 présente les résultats obtenus suite à cette première étape de la création de la liste des activités générales de la gestion des risques. Le tableau vise également à démontrer que toutes les activités de sécurité provenant des méthodes ont été considérées dans cette étape à l'exception des deux activités *M-1.3.1* et *M-2.2.1* pour les raisons mentionnées précédemment. Afin d'aider à la compréhension des résultats du tableau, voici un rappel des différentes étapes de la gestion des risques telles que définies au deuxième chapitre :

- ❖ Organisation de la démarche

1. Identification et étude du contexte
2. Identification des actifs informationnels
3. Identification et évaluation des besoins de sécurité
4. Identification et évaluation des menaces et des vulnérabilités
5. Identification et évaluation des risques
6. Identification des exigences de sécurité
7. Sélection des mesures de sécurité
8. Implantation des mesures de sécurité

Le tableau 4.4 combine les résultats des tableaux 4.1, 4.2 et 4.3 en ne conservant que les lignes représentant les activités de sécurité à considérer. La colonne « Étapes de la gestion des risques » contient les valeurs qui résultent de l'association des activités de sécurité à l'une des étapes de la gestion des risques.

Tableau 4.4

Associations entre les activités de sécurité et les étapes de la gestion des risques

Codes de référence	Activités provenant des méthodes étudiées	Étapes de la gestion des risques
	Méthode EBIOS	
E-1.1.1	Présenter l'organisme	1
E-1.1.2	Lister les contraintes pesant sur l'organisme	1
E-1.1.3	Lister les références réglementaires applicables à l'organisme	1
E-1.1.4	Faire une description fonctionnelle du SI global	1
E-1.2.1	Présenter le système-cible	1
E-1.2.2	Lister les enjeux	1
E-1.2.3	Lister les éléments essentiels	2
E-1.2.4	Faire une description fonctionnelle du système-cible	1
E-1.2.5	Lister les hypothèses	1
E-1.2.6	Lister les règles de sécurité	1
E-1.2.7	Lister les contraintes pesant sur le système-cible	1
E-1.2.8	Lister les références réglementaires spécifiques au système-cible	1
E-1.3.1	Lister et décrire les entités du système	2
E-1.3.2	Croiser les éléments essentiels et les entités	2
E-2.1.1	Choisir les critères de sécurité à prendre en compte	3
E-2.1.2	Déterminer l'échelle de besoins	3
E-2.1.3	Déterminer les impacts pertinents	3
E-2.2.1	Attribuer un besoin de sécurité par critère de sécurité (disponibilité, intégrité, confidentialité…) à chaque élément essentiel	3
E-3.1.1	Lister les méthodes d'attaques pertinentes	4
E-3.1.2	Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter	4
E-3.1.3	Caractériser, pour chaque méthode d'attaque retenue, les éléments menaçants associés par leur type (naturel, humain ou environnemental) et leur cause (accidentelle ou délibérée)	4
E-3.1.4	Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant	4
E-3.1.5	Mettre en évidence les méthodes d'attaque non retenues avec des justifications	4
E-3.2.1	Identifier les vulnérabilités des entités selon les méthodes d'attaque	4
E-3.2.2	Estimer éventuellement le niveau des vulnérabilités	4
E-3.3.1	Formuler explicitement les menaces	4
E-3.3.2	Hiérarchiser éventuellement les menaces selon leur opportunité	4
E-4.1.1	Déterminer les risques en confrontant menaces et besoins de sécurité	5
E-4.1.2	Formuler explicitement les risques	5
E-4.1.3	Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces	5
E-4.1.4	Mettre en évidence les risques non retenus (risques résiduels) avec des justifications	5
E-4.2.1	Lister les objectifs de sécurité	6
E-4.2.2	Justifier la complétude de la couverture, en vérifiant la compatibilité avec les contraintes pesant sur l'organisme et le système-cible : des risques, des hypothèses (et les enjeux) et des règles de sécurité (et les références réglementaires)	6

E-4.2.3	Classer éventuellement les objectifs de sécurité en deux catégories : objectifs de sécurité portant sur le système-cible et objectifs de sécurité portant sur l'environnement du système-cible	**6**
E-4.2.4	Mettre en évidence les défauts de couverture (risques résiduels) avec des justifications	**6**
E-4.3.1	Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité	**6**
E-4.3.2	Choisir le niveau des exigences d'assurance	**6**
E-5.1.1	Lister les exigences de sécurité fonctionnelles	**6**
E-5.1.2	Justifier la complétude de la couverture des objectifs de sécurité	**6**
E-5.1.3	Mettre en évidence les éventuels défauts de couverture (risques résiduels) avec des justifications	**6**
E-5.1.4	Classer les exigences de sécurité fonctionnelles en deux catégories : exigences de sécurité fonctionnelles portant sur le système-cible et exigences de sécurité fonctionnelles portant sur l'environnement du système-cible	**6**
E-5.1.5	Justifier éventuellement la couverture des dépendances des exigences de sécurité fonctionnelles	**6**
E-5.2.1	Lister les exigences de sécurité d'assurance	**6**
E-5.2.2	Classer éventuellement les exigences de sécurité d'assurance en deux catégories : exigences de sécurité d'assurance portant sur l'environnement du système-cible et exigences de sécurité d'assurances portant sur l'environnement du système-cible	**6**
E-5.2.3	Justifier éventuellement la couverture des dépendances des exigences de sécurité d'assurance	**6**
	Méthode MEHARI	
M-1.1.1	Identification des activités majeures et de leurs finalités	**2**
M-1.1.2	Identification des dysfonctionnements redoutés	**3**
M-1.1.3	Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés	**3**
M-1.1.4	Échelle de valeurs des dysfonctionnements	**3**
M-1.2.1	Identification des éléments à classifier	**3**
M-1.2.2	Critères de classification	**3**
M-1.2.3	Processus de classification	**3**
M-1.3.1	Plans d'action basés sur l'analyse des enjeux	*Non applicable*
M-2.1.1	Élaboration du schéma d'audit	**4**
M-2.1.2	Évaluation des services de sécurité	**4**
M-2.1.3	Synthèse des vulnérabilités	**4**
M-2.2.1	Plans d'action basés sur l'audit des vulnérabilités	*Non applicable*
M-3.1.1	Sélection des scénarios critiques devant être pris en compte pour une analyse des risques	**5**
M-3.2.1	Évaluation de l'exposition naturelle	**5**
M-3.2.2	Évaluation des facteurs de réduction de risque agissant sur la potentialité à partir d'un audit de sécurité MEHARI	**5**
M-3.2.3	Évaluation de la potentialité	**5**
M-3.2.4	Évaluation de l'impact intrinsèque	**5**
M-3.2.5	Évaluation des facteurs de réduction de risque agissant sur l'impact à partir d'un audit de sécurité MEHARI	**5**
M-3.2.6	Évaluation de la réduction d'impact	**5**

M-3.2.7	Évaluation de l'impact	5
M-3.2.8	Évaluation globale du risque	5
M-3.3.1	Plans d'action basés sur l'analyse de risques	6
	Méthode OCTAVE	
O-1.1.1	Obtenir le soutien de la haute direction pour l'étude OCTAVE	❖
O-1.1.2	Sélectionner les membres de l'équipe d'analyse	❖
O-1.1.3	Former l'équipe d'analyse	❖
O-1.1.4	Sélectionner les secteurs opérationnels de l'entreprise qui participeront à l'étude OCTAVE	1
O-1.1.5	Sélectionner les participants	❖
O-1.1.6	Coordonner la logistique	❖
O-1.1.7	Donner des instructions aux participants	❖
O-2.1.1	Identifier et prioriser les actifs utilisés par l'entreprise selon la haute direction	2
O-2.1.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon la haute direction	3
O-2.1.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon la haute direction	3
O-2.1.4	Obtenir la connaissance de la haute direction envers la stratégie de protection actuelle et des vulnérabilités de l'entreprise	4
O-2.1.5	Choisir ou confirmer les secteurs opérationnels visés par l'évaluation ainsi que les directeurs qui participeront à l'étude	❖
O-2.2.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les directeurs de secteurs opérationnels	2
O-2.2.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels	3
O-2.2.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels	3
O-2.2.4	Obtenir la connaissance des directeurs de secteurs opérationnels envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise	4
O-2.2.5	Choisir ou confirmer les membres du personnel qui participeront à l'étude	❖
O-2.2.6	Communiquer les résultats du *Processus 1*	❖
O-2.3.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les membres du personnel	2
O-2.3.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les membres du personnel	3
O-2.3.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les membres du personnel	3
O-2.3.4	Obtenir la connaissance des membres du personnel envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise	4
O-2.3.5	Communiquer les résultats des *Processus 1 et 2*	❖
O-2.4.1	Regrouper, par groupe consulté, les actifs identifiés	2
O-2.4.2	Regrouper, par groupe consulté et par actif, les exigences de sécurité	3
O-2.4.3	Regrouper, par groupe consulté et par actif, les préoccupations et leurs impacts	3
O-2.4.4	Sélectionner les actifs critiques	2
O-2.4.5	Raffiner les exigences de sécurité à l'égard des actifs critiques	3
O-2.4.6	Identifier les menaces qui pèsent sur les actifs critiques	4
O-2.4.7	Inscrire les préoccupations dans le livrable contenant les profils des	4

	actifs	
O-3.1.1	Identifier les types de composantes	4
O-3.1.2	Identifier les composantes de l'infrastructure à examiner	4
O-3.2.1	Exécuter les outils d'évaluation de vulnérabilités sur les composantes de l'infrastructure sélectionnées	4
O-3.2.2	Réviser les vulnérabilités technologiques et résumer les résultats	4
O-4.1.1	Identifier les impacts des menaces qui pèsent sur les actifs critiques	5
O-4.1.2	Créer les critères d'évaluation du risque	5
O-4.1.3	Évaluer les impacts des menaces qui pèsent sur les actifs critiques	5
O-4.2.1	Compiler les résultats des questionnaires	6
O-4.2.2	Consolider les informations recueillies sur la stratégie de protection	6
O-4.2.3	Réviser les vulnérabilités technologiques, les pratiques de la stratégie de protection, les exigences de sécurité, les vulnérabilités de l'entreprise et les informations concernant les risques	6
O-4.2.4	Créer la stratégie de protection	6
O-4.2.5	Créer les plans de mitigation	6
O-4.2.6	Créer la liste d'actions	6
O-4.2.7	Compiler un résumé des actifs	2
O-4.2.8	Compiler les profils de risques	5
O-4.2.9	Compiler la stratégie de protection de l'entreprise	6
O-4.2.10	Compiler les plans de mitigation	6
O-4.2.11	Compiler la liste d'actions	6
O-4.2.12	Réviser les informations sur les risques	5
O-4.2.13	Réviser et raffiner la stratégie de protection, les plans de mitigation et la liste d'actions	6
O-4.2.14	Créer les prochaines étapes	❖
O-4.2.15	Documenter la stratégie de protection, les plans de mitigation des risques, la liste d'actions et les prochaines étapes	6

Les résultats de cette première étape pour la création de la liste des activités générales de la gestion des risques révèlent donc que parmi les 119 activités de sécurité initialement identifiées à partir des méthodes, 117 d'entre elles ont été associées à une étape de la gestion des risques. De plus, les résultats indiquent que les différentes activités ont été reliées aux étapes 1 à 6 de la gestion des risques. Par conséquent, aucune activité de sécurité des méthodes étudiées n'a été associée aux deux dernières étapes de la phase « *Traitement des risques* » qui sont les suivantes : n° 6 - *Sélection des mesures de sécurité* et n° 7 - *Implantation des mesures de sécurité*. Il est alors possible d'en déduire que les trois méthodes de gestion des risques étudiées ne couvrent pas toutes les étapes de la gestion des risques telles que définies dans la présente recherche.

La deuxième étape visait à établir la liste finale en traitant tout d'abord chacun des regroupements d'activités produits à l'étape précédente et, ensuite, en prenant leurs résultats pour en dresser la liste complète. À l'intérieur même de chacun des regroupements d'activité de sécurité, les traitements suivants ont donc été effectués :

a. Fusionner les activités dont les concepts de sécurité, au niveau de leur but, sont identiques.

b. Pour chacune des activités prises intégralement ou suite à une fusion, créer une nouvelle activité équivalente en reformulant le titre et la description de l'activité en question de façon à utiliser des termes génériques. Le tout en considérant l'utilisation des termes adéquats selon les concepts à véhiculer et le vocabulaire général du domaine.

c. Une fois la totalité des activités générales créées dans un regroupement, les placer en ordre chronologique de réalisation afin de faciliter l'identification des interdépendances.

Après avoir appliqué ces différents traitements, chacun des regroupements contenait alors une courte liste d'activités générales de la gestion des risques de sécurité. Une difficulté est toutefois survenue qu'il est important de signaler :

- Il s'est avéré que certaines activités de sécurité provenant des méthodes pouvaient contribuer à plus d'une activité générale. Cette situation survient lorsque dans la même activité, deux tâches sont effectuées et peuvent être logiquement séparées sans risque d'altérer les résultats à produire. C'est le cas lorsque deux méthodes sont comparées et que l'une d'entre elles propose deux concepts qui se répercutent en deux activités à réaliser et que, dans la seconde méthode, celle-ci inclut les deux mêmes concepts dans une seule et même activité.

  Par exemple, l'activité *M-1.1.3 - Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés* établit à la fois une échelle de valeurs pour la gravité des dysfonctionnements et procède également à l'évaluation de ceux-ci par le biais d'entretiens avec les responsables de l'entreprise. D'un point de vue des tâches à accomplir, elles sont complémentaires, mais elles représentent deux actions bien différentes. Ainsi, l'activité *M 1.1.*3 fut l'une des sources pour deux activités générales, soit :

  - 29 - Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité;

- 30 - Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et de son environnement.

Les activités de sécurité qui ont contribué à la création de plus d'une activité générale sont annotées du caractère « * » devant leur code de référence dans les tableaux de résultats qui sont présentés plus loin dans cette section (exemple : **M-1.1.3*).

Il s'est donc avéré que plusieurs scénarios étaient possibles pour la création d'une activité générale de la gestion des risques de sécurité. La figure 4.4 résume donc ces trois scénarios tels qu'énoncés précédemment. Il est à noter que les exemples présentés dans la figure sont véritables puisqu'ils proviennent des résultats obtenus.

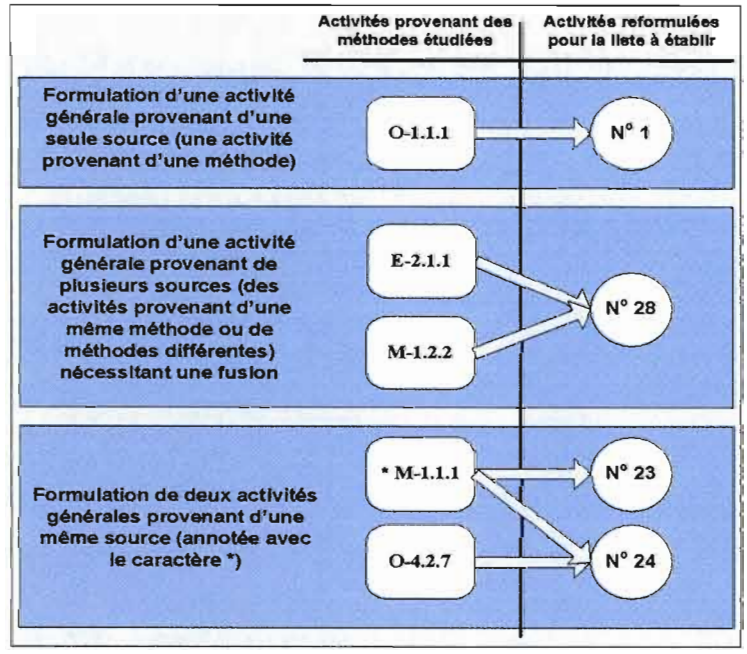

Figure 4.4 Scénarios de création d'une activité générale.

Les tableaux 4.5 à 4.11 qui suivent démontrent les traitements expliqués précédemment en fonction des trois scénarios possibles de création d'une activité générale. Chaque tableau représente un regroupement d'activités basé sur l'une des étapes de la gestion des risques.

La partie « A » de chacun des tableaux contient les activités de sécurité provenant des méthodes et ayant été associées à cette étape de la gestion des risques lors de l'étape 1 de la création

de la liste des activités générales. Quant à la partie « B », il s'agit des résultats obtenus suite aux traitements effectués pour la création des activités générales tels qu'expliqués plus tôt (les scénarios de création). Pour chaque activité générale créée, les informations suivantes sont spécifiées : un titre, une description et les sources (activités de sécurité provenant des méthodes) utilisées pour sa création.

Tableau 4.5

Tableau de création des activités générales de la gestion des risques pour l'étape ❖

Étape ❖ : Organisation de la démarche		
A) Les activités des méthodes contribuant à l'étape ❖		
	N° Activités	**Activités**
	O-1.1.1	Obtenir le soutien de la haute direction pour l'étude OCTAVE
	O-1.1.2	Sélectionner les membres de l'équipe d'analyse
	O-1.1.3	Former l'équipe d'analyse
	O-1.1.5	Sélectionner les participants
	O-1.1.6	Coordonner la logistique
	O-1.1.7	Donner des instructions aux participants
	O-2.1.5	Choisir ou confirmer les secteurs opérationnels visés par l'évaluation ainsi que les directeurs qui participeront à l'étude
	O-2.2.5	Choisir ou confirmer les membres du personnel qui participeront à l'étude
	O-2.2.6	Communiquer les résultats du Processus 1
	O-2.3.5	Communiquer les résultats des Processus 1 et 2
	O-4.2.14	Créer les prochaines étapes
B) Les activités générales formulées à partir des activités des méthodes		
	1	**Obtenir un soutien adéquat des parties prenantes du projet** L'activité consiste à obtenir les appuis nécessaires et visibles de la part des parties prenantes pour la réalisation des activités de sécurité durant la démarche et plus précisément, les aspects suivants : l'encouragement actif, la délégation des responsabilités et des autorités, l'attribution des ressources nécessaires, la participation à la révision des résultats et la prise de décisions sur les actions appropriées. Activité(s) liée(s) : O-1.1.1
	2	**Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information** L'activité consiste à former une équipe de personnes multidisciplinaires qui participeront activement à la réalisation des activités de sécurité durant la démarche, et ce, sur différents aspects du travail dont la gestion, la communication, l'analyse et l'élaboration des solutions. Activité(s) liée(s) : O-1.1.2
	3	**Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir** L'activité consiste à préparer les membres de l'équipe aux tâches qu'ils devront accomplir en les familiarisant avec le matériel à utiliser et les ateliers à réaliser. Activité(s) liée(s) : O-1.1.3

4	**Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche** L'activité consiste à identifier les personnes requises pour la réalisation des activités de sécurité et à former des groupes distincts selon leurs responsabilités dans l'entreprise, leurs implications dans la démarche ou toute autre division logique qui permettrait de couvrir tous les besoins nécessaires aux activités de sécurité de la démarche. Activité(s) liée(s) : O-1.1.5
5	**Informer les participants sur les activités de sécurité à réaliser durant la démarche** L'activité consiste à informer chacun des participants, via son groupe respectif, sur le but de la démarche de sécurité et sur le rôle qui lui est demandé d'assumer. Activité(s) liée(s) : O-1.1.7
6	**Établir la logistique de la démarche** L'activité consiste à planifier la démarche de sécurité en présentant un calendrier des activités et les éléments nécessaires pour leur réalisation (les ateliers, les personnes impliquées, le matériel, etc.). Activité(s) liée(s) : O-1.1.6
7	**Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche** L'activité consiste à obtenir une confirmation, avant de débuter les ateliers de groupe, attestant que les participants sélectionnés représentent bien les personnes adéquates dans leur domaine d'expertise au sein de l'entreprise et qu'elles ont le temps nécessaire pour prendre part à la démarche. Activité(s) liée(s) : O-2.1.5 / O-2.2.5
8	**Communiquer les résultats obtenus lors des consultations avec les groupes de participants** L'activité consiste à présenter, aux différents groupes de participants, les résultats obtenus lors des consultations avec les autres groupes pour fin de comparaison. Activité(s) liée(s) : O-2.2.6 / O-2.3.5
9	**Planifier la mise en œuvre des mesures de sécurité proposées par la démarche** L'activité consiste à planifier la mise en œuvre des mesures proposées par la démarche en précisant celles qui seront implantées, par qui et à quel moment. Activité(s) liée(s) : O-4.2.14

Tableau 4.6

Tableau de création des activités générales de la gestion des risques pour l'étape n° 1

Étape n° 1 : Identification et étude du contexte		
A) Les activités des méthodes contribuant à l'étape n° 1		
	N° Activités	**Activités**
	E-1.1.1	Présenter l'organisme
	E-1.1.2	Lister les contraintes pesant sur l'organisme
	E-1.1.3	Lister les références réglementaires applicables à l'organisme
	E-1.1.4	Faire une description fonctionnelle du SI global
	E-1.2.1	Présenter le système-cible
	E-1.2.2	Lister les enjeux
	E-1.2.4	Faire une description fonctionnelle du système-cible
	E-1.2.5	Lister les hypothèses
	E-1.2.6	Lister les règles de sécurité
	E-1.2.7	Lister les contraintes pesant sur le système-cible
	E-1.2.8	Lister les références réglementaires spécifiques au système-cible
	O-1.1.4	Sélectionner les secteurs opérationnels de l'entreprise qui participeront à l'étude OCTAVE
B) Les activités générales formulées à partir des activités des méthodes		
	10	**Décrire l'environnement de la cible** L'activité consiste à décrire sommairement l'environnement de la cible pour préciser le but, le contexte d'utilisation et son importance dans le système d'information de l'entreprise. Activité(s) liée(s) : E-1.1.1
	11	**Identifier les contraintes à l'égard de l'environnement de la cible** L'activité consiste à identifier les contraintes (stratégiques, fonctionnelles, structurelles, politiques, budgétaires, etc.) à l'égard de l'environnement de la cible, puisqu'elles pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique. Activité(s) liée(s) : E-1.1.2
	12	**Identifier le cadre légal de l'environnement de la cible** L'activité consiste à identifier les lois et les règlements auxquels l'environnement de la cible est assujetti, puisqu'ils pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique. Activité(s) liée(s) : E-1.1.3
	13	**Décrire l'aspect fonctionnel de l'environnement de la cible** L'activité consiste à décrire l'aspect fonctionnel de l'environnement de la cible afin de démontrer les domaines fonctionnels qui contribuent à la réalisation des besoins d'affaires, à obtenir une vue d'ensemble de son fonctionnement et de ses interactions avec les autres éléments du système d'information de l'entreprise et, finalement, à comprendre les interactions entre les éléments contenus dans l'environnement lui-même.

	Activité(s) liée(s) : E-1.1.4
14	**Préciser la cible de la démarche de sécurité** L'activité consiste à préciser la cible à considérer dans la démarche de sécurité en spécifiant sa portée, ses finalités et ses interactions à travers l'environnement et le système d'information de l'entreprise (acteurs, domaines fonctionnels, systèmes, etc.). Activité(s) liée(s) : E-1.2.1 / O-1.1.4
15	**Identifier les enjeux à l'égard de la cible** L'activité consiste à identifier les gains et les pertes potentiels (financiers, techniques, politiques, etc.) à l'égard de la cible et à démontrer ainsi l'importance de son rôle dans l'environnement et le système d'information de l'entreprise. Activité(s) liée(s) : E-1.2.2
16	**Décrire l'aspect fonctionnel de la cible** L'activité consiste à décrire l'aspect fonctionnel de la cible pour démontrer les traitements effectués, les intrants et les extrants informationnels, les finalités attendues et les interactions fonctionnelles avec les éléments existants de l'environnement et du système d'information de l'entreprise. Activité(s) liée(s) : E-1.2.4
17	**Identifier les hypothèses à l'égard de la cible** L'activité consiste à identifier les informations prises pour acquises à l'égard de la cible et qui ne seront pas démontrées dans la démarche de sécurité. Activité(s) liée(s) : E-1.2.5
18	**Identifier les règles de sécurité à l'égard de la cible** L'activité consiste à identifier toutes les règles et les mesures de sécurité (la politique de sécurité, les plans de continuité, etc.) auxquelles la cible est assujettie, puisqu'elles pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique. Activité(s) liée(s) : E-1.2.6
19	**Identifier les contraintes à l'égard de la cible** L'activité consiste à identifier les contraintes (financières, techniques, temporelles, de ressources, d'expertise, organisationnelles, etc.) à l'égard de la cible, puisqu'elles pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique. Activité(s) liée(s) : E-1.2.7
20	**Identifier le cadre légal de la cible** L'activité consiste à identifier les lois et les règlements auxquels la cible est assujettie, puisqu'ils pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique. Activité(s) liée(s) : E-1.2.8

Tableau 4.7

Tableau de création des activités générales de la gestion des risques pour l'étape n° 2

Étape n° 2 : Identification des actifs informationnels		
A) Les activités des méthodes contribuant à l'étape n° 2		
	N° Activités	**Activités**
	E-1.2.3	Lister les éléments essentiels
	E-1.3.1	Lister et décrire les entités du système
	E-1.3.2	Croiser les éléments essentiels et les entités
	M-1.1.1	Identification des activités majeures et de leurs finalités
	O-2.1.1	Identifier et prioriser les actifs utilisés par l'entreprise selon la haute direction
	O-2.2.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les directeurs de secteurs opérationnels
	O-2.3.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les membres du personnel
	O-2.4.1	Regrouper, par groupe consulté, les actifs identifiés
	O-2.4.4	Sélectionner les actifs critiques
	O-4.2.7	Compiler un résumé des actifs
B) Les activités générales formulées à partir des activités des méthodes		
	21	**Rencontrer les groupes de participants pour identifier les actifs importants de la cible** L'activité consiste à rencontrer les groupes de participants afin d'identifier les actifs importants faisant partie de la cible et d'en déterminer le degré d'importance relative entre eux. Activité(s) liée(s) : O-2.1.1 / O-2.2.1 / O-2.3.1
	22	**Rédiger une liste des actifs identifiés par groupes de participants rencontrés** L'activité consiste à lister les actifs importants de la cible, par groupes consultés, et à justifier leur degré d'importance relative. Activité(s) liée(s) : O-2.4.1
	23	**Identifier les actifs critiques de la cible** L'activité consiste à sélectionner, à partir des actifs importants identifiés et leur degré d'importance relative, ceux étant essentiels pour le bon fonctionnement de la cible. Activité(s) liée(s) : E-1.2.3 / *M-1.1.1 / O-2.4.4
	24	**Rédiger une liste intégrée de tous les actifs identifiés** L'activité consiste à lister l'ensemble des actifs importants de la cible et à préciser ceux ayant été jugés critiques, en y ajoutant des détails quant à leur utilisation en général, leurs buts, leurs finalités, etc. Activité(s) liée(s) : *M-1.1.1 / O-4.2.7
	25	**Identifier les actifs de support aux actifs critiques de la cible** L'activité consiste à identifier les actifs technologiques dont dépendent les actifs critiques de la cible, puisqu'une attaque pourrait en faire l'usage dans le but final d'atteindre un actif critique.

	Activité(s) liée(s) : E-1.3.1
26	**Documenter les dépendances entre les actifs critiques et les actifs de support** L'activité consiste à schématiser, de manière matricielle, les liens entre les actifs critiques et les actifs de support pour bien démontrer les dépendances existantes. Activité(s) liée(s) : E-1.3.2

Tableau 4.8

Tableau de création des activités générales de la gestion des risques pour l'étape n° 3

Étape n° 3 : Identification et évaluation des besoins de sécurité	
A) Les activités des méthodes contribuant à l'étape n° 3	
N° Activités	**Activités**
E-2.1.1	Choisir les critères de sécurité à prendre en compte
E-2.1.2	Déterminer l'échelle de besoins
E-2.1.3	Déterminer les impacts pertinents
E-2.2.1	Attribuer un besoin de sécurité par critère de sécurité (disponibilité, intégrité, confidentialité…) à chaque élément essentiel
M-1.1.2	Identification des dysfonctionnements redoutés
M-1.1.3	Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés
M-1.1.4	Échelle de valeurs des dysfonctionnements
M-1.2.1	Identification des éléments à classifier
M-1.2.2	Critères de classification
M-1.2.3	Processus de classification
O-2.1.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon la haute direction
O-2.1.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon la haute direction
O-2.2.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels
O-2.2.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels
O-2.3.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les membres du personnel
O-2.3.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les membres du personnel
O-2.4.2	Regrouper, par groupe consulté et par actif, les exigences de sécurité
O-2.4.3	Regrouper, par groupe consulté et par actif, les préoccupations et leurs impacts
O-2.4.5	Raffiner les exigences de sécurité à l'égard des actifs critiques
B) Les activités générales formulées à partir des activités des méthodes	
27	**Regrouper les actifs critiques ayant des besoins de sécurité similaires** L'activité consiste à regrouper, au besoin, les actifs critiques qui nécessitent le même degré de protection et pour lesquels l'évaluation pourrait être effectuée qu'une seule fois pour l'ensemble de ces actifs.

	Activité(s) liée(s) : M-1.2.1
28	**Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité** L'activité consiste à déterminer et à décrire les critères de sécurité (disponibilité, intégrité, confidentialité, imputabilité, etc.) qui seront utilisés dans la démarche pour évaluer les besoins de sécurité des actifs critiques de la cible. Activité(s) liée(s) : E-2.1.1 / M-1.2.2
29	**Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité** L'activité consiste à décrire une échelle de valeurs pour chacun des critères de sécurité, en spécifiant ce que chaque valeur signifie dans le contexte du critère en question incluant ses paramètres de seuil, et une échelle de valeurs exprimant des niveaux de gravité d'impact. Activité(s) liée(s) : E-2.1.2 / *M-1.1.3
30	**Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement** L'activité consiste à rencontrer les groupes de participants afin d'identifier les situations représentant une préoccupation pour eux (une menace possible, un dysfonctionnement redouté, un impact significatif, etc.) envers la cible et son environnement, ces mêmes préoccupations pouvant être caractérisées par des informations additionnelles comme une source ou une finalité générant un impact. Activité(s) liée(s) : E-2.1.3 / M-1.1.2 / *M-1.1.3 / O-2.1.2 / O-2.2.2 / O-2.3.2
31	**Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés** L'activité consiste à consolider, par groupe et par actif, les informations recueillies au moment de l'identification des préoccupations et de leurs impacts généraux envers la cible et son environnement par les groupes de participants rencontrés. Activité(s) liée(s) : O-2.4.3 / M-1.1.4
32	**Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques** L'activité consiste à rencontrer les groupes de participants afin d'évaluer les besoins de sécurité des actifs critiques, en effectuant les étapes suivantes pour chacun des actifs : attribuer une valeur pour chacun des critères de sécurité de façon globale ou en fonction de chacun des impacts pertinents, justifier la valeur résultante (la globale ou la plus élevée dans le cas des valeurs multiples) pour chaque critère de sécurité et, finalement, classer les critères en ordre d'importance de criticité selon l'actif en question. Activité(s) liée(s) : *E-2.2.1 / M-1.2.3 / O-2.1.3 / O-2.2.3 / O-2.3.3
33	**Rédiger une synthèse des besoins de sécurité pour les actifs critiques**

	L'activité consiste à consolider, sous différentes formes de présentation et de regroupement, les besoins de sécurité recueillis pour chacun des actifs critiques de la cible et, du même coup, à leur déterminer une valeur finale pour chacun des critères de sécurité et le critère qui s'avère le plus critique. Activité(s) liée(s) : *E-2.2.1 / O-2.4.2 / O-2.4.5
34	**Valider les besoins de sécurité pour les actifs critiques** L'activité consiste à présenter, à modifier au besoin et à obtenir un consensus sur les informations relatives aux besoins de sécurité pour les actifs critiques par les parties prenantes. Activité(s) liée(s) : *E-2.2.1

Tableau 4.9

Tableau de création des activités générales de la gestion des risques pour l'étape n° 4

Étape n° 4 : Identification et évaluation des menaces et des vulnérabilités	
A) Les activités des méthodes contribuant à l'étape n° 4	
N° Activités	**Activités**
E-3.1.1	Lister les méthodes d'attaques pertinentes
E-3.1.2	Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter
E-3.1.3	Caractériser, pour chaque méthode d'attaque retenue, les éléments menaçants associés par leur type (naturel, humain ou environnemental) et leur cause (accidentelle ou délibérée)
E-3.1.4	Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant
E-3.1.5	Mettre en évidence les méthodes d'attaque non retenues avec des justifications
E-3.2.1	Identifier les vulnérabilités des entités selon les méthodes d'attaque
E-3.2.2	Estimer éventuellement le niveau des vulnérabilités
E-3.3.1	Formuler explicitement les menaces
E-3.3.2	Hiérarchiser éventuellement les menaces selon leur opportunité
M-2.1.1	Élaboration du schéma d'audit
M-2.1.2	Évaluation des services de sécurité
M-2.1.3	Synthèse des vulnérabilités
O-2.1.4	Obtenir la connaissance de la haute direction envers la stratégie de protection actuelle et des vulnérabilités de l'entreprise
O-2.2.4	Obtenir la connaissance des directeurs de secteurs opérationnels envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise
O-2.3.4	Obtenir la connaissance des membres du personnel envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise
O-2.4.6	Identifier les menaces qui pèsent sur les actifs critiques
O-2.4.7	Inscrire les préoccupations dans le livrable contenant les profils des actifs
O-3.1.1	Identifier les types de composantes
O-3.1.2	Identifier les composantes de l'infrastructure à examiner
O-3.2.1	Exécuter les outils d'évaluation de vulnérabilités sur les composantes de

	l'infrastructure sélectionnés
O-3.2.2	Réviser les vulnérabilités technologiques et résumer les résultats
O-4.2.1	Compiler les résultats des questionnaires
O-4.2.2	Consolider les informations recueillies sur la stratégie de protection

B) Les activités générales formulées à partir des activités des méthodes

35	**Identifier les éléments de la cible à auditer** L'activité consiste à identifier les éléments (actifs critiques ou de support) de la cible ou reliés à celle-ci et sur lesquels un audit de sécurité sera effectué, tout en les regroupant par similarités en termes de besoin de sécurité pour une diminution de la quantité de travail, si cela est souhaité. Activité(s) liée(s) : *M-2.1.1 / O-3.1.1 / O-3.1.2
36	**Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité** L'activité consiste à sélectionner et à préparer le matériel et les outils nécessaires (questionnaires, logiciels, etc.) pour la réalisation des audits de sécurité à réaliser. Activité(s) liée(s) : *M-2.1.1
37	**Effectuer l'audit de sécurité organisationnelle de la cible** L'activité consiste à auditer les éléments de type « processus/services » relativement à leur développement et à leur utilisation, et ce, à l'aide de documents sur les bonnes pratiques en la matière, de l'analyse des exploitations possibles par les méthodes d'attaque et des questionnaires d'audit remplis lors de rencontres avec les groupes de participants. Activité(s) liée(s) : M-2.1.2 / O-2.1.4 / O-2.2.4 / O-2.3.4
38	**Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible** L'activité consiste à consolider et à raffiner au besoin les informations recueillies suite à la réalisation des audits de sécurité organisationnelle réalisés, dont celles par groupes de participants rencontrés. Activité(s) liée(s) : O-4.2.1 / O-4.2.2
39	**Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support** L'activité consiste à identifier les méthodes d'attaque sur les actifs de support, incluant l'identification et l'évaluation de leurs éléments menaçants, dont leur réalisation est possible et où un impact est prévu, tout en justifiant également celles qui auraient été intentionnellement écartées de la sélection. Activité(s) liée(s) : E-3.1.1 / E-3.1.2 / E-3.1.3 / E-3.1.4 / E-3.1.5
40	**Effectuer l'audit de sécurité technique de la cible** L'activité consiste à auditer les éléments de type « actifs » relativement à leur fonctionnement technologique, et ce, à l'aide des documents de référence en la matière, de logiciels et des gens possédant l'expertise requise pour les utiliser. Activité(s) liée(s) : E-3.2.1 / E-3.2.2 / O-3.2.1

41	**Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible** L'activité consiste à consolider, par actifs critiques concernés, les informations recueillies suite à la réalisation des audits de sécurité technique réalisés et à raffiner les résultats au besoin. Activité(s) liée(s) : O-3.2.2
42	**Documenter les informations sur les vulnérabilités identifiées** L'activité consiste à résumer et à présenter sous différentes formes (par service de sécurité, par thème de sécurité, globalement, etc.) les vulnérabilités identifiées par les audits de sécurité réalisés sur les éléments sélectionnés de la cible ou reliés à celle-ci. Activité(s) liée(s) : M-2.1.3
43	**Identifier les menaces à l'égard des actifs critiques de la cible** L'activité consiste à identifier les menaces redoutées pour chacun des actifs critiques de la cible et à les détailler en spécifiant leur type (fonctionnel ou technique), leur portée, l'actif visé, les acteurs impliqués, le motif, les éléments menaçants la méthode d'attaque, les vulnérabilités exploitées, etc. Activité(s) liée(s) : *E-3.3.1 / O-2.4.6
44	**Évaluer les menaces à l'égard des actifs critiques de la cible** L'activité consiste à quantifier les menaces en leur attribuant une valeur déterminée à l'aide d'une échelle de valeurs, où chaque niveau est clairement défini par les paramètres significatifs et les valeurs de seuil. Activité(s) liée(s) : *E-3.3.1
45	**Documenter les informations sur les menaces identifiées** L'activité consiste à documenter et à résumer les menaces identifiées pour les actifs critiques de la cible, et ce, en spécifiant les informations qui composent une menace : les méthodes d'attaque, les éléments menaçants, les valeurs obtenues à l'évaluation, la facilité de réalisation, les impacts d'une réalisation, etc. Activité(s) liée(s) : E-3.3.2 / O-2.4.7

Tableau 4.10

Tableau de création des activités générales de la gestion des risques pour l'étape n° 5

Étape n° 5 : Identification et évaluation des risques	
A) Les activités des méthodes contribuant à l'étape n° 5	
N° Activités	**Activités**
E-4.1.1	Déterminer les risques en confrontant menaces et besoins de sécurité
E-4.1.2	Formuler explicitement les risques
E-4.1.3	Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces
E-4.1.4	Mettre en évidence les risques non retenus (risques résiduels) avec des

	justifications
M-3.1.1	Sélection des scénarios critiques devant être pris en compte pour une analyse des risques
M-3.2.1	Évaluation de l'exposition naturelle
M-3.2.2	Évaluation des facteurs de réduction de risque agissant sur la potentialité à partir d'un audit de sécurité MEHARI
M-3.2.3	Évaluation de la potentialité
M-3.2.4	Évaluation de l'impact intrinsèque
M-3.2.5	Évaluation des facteurs de réduction de risque agissant sur l'impact à partir d'un audit de sécurité MEHARI
M-3.2.6	Évaluation de la réduction d'impact
M-3.2.7	Évaluation de l'impact
M-3.2.8	Évaluation globale du risque
O-4.1.1	Identifier les impacts des menaces qui pèsent sur les actifs critiques
O-4.1.2	Créer les critères d'évaluation du risque
O-4.1.3	Évaluer les impacts des menaces qui pèsent sur les actifs critiques
O-4.2.8	Compiler les profils de risques
O-4.2.12	Réviser les informations sur les risques

B) Les activités générales formulées à partir des activités des méthodes

46	**Identifier les risques potentiels envers la cible** L'activité consiste à identifier les risques potentiels qui pèsent sur les actifs critiques, en établissant plus formellement les impacts qu'aurait la réalisation de chacune des menaces, en confrontant les menaces aux besoins des sécurités des actifs critiques et en consultant des documents de référence en la matière tels que des bases de connaissances de scénarios de risques. Activité(s) liée(s) : E-4.1.1 / *M-3.1.1 / O-4.1.1
47	**Sélectionner les risques à considérer dans le cadre d'une analyse de risques** L'activité consiste à sélectionner, dans la liste des risques identifiés, ceux affectant le plus considérablement les actifs critiques de la cible et dont une évaluation plus détaillée sera effectuée, tout en justifiant également ceux qui sont écartés de la sélection. Activité(s) liée(s) : E-4.1.3 / E-4.1.4 / *M-3.1.1
48	**Définir les facteurs d'évaluation du risque** L'activité consiste à définir les outils nécessaires (les échelles de valeurs appropriées et la grille d'acceptation du risque) pour l'évaluation des risques sélectionnés, et ce, au niveau de leur potentialité, de leur impact, et de manière globale. Activité(s) liée(s) : O-4.1.2
49	**Évaluer la potentialité des risques** L'activité consiste à déterminer une valeur représentant la potentialité de chacun des risques, à l'aide de l'échelle de valeurs prédéfinie pour ce facteur d'évaluation, en fonction d'une première évaluation indépendante de toute mesure de sécurité et, ensuite, d'un ajustement à la baisse en fonction des mesures dissuasives et de prévention déjà en place pour la cible.

	Activité(s) liée(s) : M-3.2.1 / M-3.2.2 / M-3.2.3
50	**Évaluer l'impact des risques** L'activité consiste à déterminer une valeur représentant l'impact de chacun des risques, à l'aide de l'échelle de valeurs prédéfinie pour ce facteur d'évaluation, en fonction d'une première évaluation indépendante de toute mesure de sécurité et, ensuite, d'un ajustement à la baisse en fonction des mesures palliatives, de protection et de récupération déjà en place pour la cible. Activité(s) liée(s) : M-3.2.4 / M-3.2.5 / M-3.2.6 / M-3.2.7 / O-4.1.3
51	**Évaluer globalement les risques à partir de sa potentialité et de son impact** L'activité consiste à déterminer la valeur globale des risques en utilisant les valeurs obtenues suite à l'évaluation des facteurs de potentialité et d'impact pour le risque en question et en transposant celles-ci dans la grille d'acceptabilité du risque. Activité(s) liée(s) : M-3.2.8
52	**Documenter les risques évalués** L'activité consiste à documenter les risques évalués en spécifiant les informations qui lui sont reliées : la menace (éléments menaçants, méthode d'attaque employée, facilité de réalisation, etc.), les vulnérabilités exploitées, les critères de sécurité affectés, les impacts sur la cible, les actifs concernés (actifs critiques et actifs de support), les valeurs obtenues lors des évaluations, etc. Activité(s) liée(s) : E-4.1.2 / O-4.2.8
53	**Valider les risques identifiés pour les actifs critiques avec les parties prenantes** L'activité consiste à présenter, à modifier au besoin et à faire approuver les informations relatives aux risques envers les actifs critiques par les parties prenantes. Activité(s) liée(s) : O-4.2.12

Tableau 4.11

Tableau de création des activités générales de la gestion des risques pour l'étape n° 6

Étape n° 6 : Identification des exigences de sécurité	
A) Les activités des méthodes contribuant à l'étape n° 6	
N° Activités	**Activités**
E-4.2.1	Lister les objectifs de sécurité
E-4.2.2	Justifier la complétude de la couverture, en vérifiant la compatibilité avec les contraintes pesant sur l'organisme et le système-cible : des risques, des hypothèses (et les enjeux) et des règles de sécurité (et les références réglementaires)
E-4.2.3	Classer éventuellement les objectifs de sécurité en deux catégories : objectifs de sécurité portant sur le système-cible et objectifs de sécurité portant sur l'environnement du système-cible
E-4.2.4	Mettre en évidence les défauts de couverture (risques résiduels) avec des justifications

E-4.3.1	Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité
E-4.3.2	Choisir le niveau des exigences d'assurance
E-5.1.1	Lister les exigences de sécurité fonctionnelles
E-5.1.2	Justifier la complétude de la couverture des objectifs de sécurité
E-5.1.3	Mettre en évidence les éventuels défauts de couverture (risques résiduels) avec des justifications
E-5.1.4	Classer les exigences de sécurité fonctionnelles en deux catégories : exigences de sécurité fonctionnelles portant sur le système-cible et exigences de sécurité fonctionnelles portant sur l'environnement du système-cible
E-5.1.5	Justifier éventuellement la couverture des dépendances des exigences de sécurité fonctionnelles
E-5.2.1	Lister les exigences de sécurité d'assurance
E-5.2.2	Classer éventuellement les exigences de sécurité d'assurance en deux catégories : exigences de sécurité d'assurance portant sur l'environnement du système-cible et exigences de sécurité d'assurances portant sur l'environnement du système-cible
E-5.2.3	Justifier éventuellement la couverture des dépendances des exigences de sécurité d'assurance
M-3.3.1	Plans d'action basés sur l'analyse de risques
O-4.2.3	Réviser les vulnérabilités technologiques, les pratiques de la stratégie de protection, les exigences de sécurité, les vulnérabilités de l'entreprise et les informations concernant les risques
O-4.2.4	Créer la stratégie de protection
O-4.2.5	Créer les plans de mitigation
O-4.2.6	Créer la liste d'actions
O-4.2.9	Compiler la stratégie de protection de l'entreprise
O-4.2.10	Compiler les plans de mitigation
O-4.2.11	Compiler la liste d'actions
O-4.2.13	Réviser et raffiner la stratégie de protection, les plans de mitigation et la liste d'actions
O-4.2.15	Documenter la stratégie de protection, les plans de mitigation des risques, la liste d'actions et les prochaines étapes
B) Les activités générales formulées à partir des activités des méthodes	
54	**Réviser toutes les informations recueillies, traitées et produites durant la démarche** L'activité consiste à analyser et à réviser toutes les informations accumulées durant la démarche telles que le contexte de la cible et de son environnement, les actifs identifiés, les besoins de sécurité des actifs critiques, les menaces et les vulnérabilités de sécurité organisationnelle et technique, les risques, etc. Activité(s) liée(s) : O-4.2.3
55	**Déterminer les recommandations sur des exigences de sécurité de haut niveau** L'activité consiste à établir des recommandations sur des exigences de sécurité de haut niveau qui peuvent être d'ordre général (stratégique ou opérationnel) en matière de bonnes pratiques ou bien, plus précisément, dans le but de couvrir les risques identifiés durant la démarche, et ce, en spécifiant les informations suivantes : les composantes du risque qui sont ciblées (l'origine de la menace, les vulnérabilités exploitées ou les conséquences de réalisation), la portée visée (la cible ou l'environnement), le niveau de résistance et d'assurance de sécurité souhaité.

	Activité(s) liée(s) : E-4.2.1 / E-4.2.3 / E-4.3.1 / E-4.3.2 / *M-3.3.1 / O-4.2.4
56	**Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau** L'activité consiste à démontrer les liens entre les recommandations de sécurité de haut niveau établies et les risques qu'ils couvrent, et ce, en indiquant un niveau de couverture (nul, partiel et total) pour chacun des risques et en justifiant tous les cas où le niveau de couverture n'est pas total. Activité(s) liée(s) : E-4.2.2 / E-4.2.4
57	**Résumer les informations sur les recommandations de sécurité de haut niveau** L'activité consiste à résumer les informations sur les recommandations de sécurité de haut niveau de manière concise en vue de les présenter aux parties prenantes et, de plus, à indiquer les recommandations ayant été omises par le fait qu'elles ne sont pas réalisables dans le contexte de la cible ou de son environnement. Activité(s) liée(s) : O-4.2.9
58	**Déterminer les exigences de sécurité pour la mitigation des risques** L'activité consiste à déterminer les exigences de sécurité nécessaires pour mitiger les risques, et ce, en spécifiant les mesures (fonctionnelles ou d'assurance) à réaliser pour satisfaire les recommandations de sécurité de haut niveau, leur portée (la cible ou l'environnement), les dépendances qu'elles pourraient avoir avec une autre mesure et, finalement, s'il s'agit d'une mesure qui pourrait être mise en œuvre immédiatement dû au fait qu'aucun prérequis n'est nécessaire. Activité(s) liée(s) : E-5.1.1 / E-5.1.4 / E-5.1.5 / E-5.2.1 / E-5.2.2 / *M-3.3.1 / O-4.2.5 / O-4.2.6
59	**Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité** L'activité consiste à démontrer les liens entre les exigences de sécurité et les recommandations de sécurité de haut niveau qu'ils couvrent, et ce, en attribuant un niveau de couverture (nul, partiel et total) pour chacune des recommandations, en justifiant tous les cas où le niveau de couverture n'est pas total, en vérifiant si toutes les exigences de sécurité sont reliées à au moins une recommandation de sécurité de haut niveau et, finalement, en vérifiant les dépendances possibles entre les exigences proposées. Activité(s) liée(s) : E-5.1.2 / E-5.1.3 / E-5.2.3
60	**Résumer les informations sur les exigences de sécurité** L'activité consiste à résumer les informations sur les exigences de sécurité de manière concise en vue de les présenter aux parties prenantes. Activité(s) liée(s) : O-4.2.10 / O-4.2.11
61	**Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes** L'activité consiste à présenter, à modifier au besoin et à faire approuver les

	informations relatives aux recommandations de sécurité de haut niveau et aux exigences de sécurité par les parties prenantes. Activité(s) liée(s) : O-4.2.13
62	**Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité** L'activité consiste à documenter formellement les informations relatives aux recommandations de sécurité de haut niveau et aux exigences de sécurité qui ont été établies avec les parties prenantes et à les transmettre aux personnes concernées dans l'entreprise. Activité(s) liée(s) : O-4.2.15

Suite aux résultats obtenus dans les différentes parties « B » des tableaux 4.5 à 4.11, il fut ensuite possible de dresser une liste combinée des activités générales de la gestion des risques. Le nombre total d'activités générales créées fut donc de 62 tel que démontré dans le tableau 4.12 :

Tableau 4.12

Liste globale des activités générales de la gestion des risques

N°	Activités générales de la gestion des risques	Étapes
1	Obtenir un soutien adéquat des parties prenantes du projet	❖
2	Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information	
3	Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir	
4	Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche	
5	Informer les participants sur les activités de sécurité à réaliser durant la démarche	
6	Établir la logistique de la démarche	
7	Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche	
8	Communiquer les résultats obtenus lors des consultations avec les groupes de participants	
9	Planifier la mise en œuvre des mesures de sécurité proposées par la démarche	
10	Décrire l'environnement de la cible	1
11	Identifier les contraintes à l'égard de l'environnement de la cible	
12	Identifier le cadre légal de l'environnement de la cible	
13	Décrire l'aspect fonctionnel de l'environnement de la cible	
14	Préciser la cible de la démarche de sécurité	
15	Identifier les enjeux à l'égard de la cible	
16	Décrire l'aspect fonctionnel de la cible	
17	Identifier les hypothèses à l'égard de la cible	
18	Identifier les règles de sécurité à l'égard de la cible	

19	Identifier les contraintes à l'égard de la cible	
20	Identifier le cadre légal de la cible	
21	Rencontrer les groupes de participants pour identifier les actifs importants de la cible	2
22	Rédiger une liste des actifs identifiés par groupes de participants rencontrés	
23	Identifier les actifs critiques de la cible	
24	Rédiger une liste intégrée de tous les actifs identifiés	
25	Identifier les actifs de support aux actifs critiques de la cible	
26	Documenter les dépendances entre les actifs critiques et les actifs de support	
27	Regrouper les actifs critiques ayant des besoins de sécurité similaires	3
28	Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité	
29	Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité	
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement	
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés	
32	Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques	
33	Rédiger une synthèse des besoins de sécurité pour les actifs critiques	
34	Valider les besoins de sécurité pour les actifs critiques	
35	Identifier les éléments de la cible à auditer	4
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité	
37	Effectuer l'audit de sécurité organisationnelle de la cible	
38	Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible	
39	Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support	
40	Effectuer l'audit de sécurité technique de la cible	
41	Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible	
42	Documenter les informations sur les vulnérabilités identifiées	
43	Identifier les menaces à l'égard des actifs critiques de la cible	
44	Évaluer les menaces à l'égard des actifs critiques de la cible	
45	Documenter les informations sur les menaces identifiées	
46	Identifier les risques potentiels envers la cible	5
47	Sélectionner les risques à considérer dans le cadre d'une analyse de risques	
48	Définir les facteurs d'évaluation du risque	
49	Évaluer la potentialité des risques	
50	Évaluer l'impact des risques	
51	Évaluer globalement les risques à partir de sa potentialité et de son impact	
52	Documenter les risques évalués	
53	Valider les risques identifiés pour les actifs critiques avec les parties prenantes	
54	Réviser toutes les informations recueillies, traitées et produites durant la démarche	6
55	Déterminer les recommandations sur des exigences de sécurité de haut niveau	
56	Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau	

57	Résumer les informations sur les recommandations de sécurité de haut niveau	
58	Déterminer les exigences de sécurité pour la mitigation des risques	
59	Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité	
60	Résumer les informations sur les exigences de sécurité	
61	Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes	
62	Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité	

Pour démontrer que la totalité des 117 activités de sécurité ont bel et bien été considérées pour la création d'au moins une des activités générales de la gestion des risques, l'appendice A reprend le tableau 4.4 et y ajoute les activités générales de la gestion des risques auxquelles elles ont contribué.

Durant la réalisation des travaux dont les résultats sont présentés dans les tableaux 4.5 à 4.12, certains points ont été constatés et il est important de les noter :

- Deux itérations ont été nécessaires pour établir la liste finale. Suite à la première, la liste contenait un total de 85 activités générales de la gestion des risques. Après la deuxième, ce nombre s'est établi à 62. Cette situation s'explique par le fait qu'il ne fut pas simple d'établir la liste des activités générales d'un seul coup, puisque les concepts d'une méthode à l'autre sont parfois différents, d'autres fois identiques, mais très souvent similaires en partie. Cette situation amène des réflexions sur la pertinence de fusionner ou non certaines activités de sécurité provenant de méthodes différentes. Ce qui complexifie le tout, c'est que le vocabulaire utilisé n'est pas nécessairement pareil et un terme peut même avoir une définition différente d'une méthode à l'autre.

  Par exemple, lorsque vient le temps de proposer des solutions pour mitiger les risques dans une approche de gestion des risques de sécurité, il a fallu démêler les concepts utilisés par les méthodes lorsqu'elles traitent de ce sujet. Dans ce cas-ci, il s'agissait de concepts dont les termes sont très semblables, mais qui ne veulent pas nécessairement dire la même chose : les objectifs de sécurité (*EBIOS*), les exigences de sécurité (*EBIOS*), les mesures de sécurité (*MEHARI*), la stratégie de protection (*OCTAVE*) et les activités d'un plan de mitigation (*OCTAVE*).

- Aucune activité générale n'a été créée sans provenir minimalement de l'une des activités de sécurité identifiées dans les méthodes de gestion des risques étudiées pour la présente recherche. Les activités générales résultent donc toutes d'une source établie et pour laquelle une documentation formelle existe.

- Au moment de considérer chacune des activités de sécurité provenant des méthodes, il ne fut pas simple de faire abstraction de la manière dont l'activité est réalisée par rapport au but qu'elle vise. Autrement dit, si deux activités de méthodes différentes contribuent au même but, mais par des moyens différents (exemple : la manière de collecter les informations), elles ont tout de même été jugées identiques et furent fusionnées avant d'être utilisées comme source pour la création d'une activité générale.

- Au même titre que la situation de fusion énoncée juste auparavant, celle où une activité de sécurité peut contribuer à la création de plusieurs activités générales fut également à considérer avec plus d'attention. Dans ces cas-ci, des décisions ont été prises afin de déterminer si l'activité de sécurité en question présentait deux tâches distinctes et si le fait de les réaliser en deux activités séparées donnerait les mêmes résultats.

Les travaux de l'étape 2 de la création de la liste des activités générales de la gestion de risques donnèrent donc un total de 62 activités à considérer dans la suite de la démarche analytique. Les résultats montrent aussi qu'il existe des interdépendances entre ces différentes activités et principalement à travers chacun des regroupements d'activités. Cette situation est logique puisque les activités contribuent ensemble à atteindre l'objectif général de l'étape de la gestion des risques avec laquelle elles sont associées. Ces interdépendances ont déjà été prises en considération durant l'étape 2, puisque les activités générales, une fois créées dans leur regroupement respectif, ont été placées en ordre chronologique de réalisation. Ensuite, il s'agissait d'établir les interdépendances entre les différents regroupements d'activités. La tâche fut relativement facile puisque ces regroupements sont basés sur des étapes chronologiques. Cependant, il n'en demeure pas moins que le regroupement correspondant à l'étape spéciale ❖ - *Organisation de la démarche*, fut plus compliqué à établir, puisque ses activités générales interagissent directement avec celles contenues dans les autres regroupements et non pas avec l'ensemble des activités d'un regroupement.

La figure 4.5 présente les résultats de l'identification des interdépendances entre les activités générales créées. Il faut toutefois préciser que seules les dépendances directes sont présentées, puisqu'une activité hérite automatiquement de celles de ses propres dépendances.

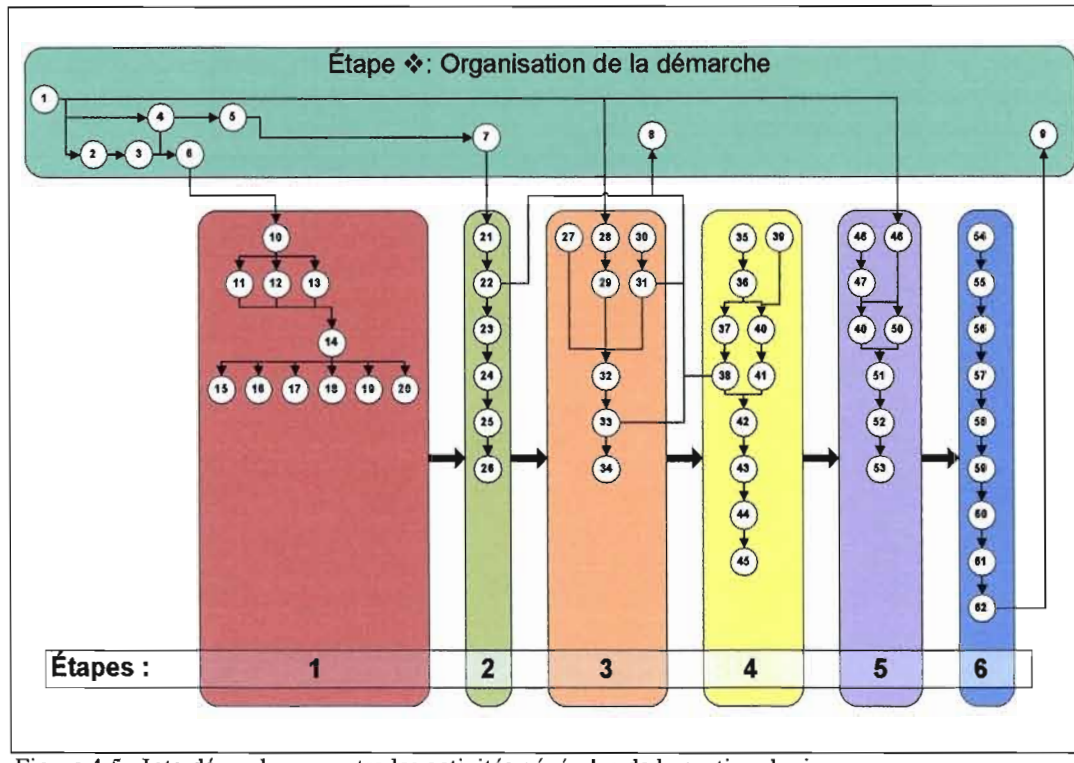

Figure 4.5 Interdépendances entre les activités générales de la gestion de risques.

Cette première étape de la démarche analytique visait à approfondir les activités de sécurité réalisées dans les méthodes de gestion de risques sélectionnées à titre de référence dans le cadre de la présente recherche. Grâce à ces activités représentant les différents concepts de leur méthode respective, une liste d'activités générales de la gestion des risques fut établie. Les activités générales seront considérées à l'étape 3 de la démarche analytique, puisqu'elle consiste à intégrer chacune d'entre elles dans un contexte de développement logiciel. Des explications entourant ce contexte sont présentées dans la section suivante.

4.2 **Étape 2 :** La présentation du cycle de développement du logiciel

Cette deuxième étape de la démarche analytique énonce les éléments de base qui seront utilisés à titre de référence pour la recherche en ce qui a trait au cycle de développement du logiciel. Comme annoncé au troisième chapitre, le modèle sélectionné est celui du *Processus Unifié*. Cette section présente cette méthode de manière plus détaillée dans le but de bien comprendre les étapes de sa démarche ainsi que les objectifs visés par celles-ci.

Le *Processus Unifié* est une méthode de développement logiciel créée par Ivar Jacobson, Grady Booch et James Rumbaugh vers la fin des années 90 [26]. La méthode présente une approche de développement logiciel itérative et incrémentale, correspondant à deux des modèles de cycle de développement du logiciel présentés au premier chapitre soit : le modèle par itération et le modèle par incrément. Ses caractéristiques importantes ont été présentées dans le troisième chapitre. Avant de présenter le *Processus Unifié* plus en détail, il est nécessaire de préciser qu'il ne faut pas confondre la gestion des risques telle qu'énoncée dans sa description et la gestion des risques de sécurité dont il est question dans la présente recherche. Les risques traités dans le *Processus Unifié* sont ceux de nature technique (implantation des technologies, de l'architecture, de performance, etc.) et non technique (la gestion des ressources humaines, la compétence des intervenants, les dates de livraison, etc.) qui pourraient affecter les objectifs du projet de développement logiciel. Malgré la présence de cette gestion des risques dans les étapes de la méthode, cela ne veut pas dire pour autant qu'il s'agit des moments appropriés pour effectuer la gestion des risques de sécurité.

Le *Processus Unifié* [27] présente quatre grandes phases à exécuter chronologiquement. La réalisation de toutes ces phases représente un cycle de développement qui aboutira à une version du logiciel. Voici les quatre phases en question :

1. **L'initialisation** : phase de lancement et plus précisément de la présentation d'un plan d'affaires du projet.
2. **L'élaboration** : phase où l'architecture de base est mise en œuvre.
3. **La construction** : phase où les fonctionnalités du logiciel sont développées et où, dans sa finalité, le logiciel devient utilisable.
4. **La transition** : phase où la version du logiciel est finalisée et remise aux utilisateurs.

Durant chacune de ces phases, des regroupements d'activités existent afin de structurer et d'ordonnancer les travaux à faire. Un regroupement d'activités, appelé « discipline », visent un objectif bien précis du développement logiciel. Bien que d'autres disciplines peuvent être ajoutées au besoin, voici celles qui sont proposées par l'approche de base du *Processus Unifié* :

a. **La spécification des besoins** : recueillir et décrire les besoins à considérer;
b. **L'analyse** : comprendre les besoins exprimés et les traduire en spécifications;
c. **La conception** : déterminer la manière dont les spécifications seront développées en termes de langage informatique;

d. **L'implémentation** : programmer les fonctionnalités du système selon les spécifications établies et les instructions résultant de la conception;
e. **Les tests** : évaluer les travaux effectués en comparant les résultats obtenus par rapport aux besoins exprimés initialement.

Durant la réalisation d'une phase, les cinq disciplines sont effectuées séquentiellement, mais plusieurs itérations de celles-ci peuvent être effectuées, d'où la notion de méthode itérative.

Afin de bien comprendre les activités effectuées durant l'approche proposée par le *Processus Unifié*, chacune des phases et ses disciplines afférentes sont présentées plus en détail dans cette section.

Phase 1 : L'initialisation

Le but premier de cette phase est de démarrer le projet en mettant sur pied le plan d'affaires dont l'intention sera de présenter aux parties prenantes, le projet logiciel et les éléments à considérer pour le rendre possible.

Les objectifs principaux de la phase d'initialisation sont les suivants : préciser la portée du projet, présenter une preuve de concept, résoudre les ambiguïtés entourant les besoins principaux, décrire l'architecture envisagée, identifier les risques critiques et établir les besoins en ce qui a trait à l'environnement de développement.

La durée de la phase d'initialisation peut être très variable selon la complexité, la grosseur et la connaissance des sujets dont il est question dans le projet. Les activités à réaliser nécessitent la participation d'un nombre limité de personnes, mais ayant des rôles différents dans l'entreprise soit : un gestionnaire de projet, un architecte technologique et un développeur. Une consultation auprès des personnes-ressources dans l'entreprise, selon leur domaine d'expertise, est importante parce qu'elle permet d'obtenir une vision globale et réaliste des travaux à effectuer. Concernant l'environnement de développement, il représente les outils informatiques et les services nécessaires pour les participants afin de réaliser le projet.

Au début de cette phase, les activités suivantes sont réalisées : planifier la phase d'initialisation et sa logistique, recueillir le maximum d'informations initiales (projets similaires, références, etc.) pour bâtir la vision du projet et définir les critères d'évaluation pour chacune des

itérations planifiées. Ces critères, représentés sous la forme d'objectifs à atteindre, porteront sur les objectifs principaux de la phase énoncés précédemment.

Bien que des activités soient réalisées dans chacune des cinq disciplines lors des différentes itérations de cette phase, la majorité des efforts requis concerne plus spécifiquement la spécification des besoins parmi les disciplines suivantes :

- **La spécification des besoins** : énumérer les besoins qui pourraient faire l'objet de fonctionnalités du système, comprendre le contexte du système, identifier les besoins fonctionnels et non fonctionnels à l'aide de la technique des cas d'utilisation.
- **L'analyse** : analyser, raffiner et structurer les besoins exprimés dans le modèle des cas d'utilisation. Rédiger une première version du modèle d'analyse qui inclut les éléments partagés donc, utilisés par plus d'un cas d'utilisation.
- **La conception** : rédiger une première version de la vue architecturale du modèle de conception afin d'y présenter l'architecture envisagée. Concevoir une preuve de concept au besoin.
- **L'implémentation** : mettre en œuvre un prototype si la preuve de concept le nécessite.
- **Les tests** : rédiger une première tentative de plans de tests. Effectuer des tests mineurs pour le prototype, s'il en existe un.

À la fin de cette phase, les activités suivantes sont réalisées : rédiger la première version du plan d'affaires, évaluer les résultats de la phase d'initialisation avec les parties prenantes afin de décider de faire suite au projet ou non et, si la décision est affirmative, débuter la planification de la phase d'élaboration.

Les travaux effectués durant cette phase résulteront en différents livrables qui seront utilisés et, éventuellement, bonifiés au cours des phases ultérieures. Voici les principaux livrables produits lors de cette phase :

- Une liste de fonctionnalités;
- Une première version des modèles d'affaires, de cas d'utilisation, d'analyse et de conception;
- Une première ébauche des modèles d'implantation et de tests;
- Une première ébauche de l'architecture cible;

- Une première ébauche d'un plan de projet global, incluant la planification des différentes phases;
- Une preuve de concept, au besoin;
- Une liste initiale de risques (techniques et non techniques);
- Une liste de priorisation des cas d'utilisation;
- Un plan d'affaires du projet, incluant le contexte d'affaires et les critères de succès.

Phase 2 : L'élaboration

Le but premier de cette phase est de produire une architecture de base fonctionnelle et sur laquelle les travaux futurs du projet pourront être développés.

Les objectifs principaux de la phase d'élaboration sont les suivants : identifier la majorité des besoins qui reste à traiter et formuler ceux qui sont fonctionnels pour décrire les processus d'affaires sous la forme de cas d'utilisation, mettre en œuvre une architecture de base fonctionnelle et stable, continuer la surveillance des risques critiques encore existants et identifier les risques significatifs afin d'estimer leurs impacts sur le plan d'affaires et sur les coûts prévus, et détailler le plan de projet.

Cette phase vise à établir les fondations du logiciel. Il s'agit, par conséquent, d'une occasion propice pour effectuer plusieurs itérations, puisque les résultats qui en découlent sont très importants pour la suite des travaux. Également, il est plus facile d'effectuer plusieurs itérations à ce stade-ci du projet, car les coûts en termes d'impacts et de ressources nécessaires sont encore mineurs. La gestion des risques portera principalement sur les risques ayant des impacts sur l'architecture et qu'il est important de réduire à un niveau acceptable dès que possible. De plus, certains outils prévus dans l'environnement de développement seront nécessaires pour aider à la réalisation des travaux, particulièrement ceux pour la gestion des versions et la gestion des configurations lors des activités d'implémentation.

Tout d'abord, trois livrables importants pour la phase d'élaboration ont été créés à la phase précédente soit : l'architecture cible, une liste des risques critiques et le plan d'affaires initial. Aussi, les parties prenantes ont donné les appuis nécessaires pour poursuivre le projet en phase d'élaboration.

Au début de cette phase, les activités suivantes sont réalisées : planifier la phase d'élaboration et sa logistique, former une équipe de réalisation, mettre à jour les besoins en ce qui a trait à l'environnement de développement et définir les critères d'évaluation pour chacune des itérations planifiées. Ces critères, représentés sous la forme d'objectifs à atteindre, porteront sur les objectifs principaux de la phase énoncés précédemment.

Bien que des activités soient réalisées dans chacune des cinq disciplines lors des différentes itérations de cette phase, la majorité des efforts requis concerne plus spécifiquement la spécification des besoins, l'analyse et la conception parmi les disciplines suivantes :

- **La spécification des besoins** : identifier les cas d'utilisation et les acteurs à traiter. Détailler et prioriser les cas d'utilisation. Structurer le modèle des cas d'utilisation afin de l'améliorer suite aux nouveaux cas traités. Concevoir les interfaces utilisateurs si elles s'avèrent utiles au niveau de l'architecture.
- **L'analyse** : examiner les éléments qui feront partie de l'architecture en prenant en considération les besoins exprimés dans les cas d'utilisation significatifs pour l'architecture. Étudier plus en détail et raffiner les cas d'utilisation permettant ainsi l'analyse des classes conceptuelles et des composants logiciels nécessaires pour produire une architecture exécutable.
- **La conception** : concevoir l'architecture selon les indications établies lors de l'analyse. Les différents cas d'utilisation dont il est question seront transposés sous la forme de sous-systèmes, de services offerts par ces sous-systèmes et de classes conceptuelles.
- **L'implémentation** : programmer et tester unitairement les éléments à concevoir pour l'architecture tels que les composantes nécessaires pour les sous-systèmes, les sous-systèmes eux-mêmes et les classes conceptuelles. Intégrer ensemble chacun des éléments produits pour former un tout qui, en définitive, s'avérera être l'architecture de base.
- **Les tests** : planifier, concevoir et exécuter les plans de tests d'intégration et de système pour évaluer l'architecture produite par rapport aux besoins exprimés.

À la fin de cette phase, les activités suivantes sont réalisées : compléter le plan d'affaires et évaluer les résultats de la phase d'élaboration avec les parties prenantes. Ces dernières doivent être convaincues de la mitigation des risques critiques et de la stabilité de l'architecture produite afin de donner suite au projet. Dans la perspective où le projet se poursuit, la planification de la première itération de la phase de construction est débutée.

Les travaux effectués durant cette phase résulteront en différents livrables qui seront utilisés et, éventuellement, bonifiés au cours des phases ultérieures. Voici les principaux livrables produits lors de cette phase :

- Une nouvelle version des modèles de cas d'utilisation, d'analyse, de conception, de déploiement et d'implantation;
- Une architecture de base fonctionnelle;
- Une description de l'architecture;
- Un modèle d'affaires complet;
- Un plan d'affaires complet;
- Une liste des risques (techniques et non techniques) critiques mise à jour;
- Un plan de projet incluant les phases de conception et de transition;
- Une première version du guide de l'utilisateur au besoin.

Phase 3 : La construction

Le but premier de cette phase est de produire une première version utilisable du logiciel qui répond adéquatement aux besoins exprimés.

Les objectifs principaux de la phase de construction sont les suivants : développer le système pour le rendre opérationnel dans l'environnement informatique de l'utilisateur, détailler les cas d'utilisation restants, modifier la description de l'architecture le cas échéant, produire et intégrer les nouveaux sous-systèmes, prioriser les cas d'utilisation à traiter et continuer la gestion des risques.

La phase de construction est celle où la majeure partie de la réalisation est effectuée, puisqu'il faut traiter la majorité des besoins exprimés. Pour ce faire, il peut être nécessaire d'augmenter les ressources afin d'être en mesure de répondre adéquatement à la charge de travail demandée. Il faut noter que les besoins qui influençaient directement l'architecture ont été considérés et traités lors de la phase d'élaboration, mais ceux-ci ne représentaient qu'une petite partie de l'ensemble des besoins.

Tout d'abord, différents livrables importants pour la phase de construction ont été créés ou modifiés à la phase précédente soit l'architecture de base fonctionnelle (incluant des composants, des sous-systèmes et des classes conceptuelles) et plusieurs des modèles de la démarche. Afin de

poursuivre le projet en phase de construction, les appuis nécessaires ont également été donnés par les parties prenantes.

Au début de cette phase, les activités suivantes sont réalisées : mettre à jour la planification de la phase en fonction des contraintes (la disponibilité des ressources, le calendrier des activités et le financement) à considérer en raison de la date réelle où la phase débute, assigner davantage de ressources humaines aux tâches à effectuer, planifier les travaux à réaliser et définir les critères d'évaluation pour chacune des itérations planifiées. Ces critères, représentés sous la forme d'objectifs à atteindre, porteront sur la réalisation des besoins fonctionnels et non fonctionnels exprimés par les cas d'utilisation et aussi sur le matériel à produire pour supporter adéquatement les premiers utilisateurs qui se serviront du logiciel durant la phase de transition.

Bien que des activités soient réalisées dans chacune des cinq disciplines lors des différentes itérations de cette phase, la majorité des efforts requis concerne plus spécifiquement la conception, l'implémentation et les tests parmi les disciplines suivantes :

- **La spécification des besoins** : identifier les derniers cas d'utilisation et acteurs à traiter. Détailler et prioriser les cas d'utilisation. Structurer le modèle des cas d'utilisation afin de l'améliorer suite aux nouveaux cas traités. Prototyper l'interface utilisateur du système.
- **L'analyse** : compléter le modèle d'analyse en mettant à jour les informations inscrites dans la partie « architecture » réalisée lors de la phase précédente. Raffiner les cas d'utilisation, les classes et les composants logiciels à traiter.
- **La conception** : concevoir les cas d'utilisation traités dans l'analyse et qui se traduiront en sous-systèmes, en services offerts par ces sous-systèmes et en classes conceptuelles.
- **L'implémentation** : créer et tester unitairement tous les sous-systèmes et les classes conceptuelles élaborés lors de la conception. Établir un plan d'intégration afin d'incorporer, d'une itération à l'autre, les différents composants logiciels à la solution globale.
- **Les tests** : Planifier, concevoir et exécuter les plans de tests d'intégration et de système selon les besoins exprimés lors de la spécification des besoins. Évaluer les résultats pour vérifier s'ils sont bien respectés.

Étant donné la quantité de besoins traités durant cette phase, d'autres activités sont réalisées de façon plus marquée entre les différentes itérations des cinq disciplines : évaluer les travaux effectués par rapport aux objectifs visés, planifier de nouveau le travail qui n'aurait pas été accompli, déterminer si l'état du système est satisfaisant pour passer à l'itération suivante, actualiser la liste des

risques, établir le plan pour la prochaine itération et mettre à jour le plan pour les itérations subséquentes.

À la fin de cette phase, les activités suivantes sont réalisées : mettre à jour le plan d'affaires du projet au besoin et le communiquer aux parties prenantes, déterminer si les tests de système sont concluants et si le système produit atteint les objectifs escomptés, obtenir l'autorisation de passer officiellement à la phase suivante et actualiser le plan de projet pour la phase de transition.

Les travaux effectués durant cette phase résulteront en différents livrables qui seront utilisés et, éventuellement, bonifiés au cours de la phase suivante, la dernière du projet. Voici les principaux livrables produits lors de cette phase :

- Un logiciel exécutable;
- Un plan de projet pour la phase de transition;
- Tous les livrables produits durant le projet incluant les modèles du système;
- Une version actualisée de la description de l'architecture;
- Une version préliminaire du guide de l'utilisateur, mais assez détaillée pour les premiers utilisateurs;
- Un plan d'affaires du projet mis à jour.

Phase 4 : La transition

Le but premier de cette phase est d'ajuster et de stabiliser le fonctionnement du logiciel mis en opération dans l'environnement informatique de l'utilisateur.

Les objectifs principaux de la phase de transition sont les suivants : démontrer que le système répond aux besoins exprimés plus tôt dans le projet afin d'être en mesure d'obtenir la satisfaction des parties prenantes, prendre en charge les différents cas problématiques qui peuvent encore survenir et qui sont rapportés par les premiers utilisateurs et, au besoin, préparer les outils facilitant l'installation du logiciel comme des scripts d'installation, des programmes de conversion des données ou des livrables additionnels.

Cette phase vise à finaliser les derniers aspects du logiciel suite aux commentaires reçus par les premiers utilisateurs selon leurs manipulations effectuées dans un environnement réel. Pour ce faire, il faut considérer les aspects suivants : s'assurer que le système répond bien à ce qui a été

demandé, relever les risques qui n'ont pas été anticipés, noter les problèmes non résolus, trouver les défauts et corriger les ambiguïtés ainsi que les lacunes présentes dans la documentation destinée à l'utilisateur. Il faut également s'attarder sur les parties du logiciel qui semblent être plus ardues pour les utilisateurs et pour lesquelles des informations ou de la formation supplémentaires pourraient être données. S'il s'avère que des modifications au système doivent être effectuées à ce stade-ci du cycle de développement logiciel, les corrections nécessaires se doivent d'être mineures pour éviter de provoquer un impact majeur sur la qualité et la stabilité du logiciel.

Au début de cette phase, les activités suivantes sont réalisées : ajuster la planification selon les travaux engendrés suite aux problèmes soulevés par les premiers utilisateurs, placer en attente les ressources nécessaires prêtes à intervenir au besoin pour corriger les problèmes identifiés et définir les critères d'évaluation pour chacune des itérations planifiées. Ces critères, représentés sous la forme d'objectifs à atteindre, porteront sur les points finaux d'acceptation en s'assurant que les premiers utilisateurs se sont réellement servis des fonctionnalités principales du logiciel, que les tests d'acceptation sont réussis, que le matériel de l'utilisateur est d'une qualité acceptable, que le matériel de formation est prêt et que les clients et les utilisateurs semblent être satisfaits du résultat final.

Durant cette phase, les cinq disciplines jouent un rôle moins important durant les itérations effectuées comparativement aux phases précédentes. Parallèlement aux cinq disciplines, trois autres regroupements de tâches sont exécutés soit : planifier le travail afin de s'ajuster à la résolution des problèmes qui surviennent, vérifier de manière plus approfondie le plan d'affaires et faire une évaluation du déroulement du projet logiciel. Voici sommairement les activités réalisées durant ces quatre regroupements de tâches :

- **Les cinq disciplines** : investir les efforts nécessaires dans les disciplines d'implémentation et de tests pour la correction d'anomalies, pour les améliorations ou pour tous les autres changements mineurs apportés. S'il s'avère qu'une modification importante doive être effectuée, il se peut que des travaux soient à réaliser au niveau de la conception.
- **La planification des itérations** : planifier de manière continuelle les travaux à réaliser, puisqu'ils peuvent survenir à tout moment. Gérer l'obtention des critères d'évaluation, des ressources nécessaires et des risques.
- **L'examen du plan d'affaires** : évaluer le plan d'affaires en ce qui concerne la rentabilité du projet par rapport aux informations quantifiables de son déroulement (le calendrier des activités, les efforts et le coût planifié). Analyser si le projet a atteint les buts fixés par l'entreprise.

- **L'évaluation des activités du projet** : Organiser une rencontre réunissant quelques-uns des participants du projet afin de faire un bilan des travaux au sujet des deux facettes suivantes : le déroulement du cycle de développement (phases et itérations) et le déroulement du projet en général.

À la fin de cette phase, le projet de développement logiciel se termine et le système est officiellement prêt à être utilisé. Le logiciel passe ensuite du mode « projet » à celui de « maintenance » qui peut également impliquer un cycle de développement logiciel adapté à cette situation.

Les travaux effectués durant cette phase résulteront en différents livrables qui seront conservés à titre de référence pour l'équipe de réalisation ou consultés par les utilisateurs. Voici les principaux livrables produits lors de cette phase :

- Un logiciel exécutable, incluant le nécessaire à son installation;
- Des documents légaux entre les parties concernées, au besoin;
- Une version complète et corrigée des livrables de base du logiciel, incluant les modèles.
- Une description de l'architecture complète mise à jour;
- Une version finale des manuels de l'utilisateur, d'opération et de système;
- Une version finale du matériel de formation;
- Des références pour les clients afin qu'ils puissent obtenir de l'information supplémentaire et de l'assistance concernant le logiciel.

Le Processus Unifié propose donc une approche structurée pour le développement logiciel. Pour faire un parallèle entre les cinq disciplines à exécuter dans chacune des phases du *Processus Unifié* et les étapes communes du développement logiciel présentées au premier chapitre, le tableau 4.13 présente un comparatif :

Tableau 4.13

Comparaisons entre les étapes du développement logiciel et celles du *Processus Unifié*

Étapes communes du développement logiciel	Étapes (disciplines) du Processus Unifié	Notes
1. La définition des besoins	a. La spécification des besoins	Équivalent
2. La conception	b. L'analyse c. La conception	La conception (étape commune) englobe les disciplines d'analyse et de conception (*Processus Unifié*)
3. L'implémentation	d. L'implémentation	L'implémentation et l'intégration

4. L'intégration		(étapes communes) correspondent à la discipline d'implémentation (*Processus Unifié*)
5. La validation	e. Les tests	Équivalent
6. La maintenance	-	La maintenance n'est pas représentée comme une discipline dans le *Processus Unifié;* toutefois, il est mentionné qu'elle est la phase suivante lorsque le développement du logiciel est terminé.

Cette deuxième étape de la démarche analytique visait à présenter le *Processus Unifié* à un niveau assez précis pour en comprendre sommairement les activités qui y sont réalisées. Ces informations seront utilisées à titre de modèle d'un cycle de développement du logiciel pour la suite de la démarche analytique. Dans la prochaine et dernière étape, c'est avec ces précisions qu'il sera possible de justifier l'intégration des différentes activités générales de la gestion des risques dans un modèle de cycle de développement du logiciel.

4.3 **Étape 3 :** L'intégration des activités générales de la gestion des risques dans un contexte de cycle de développement du logiciel

Cette troisième et dernière étape de la démarche analytique établit les liens entre les activités générales de la gestion des risques, recueillies à l'étape 1, et celles d'un cycle de développement du logiciel telles que présentées à l'étape 2. Concrètement, il s'agit de justifier l'intégration des 62 activités générales de la gestion des risques avec les différentes activités présentées dans les quatre phases du cycle de développement du logiciel définies dans le *Processus Unifié*.

Différents motifs peuvent être énoncés pour justifier la possibilité d'intégrer une activité générale de la gestion des risques dans le cycle de développement du logiciel. Pour les fins de la présente recherche, les trois motifs suivants sont ceux qui ont été considérés :

a. **Une activité du projet de développement logiciel** provoque une occasion favorable (activité similaire ou un moment clé du projet) pour réaliser une activité générale de la gestion des risques.

   Par exemple, la composition de l'équipe pour le projet de développement logiciel est également le moment propice pour sélectionner les personnes qui feront partie de l'équipe de gestion du risque (activité n° 2).

b. **Une activité du projet de développement logiciel** produit des informations dont une activité générale de la gestion des risques a besoin comme intrants informationnels nécessaires à sa réalisation.

Par exemple, la définition des besoins à traiter durant le projet de développement logiciel résulte de certaines informations qu'il est nécessaire de posséder pour préciser la cible à considérer dans la démarche de sécurité (activité n° 14).

c. **Une activité générale de la gestion des risques** peut être réalisée suite à l'achèvement d'une autre activité générale de la gestion des risques étant donné son interdépendance.

Par exemple, pour procéder à l'identification des contraintes associées à l'environnement de la cible (activité n° 11), cet environnement doit tout d'abord avoir été décrit (activité n° 10).

De ces trois motifs énoncés, les deux premiers (« a » et « b ») sont considérés comme un ancrage réel au développement logiciel, puisqu'il s'agit d'un lien direct avec une activité du projet du cycle de développement du logiciel. En revanche, le troisième (« c ») est considéré comme un ancrage par dépendance au développement logiciel, puisqu'il s'agit d'un lien indirect avec une activité du projet du cycle de développement du logiciel. Ce lien est jugé indirect, parce que l'activité de gestion des risques doit nécessairement passer par d'autres activités de la gestion des risques pour s'accrocher réellement à une activité du projet du cycle de développement du logiciel.

Bref, une activité de gestion des risques peut donc être reliée au cycle de développement logiciel par un lien direct ou par un lien indirect grâce à ses interdépendances desquelles l'une d'entre elles possède un lien direct. Avec les nombreuses interdépendances démontrées dans les résultats de l'étape 1 de la démarche analytique, les activités générales de la gestion des risques sont donc toutes attachées les unes aux autres, ce qui engendre inévitablement plusieurs motifs d'ancrage par dépendance. Les activités les plus importantes à relever sont donc celles dont le motif se traduit en ancrage réel. Les travaux d'intégration ont permis de déterminer qu'un nombre limité d'activités générales de la gestion des risques possèdent un lien direct avec le cycle de développement logiciel, les autres étant toutes intégrées par un motif d'ancrage par dépendance.

Les tableaux 4.16 à 4.26 représentent l'intégration de chacune des activités générales de la gestion des risques par rapport au cycle de développement du logiciel défini par le *Processus Unifié*.

Pour en alléger la lecture, seules les activités ayant un motif d'ancrage réel sont présentées dans ce chapitre. La totalité des tableaux pour les 62 activités générales de la gestion des risques est disponible à l'appendice B.

Avant de présenter les résultats obtenus, certaines explications s'imposent pour une meilleure compréhension des tableaux. La démarche globale utilisée pour évaluer l'intégration des activités générales de la gestion des risques fut donc de les prendre une à la fois et d'analyser, en considérant leur but et leur contexte de réalisation, dans quelles étapes du *Processus Unifié* elle devait être réalisée. Il est à noter qu'une activité générale de la gestion des risques doit parfois être réalisée une seule fois, tandis qu'une autre peut l'être à plusieurs occasions différentes. En fonction des résultats obtenus lors de l'étape 2 de la démarche analytique, les possibilités d'intégration dans les étapes du *Processus Unifié* furent donc les 27 qui apparaissent dans le tableau 4.14 :

Tableau 4.14

Étapes des quatre phases du *Processus Unifié*

Le Processus Unifié			
L'initialisation	**L'élaboration**	**La construction**	**La transition**
1. Début de la phase 2. La spécification des besoins 3. L'analyse 4. La conception 5. L'implémentation 6. Les tests 7. Fin de la phase	8. Début de la phase 9. La spécification des besoins 10. L'analyse 11. La conception 12. L'implémentation 13. Les tests 14. Fin de la phase	15. Début de la phase 16. La spécification des besoins 17. L'analyse 18. La conception 19. L'implémentation 20. Les tests 21. Fin de la phase	22. Début de la phase 23. Les cinq disciplines 24. La planification des itérations 25. L'examen du plan d'affaires 26. L'évaluation des activités du projet 27. Fin de la phase

Chacune des intégrations est représentée dans un tableau distinct et affiche les éléments suivants : le numéro de référence de l'activité générale, son titre, sa description, les activités générales préalables à sa réalisation et les informations relatives à son intégration (les étapes du *Processus*

Unifié, les justifications et les types d'ancrage). Par exemple, le tableau de l'intégration de l'activité n° 10 donne les résultats présentés dans le tableau 4.15 :

Tableau 4.15

Exemple de l'intégration d'une activité générale dans le cycle de développement du logiciel

10	**Nom :**	**Décrire l'environnement de la cible**	
	Description :	L'activité consiste à décrire sommairement l'environnement de la cible pour préciser le but, le contexte d'utilisation et son importance dans le système d'information de l'entreprise.	
	Préalable(s) :	▪ *Activité n° 6* : Établir la logistique de la démarche	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 2. La spécification des besoins	**Au moment où** il est prévu, dans les activités du projet, de comprendre le contexte du projet.	AR (b)

La première série d'informations dans le tableau (le numéro, le nom, la description et les préalables) est tirée des résultats de l'étape 1 de la démarche analytique. Concernant la série d'informations dans la partie « Intégration de l'activité », la première colonne identifie quelles sont les étapes du *Processus Unifié* pour lesquelles l'activité générale en question est intégrée. La deuxième colonne donne quelques explications justifiant l'intégration. La troisième colonne, quant à elle, indique s'il s'agit d'un ancrage réel (AR) par un motif « a » ou « b » ou un ancrage par dépendance (AD) par un motif « c » comme expliqué précédemment dans cette section.

Puisque la démarche globale d'intégration prend à la base les activités générales de la gestion des risques une à une, les informations relatives à l'intégration sont tout d'abord présentées de cette façon. Toutefois, les résultats seront ensuite présentés sous la vue du cycle de développement du logiciel afin d'être en mesure d'analyser également les résultats sous cet aspect.

Voici donc les tableaux d'intégration pour les activités de gestion de sécurité ayant un ancrage réel aux activités du cycle de développement du logiciel :

Tableau 4.16

Intégration de l'activité générale de gestion des risques n° 1

1	**Nom :**	**Obtenir un soutien adéquat des parties prenantes du projet**
	Description :	L'activité consiste à obtenir les appuis nécessaires et visibles de la part des parties prenantes pour la réalisation des activités de sécurité durant la démarche et plus précisément, les aspects suivants : l'encouragement actif, la

	délégation des responsabilités et des autorités, l'attribution des ressources nécessaires, la participation à la révision des résultats et la prise de décisions sur les actions appropriées.	
Préalable(s) :	*Aucun*	
Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 1. Début de la phase	**Au moment où** le projet débute puisqu'il s'agit du tout premier pas à franchir pour débuter à investir du temps et des ressources dans la démarche de sécurité du projet.	AR (a)
L'initialisation : 7. Fin de la phase L'élaboration : 14. Fin de la phase La construction : 21. Fin de la phase La transition : 27. Fin de la phase	**Au moment où** la phase se termine pour donner l'approbation de la continuité de la démarche de sécurité à la phase suivante (de la transition à l'élaboration, de l'élaboration à la construction et de la construction à la transition) ou pour la fin de la démarche lorsque le projet se termine (phase de transition).	AR (a)
Le projet entier	**Tout au long** des étapes du projet afin d'être efficace.	AR (a)

Tableau 4.17

Intégration de l'activité générale de gestion des risques n° 2

2	**Nom :**	**Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information**
	Description :	L'activité consiste à former une équipe de personnes multidisciplinaires qui participeront activement à la réalisation des activités de sécurité durant la démarche, et ce, sur différents aspects du travail dont la gestion, la communication, l'analyse et l'élaboration des solutions.
	Préalable(s) :	▪ *Activité n° 1* : Obtenir un soutien adéquat des parties prenantes du projet
Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'élaboration : 8. Début de la phase	**Au moment où** le projet compose son équipe de réalisation.	AR (a)

Tableau 4.18

Intégration de l'activité générale de gestion des risques n° 4

4	**Nom :**	**Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche**
	Description :	L'activité consiste à identifier les personnes requises pour la réalisation des activités de sécurité et à former des groupes distincts selon leurs responsabilités dans l'entreprise, leurs implications dans la démarche ou toute autre division logique qui permettrait de couvrir tous les besoins nécessaires aux activités de sécurité de la démarche.
	Préalable(s) :	▪ *Activité n° 1* : Obtenir un soutien adéquat des parties prenantes du projet

Intégration de l'activité		
Étapes	*Justifications*	*Ancrage*
L'initialisation : 1. Début de la phase L'élaboration : 8. Début de la phase La construction : 15. Début de la phase La transition : 22. Début de la phase	**Au moment où** la phase débute puisque les personnes sélectionnées (nouvelles lors de la phase d'initialisation, mais nouvelles ou modifiées lors des phases d'élaboration, de construction et de transition) seront amenées à participer dans la démarche de sécurité pour la phase courante.	AR (a)

Tableau 4.19

Intégration de l'activité générale de gestion des risques n° 6

6	**Nom :**	**Établir la logistique de la démarche**
	Description :	L'activité consiste à planifier la démarche de sécurité en présentant un calendrier des activités et les éléments nécessaires pour leur réalisation (les ateliers, les personnes impliquées, le matériel, etc.).
	Préalable(s) :	▪ *Activité n° 3* : Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir ▪ *Activité n° 4* : Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche

Intégration de l'activité		
Étapes	*Justifications*	*Ancrage*
L'initialisation : 1. Début de la phase L'élaboration : 8. Début de la phase La construction : 15. Début de la phase La transition : 22. Début de la phase	**Suite** à la préparation de l'équipe de réalisation et à la sélection des participants effectuées au début de la phase, puisqu'il s'agit de planifier les activités de la démarche de sécurité pour la phase courante.	AD (c)
L'initialisation : 7. Fin de la phase L'élaboration : 14. Fin de la phase La construction : 21. Fin de la phase La transition : 27. Fin de la phase	**Au moment où** l'approbation de passer à la phase suivante est donnée par les parties prenantes, puisqu'il s'agit de débuter la planification de la phase suivante (pour passer en phase d'élaboration, de construction ou de transition) ou bien de planifier les activités qui finalisent la démarche de sécurité du projet (en phase de transition).	AD (c)
Le projet entier	**Tout au long** des étapes du projet à l'exception des étapes d'examen du plan d'affaires et de l'évaluation des activités du projet qui sont réalisées durant la phase de transition.	AR (a)

Tableau 4.20

Intégration de l'activité générale de gestion des risques n° 7

7	**Nom :**	**Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche**	
	Description :	L'activité consiste à obtenir une confirmation, avant de débuter les ateliers de groupe, attestant que les participants sélectionnés représentent bien les personnes adéquates dans leur domaine d'expertise au sein de l'entreprise et qu'elles ont le temps nécessaire pour prendre part à la démarche.	
	Préalable(s) :	▪ *Activité n° 5* : Informer les participants sur les activités de sécurité à réaliser durant la démarche	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse La transition : 23. Les cinq disciplines	**Juste avant** de débuter les activités de la démarche de sécurité de la phase courante du projet où les personnes sélectionnées seront amenées à participer.	AR (a)

Tableau 4.21

Intégration de l'activité générale de gestion des risques n° 8

8	**Nom :**	**Communiquer les résultats obtenus lors des consultations avec les groupes de participants**	
	Description :	L'activité consiste à présenter, aux différents groupes de participants, les résultats obtenus lors des consultations avec les autres groupes pour fin de comparaison.	
	Préalable(s) :	▪ *Activité n° 22* : Rédiger une liste des actifs identifiés par groupes de participants rencontrés ▪ *Activité n° 31* : Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés ▪ *Activité n° 33* : Rédiger une synthèse des besoins de sécurité pour les actifs critiques ▪ *Activité n° 38* : Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 7. Fin de la phase L'élaboration : 14. Fin de la phase La construction : 21. Fin de la phase La transition : 27. Fin de la phase	**Au moment où** la phase courante se termine, puisque toutes les rencontres auront été effectuées et les résultats prêts à être véhiculés avant que les parties prenantes prennent les décisions quant à la continuité de la démarche de sécurité à la phase suivante (pour passer en phase d'élaboration, de construction ou de transition) ou de la finalité de la démarche	AR (a)

	de sécurité du projet (en phase de transition).	

Tableau 4.22

Intégration de l'activité générale de gestion des risques n° 9

9	**Nom :**	**Planifier la mise en œuvre des mesures de sécurité proposées par la démarche**	
	Description :	L'activité consiste à planifier la mise en œuvre des mesures proposées par la démarche en précisant celles qui seront implantées, par qui et à quel moment.	
	Préalable(s) :	▪ *Activité n° 62* : Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition : 23. Les cinq disciplines	**Au moment où** les exigences de sécurité sont formellement documentées et prêtes à être considérées dans la conception des spécifications à implanter pour répondre aux recommandations de sécurité de haut niveau. **Il est à noter** que la réalisation de cette activité doit se dérouler avant que l'implémentation des solutions débute.	AR (a)

Tableau 4.23

Intégration de l'activité générale de gestion des risques n° 10

10	**Nom :**	**Décrire l'environnement de la cible**	
	Description :	L'activité consiste à décrire sommairement l'environnement de la cible pour préciser le but, le contexte d'utilisation et son importance dans le système d'information de l'entreprise.	
	Préalable(s) :	▪ *Activité n° 6* : Établir la logistique de la démarche	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 2. La spécification des besoins	**Au moment où** il est prévu, dans les activités du projet, de comprendre le contexte du projet.	AR (b)

Tableau 4.24

Intégration de l'activité générale de gestion des risques n° 14

14	**Nom :**	**Préciser la cible de la démarche de sécurité**
	Description :	L'activité consiste à préciser la cible à considérer dans la démarche de sécurité en spécifiant sa portée, ses finalités et ses interactions à travers l'environnement et le système d'information de l'entreprise (acteurs,

	domaines fonctionnels, systèmes, etc.).		
Préalable(s) :	▪ *Activité n° 11* : Identifier les contraintes à l'égard de l'environnement de la cible ▪ *Activité n° 12* : Identifier le cadre légal de l'environnement de la cible ▪ *Activité n° 13* : Décrire l'aspect fonctionnel de l'environnement de la cible		
Intégration de l'activité			
Étapes		***Justifications***	***Ancrage***
L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins		**Au moment où** l'on traite initialement les besoins du projet (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AR (b)
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse		**Au moment où** l'on raffine, analyse et structure les besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AR (b)

Tableau 4.25

Intégration de l'activité générale de gestion des risques n° 21

21	**Nom :**	**Rencontrer les groupes de participants pour identifier les actifs importants de la cible**	
	Description :	L'activité consiste à rencontrer les groupes de participants afin d'identifier les actifs importants faisant partie de la cible et d'en déterminer le degré d'importance relative entre eux.	
	Préalable(s) :	▪ *Activité n° 7* : Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche ▪ *Phase n° 1* : Identification et étude du contexte	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Au moment où** les besoins à traiter sont suffisamment clairs et détaillés (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction) pour préciser la cible et où chacun des participants est confirmé.	AR (b)

Tableau 4.26

Intégration de l'activité générale de gestion des risques n° 25

25	**Nom :**	**Identifier les actifs de support aux actifs critiques de la cible**
	Description :	L'activité consiste à identifier les actifs technologiques dont dépendent les actifs critiques de la cible, puisqu'une attaque pourrait en faire l'usage dans le but final d'atteindre un actif critique.

Préalable(s) :	▪ *Activité n° 24* : Rédiger une liste intégrée de tous les actifs identifiés	
Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Au moment où** les actifs technologiques, qui seront utilisés pour supporter les actifs et ainsi réaliser la solution, sont identifiés ou changés.	AR (b)

Les tableaux 4.16 à 4.26 démontrent que sur les 62 activités générales de la gestion des risques considérées dans la démarche analytique, 11 d'entre elles sont intégrées par un lien direct avec une activité du cycle de développement du logiciel. Par conséquent, les 51 autres activités sont intégrées par un lien indirect grâce à leurs interdépendances.

Ainsi, l'identification des étapes du cycle de développement du logiciel durant lesquelles ces 51 activités doivent être réalisées est étroitement liée aux étapes identifiées pour la réalisation des 11 autres activités. Par exemple, il n'est pas possible de réaliser l'activité n° 40 (*Effectuer l'audit de sécurité technique de la cible*) avant l'étape de *La Conception,* puisque ce n'est qu'à cette étape que l'activité n° 25 (*Identifier les actifs de support aux actifs critiques de la cible*) peut être réalisée. Cette dernière activité fait partie de celles ayant un lien direct avec une activité du cycle de développement du logiciel, et sa réalisation joue inévitablement le rôle de déclencheur pour débuter plusieurs autres activités. La situation démontre donc à quel point ces 11 activités sont importantes, puisqu'elles dictent dans l'ensemble à quelles étapes du cycle de développement logiciel les autres peuvent débuter leur réalisation. Il faut noter que pour l'intégration des activités ayant un lien indirect, les étapes considérées pour leur intégration fut celles qui sont immédiates à l'achèvement de ses préalables. Autrement dit, l'activité a été considérée comme étant possible à intégrer dès que ses préalables étaient réalisés.

Avec les informations soutirées des 62 tableaux d'intégration, la figure 4.6 démontre à quelles étapes du cycle de développement du logiciel chacune des activités générales de la gestion des risques peut être réalisée. Cette même figure est présentée à l'appendice C en version plus détaillée.

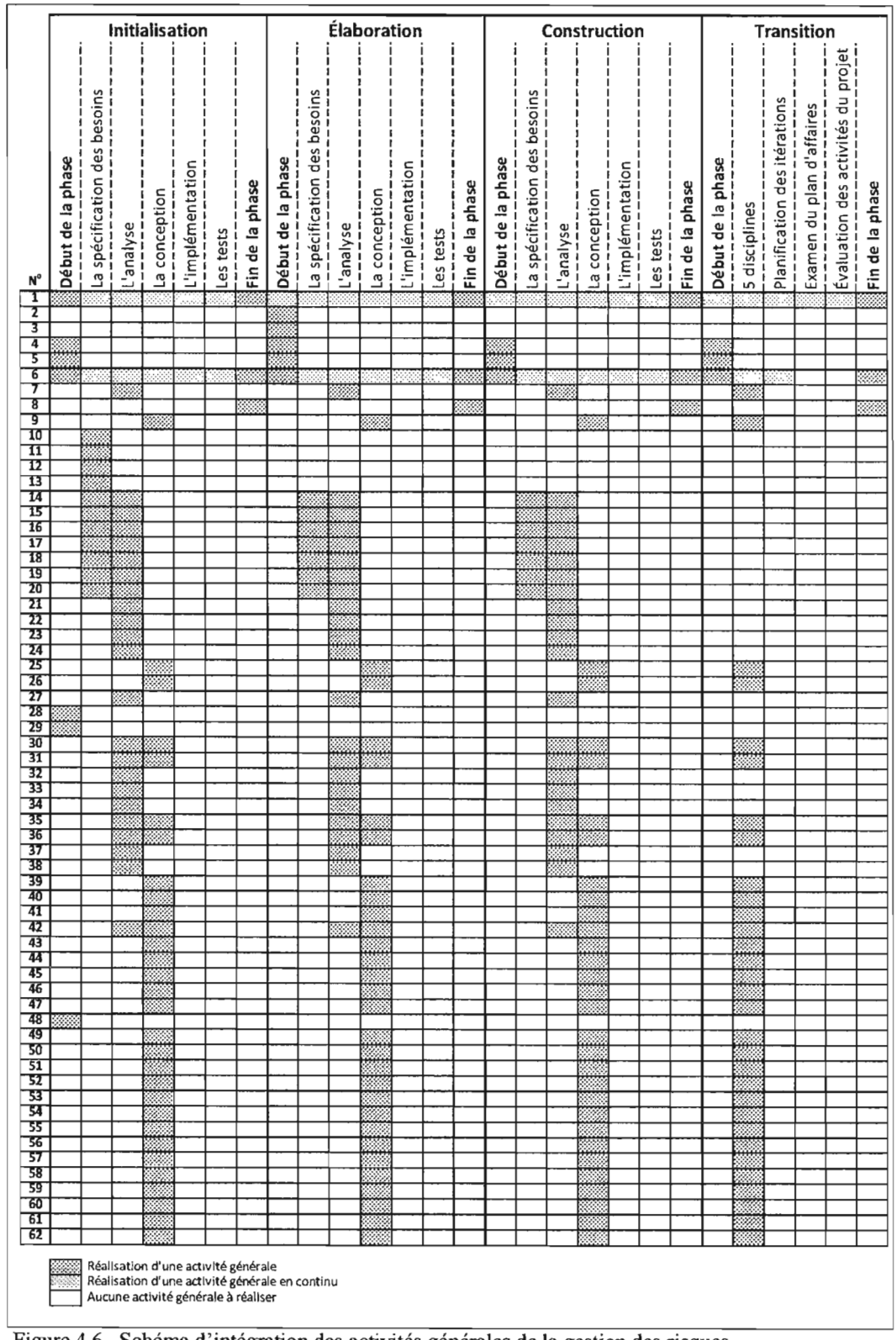

Figure 4.6 Schéma d'intégration des activités générales de la gestion des risques.

Suite à la figure 4.6, plusieurs observations peuvent être faites sur les différents résultats présentés en rapport à l'intégration des activités générales de la gestion des risques :

1. **Observations sur les activités n° 1 à 9** (Étape ❖ - Organisation de la démarche)

   La réalisation des activités reliées à l'étape de l'organisation de la démarche est disparate à travers l'ensemble des étapes du *Processus Unifié.* La situation s'explique par le fait que les activités concernent des tâches de natures différentes (planification, communication, préparation et soutien à la réalisation de la démarche) et doivent être réalisées à des moments bien différents dans le cadre d'un projet.

   Certaines activités doivent être effectuées en continu durant la presque totalité des quatre phases du *Processus Unifié.* Comme dans le cas des activités de projet du même genre, les activités n° 1 (Obtenir un soutien adéquat des parties prenantes du projet) et n° 6 (Établir la logistique de la démarche) doivent être réalisées en continu durant toutes les étapes du projet pour être efficaces et avec des interventions plus marquées à certains moments opportuns.

   L'activité qui vise à planifier la mise en œuvre des résultats obtenus durant la démarche de gestion des risques doit obligatoirement être réalisée au plus tard durant l'étape de *La conception.* Comme il a été démontré dans la figure 4.5 concernant les interdépendances entre les activités générales de la gestion des risques, la dernière à réaliser est l'activité n° 9 (Planifier la mise en œuvre des mesures de sécurité proposées par la démarche). Puisque cette activité vise à proposer des solutions de sécurité adéquates en fonction des résultats obtenus durant la démarche de gestion des risques, elle doit obligatoirement être réalisée au plus tard durant l'étape de *La conception* pour que les solutions soient considérées durant l'étape de *L'implémentation.*

2. **Observations sur les activités n° 10 à 20** (Étape 1 - Identification et étude du contexte)

   Il existe des similarités entre certaines activités de l'étape d'identification et de l'étude du contexte par rapport à celles de la phase de *L'initialisation.* Les activités n° 10 (Décrire l'environnement de la cible), n° 11 (Identifier les contraintes à l'égard de l'environnement de la cible), n° 12 (Identifier le cadre légal de l'environnement de la

cible) et n° 13 (Décrire l'aspect fonctionnel de l'environnement de la cible) sont étroitement similaires à certaines activités de projet réalisées dans la phase *L'initialisation*. L'un des objectifs de cette phase est justement la compréhension de la portée du projet et, aussi, la compréhension du contexte du système au moment de l'étape *La spécification des besoins*. De plus, ces activités ne sont réalisées qu'une seule fois, autant du côté de la démarche de gestion des risques que de celui du cycle de développement du logiciel.

Les activités qui ont trait à la cible de sécurité doivent être réalisées durant l'étape de *La spécification des besoins*, mais également durant celle de *L'analyse*. Les activités n° 14 à 20, qui concernent la prise de connaissance de la cible visée par la démarche de sécurité, doivent se dérouler à la fois durant l'étape de *La spécifications des besoins*, mais également lors de l'étape de *L'analyse*. Ceci est dû au fait que les besoins à traiter durant le projet logiciel sont identifiés lors de la spécification des besoins, mais détaillés au moment de l'analyse. De nouvelles informations à prendre en considération pour la cible de sécurité peuvent donc être amenées durant les deux étapes en question.

3. **Observations sur les activités n° 21 à 26** (Étape 2 - Identification des actifs informationnels)

Les activités visant l'identification des actifs doivent être réalisées durant l'étape de *L'analyse*, mais également durant celle de *La conception*. Les actifs informationnels critiques à considérer durant la démarche de gestion des risques peuvent être identifiés lors de l'étape de *L'analyse*, mais il faut nécessairement attendre à l'étape de *La conception* pour identifier les actifs de support. C'est seulement à ce moment-là que les actifs de nature technologique sont identifiés.

Les actifs de support peuvent encore être changés durant la phase de la *Transition*. Contrairement aux actifs informationnels critiques, les actifs de support sont de nature technologique et sont susceptibles d'être changés jusqu'à la dernière phase du *Processus Unifié*. C'est pourquoi les résultats démontrent que les activités n° 25 (Identifier les actifs de support aux actifs critiques de la cible) et n° 26 (Documenter les dépendances entre les actifs critiques et les actifs de support) sont intégrées à des étapes de la phase de la *Transition*.

4. **Observation sur les activités n° 27 à 34** (Étape 3 - Identification et évaluation des besoins de sécurité)

   L'ensemble des activités pour évaluer les besoins de sécurité est réalisée majoritairement durant l'étape de *L'analyse*, mais également durant celle de *La conception*. Cette situation est liée au fait que chaque activité d'identification des actifs à considérer entraîne nécessairement des activités reliées à l'identification et l'évaluation des besoins de sécurité à leur égard. Puisque la majorité des actifs est identifiée durant l'étape de *L'analyse*, ces activités peuvent être réalisées durant cette même étape. Cependant, l'identification et l'évaluation des besoins de sécurité doivent également prendre en compte les actifs de support qui ne sont identifiés qu'à l'étape de *La conception*.

   Certaines activités peuvent avoir été réalisées préalablement au projet de développement logiciel. Les activités n° 28 (Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité) et n° 29 (Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité) pourraient ne pas avoir à être réalisées si le projet possède déjà ces informations à titre d'intrants informationnels au projet. Cette situation s'explique par le fait que les informations produites par cette activité peuvent également provenir de travaux antérieurs.

5. **Observations sur les activités n° 35 à 45** (Étape 4 - Identification et évaluation des menaces et des vulnérabilités)

   Certaines activités reliées à l'audit peuvent être réalisées durant l'étape de *L'analyse*, tandis que d'autres doivent attendre l'étape de *La conception*. La réalisation des activités reliées à l'audit organisationnel peut être effectuée durant la discipline *L'analyse*, parce qu'il s'agit du moment où les besoins d'affaires sont énoncés et compris. Quant à la réalisation des activités reliées à l'audit technique, le moment diffère puisque les besoins technologiques sont seulement précisés à l'étape de *La conception*. C'est pourquoi les résultats d'intégration montrent que les activités communes pour les deux types d'audits, la préparation et la rédaction des résultats obtenus, sont réalisées durant les deux phases en question. Ce qui n'est pas le cas pour la réalisation proprement dite des activités d'audit selon leur nature.

L'activité qui consiste à évaluer les méthodes d'attaques possibles ne peut pas être réalisée avant l'étape de *La conception*. Les informations identifiées lors de l'activité n° 39 (Identifier les méthodes d'attaque pertinentes et leurs éléments menaçants à l'égard des actifs de support) sont basées sur les actifs de support. Puisque ceux-ci sont identifiés qu'à l'étape de *La conception*, il en va de même pour ce qui est de réaliser l'activité d'évaluation des méthodes d'attaques à leurs égards.

Les activités traitant des menaces à l'égard des actifs ne peuvent pas être réalisées avant l'étape de *La conception*. Puisque les activités n° 43 (Identifier les menaces à l'égard des actifs critiques de la cible), n° 44 (Évaluer les menaces à l'égard des actifs critiques de la cible) et n° 45 (Documenter les informations sur les menaces identifiées) ont besoin à la fois des résultats sur les méthodes d'attaques, les audits organisationnels et les audits techniques, ces activités doivent obligatoirement attendre à l'étape de *La conception* pour être réalisées afin de posséder tous les renseignements nécessaires.

6. **Observation sur les activités n° 46 à 53** (Étape *5 - Identification et évaluation des risques*)

Une activité peut avoir été réalisée préalablement au projet de développement logiciel. L'activité n° 48 (Définir les facteurs d'évaluation du risque) pourrait ne pas avoir à être réalisée si le projet possède déjà ces informations à titre d'intrants informationnels au projet. Cette situation s'explique par le fait que les informations produites par cette activité peuvent également provenir de travaux antérieurs.

Les activités qui concernent l'étape d'identification et d'évaluation des risques ne peuvent pas être réalisées avant l'étape de *La conception*. Les différentes activités reliées aux risques doivent nécessairement être réalisées lors de l'étape de *La conception*, puisque c'est seulement au moment de cette étape que tous les intrants informationnels nécessaires pour les réaliser (les besoins et les menaces de sécurité) sont disponibles.

7. **Observation sur les activités n° 54 à 62** (Étape *6 - Identification des exigences de sécurité*)

   Les activités qui concernent l'étape d'identification des exigences de sécurité ne peuvent pas être réalisées avant l'étape de *La conception*. Les activités qui ont trait à l'identification des exigences de sécurité ont besoin des informations concernant les risques à traiter. Étant donné que ces informations ne sont disponibles qu'au moment de l'étape de *La conception*, la réalisation de ces activités doit, du même coup, attendre à cette étape pour être effectuée.

La figure 4.7 reprend celle présentée plus tôt à l'étape 1 de la démarche analytique où étaient affichées les interdépendances entre les activités générales de la gestion des risques. Cette fois, la figure contient en plus les résultats des travaux d'intégration en affichant en rouge les activités identifiées comme ayant un lien direct avec celles du cycle de développement logiciel.

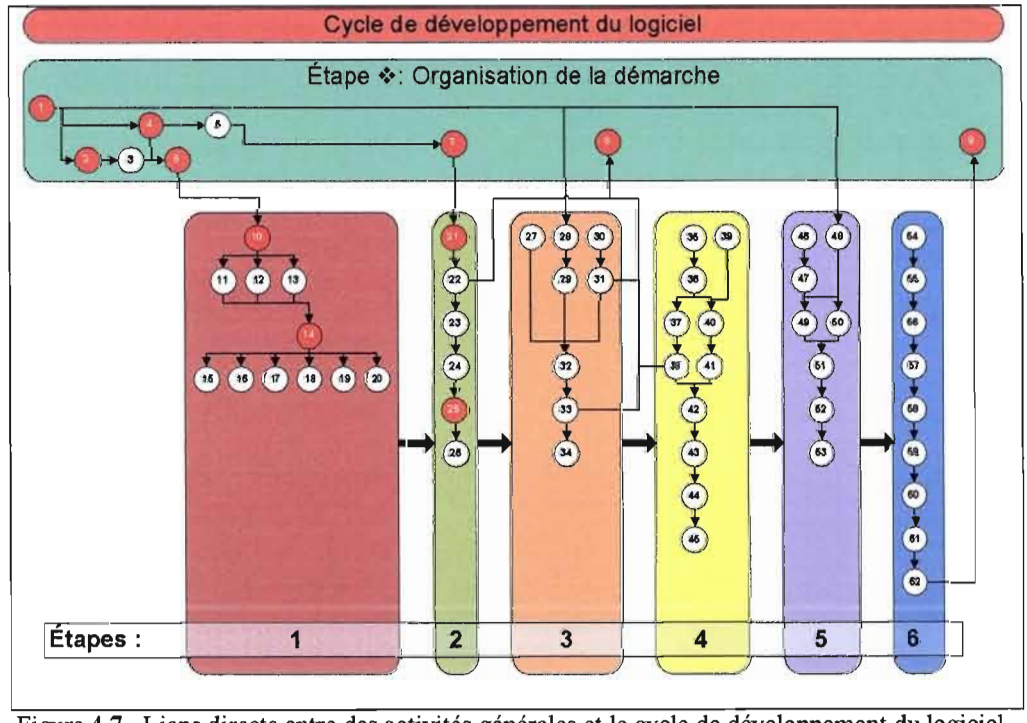

Figure 4.7 Liens directs entre des activités générales et le cycle de développement du logiciel.

Le point à noter suite à la présentation de la figure 4.7, est que les 11 activités en rouges sont incluses dans seulement trois des sept étapes de la gestion des risques considérées dans la démarche analytique. Les résultats démontrent à quel point ces trois étapes jouent un rôle primordial dans la réalisation de la démarche de gestion des risques :

- ❖ Organisation de la démarche
- 1. Identification et étude du contexte
- 2. Identification des actifs informationnels

Les tableaux 4.27 à 4.30 démontre encore une fois les résultats obtenus, mais du point de vue du cycle de développement du logiciel. Il est ainsi possible de constater, pour chaque étape du *Processus Unifié*, quelles activités générales de la gestion des risques doivent être réalisées.

Tableau 4.27

Activités de la gestion des risques pour la phase *L'Initialisation* du *Processus Unifié*

L'initialisation		
Début de la phase		
	1	Obtenir un soutien adéquat des parties prenantes du projet
	4	Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche
	5	Informer les participants sur les activités de sécurité à réaliser durant la démarche
	6	Établir la logistique de la démarche
	28	Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité
	29	Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité
	48	Définir les facteurs d'évaluation du risque
La spécification des besoins		
	1	Obtenir un soutien adéquat des parties prenantes du projet
	6	Établir la logistique de la démarche
	10	Décrire l'environnement de la cible
	11	Identifier les contraintes à l'égard de l'environnement de la cible
	12	Identifier le cadre légal de l'environnement de la cible
	13	Décrire l'aspect fonctionnel de l'environnement de la cible
	14	Préciser la cible de la démarche de sécurité
	15	Identifier les enjeux à l'égard de la cible
	16	Décrire l'aspect fonctionnel de la cible
	17	Identifier les hypothèses à l'égard de la cible
	18	Identifier les règles de sécurité à l'égard de la cible
	19	Identifier les contraintes à l'égard de la cible
	20	Identifier le cadre légal de la cible

L'analyse	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
7	Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche
14	Préciser la cible de la démarche de sécurité
15	Identifier les enjeux à l'égard de la cible
16	Décrire l'aspect fonctionnel de la cible
17	Identifier les hypothèses à l'égard de la cible
18	Identifier les règles de sécurité à l'égard de la cible
19	Identifier les contraintes à l'égard de la cible
20	Identifier le cadre légal de la cible
21	Rencontrer les groupes de participants pour identifier les actifs importants de la cible
22	Rédiger une liste des actifs identifiés par groupes de participants rencontrés
23	Identifier les actifs critiques de la cible
24	Rédiger une liste intégrée de tous les actifs identifiés
27	Regrouper les actifs critiques ayant des besoins de sécurité similaires
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
32	Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques
33	Rédiger une synthèse des besoins de sécurité pour les actifs critiques
34	Valider les besoins de sécurité pour les actifs critiques
35	Identifier les éléments de la cible à auditer
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
37	Effectuer l'audit de sécurité organisationnelle de la cible
38	Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible
42	Documenter les informations sur les vulnérabilités identifiées
La conception	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
9	Planifier la mise en œuvre des mesures de sécurité proposées par la démarche
25	Identifier les actifs de support aux actifs critiques de la cible
26	Documenter les dépendances entre les actifs critiques et les actifs de support
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
35	Identifier les éléments de la cible à auditer
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
39	Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support

40	Effectuer l'audit de sécurité technique de la cible
41	Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible
42	Documenter les informations sur les vulnérabilités identifiées
43	Identifier les menaces à l'égard des actifs critiques de la cible
44	Évaluer les menaces à l'égard des actifs critiques de la cible
45	Documenter les informations sur les menaces identifiées
46	Identifier les risques potentiels envers la cible
47	Sélectionner les risques à considérer dans le cadre d'une analyse de risques
L'implémentation	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
Les tests	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
Fin de la phase	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
8	Communiquer les résultats obtenus lors des consultations avec les groupes de participants

Tableau 4.28

Activités de la gestion des risques pour la phase *L'élaboration* du *Processus Unifié*

L'élaboration	
Début de la phase	
1	Obtenir un soutien adéquat des parties prenantes du projet
2	Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information
3	Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir
4	Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche
5	Informer les participants sur les activités de sécurité à réaliser durant la démarche
6	Établir la logistique de la démarche
La spécification des besoins	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
14	Préciser la cible de la démarche de sécurité
15	Identifier les enjeux à l'égard de la cible
16	Décrire l'aspect fonctionnel de la cible
17	Identifier les hypothèses à l'égard de la cible
18	Identifier les règles de sécurité à l'égard de la cible
19	Identifier les contraintes à l'égard de la cible
20	Identifier le cadre légal de la cible
L'analyse	

1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
7	Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche
14	Préciser la cible de la démarche de sécurité
15	Identifier les enjeux à l'égard de la cible
16	Décrire l'aspect fonctionnel de la cible
17	Identifier les hypothèses à l'égard de la cible
18	Identifier les règles de sécurité à l'égard de la cible
19	Identifier les contraintes à l'égard de la cible
20	Identifier le cadre légal de la cible
21	Rencontrer les groupes de participants pour identifier les actifs importants de la cible
22	Rédiger une liste des actifs identifiés par groupes de participants rencontrés
23	Identifier les actifs critiques de la cible
24	Rédiger une liste intégrée de tous les actifs identifiés
27	Regrouper les actifs critiques ayant des besoins de sécurité similaires
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
32	Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques
33	Rédiger une synthèse des besoins de sécurité pour les actifs critiques
34	Valider les besoins de sécurité pour les actifs critiques
35	Identifier les éléments de la cible à auditer
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
37	Effectuer l'audit de sécurité organisationnelle de la cible
38	Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible
42	Documenter les informations sur les vulnérabilités identifiées
La conception	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
9	Planifier la mise en œuvre des mesures de sécurité proposées par la démarche
25	Identifier les actifs de support aux actifs critiques de la cible
26	Documenter les dépendances entre les actifs critiques et les actifs de support
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
35	Identifier les éléments de la cible à auditer
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
39	Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support
40	Effectuer l'audit de sécurité technique de la cible

41	Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible
42	Documenter les informations sur les vulnérabilités identifiées
43	Identifier les menaces à l'égard des actifs critiques de la cible
44	Évaluer les menaces à l'égard des actifs critiques de la cible
45	Documenter les informations sur les menaces identifiées
46	Identifier les risques potentiels envers la cible
47	Sélectionner les risques à considérer dans le cadre d'une analyse de risques
49	Évaluer la potentialité des risques
50	Évaluer l'impact des risques
51	Évaluer globalement les risques à partir de sa potentialité et de son impact
52	Documenter les risques évalués
53	Valider les risques identifiés pour les actifs critiques avec les parties prenantes
54	Réviser toutes les informations recueillies, traitées et produites durant la démarche
55	Déterminer les recommandations sur des exigences de sécurité de haut niveau
56	Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau
57	Résumer les informations sur les recommandations de sécurité de haut niveau
58	Déterminer les exigences de sécurité pour la mitigation des risques
59	Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité
60	Résumer les informations sur les exigences de sécurité
61	Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes
62	Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité
L'implémentation	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
Les tests	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
Fin de la phase	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
8	Communiquer les résultats obtenus lors des consultations avec les groupes de participants

Tableau 4.29

Activités de la gestion des risques pour la phase *La construction* du *Processus Unifié*

La construction	
Début de la phase	
1	Obtenir un soutien adéquat des parties prenantes du projet
4	Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche

	5	Informer les participants sur les activités de sécurité à réaliser durant la démarche
	6	Établir la logistique de la démarche
La spécification des besoins		
	1	Obtenir un soutien adéquat des parties prenantes du projet
	6	Établir la logistique de la démarche
	14	Préciser la cible de la démarche de sécurité
	15	Identifier les enjeux à l'égard de la cible
	16	Décrire l'aspect fonctionnel de la cible
	17	Identifier les hypothèses à l'égard de la cible
	18	Identifier les règles de sécurité à l'égard de la cible
	19	Identifier les contraintes à l'égard de la cible
	20	Identifier le cadre légal de la cible
L'analyse		
	1	Obtenir un soutien adéquat des parties prenantes du projet
	6	Établir la logistique de la démarche
	7	Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche
	14	Préciser la cible de la démarche de sécurité
	15	Identifier les enjeux à l'égard de la cible
	16	Décrire l'aspect fonctionnel de la cible
	17	Identifier les hypothèses à l'égard de la cible
	18	Identifier les règles de sécurité à l'égard de la cible
	19	Identifier les contraintes à l'égard de la cible
	20	Identifier le cadre légal de la cible
	21	Rencontrer les groupes de participants pour identifier les actifs importants de la cible
	22	Rédiger une liste des actifs identifiés par groupes de participants rencontrés
	23	Identifier les actifs critiques de la cible
	24	Rédiger une liste intégrée de tous les actifs identifiés
	27	Regrouper les actifs critiques ayant des besoins de sécurité similaires
	30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
	31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
	32	Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques
	33	Rédiger une synthèse des besoins de sécurité pour les actifs critiques
	34	Valider les besoins de sécurité pour les actifs critiques
	35	Identifier les éléments de la cible à auditer
	36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
	37	Effectuer l'audit de sécurité organisationnelle de la cible
	38	Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible
	42	Documenter les informations sur les vulnérabilités identifiées
La conception		
	1	Obtenir un soutien adéquat des parties prenantes du projet

	6	Établir la logistique de la démarche
	9	Planifier la mise en œuvre des mesures de sécurité proposées par la démarche
	25	Identifier les actifs de support aux actifs critiques de la cible
	26	Documenter les dépendances entre les actifs critiques et les actifs de support
	30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
	31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
	35	Identifier les éléments de la cible à auditer
	36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
	39	Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support
	40	Effectuer l'audit de sécurité technique de la cible
	41	Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible
	42	Documenter les informations sur les vulnérabilités identifiées
	43	Identifier les menaces à l'égard des actifs critiques de la cible
	44	Évaluer les menaces à l'égard des actifs critiques de la cible
	45	Documenter les informations sur les menaces identifiées
	46	Identifier les risques potentiels envers la cible
	47	Sélectionner les risques à considérer dans le cadre d'une analyse de risques
	49	Évaluer la potentialité des risques
	50	Évaluer l'impact des risques
	51	Évaluer globalement les risques à partir de sa potentialité et de son impact
	52	Documenter les risques évalués
	53	Valider les risques identifiés pour les actifs critiques avec les parties prenantes
	54	Réviser toutes les informations recueillies, traitées et produites durant la démarche
	55	Déterminer les recommandations sur des exigences de sécurité de haut niveau
	56	Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau
	57	Résumer les informations sur les recommandations de sécurité de haut niveau
	58	Déterminer les exigences de sécurité pour la mitigation des risques
	59	Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité
	60	Résumer les informations sur les exigences de sécurité
	61	Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes
	62	Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité
L'implémentation		
	1	Obtenir un soutien adéquat des parties prenantes du projet
	6	Établir la logistique de la démarche
Les tests		
	1	Obtenir un soutien adéquat des parties prenantes du projet
	6	Établir la logistique de la démarche
Fin de la phase		
	1	Obtenir un soutien adéquat des parties prenantes du projet

6	Établir la logistique de la démarche
8	Communiquer les résultats obtenus lors des consultations avec les groupes de participants

Tableau 4.30

Activités de la gestion des risques pour la phase *La transition* du *Processus Unifié*

La transition	
Début de la phase	
1	Obtenir un soutien adéquat des parties prenantes du projet
4	Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche
5	Informer les participants sur les activités de sécurité à réaliser durant la démarche
6	Établir la logistique de la démarche
Les cinq disciplines	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
7	Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche
9	Planifier la mise en œuvre des mesures de sécurité proposées par la démarche
25	Identifier les actifs de support aux actifs critiques de la cible
26	Documenter les dépendances entre les actifs critiques et les actifs de support
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés
35	Identifier les éléments de la cible à auditer
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité
39	Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support
40	Effectuer l'audit de sécurité technique de la cible
41	Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible
42	Documenter les informations sur les vulnérabilités identifiées
43	Identifier les menaces à l'égard des actifs critiques de la cible
44	Évaluer les menaces à l'égard des actifs critiques de la cible
45	Documenter les informations sur les menaces identifiées
46	Identifier les risques potentiels envers la cible
47	Sélectionner les risques à considérer dans le cadre d'une analyse de risques
49	Évaluer la potentialité des risques
50	Évaluer l'impact des risques
51	Évaluer globalement les risques à partir de sa potentialité et de son impact
52	Documenter les risques évalués
53	Valider les risques identifiés pour les actifs critiques avec les parties prenantes
54	Réviser toutes les informations recueillies, traitées et produites durant la

	démarche
55	Déterminer les recommandations sur des exigences de sécurité de haut niveau
56	Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau
57	Résumer les informations sur les recommandations de sécurité de haut niveau
58	Déterminer les exigences de sécurité pour la mitigation des risques
59	Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité
60	Résumer les informations sur les exigences de sécurité
61	Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes
62	Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité
La planification des itérations	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
L'examen du plan d'affaires	
1	Obtenir un soutien adéquat des parties prenantes du projet
L'évaluation des activités du projet	
1	Obtenir un soutien adéquat des parties prenantes du projet
Fin de la phase	
1	Obtenir un soutien adéquat des parties prenantes du projet
6	Établir la logistique de la démarche
8	Communiquer les résultats obtenus lors des consultations avec les groupes de participants

Les tableaux 4.27 à 4.30 mettent en évidence une autre observation concernant les résultats obtenus suite à l'intégration des activités générales de la gestion des risques dans le cycle de développement logiciel. Aucune des activités, mises à part les deux qui ont été considérées comme en continu durant tout le projet, n'a été intégrée dans les étapes de *L'implémentation* et de *Les tests*. Cette situation s'explique par le fait que la liste des activités générales de la gestion des risques a été produite en fonction des activités de sécurité proposées par les trois méthodes étudiées. Suite aux travaux de l'étape 1 de la démarche analytique, les résultats avaient démontré qu'aucune activité n'était reliée aux deux dernières étapes de la gestion des risques qui concernent justement la sélection précise de mesures de sécurité et leur implantation. Si des activités générales de la gestion des risques avaient été identifiées pour ces deux dernières étapes, ces activités auraient possiblement été intégrées dans les deux étapes de *L'implémentation* et de *Les tests* du *Processus Unifié*.

Avant de conclure l'étape 3 de la démarche analytique, quelques difficultés ont été rencontrées durant la réalisation des travaux d'intégration et il s'avère important de les spécifier :

- Il a fallu prendre en considération les activités qui, durant une seule et même phase, ne devaient être réalisées qu'une seule fois par rapport à celles qui devaient l'être plusieurs fois. Ces dernières pouvaient alors être intégrées dans les étapes représentées par les cinq disciplines, puisque l'objectif du *Processus Unifié* est de les réaliser de façon itérative. Pour celles à réaliser qu'à une seule reprise, des étapes explicites de *Début de la phase* et de *Fin de la phase* ont du être ajoutées dans chacune des phases pour les fins des travaux d'intégration.

- Les trois premières phases du *Processus Unifié* (*L'initialisation*, *L'élaboration* et *La construction*) ont toutes trois les mêmes étapes à réaliser. Ce n'est pas le cas pour la dernière, celle de *La transition*, qui présente des étapes quelque peu différentes, étant donné qu'elle vise à conclure le projet de développement logiciel. Cette différence a donc demandé une attention particulière à son égard durant les travaux d'intégration.

- Certaines activités peuvent avoir été réalisées préalablement à la démarche de gestion des risques, ce qui amène une situation particulière par rapport aux autres activités générales de la gestion des risques à réaliser. Il a donc fallu traiter ces activités d'une manière différente afin d'illustrer ce fait dans les tableaux et figures affichant les résultats obtenus.

Cette troisième étape de la démarche analytique consistait à intégrer les différentes activités générales de la gestion des risques dans un contexte de cycle de développement logiciel. Les résultats obtenus durant les travaux de cette étape, expliqués et démontrés sous la forme de plusieurs tableaux et figures, représentent les informations finales résultantes des trois étapes de la démarche analytique.

En résumé, les activités effectuées dans les méthodes de gestion des risques EBIOS, MÉHARI et OCTAVE ont été présentées, extraites et fusionnées pour en dégager une nouvelle série d'activités générales de la gestion des risques. Ensuite, les étapes du modèle de cycle de développement logiciel, telles que proposées par le *Processus Unifié*, ont été présentées plus en détail. Finalement, chacune des activités générales de la gestion des risques a fait l'objet d'une intégration justifiée dans les étapes du *Processus Unifié*.

Ce quatrième chapitre visait à démontrer la possibilité d'intégrer des activités de gestion des risques, provenant de sources établies dans le domaine, dans un contexte de cycle de développement du logiciel. Le prochain chapitre présentera tout d'abord la synthèse et les conclusions globales à tirer par rapport aux résultats obtenus dans ce présent chapitre et, ensuite, le positionnement final à l'égard de l'hypothèse principale qui a été émise dans le troisième chapitre de la présente recherche.

CHAPITRE V

LE SOMMAIRE DES RÉSULTATS DE LA DÉMARCHE ANALYTIQUE

Les travaux effectués lors de la démarche analytique, présentée au quatrième chapitre, ont révélé différents résultats sur l'intégration des activités générales de la gestion des risques dans le contexte du développement logiciel. Ainsi, le cinquième chapitre consiste à récapituler ces résultats dans le but de les interpréter aux moyens de synthèses et de comparaisons à l'égard de l'hypothèse principale de la recherche.

La première section de ce chapitre présente des synthèses sur les principaux résultats obtenus lors de chacune des trois étapes de la démarche analytique auxquels s'ajouteront des vérifications par rapport aux mesures visées et préalablement établies pour l'étape. La deuxième section aborde plus précisément le résultat d'ensemble de la démarche analytique afin d'établir un positionnement face à l'hypothèse principale de la recherche. Pour terminer, la troisième section énoncera les conclusions finales à déduire suite aux résultats obtenus.

Dans l'ensemble du document, le rôle de ce chapitre consiste à présenter le dénouement de la recherche, en faisant une rétrospective sur les résultats obtenus durant la démarche analytique par rapport aux objectifs qui ont été fixés pour la recherche.

5.1 Synthèses des résultats obtenus

Cette section vise à résumer les résultats obtenus lors des trois étapes de la démarche analytique, soit : l'identification des activités générales des méthodes de gestion des risques, la présentation du contexte de cycle de développement logiciel et l'intégration des activités générales de la gestion des risques dans un contexte de cycle de développement du logiciel.

5.1.1 Retour sur les résultats de l'étape 1

Cette première étape avait pour but de détailler les méthodes de gestion des risques sélectionnées, de synthétiser leurs activités et, à partir de celles-ci, de dresser une liste d'activités générales de la gestion des risques. Voici un résumé des résultats obtenus :

a) Le détail des trois méthodes de gestion des risques a été présenté :

EBIOS propose une série d'activités de sécurité à réaliser au cours de cinq étapes principales : l'étude du contexte, l'expression des besoins de sécurité, l'étude des menaces, l'identification des objectifs de sécurité et la détermination des exigences de sécurité.

MEHARI propose une série d'activités de sécurité à réaliser, regroupées en trois modules distincts : l'analyse des enjeux de la sécurité et de la classification des informations et ressources, le diagnostic de l'état des services de sécurité et l'analyse de situations de risque.

OCTAVE propose une série d'activités de sécurité à réaliser, réparties dans huit processus divisés en trois phases globales : identifier les profils de menaces basés sur les actifs, identifier les vulnérabilités de l'infrastructure et développer la stratégie de sécurité.

b) En fonction de leur découpage méthodologique, les trois méthodes de gestion des risques représentent un total de 119 activités de sécurité distribuées de la manière suivante :

- 45 activités pour la méthode *EBIOS*

- 22 activités pour la méthode *MEHARI*
- 52 activités pour la méthode *OCTAVE*

c) Des 119 activités de sécurité provenant des méthodes de gestion des risques, 117 ont été conservées pour dresser la liste des activités générales de la gestion des risques.

d) Une liste des activités générales de la gestion des risques a été produite et contient 62 activités représentant les 117 activités recensées dans les trois méthodes de gestion des risques sélectionnées.

e) Durant la démarche de création de la liste des activités générales de la gestion des risques, les 117 activités ont été associées à l'une des étapes de la gestion des risques. Cela a permis du même coup de positionner chacune des méthodes étudiées par rapport aux neuf étapes de la gestion des risques présentées dans le deuxième chapitre :

- La méthode *EBIOS* couvre les étapes 1 à 6;
- La méthode *MEHARI* couvre les étapes 1 à 6;
- La méthode *OCTAVE* couvre les étapes 1 à 6 et l'étape spéciale ❖.

f) Les 62 activités générales de la gestion des risques ont été regroupées en fonction des étapes de la gestion des risques, donnant un total de sept groupes distincts :

- Organisation de la démarche (9 activités, n°s 1 à 9)
- Identification et étude du contexte (11 activités, n°s 10 à 20)
- Identification des actifs informationnels (6 activités, n°s 21 à 26)
- Identification et évaluation des besoins de sécurité (8 activités, n°s 27 à 34)
- Identification et évaluation des menaces et des vulnérabilités (11 activités, n°s 35 à 45)
- Identification et évaluation des risques (8 activités, n°s 46 à 53)
- Identification des exigences de sécurité (9 activités, n°s 54 à 62)

g) Durant la démarche de création de la liste des activités générales de la gestion des risques, les interdépendances de ces activités pour leur réalisation ont pu être identifiées.

Ensuite, il est possible de vérifier si les mesures concrètes visées par l'étape 1, énoncées lors de l'élaboration de sa démarche dans le troisième chapitre, ont été réalisées en vérifiant avec les résultats présentés ci-dessus :

- ✓ Identifier la liste des activités de sécurité proposées dans chacune des méthodes étudiées : résultats *a* et *b*.

- ✓ Positionner chacune des méthodes par rapport aux étapes générales de la gestion des risques présentées dans le deuxième chapitre : résultat *e*.

- ✓ Positionner chacune des activités de sécurité identifiées par rapport aux étapes générales de la gestion des risques présentées dans le deuxième chapitre : résultat *e*.

- ✓ Dresser une liste des activités générales de la gestion des risques à partir uniquement des activités de sécurité identifiées dans les méthodes étudiées : résultat *d*.

- ✓ Identifier les dépendances existantes entre les différentes activités générales de la gestion des risques : résultat *g*.

5.1.2 Retour sur les résultats de l'étape 2

Cette deuxième étape avait pour but de détailler le cycle de développement du logiciel proposé par le *Processus Unifié*. Voici un résumé des résultats obtenus :

a. La méthode propose un cycle d'activités comprenant quatre grandes phases à réaliser séquentiellement : l'initialisation, l'élaboration, la construction et la transition.

b. Dans la réalisation d'une phase, certaines activités sont réalisées une seule fois (au début ou à la fin), tandis que d'autres peuvent l'être à plusieurs reprises par l'itération des cinq disciplines suivantes : la spécification des besoins, l'analyse, la conception, l'implémentation et les tests.

Ensuite, il est possible de vérifier si les mesures concrètes visées par l'étape 2, énoncées lors de l'élaboration de sa démarche dans le troisième chapitre, ont été réalisées en vérifiant avec les résultats présentés ci-dessus :

- ✓ Détailler les étapes réalisées dans un cycle de développement du logiciel telles que définies par le Processus Unifié : résultats *a* et *b*.

5.1.3 Retour sur les résultats de l'étape 3

Cette troisième étape avait pour but d'intégrer les activités générales de la gestion des risques avec les autres activités du cycle de développement logiciel proposées par le *Processus Unifié*. Voici un résumé des résultats obtenus :

a. Les 62 activités générales de la gestion des risques ont été intégrées une à une dans les étapes proposées par les phases du *Processus Unifié,* et ce, selon le contexte de l'activité en question, les informations nécessaires à sa réalisation et ses dépendances envers les autres activités de sécurité.

b. Parmi les 62 activités intégrées, 11 d'entre elles ont un lien direct avec une activité du cycle de développement du logiciel. Les 51 autres activités sont intégrées via leurs interdépendances avec au moins l'une des 11 activités ayant un lien direct.

c. La proportion des 62 activités générales de la gestion des risques à réaliser, durant chacune des phases du *Processus Unifié*, est la suivante :

   - Phase d'initialisation : 60 des 62 activités (97 %) générales sont à réaliser;
   - Phase d'élaboration : 55 des 62 activités (89 %) générales sont à réaliser;
   - Phase de construction : 53 des 62 activités (85 %) générales sont à réaliser;
   - Phase de transition : 36 des 62 activités (58 %) générales sont à réaliser.

d. Aucune activité, à l'exception de celles qui sont effectuées en continu, n'a été intégrée dans les étapes de *L'implantation* et de *Les tests* du *Processus Unifié*.

Ensuite, il est possible de vérifier si les mesures concrètes visées par l'étape 3, énoncées lors de l'élaboration de sa démarche dans le troisième chapitre, ont été réalisées en vérifiant avec les résultats présentés ci-dessus :

- ✓ Intégrer toutes les activités générales de gestion des risques dans le cycle de développement du logiciel : résultat *a*.

- ✓ Identifier les activités de sécurité qui sont concrètement liées à une activité du cycle de développement du logiciel par rapport à celles qui le sont par l'intermédiaire d'une autre activité de sécurité intégrée : résultat *b*.

5.2 Positionnement des résultats obtenus face à l'hypothèse principale de la recherche

Cette section vise à analyser le résultat global obtenu lors de la démarche analytique pour valider l'hypothèse principale de la recherche. Voici un rappel de cette hypothèse :

> *Les activités de sécurité véhiculées dans les méthodes de gestion des risques pour la sécurité des systèmes d'information peuvent être appliquées dans les étapes du cycle de développement du logiciel, et ce, dans le but de diminuer la présence de vulnérabilités de sécurité au moment où le logiciel sera achevé et mis en opération.*

Cette hypothèse comporte plusieurs parties qu'il est possible de séparer, permettant ainsi de les juger plus facilement par rapport aux résultats obtenus lors de la démarche analytique. Une fois toutes ces parties analysées, il est alors possible d'établir un positionnement général face à l'hypothèse complète.

La partie « ***Les activités de sécurité véhiculées dans les méthodes de gestion des risques pour la sécurité des systèmes d'information...*** » se rapporte directement à la première étape de la démarche analytique. Les activités de sécurité véhiculées dont il est question sont représentées par la liste d'activités générales de la gestion des risques qui a été créée par l'analyse, la synthèse et la généralisation des activités prônées par trois méthodes connues dans le domaine.

La partie « ***... peuvent être appliqués dans les étapes du cycle de développement du logiciel...*** » concerne spécifiquement la deuxième et la troisième étape de la démarche analytique. Après avoir exposé les différentes étapes du modèle de cycle de développement logiciel, il a été démontré qu'il y avait un lien direct ou indirect possible entre chacune des activités générales de la gestion des risques et le cycle de développement du logiciel, permettant ainsi leur intégration. L'enjeu réel n'était pas de pouvoir ou non les intégrer, puisqu'il est théoriquement toujours possible de faire une activité voulue, mais plutôt d'établir comment elles peuvent être logiquement attachées aux étapes du cycle de développement logiciel.

La partie « ***... et ce, dans le but de diminuer la présence de vulnérabilités de sécurité au moment où le logiciel sera achevé et mis en opération.*** » fait référence aux études et travaux,

présentés au premier chapitre, qui affirment que l'ajout d'activités de sécurité durant les étapes du développement logiciel favorise la diminution de vulnérabilités de sécurité dans les logiciels produits. Puisque l'une de ses activités de sécurité est celle de la gestion des risques, et qu'il a été démontré qu'elle pouvait être intégrée durant les étapes du développement logiciel, l'objectif visant à diminuer la présence de vulnérabilités de sécurité au moment où le logiciel sera achevé et mise en opération est donc atteint.

Donc, en rassemblant toutes les parties de l'hypothèse, il a été démontré qu'il est possible de justifier l'intégration des activités de sécurité reliées à la gestion des risques dans un cycle de développement du logiciel dans le but de diminuer les vulnérabilités de sécurité avant leur mise en production.

5.3 Conclusions finales sur les résultats obtenus

Cette section vise à présenter les conclusions finales sur les résultats obtenus afin de permettre le dégagement d'une opinion générale sur la recherche présentée dans ce document.

Les activités de sécurité reliées à la gestion des risques peuvent s'intégrer aux étapes du cycle de développement du logiciel au même titre que les activités du projet. Elles doivent être réalisées en continu durant tout le projet et nécessitent une grande facilité et rapidité d'adaptation aux étapes du projet de développement logiciel.

Pour que les activités de sécurité donnent les résultats escomptés une fois intégrées, **les facteurs de succès à noter** sont la participation active des intervenants du projet et l'utilisation d'un outillage adéquat (logiciel, gabarit, etc.) pour les réaliser.

Les bénéfices escomptés par l'intégration des activités de sécurité dans le cycle de développement du logiciel sont : l'assurance de considérer adéquatement la sécurité informatique sur les aspects les plus importants de la solution en fonction des besoins en la matière, la contribution à l'élaboration d'une solution qui minimise les vulnérabilités de sécurité et la sensibilisation auprès des intervenants sur les aspects de la sécurité informatique.

Avant de conclure, il faut noter que les résultats obtenus dans cette recherche sont fortement liés aux intrants informationnels de base utilisés, dont les principaux sont le *Processus Unifié* et les méthodes *EBIOS, MEHARI et OCTAVE*, et à la démarche utilisée pour justifier l'intégration des activités générales de la gestion des risques dans les étapes du cycle de développement du logiciel.

En résumé, les informations présentées dans ce chapitre établissent les liens entre les résultats obtenus durant la démarche analytique, les fondements établis pour la recherche et les thèmes présentés auparavant concernant le développement logiciel et les méthodes de gestion des risques. Des synthèses sur les résultats obtenus ont tout d'abord été énoncées. Ensuite, l'hypothèse principale a été revue et analysée par rapport à ces mêmes résultats dans le but de la confirmer ou de l'infirmer. Pour terminer, des conclusions finales ont été formulées pour donner une perception générale aux lecteurs sur le résultat global de la recherche.

Ce cinquième et dernier chapitre visait à présenter sommairement les résultats obtenus durant la démarche analytique pour les mettre en perspective avec les objectifs fixés et, de cette façon, conclure la présente recherche.

LA CONCLUSION

Ce mémoire s'intéressait principalement au domaine du développement logiciel et de la sécurité informatique. Il visait à présenter une approche qui contribuait à mettre en application leurs concepts respectifs de façon conjointe, puisque la sécurité est actuellement un enjeu important dans le domaine de l'informatique. La recherche présentée dans ce mémoire ne visait pas toute la gamme d'activités de sécurité qu'il est possible de mettre en application durant un projet de développement logiciel, mais bien de préciser davantage l'une d'entre elles, soit la gestion des risques de sécurité.

L'origine même de ce mémoire prend sa source d'une problématique qui consiste en la présence des vulnérabilités de sécurité dans les logiciels mis en opération et qui, par conséquent, représente des risques considérables pour les utilisateurs. La contribution de cette recherche au domaine du développement logiciel était donc de détailler une solution qui prendrait davantage en considération la sécurité informatique durant le développement logiciel via la réalisation d'activités reliées à la gestion des risques de sécurité, et ce, à des moments opportuns durant le cycle de développement du logiciel. Bien que plusieurs autres projets de recherche et diverses publications traitent de ce sujet, aucun d'entre eux ne détaille cette approche jusqu'au niveau de ses activités de sécurité à réaliser ou ne se sert explicitement des méthodes reconnues en la matière comme source d'informations principales.

Pour ce faire, l'objectif consistait à se baser sur les concepts existants et reconnus dans les domaines étudiés, pour ensuite les mettre en relation et faire progresser la recherche de manière à utiliser graduellement les résultats obtenus. À la toute fin, les résultats finaux devaient servir à valider l'hypothèse émise quant à la solution proposée. La recherche était donc basée sur une approche déductive où les travaux découlaient fortement des concepts reconnus dans les domaines étudiés et des résultats obtenus graduellement durant les travaux de la recherche.

Tout d'abord, introduit dès le début de ce mémoire, le contexte de la recherche présentait les sujets importants qui ont servi d'intrants informationnels à sa réalisation. Ainsi, les étapes communes et les modèles de développement existants pour le domaine du développement logiciel furent énoncés. Ensuite, la sécurité informatique, mais plus précisément les concepts de la gestion des

risques de sécurité pour les systèmes d'information, a été abordée. Une fois la mise en contexte établie, les fondements même de la recherche furent exposés. L'objectif était de présenter la problématique visée et de lier les sujets introduits et leurs utilisations dans la solution élaborée par la suite au moyen d'une démarche analytique. Cette démarche fut réalisée en trois grandes étapes : produire une liste des activités générales de la gestion des risques à partir de trois méthodes de référence étudiées (*EBIOS*, *MEHARI* et *OCTAVE*), présenter les activités réalisées dans le cadre des étapes d'un cycle de développement du logiciel (*Processus Unifié*) et, finalement, intégrer ces mêmes activités générales de la gestion des risques dans les étapes du cycle de développement logiciel. Pour conclure, le tout fut résumé dans un sommaire des résultats de la recherche.

Concernant ces résultats, la première étape de la démarche analytique produisit une liste contenant 62 activités générales de la gestion des risques, et ce, à partir des 117 activités de sécurité provenant de l'étude des méthodes de référence. La deuxième étape présenta des détails sur les 27 étapes attribuables aux quatre phases du cycle de développement logiciel telles que proposées par la source de référence. La troisième étape démontra l'intégration, dans les étapes du cycle de développement logiciel, des 62 activités générales de la gestion des risques identifiées précédemment. Il en résultat que 11 d'entre elles étaient directement reliées à une activité effectuée lors d'une étape du cycle de développement du logiciel. Pour ce qui est des 51 autres activités, leurs interdépendances faisaient en sorte qu'elles pouvaient être intégrées, mais que leur réalisation était fortement liée à celle des 11 activités en question. En somme, les résultats ont démontré qu'il est possible d'accomplir les activités de gestion des risques durant les étapes du cycle de développement du logiciel. Toutefois, certaines d'entre elles représentent des jalons importants pour la réalisation de l'ensemble de ces activités. Sur une vue d'ensemble, il convient donc de dire que si sa réalisation est effectuée à des moments opportuns durant le cycle de développement logiciel, la gestion des risques de sécurité peut contribuer à diminuer la présence de vulnérabilités de sécurité dans les logiciels produits.

Il est important de souligner que les résultats obtenus sont fortement liés aux intrants informationnels utilisés. Donc, les résultats pourraient sensiblement être différents si d'autres intrants étaient employés avec la même démarche que celle utilisée dans la présente recherche. Il faut aussi noter que la tâche de produire la liste des activités générales de la gestion des risques fut difficile, puisqu'il s'agissait de regrouper les résultats de trois méthodes différentes. La tentation de modifier la liste générale pour la bonifier fut présente, mais cette limitation fut respectée. L'objectif était bel et bien de se baser sur les activités proposées dans les méthodes reconnues et une altération aux résultats intermédiaires aurait biaisé l'objectif et le résultat global de la recherche.

En continuité aux travaux réalisés dans le cadre de la recherche présentée dans ce mémoire, il serait intéressant de mettre les résultats obtenus à l'épreuve par une expérimentation réelle dans le cadre d'un projet de développement logiciel. De plus, le défi abordé à l'étape 1 de la démarche analytique, qui consistait à créer une liste d'activités générales de la gestion des risques à partir de méthodes reconnues dans le domaine, constitue à lui seul un sujet qui pourrait être exploré davantage. Dans cette optique, la norme *ISO/CEI 27005* [28] viendrait contribuer à cette exploration, puisqu'elle amène les tous récents travaux du marché effectués dans le domaine de la gestion du risque en matière de sécurité de l'information. Ce mémoire visait à démontrer la pertinence et la possibilité d'utiliser les activités de sécurité, provenant d'une approche par la gestion des risques, dans le domaine du développement logiciel. Avec une expérimentation des résultats et une bonification au niveau des activités de sécurité pour la gestion des risques, la table serait alors mise pour élaborer une méthode de gestion des risques spécifique au domaine de développement logiciel et, surtout, adaptée aux étapes de son cycle. Les activités de sécurité qui découleraient de cette méthode pourraient alors offrir leur plein potentiel.

APPENDICE A

TABLEAU DE COUVERTURE DES ACTIVITÉS DE SÉCURITÉ PROVENANT DES MÉTHODES ÉTUDIÉES

Codes de référence	Activités de sécurité provenant des méthodes étudiées	Activités générales de la gestion des risques
	Méthode EBIOS	
E-1.1.1	Présenter l'organisme	10
E-1.1.2	Lister les contraintes pesant sur l'organisme	11
E-1.1.3	Lister les références réglementaires applicables à l'organisme	12
E-1.1.4	Faire une description fonctionnelle du SI global	13
E-1.2.1	Présenter le système-cible	14
E-1.2.2	Lister les enjeux	15
E-1.2.3	Lister les éléments essentiels	23
E-1.2.4	Faire une description fonctionnelle du système-cible	16
E-1.2.5	Lister les hypothèses	17
E-1.2.6	Lister les règles de sécurité	18
E-1.2.7	Lister les contraintes pesant sur le système-cible	19
E-1.2.8	Lister les références réglementaires spécifiques au système-cible	20
E-1.3.1	Lister et décrire les entités du système	25
E-1.3.2	Croiser les éléments essentiels et les entités	26
E-2.1.1	Choisir les critères de sécurité à prendre en compte	28
E-2.1.2	Déterminer l'échelle de besoins	29
E-2.1.3	Déterminer les impacts pertinents	30
E-2.2.1	Attribuer un besoin de sécurité par critère de sécurité (disponibilité, intégrité, confidentialité…) à chaque élément essentiel	32, 33, 34
E-3.1.1	Lister les méthodes d'attaques pertinentes	39
E-3.1.2	Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter	39
E-3.1.3	Caractériser, pour chaque méthode d'attaque retenue, les éléments menaçants associés par leur type (naturel, humain ou environnemental) et leur cause (accidentelle ou délibérée)	39
E-3.1.4	Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant	39
E-3.1.5	Mettre en évidence les méthodes d'attaque non retenues avec des justifications	39
E-3.2.1	Identifier les vulnérabilités des entités selon les méthodes d'attaque	40
E-3.2.2	Estimer éventuellement le niveau des vulnérabilités	40
E-3.3.1	Formuler explicitement les menaces	43, 44
E-3.3.2	Hiérarchiser éventuellement les menaces selon leur opportunité	45
E-4.1.1	Déterminer les risques en confrontant menaces et besoins de sécurité	46
E-4.1.2	Formuler explicitement les risques	52

E-4.1.3	Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces	47
E-4.1.4	Mettre en évidence les risques non retenus (risques résiduels) avec des justifications	47
E-4.2.1	Lister les objectifs de sécurité	55
E-4.2.2	Justifier la complétude de la couverture, en vérifiant la compatibilité avec les contraintes pesant sur l'organisme et le système-cible : des risques, des hypothèses (et les enjeux) et des règles de sécurité (et les références réglementaires)	56
E-4.2.3	Classer éventuellement les objectifs de sécurité en deux catégories : objectifs de sécurité portant sur le système-cible et objectifs de sécurité portant sur l'environnement du système-cible	55
E-4.2.4	Mettre en évidence les défauts de couverture (risques résiduels) avec des justifications	56
E-4.3.1	Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité	55
E-4.3.2	Choisir le niveau des exigences d'assurance	55
E-5.1.1	Lister les exigences de sécurité fonctionnelles	58
E-5.1.2	Justifier la complétude de la couverture des objectifs de sécurité	59
E-5.1.3	Mettre en évidence les éventuels défauts de couverture (risques résiduels) avec des justifications	59
E-5.1.4	Classer les exigences de sécurité fonctionnelles en deux catégories : exigences de sécurité fonctionnelles portant sur le système-cible et exigences de sécurité fonctionnelles portant sur l'environnement du système-cible	58
E-5.1.5	Justifier éventuellement la couverture des dépendances des exigences de sécurité fonctionnelles	58
E-5.2.1	Lister les exigences de sécurité d'assurance	58
E-5.2.2	Classer éventuellement les exigences de sécurité d'assurance en deux catégories : exigences de sécurité d'assurance portant sur l'environnement du système-cible et exigences de sécurité d'assurances portant sur l'environnement du système-cible	58
E-5.2.3	Justifier éventuellement la couverture des dépendances des exigences de sécurité d'assurance	59
Méthode MEHARI		
M-1.1.1	Identification des activités majeures et de leurs finalités	23, 24
M-1.1.2	Identification des dysfonctionnements redoutés	30
M-1.1.3	Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés	29, 30
M-1.1.4	Échelle de valeurs des dysfonctionnements	31
M-1.2.1	Identification des éléments à classifier	27
M-1.2.2	Critères de classification	28
M-1.2.3	Processus de classification	32
M-1.3.1	Plans d'action basés sur l'analyse des enjeux	*Non applicable*
M-2.1.1	Élaboration du schéma d'audit	35, 36
M-2.1.2	Évaluation des services de sécurité	37
M-2.1.3	Synthèse des vulnérabilités	42
M-2.2.1	Plans d'action basés sur l'audit des vulnérabilités	*Non applicable*
M-3.1.1	Sélection des scénarios critiques devant être pris en compte pour une analyse des risques	46, 47
M-3.2.1	Évaluation de l'exposition naturelle	49

M-3.2.2	Évaluation des facteurs de réduction de risque agissant sur la potentialité à partir d'un audit de sécurité MEHARI	49
M-3.2.3	Évaluation de la potentialité	49
M-3.2.4	Évaluation de l'impact intrinsèque	50
M-3.2.5	Évaluation des facteurs de réduction de risque agissant sur l'impact à partir d'un audit de sécurité MEHARI	50
M-3.2.6	Évaluation de la réduction d'impact	50
M-3.2.7	Évaluation de l'impact	50
M-3.2.8	Évaluation globale du risque	51
M-3.3.1	Plans d'action basés sur l'analyse de risques	55, 58
	Méthode OCTAVE	
O-1.1.1	Obtenir le soutien de la haute direction pour l'étude OCTAVE	1
O-1.1.2	Sélectionner les membres de l'équipe d'analyse	2
O-1.1.3	Former l'équipe d'analyse	3
O-1.1.4	Sélectionner les secteurs opérationnels de l'entreprise qui participeront à l'étude OCTAVE	14
O-1.1.5	Sélectionner les participants	4
O-1.1.6	Coordonner la logistique	6
O-1.1.7	Donner des instructions aux participants	5
O-2.1.1	Identifier et prioriser les actifs utilisés par l'entreprise selon la haute direction	21
O-2.1.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon la haute direction	30
O-2.1.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon la haute direction	32
O-2.1.4	Obtenir la connaissance de la haute direction envers la stratégie de protection actuelle et des vulnérabilités de l'entreprise	37
O-2.1.5	Choisir ou confirmer les secteurs opérationnels visés par l'évaluation ainsi que les directeurs qui participeront à l'étude	7
O-2.2.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les directeurs de secteurs opérationnels	21
O-2.2.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels	30
O-2.2.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les directeurs de secteurs opérationnels	32
O-2.2.4	Obtenir la connaissance des directeurs de secteurs opérationnels envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise	37
O-2.2.5	Choisir ou confirmer les membres du personnel qui participeront à l'étude	7
O-2.2.6	Communiquer les résultats du *Processus 1*	8
O-2.3.1	Identifier et prioriser les actifs utilisés par l'entreprise selon les membres du personnel	21
O-2.3.2	Identifier les préoccupations à l'égard des actifs les plus importants de l'entreprise selon les membres du personnel	30
O-2.3.3	Identifier les exigences de sécurité pour les actifs les plus importants de l'entreprise selon les membres du personnel	32
O-2.3.4	Obtenir la connaissance des membres du personnel envers la stratégie de protection actuelle et des vulnérabilités présentes dans l'entreprise	37

O-2.3.5	Communiquer les résultats des *Processus 1 et 2*	8
O-2.4.1	Regrouper, par groupe consulté, les actifs identifiés	22
O-2.4.2	Regrouper, par groupe consulté et par actif, les exigences de sécurité	33
O-2.4.3	Regrouper, par groupe consulté et par actif, les préoccupations et leurs impacts	31
O-2.4.4	Sélectionner les actifs critiques	23
O-2.4.5	Raffiner les exigences de sécurité à l'égard des actifs critiques	33
O-2.4.6	Identifier les menaces qui pèsent sur les actifs critiques	43
O-2.4.7	Inscrire les préoccupations dans le livrable contenant les profils des actifs	45
O-3.1.1	Identifier les types de composantes	35
O-3.1.2	Identifier les composantes de l'infrastructure à examiner	35
O-3.2.1	Exécuter les outils d'évaluation de vulnérabilités sur les composantes de l'infrastructure sélectionnées	40
O-3.2.2	Réviser les vulnérabilités technologiques et résumer les résultats	41
O-4.1.1	Identifier les impacts des menaces qui pèsent sur les actifs critiques	46
O-4.1.2	Créer les critères d'évaluation du risque	48
O-4.1.3	Évaluer les impacts des menaces qui pèsent sur les actifs critiques	50
O-4.2.1	Compiler les résultats des questionnaires	38
O-4.2.2	Consolider les informations recueillies sur la stratégie de protection	38
O-4.2.3	Réviser les vulnérabilités technologiques, les pratiques de la stratégie de protection, les exigences de sécurité, les vulnérabilités de l'entreprise et les informations concernant les risques	54
O-4.2.4	Créer la stratégie de protection	55
O-4.2.5	Créer les plans de mitigation	58
O-4.2.6	Créer la liste d'actions	58
O-4.2.7	Compiler un résumé des actifs	24
O-4.2.8	Compiler les profils de risques	52
O-4.2.9	Compiler la stratégie de protection de l'entreprise	57
O-4.2.10	Compiler les plans de mitigation	60
O-4.2.11	Compiler la liste d'actions	60
O-4.2.12	Réviser les informations sur les risques	53
O-4.2.13	Réviser et raffiner la stratégie de protection, les plans de mitigation et la liste d'actions	61
O-4.2.14	Créer les prochaines étapes	9
O-4.2.15	Documenter la stratégie de protection, les plans de mitigation des risques, la liste d'actions et les prochaines étapes	62

APPENDICE B

TABLEAUX D'INTÉGRATION DES ACTIVITÉS GÉNÉRALES DE LA GESTION DES RISQUES

Étape ❖ : Organisation de la démarche

1	**Nom :**	**Obtenir un soutien adéquat des parties prenantes du projet**	
	Description :	L'activité consiste à obtenir les appuis nécessaires et visibles de la part des parties prenantes pour la réalisation des activités de sécurité durant la démarche et plus précisément, les aspects suivants : l'encouragement actif, la délégation des responsabilités et des autorités, l'attribution des ressources nécessaires, la participation à la révision des résultats et la prise de décisions sur les actions appropriées.	
	Préalable(s) :	*Aucun*	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 1. Début de la phase	**Au moment où** le projet débute puisqu'il s'agit du tout premier pas à franchir pour débuter à investir du temps et des ressources dans la démarche de sécurité du projet.	AR (a)
	L'initialisation : 7. Fin de la phase L'élaboration : 14. Fin de la phase La construction : 21. Fin de la phase La transition : 27. Fin de la phase	**Au moment où** la phase se termine pour donner l'approbation de la continuité de la démarche de sécurité à la phase suivante (de la transition à l'élaboration, de l'élaboration à la construction et de la construction à la transition) ou pour la fin de la démarche lorsque le projet se termine (phase de transition).	AR (a)
	Le projet entier	**Tout au long** des étapes du projet afin d'être efficace.	AR (a)

2	**Nom :**	**Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information**	
	Description :	L'activité consiste à former une équipe de personnes multidisciplinaires qui participeront activement à la réalisation des activités de sécurité durant la démarche, et ce, sur différents aspects du travail dont la gestion, la communication, l'analyse et l'élaboration des solutions.	
	Préalable(s) :	▪ *Activité n°1* : Obtenir un soutien adéquat des parties prenantes du projet	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'élaboration : 8. Début de la phase	**Au moment où** le projet compose son équipe de réalisation.	AR (a)

3	**Nom :**	**Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir**	
	Description :	L'activité consiste à préparer les membres de l'équipe aux tâches qu'ils devront accomplir en les familiarisant avec le matériel à utiliser et les ateliers à réaliser.	
	Préalable(s) :	▪ *Activité n° 2* : Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'élaboration : 8. Début de la phase	**Suite** à la composition de l'équipe de gestion du risque puisqu'ils seront impliqués dès la phase d'élaboration.	AD (c)

4	**Nom :**	**Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche**	
	Description :	L'activité consiste à identifier les personnes requises pour la réalisation des activités de sécurité et à former des groupes distincts selon leurs responsabilités dans l'entreprise, leurs implications dans la démarche ou toute autre division logique qui permettrait de couvrir tous les besoins nécessaires aux activités de sécurité de la démarche.	
	Préalable(s) :	▪ *Activité n° 1* : Obtenir un soutien adéquat des parties prenantes du projet	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 1. Début de la phase L'élaboration : 8. Début de la phase La construction : 15. Début de la phase La transition : 22. Début de la phase	**Au moment où** la phase débute puisque les personnes sélectionnées (nouvelles lors de la phase d'initialisation, mais nouvelles ou modifiées lors des phases d'élaboration, de construction et de transition) seront amenées à participer dans la démarche de sécurité pour la phase courante.	AR (a)

5	**Nom :**	**Informer les participants sur les activités de sécurité à réaliser durant la démarche**	
	Description :	L'activité consiste à informer chacun des participants, via son groupe respectif, sur le but de la démarche de sécurité et sur le rôle qui lui est demandé d'assumer.	
	Préalable(s) :	▪ *Activité n° 4* : Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 1. Début de la phase L'élaboration : 8. Début de la phase La construction : 15. Début de la phase La transition : 22. Début de la phase	**Suite** à leur sélection puisqu'ils seront amenés à participer dans la démarche de sécurité pour la phase courante.	AD (c)

6	**Nom :**	**Établir la logistique de la démarche**	
	Description :	L'activité consiste à planifier la démarche de sécurité en présentant un calendrier des activités et les éléments nécessaires pour leur réalisation (les ateliers, les personnes impliquées, le matériel, etc.).	
	Préalable(s) :	▪ *Activité n° 3* : Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir ▪ *Activité n° 4* : Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 1. Début de la phase L'élaboration : 8. Début de la phase La construction : 15. Début de la phase La transition : 22. Début de la phase	**Suite** à la préparation de l'équipe de réalisation et à la sélection des participants effectuées au début de la phase, puisqu'il s'agit de planifier les activités de la démarche de sécurité pour la phase courante.	AD (c)
	L'initialisation : 7. Fin de la phase L'élaboration : 14. Fin de la phase La construction : 21. Fin de la phase La transition : 27. Fin de la phase	**Au moment où** l'approbation de passer à la phase suivante est donnée par les parties prenantes, puisqu'il s'agit de débuter la planification de la phase suivante (pour passer en phase d'élaboration, de construction ou de transition) ou bien de planifier les activités qui finalisent la démarche de sécurité du projet (en phase de transition).	AD (c)
	Le projet entier	**Tout au long** des étapes du projet à l'exception des étapes d'examen du plan d'affaires et de l'évaluation des activités du projet qui sont réalisées durant la phase de transition.	AR (a)

7	**Nom :**	**Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche**	
	Description :	L'activité consiste à obtenir une confirmation, avant de débuter les ateliers de groupe, attestant que les participants sélectionnés représentent bien les personnes adéquates dans leur domaine d'expertise au sein de l'entreprise et qu'elles ont le temps nécessaire pour prendre part à la démarche.	
	Préalable(s) :	▪ *Activité n° 5* : Informer les participants sur les activités de sécurité à réaliser durant la démarche	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse La transition : 23. Les cinq disciplines	**Juste avant** de débuter les activités de la démarche de sécurité de la phase courante du projet où les personnes sélectionnées seront amenées à participer.	AR (a)

8	**Nom :**	**Communiquer les résultats obtenus lors des consultations avec les groupes de participants**
	Description :	L'activité consiste à présenter, aux différents groupes de participants, les résultats obtenus lors des consultations avec les autres groupes pour fin de comparaison.
	Préalable(s) :	▪ *Activité n° 22* : Rédiger une liste des actifs identifiés par groupes de participants rencontrés ▪ *Activité n° 31* : Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés ▪ *Activité n° 33* : Rédiger une synthèse des besoins de sécurité pour les actifs critiques ▪ *Activité n° 38* : Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 7. Fin de la phase L'élaboration : 14. Fin de la phase La construction : 21. Fin de la phase La transition : 27. Fin de la phase	**Au moment où** la phase courante se termine, puisque toutes les rencontres auront été effectuées et les résultats prêts à être véhiculés avant que les parties prenantes prennent les décisions quant à la continuité de la démarche de sécurité à la phase suivante (pour passer en phase d'élaboration, de construction ou de transition) ou de la finalité de la démarche de sécurité du projet (en phase de transition).	AR (a)

9	**Nom :**	**Planifier la mise en œuvre des mesures de sécurité proposées par la démarche**
	Description :	L'activité consiste à planifier la mise en œuvre des mesures proposées par la démarche en précisant celles qui seront implantées, par qui et à quel moment.
	Préalable(s) :	▪ *Activité n° 62* : Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition : 23. Les cinq disciplines	**Au moment où** les exigences de sécurité sont formellement documentées et prêtes à être considérées dans la conception des spécifications à implanter pour répondre aux recommandations de sécurité de haut niveau. **Il est à noter** que la réalisation de cette activité doit se dérouler avant la que l'implémentation des solutions débute.	AR (a)

Étape n° 1 : Identification et étude du contexte

10	Nom :	**Décrire l'environnement de la cible**	
	Description :	L'activité consiste à décrire sommairement l'environnement de la cible pour préciser le but, le contexte d'utilisation et son importance dans le système d'information de l'entreprise.	
	Préalable(s) :	▪ *Activité n° 6* : Établir la logistique de la démarche	
	Intégration de l'activité		
	Étapes	*Justifications*	*Ancrage*
	L'initialisation : 2. La spécification des besoins	**Au moment où** il est prévu, dans les activités du projet, de comprendre le contexte du projet.	AR (b)

11	Nom :	**Identifier les contraintes à l'égard de l'environnement de la cible**	
	Description :	L'activité consiste à identifier les contraintes (stratégiques, fonctionnelles, structurelles, politiques, budgétaires, etc.) à l'égard de l'environnement de la cible, puisqu'elles pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique.	
	Prérequis :	▪ *Activité n° 10* : Décrire l'environnement de la cible	
	Intégration de l'activité		
	Étapes	*Justifications*	*Ancrage*
	L'initialisation : 2. La spécification des besoins	**Suite** à la description de l'environnement de la cible.	AD (c)

12	Nom :	**Identifier le cadre légal de l'environnement de la cible**	
	Description :	L'activité consiste à identifier les lois et les règlements auxquels l'environnement de la cible est assujetti, puisqu'ils pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique.	
	Prérequis :	▪ *Activité n° 10* : Décrire l'environnement de la cible	
	Intégration de l'activité		
	Étapes	*Justifications*	*Ancrage*
	L'initialisation : 2. La spécification des besoins	**Suite** à la description de l'environnement de la cible.	AD (c)

13	Nom :	**Décrire l'aspect fonctionnel de l'environnement de la cible**	
	Description :	L'activité consiste à décrire l'aspect fonctionnel de l'environnement de la cible afin de démontrer les domaines fonctionnels qui contribuent à la réalisation des besoins d'affaires, à obtenir une vue d'ensemble de son fonctionnement et de ses interactions avec les autres éléments du système d'information de l'entreprise et, finalement, à comprendre les interactions entre les éléments contenus dans l'environnement lui-même.	
	Prérequis :	▪ *Activité n° 10* : Décrire l'environnement de la cible	
	Intégration de l'activité		
	Étapes	*Justifications*	*Ancrage*
	L'initialisation : 2. La spécification des besoins	**Suite** à la description de l'environnement de la cible.	AD (c)

14	Nom :	**Préciser la cible de la démarche de sécurité**
	Description :	L'activité consiste à préciser la cible à considérer dans la démarche de sécurité en spécifiant sa portée, ses finalités et ses interactions à travers

	l'environnement et le système d'information de l'entreprise (acteurs, domaines fonctionnels, systèmes, etc.).
Préalable(s) :	▪ *Activité n° 11* : Identifier les contraintes à l'égard de l'environnement de la cible ▪ *Activité n° 12* : Identifier le cadre légal de l'environnement de la cible ▪ *Activité n° 13* : Décrire l'aspect fonctionnel de l'environnement de la cible

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Au moment où** l'on traite initialement les besoins du projet (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AR (b)
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Au moment où** l'on raffine, analyse et structure les besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AR (b)

15	**Nom :**	**Identifier les enjeux à l'égard de la cible**
	Description :	L'activité consiste à identifier les gains et les pertes potentiels (financiers, techniques, politiques, etc.) à l'égard de la cible et à démontrer ainsi l'importance de son rôle dans l'environnement et le système d'information de l'entreprise.
	Préalable(s) :	▪ *Activité n° 14* : Préciser la cible de la démarche de sécurité

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Suite** à la précision initiale de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la précision plus détaillée de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

16	**Nom :**	**Décrire l'aspect fonctionnel de la cible**
	Description :	L'activité consiste à décrire l'aspect fonctionnel de la cible pour démontrer les traitements effectués, les intrants et les extrants informationnels, les finalités attendues et les interactions fonctionnelles avec les éléments existants de l'environnement et du système d'information de l'entreprise.
	Préalable(s) :	▪ *Activité n° 14* : Préciser la cible de la démarche de sécurité

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***

L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Suite** à la précision initiale de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la précision plus détaillée de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

17	**Nom :**	**Identifier les hypothèses à l'égard de la cible**	
	Description :	L'activité consiste à identifier les informations prises pour acquises à l'égard de la cible et qui ne seront pas démontrées dans la démarche de sécurité.	
	Préalable(s) :	▪ *Activité n° 14* : Préciser la cible de la démarche de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Suite** à la précision initiale de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la précision plus détaillée de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

18	**Nom :**	**Identifier les règles de sécurité à l'égard de la cible**	
	Description :	L'activité consiste à identifier toutes les règles et les mesures de sécurité (la politique de sécurité, les plans de continuité, etc.) auxquelles la cible est assujettie, puisqu'elles pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique.	
	Préalable(s) :	▪ *Activité n° 14* : Préciser la cible de la démarche de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Suite** à la précision initiale de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction :	**Suite** à la précision plus détaillée de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux	AD (c)

17. L'analyse	restants à traiter à la construction).	

19	**Nom :**	**Identifier les contraintes à l'égard de la cible**	
	Description :	L'activité consiste à identifier les contraintes (financières, techniques, temporelles, de ressources, d'expertise, organisationnelles, etc.) à l'égard de la cible, puisqu'elles pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique.	
	Préalable(s) :	▪ *Activité n° 14* : Préciser la cible de la démarche de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Suite** à la précision initiale de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la précision plus détaillée de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

20	**Nom :**	**Identifier le cadre légal de la cible**	
	Description :	L'activité consiste à identifier les lois et les règlements auxquels la cible est assujettie, puisqu'ils pourraient influencer les décisions quant aux orientations prises en matière de sécurité informatique.	
	Préalable(s) :	▪ *Activité n° 14* : Préciser la cible de la démarche de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 2. La spécification des besoins L'élaboration : 9. La spécification des besoins La construction : 16. La spécification des besoins	**Suite** à la précision initiale de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la précision plus détaillée de la cible de la démarche de sécurité par l'expression des besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

Étape n° 2 : Identification des actifs informationnels

21	**Nom :**	**Rencontrer les groupes de participants pour identifier les actifs importants de la cible**
	Description :	L'activité consiste à rencontrer les groupes de participants afin d'identifier les actifs importants faisant partie de la cible et d'en déterminer le degré

	d'importance relative entre eux.
Préalable(s) :	▪ *Activité n° 7* : Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche ▪ *Phase n° 1* : Identification et étude du contexte

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Au moment où** les besoins à traiter sont suffisamment clairs et détaillés (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction) pour préciser la cible et où chacun des participants est confirmé.	AR (b)

22		
	Nom :	**Rédiger une liste des actifs identifiés par groupes de participants rencontrés**
	Description :	L'activité consiste à lister les actifs importants de la cible, par groupes consultés, et à justifier leur degré d'importance relative.
	Préalable(s) :	▪ *Activité n° 21* : Rencontrer les groupes de participants pour identifier les actifs importants de la cible

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** aux rencontres effectuées avec les groupes de participants pour l'identification des actifs importants liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

23		
	Nom :	**Identifier les actifs critiques de la cible**
	Description :	L'activité consiste à sélectionner, à partir des actifs importants identifiés et leur degré d'importance relative, ceux étant essentiels pour le bon fonctionnement de la cible.
	Préalable(s) :	▪ *Activité n° 22* : Rédiger une liste des actifs identifiés par groupes de participants rencontrés

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la consolidation des informations sur les actifs importants identifiés et liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

24		
	Nom :	**Rédiger une liste intégrée de tous les actifs identifiés**
	Description :	L'activité consiste à lister l'ensemble des actifs importants de la cible et à préciser ceux ayant été jugés critiques, en y ajoutant des détails quant à leur utilisation en général, leurs buts, leurs finalités, etc.
	Préalable(s) :	▪ *Activité n° 23* : Identifier les actifs critiques de la cible

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'identification des actifs importants et ceux jugés critiques qui sont liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

25	**Nom :**	**Identifier les actifs de support aux actifs critiques de la cible**
	Description :	L'activité consiste à identifier les actifs technologiques dont dépendent les actifs critiques de la cible, puisqu'une attaque pourrait en faire l'usage dans le but final d'atteindre un actif critique.
	Préalable(s) :	▪ *Activité n° 24* : Rédiger une liste intégrée de tous les actifs identifiés

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Au moment où** les actifs technologiques, qui seront utilisés pour supporter les actifs et ainsi réaliser la solution, sont identifiés ou changés.	AR (b)

26	**Nom :**	**Documenter les dépendances entre les actifs critiques et les actifs de support**
	Description :	L'activité consiste à schématiser, de manière matricielle, les liens entre les actifs critiques et les actifs de support pour bien démontrer les dépendances existantes.
	Préalable(s) :	▪ *Activité n° 25* : Identifier les actifs de support aux actifs critiques de la cible

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification des actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

Étape n° 3 : Identification et évaluation des besoins de sécurité

27	**Nom :**	**Regrouper les actifs critiques ayant des besoins de sécurité similaires**
	Description :	L'activité consiste à regrouper, au besoin, les actifs critiques qui nécessitent le même degré de protection et pour lesquels l'évaluation pourrait être effectuée qu'une seule fois pour l'ensemble de ces actifs.

Préalable(s) :	▪ *Phase n° 2* : Identification des actifs informationnels	
Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'identification des actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

28	**Nom :**	**Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité**
	Description :	L'activité consiste à déterminer et à décrire les critères de sécurité (disponibilité, intégrité, confidentialité, imputabilité, etc.) qui seront utilisés dans la démarche pour évaluer les besoins de sécurité des actifs critiques de la cible.
	Préalable(s) :	▪ *Activité n° 1* : Obtenir un soutien adéquat des parties prenantes du projet
	Intégration de l'activité	
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 1. Début de la phase	**Au moment où** le projet débute puisqu'ils seront utilisés dès la phase d'initialisation du projet. **Il est à noter** que la réalisation de cette activité n'est pas nécessaire si les critères de sécurité sont récupérés à titre d'intrants au projet.	

29	**Nom :**	**Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité**
	Description :	L'activité consiste à décrire une échelle de valeurs pour chacun des critères de sécurité, en spécifiant ce que chaque valeur signifie dans le contexte du critère en question incluant ses paramètres de seuil, et une échelle de valeurs exprimant des niveaux de gravité d'impact.
	Préalable(s) :	▪ *Activité n° 28* : Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité
	Intégration de l'activité	
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 1. Début de la phase	**Suite** à la détermination des critères de sécurité à considérer pour évaluer les besoins de sécurité. **Il est à noter** que la réalisation de cette activité n'est pas nécessaire si les échelles de valeurs sont récupérées à titre d'intrants au projet.	AD (c)

30	**Nom :**	**Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement**
	Description :	L'activité consiste à rencontrer les groupes de participants afin d'identifier

	les situations représentant une préoccupation pour eux (une menace possible, un dysfonctionnement redouté, un impact significatif, etc.) envers la cible et son environnement, ces mêmes préoccupations pouvant être caractérisées par des informations additionnelles comme une source ou une finalité générant un impact.
Préalable(s) :	▪ *Phase n° 2* : Identification des actifs informationnels

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'identification des actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification des actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

31	**Nom :**	**Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés**
	Description :	L'activité consiste à consolider, par groupe et par actif, les informations recueillies au moment de l'identification des préoccupations et de leurs impacts généraux envers la cible et son environnement par les groupes de participants rencontrés.
	Préalable(s) :	▪ *Activité n° 30* : Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'identification, en groupe, des préoccupations et leurs impacts à l'égard des actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification, en groupe, des préoccupations et leurs impacts à l'égard des actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

32	**Nom :**	**Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques**
	Description :	L'activité consiste à rencontrer les groupes de participants afin d'évaluer les besoins de sécurité des actifs critiques, en effectuant les étapes suivantes pour chacun des actifs : attribuer une valeur pour chacun des critères de sécurité de façon globale ou en fonction de chacun des impacts pertinents, justifier la valeur résultante (la globale ou la plus élevée dans le cas des valeurs multiples) pour chaque critère de sécurité et, finalement, classer les critères en ordre d'importance de criticité selon l'actif en question.
	Préalable(s) :	▪ *Activité n° 27* : Regrouper les actifs critiques ayant des besoins de sécurité similaires ▪ *Activité n° 29* : Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité ▪ *Activité n° 31* : Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'identification des actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction), à leur regroupement en besoins de sécurité similaires, à l'obtention des informations nécessaires pour faire leur évaluation (critères de sécurité, échelles de valeurs et impacts pertinents).	AD (c)

33	**Nom :**	**Rédiger une synthèse des besoins de sécurité pour les actifs critiques**
	Description :	L'activité consiste à consolider, sous différentes formes de présentation et de regroupement, les besoins de sécurité recueillis pour chacun des actifs critiques de la cible et, du même coup, à leur déterminer une valeur finale pour chacun des critères de sécurité et le critère qui s'avère le plus critique.
	Préalable(s) :	▪ *Activité n° 32* : Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques

Intégration de l'activité

Étapes	*Justifications*	*Ancrage*
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'évaluation, en groupe, des besoins de sécurité des actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

34	**Nom :**	**Valider les besoins de sécurité pour les actifs critiques**
	Description :	L'activité consiste à présenter, à modifier au besoin et à obtenir un consensus sur les informations relatives aux besoins de sécurité pour les actifs critiques par les parties prenantes.
	Préalable(s) :	▪ *Activité n° 33* : Rédiger une synthèse des besoins de sécurité pour les actifs critiques

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la consolidation des informations sur les besoins de sécurité des actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

Étape n° 4 : Identification et évaluation des menaces et des vulnérabilités

35	**Nom :**	**Identifier les éléments de la cible à auditer**
	Description :	L'activité consiste à identifier les éléments (actifs critiques ou de support) de la cible ou reliés à celle-ci et sur lesquels un audit de sécurité sera effectué, tout en les regroupant par similarités en termes de besoin de sécurité pour une diminution de la quantité de travail, si cela est souhaité.
	Préalable(s) :	▪ *Phase n° 3* : Identification et évaluation des besoins de sécurité

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la consolidation des informations concernant les préoccupations et de leurs impacts identifiés pour les actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations concernant les préoccupations et de leurs impacts identifiés pour les actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

36	**Nom :**	**Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité**
	Description :	L'activité consiste à sélectionner et à préparer le matériel et les outils nécessaires (questionnaires, logiciels, etc.) pour la réalisation des audits de sécurité à réaliser.
	Préalable(s) :	▪ *Activité n° 35* : Identifier les éléments de la cible à auditer

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'identification des éléments de la cible à auditer concernant les actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification des éléments de la cible à auditer concernant les actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

37	**Nom :**	**Effectuer l'audit de sécurité organisationnelle de la cible**	
	Description :	L'activité consiste à auditer les éléments de type « processus/services » relativement à leur développement et à leur utilisation, et ce, à l'aide de documents sur les bonnes pratiques en la matière, de l'analyse des exploitations possibles par les méthodes d'attaque et des questionnaires d'audit remplis lors de rencontres avec les groupes de participants.	
	Préalable(s) :	▪ *Activité n° 36* : Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la préparation du matériel approprié pour faire les travaux d'audit.	AD (c)

38	**Nom :**	**Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible**	
	Description :	L'activité consiste à consolider et à raffiner au besoin les informations recueillies suite à la réalisation des audits de sécurité organisationnelle réalisés, dont celles par groupes de participants rencontrés.	
	Préalable(s) :	▪ *Activité n° 37*: Effectuer l'audit de sécurité organisationnelle de la cible	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à l'audit de sécurité organisationnelle de la cible concernant les actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)

39	**Nom :**	**Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support**	
	Description :	L'activité consiste à identifier les méthodes d'attaque sur les actifs de support, incluant l'identification et l'évaluation de leurs éléments menaçants, dont leur réalisation est possible et où un impact est prévu, tout en justifiant également celles qui auraient été intentionnellement écartées de la sélection.	
	Préalable(s) :	▪ *Phase n° 2* : Identification des actifs informationnels	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation :	**Suite** à l'identification des actifs de support	AD (c)

4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	(les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	

40	**Nom :**	**Effectuer l'audit de sécurité technique de la cible**	
	Description :	L'activité consiste à auditer les éléments de type « actifs » relativement à leur fonctionnement technologique, et ce, à l'aide des documents de référence en la matière, de logiciels et des gens possédant l'expertise requise pour les utiliser.	
	Préalable(s) :	▪ *Activité n° 36* : Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité ▪ *Activité n° 39* : Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification des méthodes d'attaques et de leurs éléments menaçants, ainsi qu'à la préparation du matériel approprié pour faire les travaux d'audit.	AD (c)

41	**Nom :**	**Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible**	
	Description :	L'activité consiste à consolider, par actifs critiques concernés, les informations recueillies suite à la réalisation des audits de sécurité technique réalisés et à raffiner les résultats au besoin.	
	Préalable(s) :	▪ *Activité n° 40* : Effectuer l'audit de sécurité technique de la cible	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'audit de sécurité technique de la cible concernant les actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

42	**Nom :**	**Documenter les informations sur les vulnérabilités identifiées**
	Description :	L'activité consiste à résumer et à présenter sous différentes formes (par service de sécurité, par thème de sécurité, globalement, etc.) les vulnérabilités identifiées par les audits de sécurité réalisés sur les éléments sélectionnés de la cible ou reliés à celle-ci.
	Préalable(s) :	▪ Activité *n°* 38 : Rédiger une synthèse des résultats de l'audit de sécurité

	organisationnelle de la cible ▪ Activité *n°* 41 : Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 3. L'analyse L'élaboration : 10. L'analyse La construction : 17. L'analyse	**Suite** à la consolidation des informations relatives à l'audit de sécurité organisationnelle de la cible concernant les actifs critiques liés aux besoins à traiter (ceux de base à l'initialisation, ceux ayant de l'impact sur l'architecture à l'élaboration ou ceux restants à traiter à la construction).	AD (c)
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations relatives à l'audit de sécurité technique de la cible concernant les actifs de support (les nouveaux à l'initialisation, les nouveaux ou modifiés à l'élaboration, les nouveaux ou modifiés à la construction et les modifiés à la transition) aux actifs critiques.	AD (c)

43	**Nom :**	**Identifier les menaces à l'égard des actifs critiques de la cible**
	Description :	L'activité consiste à identifier les menaces redoutées pour chacun des actifs critiques de la cible et à les détailler en spécifiant leur type (fonctionnel ou technique), leur portée, l'actif visé, les acteurs impliqués, le motif, les éléments menaçants la méthode d'attaque, les vulnérabilités exploitées, etc.
	Préalable(s) :	▪ *Activité n° 42* : Documenter les informations sur les vulnérabilités identifiées

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations sur les vulnérabilités organisationnelles et techniques identifiées par les activités d'audit de sécurité.	AD (c)

44	**Nom :**	**Évaluer les menaces à l'égard des actifs critiques de la cible**
	Description :	L'activité consiste à quantifier les menaces en leur attribuant une valeur déterminée à l'aide d'une échelle de valeurs, où chaque niveau est clairement défini par les paramètres significatifs et les valeurs de seuil.
	Préalable(s) :	▪ *Activité n° 43* : Identifier les menaces à l'égard des actifs critiques de la cible

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception	**Suite** à l'identification des menaces à l'égard des actifs critiques de la cible.	AD (c)

La construction : 18. La conception La transition 23. Les cinq disciplines		

45	**Nom :**	**Documenter les informations sur les menaces identifiées**
	Description :	L'activité consiste à documenter et à résumer les menaces identifiées pour les actifs critiques de la cible, et ce, en spécifiant les informations qui composent une menace : les méthodes d'attaque, les éléments menaçants, les valeurs obtenues à l'évaluation, la facilité de réalisation, les impacts d'une réalisation, etc.
	Préalable(s) :	▪ *Activité n° 44* : Évaluer les menaces à l'égard des actifs critiques de la cible

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'évaluation des menaces à l'égard des actifs critiques de la cible.	AD (c)

Étape n° 5 : Identification et évaluation des risques

46	**Nom :**	**Identifier les risques potentiels envers la cible**
	Description :	L'activité consiste à identifier les risques potentiels qui pèsent sur les actifs critiques, en établissant plus formellement les impacts qu'aurait la réalisation de chacune des menaces, en confrontant les menaces aux besoins des sécurités des actifs critiques et en consultant des documents de référence en la matière tels que des bases de connaissances de scénarios de risques.
	Préalable(s) :	▪ *Phase n° 3*: Identification et évaluation des besoins de sécurité ▪ *Phase n° 4*: Identification et évaluation des menaces et des vulnérabilités

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations relatives aux besoins de sécurité pour les actifs critiques et aux menaces à leurs égards.	AD (c)

47	**Nom :**	**Sélectionner les risques à considérer dans le cadre d'une analyse de risques**
	Description :	L'activité consiste à sélectionner, dans la liste des risques identifiés, ceux

	affectant le plus considérablement les actifs critiques de la cible et dont une évaluation plus détaillée sera effectuée, tout en justifiant également ceux qui sont écartés de la sélection.
Préalable(s) :	▪ *Activité n° 46* : Identifier les risques potentiels envers la cible

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification des risques potentiels envers les actifs critiques de la cible.	AD (c)

48	**Nom :**	**Définir les facteurs d'évaluation du risque**
	Description :	L'activité consiste à définir les outils nécessaires (les échelles de valeurs appropriées et la grille d'acceptation du risque) pour l'évaluation des risques sélectionnés, et ce, au niveau de leur potentialité, de leur impact, et de manière globale.
	Préalable(s) :	▪ *Activité n° 1* : Obtenir un soutien adéquat des parties prenantes du projet

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 1. Début de la phase	**Au moment où** le projet débute puisqu'ils seront utilisés dès la phase d'initialisation du projet. **Il est à noter** que la réalisation de cette activité n'est pas nécessaire si les outils nécessaires à l'évaluation des risques sont récupérés à titre d'intrants au projet.	

49	**Nom :**	**Évaluer la potentialité des risques**
	Description :	L'activité consiste à déterminer une valeur représentant la potentialité de chacun des risques, à l'aide de l'échelle de valeurs prédéfinie pour ce facteur d'évaluation, en fonction d'une première évaluation indépendante de toute mesure de sécurité et, ensuite, d'un ajustement à la baisse en fonction des mesures dissuasives et de prévention déjà en place pour la cible.
	Préalable(s) :	▪ *Activité n° 47* : Sélectionner les risques à considérer dans le cadre d'une analyse de risques ▪ *Activité n° 48* : Définir les facteurs d'évaluation du risque

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la sélection des risques à traiter et à l'obtention des facteurs d'évaluation du risque en ce qui a trait à la potentialité.	AD (c)

50	**Nom :**	**Évaluer l'impact des risques**
	Description :	L'activité consiste à déterminer une valeur représentant l'impact de chacun des risques, à l'aide de l'échelle de valeurs prédéfinie pour ce facteur d'évaluation, en fonction d'une première évaluation indépendante de toute mesure de sécurité et, ensuite, d'un ajustement à la baisse en fonction des mesures palliatives, de protection et de récupération déjà en place pour la cible.
	Préalable(s) :	▪ *Activité n° 47* : Sélectionner les risques à considérer dans le cadre d'une analyse de risques ▪ *Activité n° 48* : Définir les facteurs d'évaluation du risque

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la sélection des risques à traiter et à l'obtention des facteurs d'évaluation du risque en ce qui a trait à l'impact.	AD (c)

51	**Nom :**	**Évaluer globalement les risques à partir de sa potentialité et de son impact**
	Description :	L'activité consiste à déterminer la valeur globale des risques en utilisant les valeurs obtenues suite à l'évaluation des facteurs de potentialité et d'impact pour le risque en question et en transposant celles-ci dans la grille d'acceptabilité du risque.
	Préalable(s) :	▪ *Activité n° 49* : Évaluer la potentialité des risques ▪ *Activité n° 50* : Évaluer l'impact des risques

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'évaluation de la potentialité et de l'impact de chacun des risques traités à l'égard des actifs critiques de la cible.	AD (c)

52	**Nom :**	**Documenter les risques évalués**
	Description :	L'activité consiste à documenter les risques évalués en spécifiant les informations qui lui sont reliées : la menace (éléments menaçants, méthode d'attaque employée, facilité de réalisation, etc.), les vulnérabilités exploitées, les critères de sécurité affectés, les impacts sur la cible, les actifs concernés (actifs critiques et actifs de support), les valeurs obtenues lors des évaluations, etc.
	Préalable(s) :	▪ *Activité n° 51* : Évaluer globalement les risques à partir de sa potentialité et de son impact

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***

L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'évaluation globale de chacun des risques traités à l'égard des actifs critiques de la cible.	AD (c)

53	**Nom :**	**Valider les risques identifiés pour les actifs critiques avec les parties prenantes**
	Description :	L'activité consiste à présenter, à modifier au besoin et à faire approuver les informations relatives aux risques envers les actifs critiques par les parties prenantes.
	Préalable(s) :	▪ *Activité n° 52* : Documenter les risques évalués

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations relatives aux risques traités à l'égard des actifs critiques de la cible.	AD (c)

Étape n° 6 : Identification des exigences de sécurité

54	**Nom :**	**Réviser toutes les informations recueillies, traitées et produites durant la démarche**
	Description :	L'activité consiste à analyser et à réviser toutes les informations accumulées durant la démarche telles que le contexte de la cible et de son environnement, les actifs identifiés, les besoins de sécurité des actifs critiques, les menaces et les vulnérabilités de sécurité organisationnelle et technique, les risques, etc.
	Préalable(s) :	▪ *Phase n° 5* : Identification et évaluation des risques

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la production de toutes les informations accumulées durant la démarche de sécurité relativement à l'identification de l'environnement et de la cible, des actifs, des besoins de sécurité, des menaces et des risques.	AD (c)

55	**Nom :**	**Déterminer les recommandations sur des exigences de sécurité de haut niveau**

Description :	L'activité consiste à établir des recommandations sur des exigences de sécurité de haut niveau qui peuvent être d'ordre général (stratégique ou opérationnel) en matière de bonnes pratiques ou bien, plus précisément, dans le but de couvrir les risques identifiés durant la démarche, et ce, en spécifiant les informations suivantes : les composantes du risque qui sont ciblées (l'origine de la menace, les vulnérabilités exploitées ou les conséquences de réalisation), la portée visée (la cible ou l'environnement), le niveau de résistance et d'assurance de sécurité souhaité.
Préalable(s) :	▪ *Activité n° 54* : Réviser toutes les informations recueillies, traitées et produites durant la démarche

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la révision de toutes les informations produites durant la démarche de sécurité.	AD (c)

56	**Nom :**	**Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau**
	Description :	L'activité consiste à démontrer les liens entre les recommandations de sécurité de haut niveau établies et les risques qu'ils couvrent, et ce, en indiquant un niveau de couverture (nul, partiel et total) pour chacun des risques et en justifiant tous les cas où le niveau de couverture n'est pas total.
	Préalable(s) :	▪ *Activité n° 55* : Déterminer les recommandations sur des exigences de sécurité de haut niveau

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***
L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à l'identification des risques à traiter à l'égard des actifs critiques de la cible et à la détermination des recommandations de sécurité de haut niveau pour les adresser.	AD (c)

57	**Nom :**	**Résumer les informations sur les recommandations de sécurité de haut niveau**
	Description :	L'activité consiste à résumer les informations sur les recommandations de sécurité de haut niveau de manière concise en vue de les présenter aux parties prenantes et, de plus, à indiquer les recommandations ayant été omises par le fait qu'elles ne sont pas réalisables dans le contexte de la cible ou de son environnement.
	Préalable(s) :	▪ *Activité n° 56* : Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau

Intégration de l'activité		
Étapes	***Justifications***	***Ancrage***

L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la détermination des recommandations de sécurité de haut niveau et à la vérification de leur couverture sur les risques à traiter à l'égard des actifs critiques de la cible.	AD (c)

58	**Nom :**	**Déterminer les exigences de sécurité pour la mitigation des risques**	
	Description :	L'activité consiste à déterminer les exigences de sécurité nécessaires pour mitiger les risques, et ce, en spécifiant les mesures (fonctionnelles ou d'assurance) à réaliser pour satisfaire les recommandations de sécurité de haut niveau, leur portée (la cible ou l'environnement), les dépendances qu'elles pourraient avoir avec une autre mesure et, finalement, s'il s'agit d'une mesure qui pourrait être mise en œuvre immédiatement dû au fait qu'aucun prérequis n'est nécessaire.	
	Préalable(s) :	▪ *Activité n° 57* : Résumer les informations sur les recommandations de sécurité de haut niveau	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations relatives aux recommandations de sécurité de haut niveau.	AD (c)

59	**Nom :**	**Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité**	
	Description :	L'activité consiste à démontrer les liens entre les exigences de sécurité et les recommandations de sécurité de haut niveau qu'ils couvrent, et ce, en attribuant un niveau de couverture (nul, partiel et total) pour chacune des recommandations, en justifiant tous les cas où le niveau de couverture n'est pas total, en vérifiant si toutes les exigences de sécurité sont reliées à au moins une recommandation de sécurité de haut niveau et, finalement, en vérifiant les dépendances possibles entre les exigences proposées.	
	Préalable(s) :	▪ *Activité n° 58* : Déterminer les exigences de sécurité pour la mitigation des risques	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la détermination des recommandations de sécurité de haut niveau et à la détermination des exigences de sécurité pour les adresser.	AD (c)

60	**Nom :**	**Résumer les informations sur les exigences de sécurité**	
	Description :	L'activité consiste à résumer les informations sur les exigences de sécurité de manière concise en vue de les présenter aux parties prenantes.	
	Préalable(s) :	▪ *Activité n° 59* : Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la détermination des exigences de sécurité et à la vérification de leur couverture sur les recommandations de sécurité de haut niveau.	AD (c)

61	**Nom :**	**Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes**	
	Description :	L'activité consiste à présenter, à modifier au besoin et à faire approuver les informations relatives aux recommandations de sécurité de haut niveau et aux exigences de sécurité par les parties prenantes.	
	Préalable(s) :	▪ Activité *n°* 60 : Résumer les informations sur les exigences de sécurité	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la consolidation des informations relatives aux recommandations de sécurité de haut niveau et aux exigences de sécurité qui en ont découlé.	AD (c)

62	**Nom :**	***Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité***	
	Description :	L'activité consiste à documenter formellement les informations relatives aux recommandations de sécurité de haut niveau et aux exigences de sécurité qui ont été établies avec les parties prenantes et à les transmettre aux personnes concernées dans l'entreprise.	
	Préalable(s) :	▪ *Activité n° 61* : Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes	
	Intégration de l'activité		
	Étapes	***Justifications***	***Ancrage***
	L'initialisation : 4. La conception L'élaboration : 11. La conception La construction : 18. La conception La transition 23. Les cinq disciplines	**Suite** à la validation des informations relatives aux recommandations de sécurité de haut niveau et aux exigences de sécurité qui en ont découlé.	AD (c)

APPENDICE C

TABLEAU DÉTAILLÉ DES RÉSULTATS DE L'INTÉGRATION DES ACTIVITÉS GÉNÉRALES DE LA GESTION DES RISQUES

		L'initialisalon							L'élaboration							La construction							La transition					
N°	Activités générales de la gestion des risques	Début de la phase	La spécification des besoins	L'analyse	La conception	L'implémentation	Les tests	Fin de la phase	Début de la phase	La spécification des besoins	L'analyse	La conception	L'implémentation	Les tests	Fin de la phase	Début de la phase	La spécification des besoins	L'analyse	La conception	L'implémentation	Les tests	Fin de la phase	Début de la phase	5 disciplines	Planification des itérations	Examen du plan d'affaires	Évaluation des activités du projet	Fin de la phase
1	Obtenir un soutien adéquat des parties prenantes du projet	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
2	Sélectionner les personnes qui feront partie de l'équipe de gestion du risque en sécurité de l'information								■																			
3	Former l'équipe de gestion du risque en sécurité de l'information aux tâches à accomplir								■																			
4	Sélectionner les personnes qui participeront à la réalisation des activités de sécurité de la démarche	■							■							■							■					
5	Informer les participants sur les activités de sécurité à réaliser durant la démarche	■							■							■							■					
6	Établir la logistique de la démarche	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■
7	Confirmer la sélection des participants avant de débuter les activités de sécurité de la démarche			■							■							■						■				
8	Communiquer les résultats obtenus lors des consultations avec les groupes de participants							■							■							■						■
9	Planifier la mise en œuvre des mesures de sécurité proposées par la démarche				■							■							■					■				
10	Décrire l'environnement de la cible		■																									
11	Identifier les contraintes à l'égard de l'environnement de la cible		■																									
12	Identifier le cadre légal de l'environnement de la cible		■																									
13	Décrire l'aspect fonctionnel de l'environnement de la cible		■																									
14	Préciser la cible de la démarche de sécurité		■	■						■	■						■	■										
15	Identifier les enjeux à l'égard de la cible		■	■						■	■						■	■										
16	Décrire l'aspect fonctionnel de la cible		■	■						■	■						■	■										
17	Identifier les hypothèses à l'égard de la cible		■	■						■	■						■	■										
18	Identifier les règles de sécurité à l'égard de la cible		■	■						■	■						■	■										
19	Identifier les contraintes à l'égard de la cible		■	■						■	■						■	■										
20	Identifier le cadre légal de la cible		■	■						■	■						■	■										
21	Rencontrer les groupes de participants pour identifier les actifs importants de la cible			■							■							■										
22	Rédiger une liste des actifs identifiés par groupes de participants rencontrés			■							■							■										
23	Identifier les actifs critiques de la cible			■							■							■										
24	Rédiger une liste intégrée de tous les actifs identifiés			■							■							■										
25	Identifier les actifs de support aux actifs critiques de la cible				■							■							■					■				
26	Documenter les dépendances entre les actifs critiques et les actifs de support				■							■							■					■				
27	Regrouper les actifs critiques ayant des besoins de sécurité similaires			■							■							■										
28	Déterminer les critères de sécurité à considérer pour évaluer les besoins de sécurité	■																										
29	Décrire les échelles de valeurs reliées aux critères de sécurité et aux niveaux de gravité	■																										
30	Rencontrer les groupes de participants pour identifier les préoccupations et évaluer leurs impacts à l'égard de la cible (actifs critiques et de support) et son environnement			■	■						■	■						■	■					■				
31	Rédiger une synthèse des préoccupations et de leurs impacts identifiés pour la cible (actifs critiques et de support) et de son environnement par groupes de participants rencontrés			■	■						■	■						■	■					■				

		L'initialisaion							L'élaboration							La construction							La transition					
N°	Activités générales de la gestion des risques	Début de la phase	La spécification des besoins	L'analyse	La conception	L'implémentation	Les tests	Fin de la phase	Début de la phase	La spécification des besoins	L'analyse	La conception	L'implémentation	Les tests	Fin de la phase	Début de la phase	La spécification des besoins	L'analyse	La conception	L'implémentation	Les tests	Fin de la phase	Début de la phase	5 disciplines	Planification des itérations	Examen du plan d'affaires	Évaluation des activités du projet	Fin de la phase
32	Rencontrer les groupes de participants pour évaluer les besoins de sécurité des actifs critiques																											
33	Rédiger une synthèse des besoins de sécurité pour les actifs critiques																											
34	Valider les besoins de sécurité pour les actifs critiques																											
35	Identifier les éléments de la cible à auditer																											
36	Préparer le matériel et les outils nécessaires pour réaliser les audits de sécurité																											
37	Effectuer l'audit de sécurité organisationnelle de la cible																											
38	Rédiger une synthèse des résultats de l'audit de sécurité organisationnelle de la cible																											
39	Identifier les méthodes d'attaque pertinentes et leurs éléments menaçant à l'égard des actifs de support																											
40	Effectuer l'audit de sécurité technique de la cible																											
41	Rédiger une synthèse des résultats de l'audit de sécurité technique de la cible																											
42	Documenter les informations sur les vulnérabilités identifiées																											
43	Identifier les menaces à l'égard des actifs critiques de la cible																											
44	Évaluer les menaces à l'égard des actifs critiques de la cible																											
45	Documenter les informations sur les menaces identifiées																											
46	Identifier les risques potentiels envers la cible																											
47	Sélectionner les risques à considérer dans le cadre d'une analyse de risques																											
48	Définir les facteurs d'évaluation du risque																											
49	Évaluer la potentialité des risques																											
50	Évaluer l'impact des risques																											
51	Évaluer globalement les risques à partir de sa potentialité et de son impact																											
52	Documenter les risques évalués																											
53	Valider les risques identifiés pour les actifs critiques avec les parties prenantes																											
54	Réviser toutes les informations recueillies, traitées et produites durant la démarche																											
55	Déterminer les recommandations sur des exigences de sécurité de haut niveau																											
56	Vérifier la couverture des risques identifiés par les recommandations de sécurité de haut niveau																											
57	Résumer les informations sur les recommandations de sécurité de haut niveau																											
58	Déterminer les exigences de sécurité pour la mitigation des risques																											
59	Vérifier la couverture des recommandations de sécurité de haut niveau par les exigences de sécurité																											
60	Résumer les informations sur les exigences de sécurité																											
61	Valider les recommandations de sécurité de haut niveau et les exigences de sécurité avec les parties prenantes																											
62	Documenter formellement les recommandations de sécurité de haut niveau et les exigences de sécurité																											

Réalisation d'une activité générale
Réalisation d'une activité générale en continu
Aucune activité générale à réaliser

LEXIQUE

Actif informationnel. Inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles d'une entreprise ou d'une organisation, à l'exception des ressources humaines.

Analyse de risque. Activité constituant une étape de l'analyse de sécurité informatique, et qui consiste à identifier tous les risques informatiques auxquels est exposé l'actif informationnel de l'organisation, à les quantifier et à en déterminer l'importance relative.

Audit informatique. Audit qui permet une analyse de façon exhaustive et globale du fonctionnement d'un centre ou d'un service informatique, afin de mesurer l'adéquation entre les ressources matérielles et humaines mises en œuvre, les besoins de l'entreprise, les objectifs recherchés et les résultats attendus.

Base de connaissances. Élément d'un système expert contenant des informations représentant les connaissances acquises dans un domaine particulier.

Besoin d'affaires. Besoin ressenti dans une entreprise ou une organisation et qui implique le développement de ses processus d'affaires, de manière à améliorer sa situation ou à faciliter la conduite de sa mission.

Cas d'utilisation. Outil utilisé en développement de logiciels, permettant de décrire une utilisation possible d'un logiciel.

Cycle de développement du logiciel. Ensemble d'activités mises en œuvre dans un ordre donné pour réaliser un logiciel.

Composant logiciel. Logiciel, programme ou élément d'un logiciel ou d'un programme qui constitue un module indépendant utilisé comme élément d'un système plus complexe et qui est spécialement conçu pour fonctionner sans problèmes avec d'autres logiciels ou programmes.

Gestion des risques. Ensemble des activités qui consistent à recenser les risques auxquels l'entité est exposée, puis à définir et à mettre en place les mesures préventives appropriées en vue de supprimer ou d'atténuer les conséquences d'un risque couru.

Interface utilisateur. Ensemble des outils développés et mis à la disposition de l'utilisateur pour dialoguer avec l'ordinateur.

Impact. Effet ou conséquence d'un événement sur le projet, sur l'actif informationnel ou sur l'environnement, et qui peut influer sur l'atteinte des objectifs de l'organisation.

Logiciel. Ensemble des programmes destinés à effectuer un traitement particulier sur un ordinateur.

Maîtrise des risques. Activité par laquelle, à la suite d'une analyse des risques informatiques, une entreprise ou une organisation prend en charge certains risques acceptables et décide de confier la gestion des autres risques à des sociétés extérieures spécialisées.

Menace informatique. Événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique.

Mesure de sécurité. Moyen concret qui assure, partiellement ou totalement, la protection de l'actif informationnel contre une ou plusieurs menaces informatiques, et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces menaces ou à minimiser les pertes qui en résultent.

Potentialité. Caractère de ce qui peut être développé.

Processus d'affaires. Suite cohérente d'activités et d'opérations commerciales qu'une entreprise ou une organisation entretient avec des tiers, traduisant les besoins de ses clients et les exigences de son environnement, et tenant compte ou non de ses activités internes, de manière à les agencer selon une logique de création de valeur.

Risque informatique. Probabilité plus ou moins grande de voir une menace informatique se transformer en événement réel entraînant une perte.

Risque résiduel. Portion du risque informatique qui demeure, une fois que les mesures de sécurité informatiques visant à le réduire ont été mises en application.

Sécurité informatique. Ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service.

Spécification logicielle. Caractéristiques que comporte la composante logicielle d'un système informatique.

Système d'information. Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation.

Système informatique. Ensemble des éléments matériels (l'ordinateur et ses périphériques) et logiciels nécessaires au traitement des données.

Vulnérabilité. Faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent.

Source : *Office québécois de la langue française – Le grand dictionnaire terminologique*

http://www.oqlf.gouv.qc.ca/ressources/gdt.html

RÉFÉRENCES

1. Open Web Application Security Project (OWASP), OWASP CLASP Project, version 1.2 http://www.owasp.org/index.php/Category:OWASP_CLASP_Project.

2. Grance, Tim, Joan Hash et Marc Stevens, Security Considerations in the Information System Development Life Cycle, National Institute of Standards and Technology (NIST), Special Publication 800-64, 2003.

3. MSDN - Security Developer Center, The Microsoft Security Development Lifecycle (SDL), Microsoft Corporation, 2009, http://msdn.microsoft.com/en-us/security/cc448177.aspx

4. Department of Homeland Security (DHS), SECURITY IN THE SOFTWARE LIFECYCLE, Making Software Development Processes – and Software Produced by Them, More Secure, Draft Version 1.2, 2006.

5. Over, James W., Team Software Process for Secure Systems Development, Carnegie Mellon University, Version 1.0, 2003, http://www.sei.cmu.edu/tsp/publications/tsp-secure.pdf

6. ISO/CEI 27002:2005, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information, 2005.

7. Mayer, Nicolas, et Jean-Philippe Humbert, La gestion des risques pour les systèmes d'information, 2006, magasine MISC no 24, ISSN : 1631-9036.

8. European Network and Information Security Agency (ENISA), Inventory of risk assessment and risk management methods, Version 1.0, 2006.

9. Cordoue, Elian, 70 % des risques de sécurité relèvent de la couche applicative, LeMondeInformatiquer, 2006, http://www.lemondeinformatique.fr/actualites/lire-70-des-risques-de-securite-relevent-de-la-couche-applicative-18650.html

10. Mullaney, Jennette, SDLC lacks application security practices, SearchSoftwareQuality.com, 2006, http://searchsoftwarequality.techtarget.com/news/article/0,289142,sid92_gci1230072,00.html

11. Kramkow, Leif, Proplème ou pas ? 2008 : Les vulnérabilités des applications Web atteignent un point d'inflexion, Mag Securs, 2009, http://www.mag-securs.com/spip.php?article12905

12. Ashbaugh, Douglas A., Assessing Information Security Risks in the Software Development Life Cycle, CrossTalk – The Journal of Defense Software Engineering, 2006, http://www.stsc.hill.af.mil/crosstalk/2006/09/0609Ashbaugh.html

13. Stonebumer, Gary, Alice Goguen et Alexis Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology (NIST), Special Publication 800-30, 2002.

14. MSDN – Microsoft patterns & practices Developer Center, Chapter 2 – Threats and Countermeasures , Microsoft Corporation, 2009, http://msdn.microsoft.com/en-us/library/aa302418.aspx

15. MSDN – Microsoft patterns & practices Developer Center, Chapter 3 – Threat Modeling, Microsoft Corporation, 2009, http://msdn.microsoft.com/en-us/library/aa302419.aspx

16. Verdon, Denis, Gary McGraw, Risk Analysis in Software Design, Building Securiy In, 2004, https://buildsecurityin.us-cert.gov/daisy/bsi/123-BSI/version/5/part/4/data/bsi3-risk.pdf?branch=main&language=default

17. Wikipedia, Unified Process, http://en.wikipedia.org/wiki/Unified_Process

18. Direction centrale de la sécurité des systèmes d'information (DCSSI), EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité, http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html

19. POGGI, Sébastien, Rapport de veille sur les standards et méthodes en matière de sécurité informatique, CASES Luxembourg, Portail de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, 2005, http://www.cases.public.lu/fr/publications/recherche/r2sic/wp11_1.pdf

20. Cyberworld Awareness Security Enhancement Structure (CASES) Luxembourg, L'analyse des risques, Portail de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, http://www.cases.public.lu/fr/theorie/analyse_des_risques/index.html

21. Léger, Marc-André, Une grille d'évaluation des méthodologies d'analyse de risque, Université de Sherbrooke, 2006.

22. POGGI, Sébastien, Étude comparée de référentiels et méthodes utilisées en sécurité informatique, CASES Luxembourg, Portail de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, 2005, http://www.cases.public.lu/fr/publications/recherche/r2sic/wp11_2.pdf

23. Club de la Sécurité de l'information Français (CLUSIF), Présentation de MEHARI, https://www.clusif.asso.fr/fr/production/mehari/

24. Carnegie Mellon University's Computer Emergency Response Team (CERT), OCTAVE, http://www.cert.org/octave/

25. Vidalis, Stilianos, A Critical Discussion of Risk and Threat Analysis – Methods and Methodologies, School of Computing, University of Glamorgan, Technical Report CS-04-03, 2004, http://www.glam.ac.uk/socschool/research/publications/technical/CS-04-03.pdf

26. Jacobson, Ivar, Grady Booch et James Rumbaugh, The Unified Software Development Process, 1st edition, Rational Software Corporation, Addison-Wesley, 1999, ISBN: 0201571692.

27. Larman, Craig, UML et les Design Patterns, 2e édition, CampusPress, 2003, ISBN : 2744016233.

28. ISO/CEI 27005:2008, Technologies de l'information – Techniques de sécurité – Gestion du risque en sécurité de l'information, 2008.

BIBLIOGRAPHIE

Alberts, Christopher, Audrey Dorofee, James Stevens et Carol Woody, Introduction to the OCTAVE Approach, Carnegie Mellon – Software Engineering Institute, 2003.

Ashbaugh, Douglas A., Assessing Information Security Risks in the Software Development Life Cycle, CrossTalk – The Journal of Defense Software Engineering, 2006, http://www.stsc.hill.af.mil/crosstalk/2006/09/0609Ashbaugh.html

Carnegie Mellon University's Computer Emergency Response Team (CERT), OCTAVE, http://www.cert.org/octave/

Club de la Sécurité de l'information Français (CLUSIF), Présentation de MEHARI, https://www.clusif.asso.fr/fr/production/mehari/

Club informatique des grandes entreprises françaises, Sécurité des systèmes d'information (CIGREF) – Quelle politique globale de gestion des risques?, 2002.

Comment ça marche.net, Cycle de vie d'un logiciel, http://www.commentcamarche.net/contents/genie-logiciel/cycle-de-vie.php3

Cyberworld Awareness Security Enhancement Structure (CASES) Luxembourg, Portail de la sécurité de l'information, http://www.cases.public.lu/fr/index.html

Department of Homeland Security (DHS), SECURITY IN THE SOFTWARE LIFECYCLE, Making Software Development Processes – and Software Produced by Them, More Secure, Draft Version 1.2, 2006.

Direction centrale de la sécurité des systèmes d'information (DCSSI), EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité, http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html

European Network and Information Security Agency (ENISA), Inventory of risk assessment and risk management methods, Version 1.0, 2006.

Etiévant, Hugo, Norme de sécurité : les méthodes d'analyse des risques, Developpez.com, 2006, http://cyberzoide.developpez.com/securite/methodes-analyse-risques/

Grance, Tim, Joan Hash et Marc Stevens, Security Considerations in the Information System Development Life Cycle, National Institute of Standards and Technology (NIST), Special Publication 800-64, 2003.

Information Systems Security Association (ISSA) – France, Quelle méthode d'analyse de risques ? – Panorama des solutions et méthodes, Conférence annuelle 7799, 24 mai 2005.

ISIQ, Pour la sécurité de l'information, https://www.isiq.ca/accueil.html

ISO/CEI 27002:2005, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information, 2005.

ISO/CEI 27005:2008, Technologies de l'information – Techniques de sécurité – Gestion du risque en sécurité de l'information, 2008.

Jacobson, Ivar, Grady Booch et James Rumbaugh, The Unified Software Development Process, 1st edition, Rational Software Corporation, Addison-Wesley, 1999, ISBN: 0201571692.

Jarzombek, Joe, Karen Mercedes Goertzel, Security in the Software Life Cycle, CrossTalk – The Journal of Defense Software Engineering, 2006, http://www.stsc.hill.af.mil/Crosstalk/2006/09/0609JarzombekGoertzel.html

Lachapelle, Éric, Pierre Corbel, Méhari – Méthode Harmonisée d'Analyse des Risques, VERIDON.

Lachapelle, Éric, René St-Germain, OCTAVE – Évaluation des menaces critique, ressources et vulnérabilités, VERIDON.

Larman, Craig, UML et les Design Patterns, 2e édition, CampusPress, 2003, ISBN : 2744016233.

Léger, Marc-André, Une grille d'évaluation des méthodologies d'analyse de risque, Université de Sherbrooke, 2006.

Mayer, Nicolas, et Jean-Philippe Humbert, La gestion des risques pour les systèmes d'information, 2006, magasine MISC no 24, ISSN : 1631-9036.

MSDN – Microsoft patterns & practices Developer Center, Improving Web Application Security: Threats and Countermeasures, Microsoft Corporation, 2009, http://msdn.microsoft.com/en-us/library/ms994921.aspx

MSDN - Security Developer Center, The Microsoft Security Development Lifecycle (SDL), Microsoft Corporation, 2009, http://msdn.microsoft.com/en-us/security/cc448177.aspx

Open Web Application Security Project (OWASP), OWASP CLASP Project, version 1.2 http://www.owasp.org/index.php/Category:OWASP_CLASP_Project.

Over, James W., Team Software Process for Secure Systems Development, Carnegie Mellon University, Version 1.0, 2003, http://www.sei.cmu.edu/tsp/publications/tsp-secure.pdf

POGGI, Sébastien, Étude comparée de référentiels et méthodes utilisées en sécurité informatique, CASES Luxembourg, Portail de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, 2005.

POGGI, Sébastien, Rapport de veille sur les standards et méthodes en matière de sécurité informatique, CASES Luxembourg, Portail de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, 2005.

Stonebumer, Gary, Alice Goguen et Alexis Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology (NIST), Special Publication 800-30, 2002.

Verdon, Denis, Gary McGraw, Risk Analysis in Software Design, Building Security In, 2004, https://buildsecurityin.us-cert.gov/daisy/bsi/123-BSI/version/5/part/4/data/bsi3risk.pdf

Vidalis, Stilianos, A Critical Discussion of Risk and Threat Analysis – Methods and Methodologies, School of Computing, University of Glamorgan, Technical Report CS-04-03, 2004.

Wikipedia, Cycle de développement, http://fr.wikipedia.org/wiki/Cycle_de_développement

Wikipedia, Sécurité du système d'information, http://fr.wikipedia.org/wiki/Sécurité_informatique

Wikipedia, Unified Process, http://en.wikipedia.org/wiki/Unified_Process

Ysosecure, Gestion des risques informatiques et management de la sécurité de l'information, http://www.ysosecure.com/