MASTER EN SCIENCES INFORMATIQUES

Conception et développement d'un outil méthodologique d'évaluation autonome de maturité en termes de sécurité de l'information dans les PME

Beaufay, Tancred

Award date:
2015

Awarding institution:
Universite de Namur

Université de Namur
Faculté d'informatique
Année académique 2014-2015

Conception et développement d'un outil méthodologique d'évaluation autonome de la maturité en termes de sécurité de l'information dans les PME

Tancred Beaufay

Maître de stage : Jean-Noël Colin

Promoteur : _____ (Signature pour approbation du dépôt - REE art. 40)
Jean-Noël Colin

Mémoire présenté en vue de l'obtention du grade de
Master en Sciences Informatiques.

Résumé

Le but de ce mémoire est de mettre en place une méthodologie, supportée par un outil d'automatisation, permettant de réaliser une évaluation autonome du niveau de maturité en termes de sécurité de l'information dans les petites et moyennes entreprises. La méthodologie prend la forme d'un questionnaire Excel stand-alone qui affiche les question dynamiquement.

La méthodologie aura une vocation didactique en permettant à un utilisateur novice, au travers de questions facilement compréhensibles dont la lecture suffit à faire comprendre les idées véhiculées, d'identifier ses besoins de sécurité et d'évaluer le niveau de risque en termes de sécurité de l'information auquel son entreprise s'expose. Par ailleurs, ces niveaux de risque seront disponibles sous une forme facilement compréhensible.

Cette méthodologie se déroule en deux phases : la première propose des questions organisées en sections, avec une liste de réponses prédéfinies pour chaque question, et la seconde utilise les informations fournies par l'utilisateur afin de réaliser un calcul des scores qui, sous forme de graphiques, illustreront le niveau de risque d'une entreprise.

La structure de ce document suivra les phases décrites dans ce résumé, toutefois, trois chapitres viendront s'y ajouter. Le premier, abordant la modélisation de la méthodologie, se situera au tout début, tandis que les deux autres, présentant respectivement la validation de la méthodologie et plusieurs pistes d'amélioration à considérer pour des travaux ultérieurs, viendront s'ajouter à la fin du document.

Mots-clés: méthodologie, évaluation, besoins, sécurité, risque.

Abstract

The goal of this thesis is to set-up a methodology, supported by an automating tool, allowing to realise an autonomous level of risk evaluation in terms of information security for small and medium-sized companies. The methodology takes the shape of a stand-alone Excel questionnaire that displays questions in a dynamic fashion.

The methodology will have a didactic vocation allowing a novice user, by means of easily comprehensible questions the reading of which suffices to understand their underlying ideas, to identify his security needs and to evaluate the level of risk his company exposes itself to. In addition these levels of risk will be available under an easily understandable form.

This methodology follows two steps : the first provides questions organised in sections, with a list of predetermined answers for each question, and the second uses that data to compute scores which will illustrate the level of risk of a company through charts.

The structure of this document follows the steps described in this resume, however, three chapters will be added. The first, approaching the modeling of the methodology, will be located in the beginning, whereas the other two, respectively presenting the validation of the methodology and several improvements to be considered for future works, will be added at the end of the document.

Keywords: methodology, evaluation, needs, security, risk.

Avant-propos

Je souhaite remercier Monsieur Jean-Noël Colin, mon promoteur et maître de stage, pour son accompagnement soutenu tout au long de ce travail. Son aide a été abondante et précieuse, dans les bons comme dans les mauvais moments.

Je tiens également à remercier Monsieur Gautier Dallons et le CETIC, le Centre d'Excellence en Technologies de l'Information et de la Communication, qui ont soutenu ce projet et m'ont apporté la motivation nécessaire au cours de sa réalisation.

Par ailleurs, je voudrais aussi remercier les entreprises wallonnes, qui m'ont autorisé à les interviewer ainsi qu'à tester cette méthodologie en leur sein, pour leur intérêt et leur disponibilité.

Finalement, je voudrais adresser une merci tout particulier à mes parents et à Monsieur Cédric de Quirini, pour leur soutien et leur aide, mais surtout pour leurs nombreuses relectures, ainsi qu'à ma grand-mère pour son soutien tout au long de l'année.

Table des matières

Table des figures

Liste des tableaux

Introduction

De nos jours, l'informatique a une place de plus en plus importante dans les entreprises, indépendamment de leur secteur d'activité. Or, bien que sa démocratisation soit très rapide et amène beaucoup d'avantages au niveau de la compétitivité de ces sociétés, l'informatique possède un bagage conséquent de dangers, au niveau de la sécurité de l'information, dont les enjeux sont aussi divers qu'important.

Les systèmes d'informations contiennent, communiquent et traitent des données souvent vitales au fonctionnement des entreprises, sans pour autant que ces dernières ne soient toujours conscientes de leur importance, ou encore du risque auquel elles font face. Et, même s'il existe des méthodes et des standards abordant cette thématique, ils sont de loin trop complexes pour être utilisés facilement et efficacement dans le but de produire des résultats accessibles. Ainsi, il est nécessaire d'aider ces organisations mieux comprendre ces dangers et comment les appréhender.

Dans cette optique, ce mémoire propose une méthodologie d'évaluation autonome de la maturité en termes de sécurité de l'information dans une organisation au travers d'un questionnaire dynamique supporté par un outil. La démarche se veut simple, autoportante et didactique, afin de guider les utilisateurs et de les aider à se familiariser avec le domaine de la sécurité, au fur et à mesure de ses étapes. A cet effet, elle présente des questions formulées aussi simplement que possible, illustrées par des exemples et proposant chacune une liste finie de propositions de réponses, dont certaines permettent de débloquer d'autres questions afin d'approfondir une évaluation.

Ce document est divisé en plusieurs chapitres et chacun représente une étape du travail réalisé dans le cadre de ce mémoire.

Tout d'abord, nous commencerons avec la présentation, dans le chapitre 1, des concepts qui ont été étudiés pour la réalisation de ce travail.

Ensuite, nous continuerons avec le chapitre 2 dans lequel la structure et le déroulement de la méthodologie seront expliqués au travers de diagrammes dont la construction sera aussi présentée.

Dans le chapitre 3, nous aborderons la conception du contenu de la méthodologie : questions, réponses, liens et échelles de valeurs des ensembles de réponses, mais aussi les démarches employées pour réaliser ces tâches.

Par la suite, nous montrerons dans le chapitre 4 les différentes formules utilisées afin de calculer les résultats d'une évaluation selon cette méthodologie et de définir des intervalles d'inacceptabilité de ces résultats.

Le chapitre 5 présentera l'étape de validation de cette méthodologie, la démarche suivie et les résultats obtenus.

Nous finirons avec le chapitre 6, qui aborde les limites de cette proposition de solution, mais aussi les pistes d'amélioration permettant d'y remédier.

Ces différents chapitres illustrent les étapes suivies au cours de ce travail, de sa conception, au regard critique posé sur les résultats des tests.

Chapitre 1

Contexte

Dans ce chapitre, nous allons présenter le contexte de ce mémoire ainsi que les éléments ciblés dans la recherche de solution à la problématique qu'il pose.

Pour commencer, nous présenterons l'état actuel de la sécurité de l'information dans les petites et moyennes entreprises afin d'illustrer la problématique de ce mémoire et de motiver le besoin d'une proposition de solution.

Ensuite, nous parlerons des standards de la sécurité de l'information, notamment ceux de la famille ISO/IEC 2700x, car il s'agit d'un point d'entrée intéressant au domaine de la sécurité de l'information, dont il donne entre autres la définition, ainsi que celle du risque.

De plus, nous présenterons des méthodes d'analyse de risque car il s'agit d'une approche pertinente à la mise en évidence du risque qui permettra d'évaluer la maturité en termes de sécurité de l'information. Ainsi, il convient de prendre connaissance de celles qui existent déjà, mais aussi de leur fonctionnement dans le but de développer une approche cohérente et correcte qui permette notamment de comprendre le risque, d'où il provient et sa dangerosité.

Par après, nous aborderons la conception de questionnaires car la méthodologie prendra cette forme. Ainsi, il est important de nous intéresser aux tenants et aux aboutissants de ce concept afin de produire un questionnaire de qualité, cohérent et dont l'utilisation permet de réaliser une évaluation de la maturité en termes de sécurité de l'information. La création du questionnaire devra évidemment tenir compte des concepts de l'analyse de risque.

En outre, nous parlerons du sujet des métriques car la méthodologie doit calculer des scores. Or, pour réaliser cette tâche il est nécessaire de se familiariser avec le concept des mesures et de leur mise en place afin de pouvoir quantifier les réponses aux questions du questionnaire méthodologique, développer des formules et utiliser tous ces éléments afin de calculer des scores de résultats.

Par la suite, nous aborderons les modèles de maturité car il s'agit d'une mé-

thodologie d'évaluation de la maturité en termes de sécurité de l'information. De ce fait, il convient de comprendre ce concept afin de pouvoir l'appliquer à la proposition de solution. Cette section présente notamment une liste de modèles de maturité existants, mais aussi d'outils en faisant l'usage. Nous l'intégrons à ce document dans le but de montrer qu'ils sont répandus et communément acceptés dans le domaine de la sécurité de l'information, mais aussi afin de proposer des pistes d'inspiration pour déterminer quel modèle reprendre, ou sur quels modèles se baser afin d'en développer un nouveau, pour la méthodologie.

Finalement, nous terminerons avec la présentation du but de ce mémoire dans ce contexte.

1.1 Etat de la sécurité dans les PME

Au fil des dernières décennies, les technologies de l'information se sont popularisées dans les mondes de l'industrie et des affaires et les ont transformés à tel point qu'elles en sont devenues un outil sans lequel la plupart des entreprises ne peuvent pas exister. En effet, dans la majorité des sociétés, l'informatique a une place toute choisie pour assurer le fonctionnement, la compétitivité, l'image et jusqu'à la survie même de celles-ci[13].

Or, de nos jours, encore beaucoup d'entreprises n'ont que peu ou pas de considération pour la sécurité de l'information directement liée à ces diverses technologies et à d'autres aspects intervenant dans ce cadre, tels que le facteur humain, ou encore la protection des actifs des sociétés. Ce problème est principalement une conséquence d'un manque de connaissances de ce domaine, mais aussi d'un manque d'accessibilité de celui-ci. En effet, ces sociétés ne connaissent pas leurs besoins en termes de sécurité car elles n'en comprennent pas les enjeux, ni les dangers auxquels elles s'exposent. Et même s'il existe déjà des standards, comme par exemple les ISO/IEC de la famille 2700x qui expliquent, entre autres, l'intérêt d'un "Information Security Management System", ainsi que les lignes de conduite à suivre pour en créer un de qualité; elles sont complexes et nécessitent une étude afin de déterminer quels aspects sont à prendre en compte ou à écarter, selon les besoins de l'entreprise[20, 13, 16].

De plus, il existe déjà des méthodes de gestion des risques qui permettent d'identifier et d'estimer les risques relatifs à la sécurité des systèmes d'information et qui donnent des recommandations. Cependant, elles sont souvent longues à mettre en oeuvre et ne sont pas suffisamment compréhensibles pour le public visé. Cette situation met en évidence la nécessité de fournir une vision de la sécurité de l'information, accessible à un public plus large que celui ciblé par les méthodes et les standards existants. En outre, cette approche devrait donner à ses utilisateurs la possibilité de se familiariser avec le domaine de la sécurité

de l'information et ses enjeux ; mais aussi d'identifier leurs besoins de sécurité insoupçonnés et de comprendre les risques auxquels ils s'exposent, tout en leur donnant des pistes de solution en fin de parcours.

Toutefois, il est nécessaire de nuancer ces informations, car même si les entreprises dont nous parlons montrent des lacunes, elles ne sont pas pour autant complètement démunies. En effet, des recherches ont été effectuées dans le cadre de ce travail, notamment grâce à des interviews portant sur la sécurité de l'information et dont le support se trouve dans l'annexe J. Ainsi, durant le mois de décembre 2014, nous avons questionné plusieurs entreprises wallonnes dont voici la liste :

1. Finomat, une agence immobilière de quatre employés implantée à Namur.

2. Au Plus Net, entreprise/coopérative d'insertion à finalité sociale située à Namur. Elle propose des services de nettoyage et se compose de deux gestionnaires et de 30 travailleurs.

3. Bibliopolis, une entreprise de vente de livres dont le siège social est à Bruxelles. Elle se compose de deux responsables achats qui sont les patrons, d'un comptable et des gérants des sept implantations au travers de la Belgique, pour un total d'environ 15 travailleurs.

4. Priminfo, une entreprise d'assemblage, de livraison et d'installation d'ordinateurs, située à Novilles-les-Bois. Elle se compose d'environ 50 travailleurs en comptant ses deux sous-traitants.

Les informations collectées montrent que certaines entreprises mettent déjà en place des moyens de protection tels que des mots de passe, des backups de certaines données, etc. Cependant, ces bonnes pratiques ne sont souvent pas faites correctement, ni portées jusqu'au bout de ce dont nous serions en droit d'attendre. Ainsi, nous nous rendons compte qu'il s'agit, par exemple de mots de passe trop simples, ou dont le choix est laissé à la discrétion des utilisateurs et non déterminé selon une procédure assurant la qualité de ces derniers. Ou encore, les backups sont faits sur des supports de taille disproportionnée et souvent laissés dans le même emplacement que celui où se trouvent les données sauvegardées.

Ces derniers éléments soulignent davantage l'intérêt de proposer une solution permettant de familiariser les utilisateurs avec la sécurité de l'information et de les amener à une prise de conscience des vulnérabilités et du danger auquel ils s'exposent, mais aussi à l'identification des biens essentiels à leur entreprise et de leurs besoins de sécurité[20].

1.2 Les standards de la famille ISO/IEC 2700x

Le risque et la sécurité de l'information sont les idées directrices de ce mémoire mais il s'agit aussi des thèmes principaux des standards de la famille des ISO/IEC 2700x. Dans cette section, nous introduisons ces notions et nous continuons avec la présentation des standards qui nous intéressent.

Commençons tout d'abord par présenter la définition du risque. Il s'agit de : "la possibilité qu'une menace exploite une vulnérabilité d'un actif ou d'un groupe d'actifs et nuise à donc une organisation"[25]. Afin de bien comprendre cette définition, il est nécessaire de définir son vocabulaire :

1. Une menace est : "la cause potentielle d'un incident indésirable qui peut nuire à un système ou une organisation"[25].
2. Une vulnérabilité est : "une faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une menace"[25].
3. Un actif est : "tout élément représentant de la valeur pour une organisation"[25].

Ensuite, nous définissons la sécurité de l'information comme l'ensemble des processus et pratiques liées principalement aux actifs informationnels des entreprises, mais aussi et plus généralement à tout ce qui se trouve dans le périmètre de ces sociétés et dont le but est de protéger ces dernières contre les impacts d'éventuelles menaces, d'origine internes comme externes, délibérées comme accidentelles, humaines comme non-humaines, indépendamment de leur ampleur, auxquelles elles sont susceptibles d'être vulnérables.

Comme nous l'avons évoqué préalablement, ces problèmes concernent les entreprises dans leur ensemble. Or, comme celles-ci sont actives dans différents secteurs, les difficultés de l'une ne seront pas celles d'une autre, ni ne porteront forcément sur les mêmes sujets, ni n'auront les mêmes impacts sur les actifs. Voila pourquoi la notion de standard est importante. En effet, elle offre un langage commun pour répondre de manière générique aux problèmes liés à la sécurité de l'information et s'adresser à toutes les entreprises, indépendemment de leur caractéristiques distinctives. Ce langage leur donne ainsi la possibilité de mettre en évidence les problèmes, les manques et les risques auxquels elles s'exposent grâce à l'utilisation de documents neutres couvrant l'ensemble, ou tout du moins une grande partie, du domaine.

La famille ISO/IEC 2700x[30], dont nous allons présenter certains standards, est développée, maintenue et validée par deux organisations, "The International Organization for Standardization" ou ISO, et "The International Electrotechnical Commission" ou IEC. Elle propose une vaste collection de méthodes, conseils et pratiques nécessaires à la définition, motivation, mise en place, gestion, au maintient et à la mesure des performances d'un système de management de la

sécurité de l'information, ou SMSI. Ces standards sont prévus afin de s'adresser à toutes sortes d'organisations, indépendamment de facteurs comme la taille, ou le secteur d'activité, etc.

Les tableaux 1.1 et 1.2 listent l'ensemble des standards de la famille des ISO/IEC 2700x.

Famille ISO/IEC 2700x
ISO/IEC 27000 : Vue d'ensemble et dictionnaire
ISO/IEC 27001 : Exigences du SMSI
ISO/IEC 27002 : Code de bonne pratique pour le management de la sécurité de l'information
ISO/IEC 27003 : Guide d'implémentation du SMSI
ISO/IEC 27004 : Indicateurs
ISO/IEC 27005 : Gestion des risques liés à la sécurité de l'information
ISO/IEC 27006 : Exigences pour les organismes procédant à l'audit et à la certification des SMSI
ISO/IEC 27007 : Lignes directrices pour l'audit des SMSI
ISO/IEC 27008 : Lignes directrices pour les auditeurs des contrôles de sécurité de l'information
ISO/IEC 27010 : Gestion de la sécurité de l'information des communications intersectorielles et inter-organisationnelles
ISO/IEC 27011 : Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002
ISO/IEC 27013 : Guide sur la mise en oeuvre intégrée d'ISO/IEC 27001 et ISO/IEC 20000-1
ISO/IEC 27014 : Gouvernance de la sécurité de l'information
ISO/IEC 27015 : Lignes directrices pour le management de la sécurité de l'information pour les services financiers
ISO/IEC 27016 : Économie organisationnelle
ISO/IEC 27018 : Code de bonnes pratiques pour la protection des informations personnelles identifiables(PII) dans l'informatique en nuage public agissant comme processeur de PII
ISO/IEC 27019 : Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/IEC 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie
ISO/IEC 27023 : Mappage des éditions révisées de l'ISO/IEC 27001 et de l'ISO/IEC 27002
ISO/IEC 27031 : Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité
ISO/IEC 27032 : Lignes directrices pour la cybersécurité
ISO/IEC 27034 : Sécurité des applications
ISO/IEC 27035 : Gestion des incidents de sécurité de l'information
ISO/IEC 27036 : Sécurité d'information pour la relation avec le fournisseur

TABLE 1.1 – Tableau des standards de la famille ISO/IEC 2700x - 1/2

ISO/IEC 27037 : Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques
ISO/IEC 27038 : Spécifications pour la rédaction numérique
ISO/IEC 27039 : Sélection, déploiement et opérations des systèmes de détection d'intrusion
ISO/IEC 27040 : Sécurité de stockage
ISO/IEC 27041 : Directives sur la façon d'assurer l'aptitude à l'emploi et l'adéquation d'une méthode d'investigation d'incident
ISO/IEC 27042 : Lignes directrices pour l'analyse et l'interprétation de preuves numériques
ISO/IEC 27043 : Principes d'investigation numérique et les processus
ISO 27799 : Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

TABLE 1.2 – Tableau des standards de la famille ISO/IEC 2700x - 2/2

Toutefois, il est évident que la lecture de tous les standards de cette famille représente une charge de travail très importante et ainsi nous présentons uniquement les ISO/IEC 27000 à 27005. De plus, ces documents sont forts importants dans le cadre de ce travail car ils abordent des thèmes présents au coeur de ce mémoire. En effet, ils introduisent les sujets de la sécurité de l'information, du risque et de sa gestion, les bonnes pratiques afin d'améliorer la sécurité de l'information, comment mettre en place un bon SMSI et évaluer sa performance en mesurant le niveau de sécurité qu'il apporte.

1.2.1 ISO/IEC 27000 : Vue d'ensemble et dictionnaire

Ce standard[25, 19], sorti en mai 2009, est le premier de sa famille et introduit les autres. Il contient la définition de termes spécifiques au domaine de la sécurité et nécessaires à la compréhension du vocabulaire employé dans le cadre d'un système de management de la sécurité de l'information et des autres standards de cette famille. De plus, ce standard présente une vue d'ensemble d'un SMSI. A cet effet, il en explique les principes fondateurs, l'importance, les actifs qu'il manipule et leur nature, et une partie des pré-requis à satisfaire pour une implémentation efficace et réussie.

Finalement, ce standard propose une introduction rapide au restant des standards de sa famille.

1.2.2 ISO/IEC 27001 : Exigences du SMSI

Ce standard[26, 19, 34], dont la seconde édition date d'octobre 2013, est le tout premier de sa famille à être sorti. Ainsi, il a motivé le besoin de produire les autres, listés dans les tableaux 1.1 et 1.2, avec lesquels il s'accorde. Il illustre au travers de sept aspects l'ensemble des impératifs à observer pour qu'une organisation puisse mettre en place, préserver et améliorer continuellement son système de management de la sécurité de l'information. Par ailleurs, le respect de toutes ces exigences génériques, dans le but d'inclure toutes les organisations indépendamment de leurs différences, permet d'obtenir une certification ISO/IEC 27001.
Ces septs aspects sont les suivants[26] :

1. Contexte de l'organisation : Il s'agit de comprendre l'organisation et son contexte, les besoins et les attentes des parties prenantes, de spécifier la portée du SMSI, et de mettre en place, maintenir et améliorer ce SMSI tout en respectant les exigences de ce document tout au long du processus. Cet aspect est primordial car il permet de saisir la situation et les besoins de l'organisation et ainsi de définir dans quelle mesure satisfaire et maintenir les exigences des autres aspects.
2. Direction(Leadership) : Il s'agit d'engager les directeurs et autres responsables dans la mise en place d'un SMSI. Il est de leur responsabilité d'amener le personnel à observer les concepts de la sécurité de l'information, en lui donnant les moyens nécessaires, mais aussi en déterminant des politiques de sécurité et en s'assurant que le personnel est au courant de ses responsabilités en termes de sécurité de l'information.
3. Planification : Il s'agit de déterminer quels sont les problèmes de sécurité qui peuvent survenir, de définir et implémenter les démarches d'évalua-

tion et de traitement du risque, d'identifier les objectifs de sécurité à atteindre et comment les satisfaire.

4. Support : Il s'agit d'identifier et de mettre à disposition les ressources nécessaires à la mise en place, au maintient et à l'amélioration d'un SMSI. Cela inclut la prise en considération des compétences du personnel, son éducation en termes de sécurité de l'information, la mise en place de protocoles pour la communication d'informations, mais aussi la création, la mise à jour et le maintient d'une documentation des informations pertinentes pour le SMSI.
5. Opération : Il s'agit d'exécuter les plans définis lors de l'étape de planification et de documenter ces actions afin de vérifier si elles ont réussi. Cela inclut l'application périodique du processus d'évaluation du risque et la documentation de ses résultats, mais aussi l'application du plan de traitement du risque, si cela s'avère nécessaire, avec documentation des résultats.
6. Evaluation de la performance : Il s'agit de mesurer l'efficacité du SMSI et ainsi le niveau de qualité de la sécurité de l'information. A cet effet, il est nécessaire de soumettre le SMSI à des audits internes et des révisions par le management afin de s'assurer qu'il respecte bien les exigences de l'organisation et de ce standard et qu'il permet d'atteindre les objectifs de sécurités.
7. Amélioration : Il s'agit de résoudre les problèmes mis en évidence dans l'étape précédente, en appliquant des actions visant à améliorer le SMSI. Ce procédé doit être continuellement observé afin d'assurer que le SMSI reste adéquat et performant.

Finalement, ce standard propose aussi une annexe contenant l'ensemble des objectifs de l'ISO/IEC 27002.

1.2.3 ISO/IEC 27002 : Code de bonne pratique

Ce standard[21, 19, 34], originellement appelée ISO/IEC 17799, en est à sa seconde édition datant d'octobre 2013. Son but principal est de fournir un recueil de lignes de conduite et bonnes pratiques efficaces, satisfaisant les objectifs de contrôle mis en évidence dans l'annexe de l'ISO/IEC 27001, pour la gestion des problèmes liés à la sécurité de l'information. De plus, ce standard donne également des conseils à propos des choix et de la mise en place correcte de ces pratiques.

Par ailleurs, ce référentiel explique comment une entreprise peut développer ses propres mesures de sécurité ou adapter celles déjà existantes afin que ces

dernières correspondent mieux aux situations rencontrées dans le contexte spécifique à cette entreprise. Ainsi, ce standard s'adresse aux organisations dont l'objectif est d'améliorer leur sécurité de l'information au travers de l'observation, l'adaptation ou la création, et ensuite l'application de mesures de sécurité, chacune répondant à un objectif spécifique pour la protection de l'information. Il est structuré en quatorze domaines dont voici la liste[21] :

5. Politiques de protection de l'information
6. Organisation de la protection de l'information
7. Protection contre les ressources humaines
8. Gestion des actifs
9. Contrôle d'accès
10. Cryptographie
11. Protection physique et environnementale
12. Protection des opérations
13. Protection des communications
14. Acquisition, développement et maintenance du système
15. Relations avec les fournisseurs
16. Gestion des incidents de protection de l'information
17. Aspects de la protection de l'information lors la gestion de la continuité du business
18. Conformité

Chaque domaine contient une ou plusieurs clauses. Chaque clause définit un objectif de sécurité et ce dernier est adressé par une ou plusieurs mesures de sécurité pour lesquelles des conseils de mise en oeuvre et parfois des information supplémentaires sont proposées[21].

Finalement, ce recueil n'est pas absolu et il peut être nécessaire d'en faire intervenir d'autres afin de prendre en compte la totalité des mesures existantes.

1.2.4 ISO/IEC 27003 : Guide d'implémentation du SMSI

Ce standard[22, 34], dont la première édition date de février 2010, définit un processus en cinq étapes dont l'objectif est de créer un canevas complet de mise en place d'un système de management de la sécurité de l'information d'une organisation. Ce procédé s'aligne avec l'ISO/IEC 27001 et fournit une description complète du cheminement, accompagnée d'une liste de contrôle en annexe afin de s'assurer que tous les points ont bien été considérés, depuis le début de l'initiative jusqu'à l'établissement du plan.

Finalement, ce standard donne des conseils pratiques pour convaincre les gestionnaires d'une organisation de donner l'autorisation d'implémenter un SMSI, définir le périmètre du SMSI, effectuer une analyse des exigences de sécurité, faire une évaluation du risque et planifier son traitement, et enfin, établir le canevas final intégrant l'ensemble de ces points.

1.2.5 ISO/IEC 27004 : Indicateurs

Ce standard[23, 34], dont la première édition date de décembre 2009, propose une démarche visant à mettre en place un programme de mesure de la sécurité de l'information. A cet effet, le document fournit des conseils afin d'orienter la définition, la création et l'application de métriques. De plus, il propose aussi des modèles et des exemples en annexe afin de guider les utilisateurs. Les métriques servent à déterminer la performance du SMSI analysé, selon les exigences illustrées dans l'ISO/IEC 27001.

Par ailleurs, cette approche prend tout son sens à partir du moment où l'on commence à enregistrer les résultats obtenus grâce à l'application périodique des métriques validées par l'organisation. En effet, la comparaison des différents bilans permet de souligner les problèmes découlant d'un manque d'efficience du système de management analysé, ou de la violation de certaines exigences.

Finalement, ce standard présente divers facteurs ayant une influence importante sur la réussite de l'application de métriques, dont un des plus intéressant est la dimension des organisations[23]. De fait, les plus grandes d'entre elles sont souvent obligées de développer plus de métriques et de les appliquer plus souvent que leurs homologues de taille réduite, afin d'obtenir des résultats fiables et utilisables et de couvrir la totalité de leur périmètre.

1.2.6 ISO/IEC 27005 : Gestion des risques liés à la sécurité de l'information

Ce standard[24, 7, 34], dont la première édition date de juin 2008, illustre un processus de gestion du risque lié à la sécurité de l'information, comme le montre la figure 1.1. Toutefois, ce processus n'est pas absolu et il est de la responsabilité de chaque organisation de déterminer leur démarche de gestion du risque.

Le processus se divise en six étapes[24, 34]. La première, l'établissement du contexte, sert à cadrer l'analyse de risque et à définir sa portée. Ensuite, la seconde, permet d'analyser le risque en l'identifiant et en l'estimant, et d'évaluer le danger en comparant les différents niveaux de risque. Par après, l'étape de traitement du risque propose plusieurs options pour l'appréhender, soit le diminuer, le tolérer, l'éluder, ou le transférer. La quatrième est l'acceptation

du risque, notamment le risque résiduel mis en évidence à l'étape précédente. L'avant dernière parle de l'échange des informations obtenues dans les étapes précédentes, entre les différents corps décisionnels de l'organisation. Et enfin, la dernière souligne l'importance d'effectuer ce processus périodiquement afin de détecter tout changement au niveau des étapes du cycle et de pouvoir les adresser au plus vite.

Finalement, ce standard propose une annexe comprenant une liste des sources de menaces et des menaces susceptibles de mettre une entreprise en danger, avec les listes des vulnérabilités permettant de les exploiter et des critères de classement. Ces derniers spécifient l'origine et le type des menaces et des vulnérabilités[24].

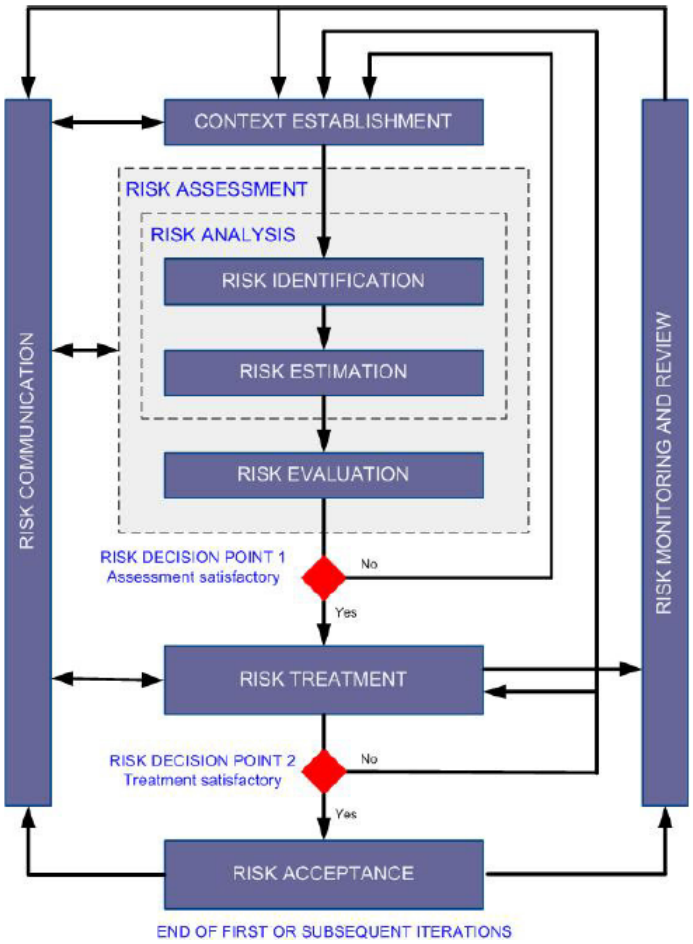


FIGURE 1.1 – ISO/IEC 27005 : Processus de gestion de risque en sécurité de l'information [24]

1.3 Les méthodes existantes

Dans le domaine de la sécurité de l'information, il existe plusieurs méthodes permettant de réaliser des analyses de risque, à l'image d'EBIOS. Ainsi, cette section va en présenter plusieurs, rencontrées au cours de la recherche dans la littérature des outils d'analyse de risque : EBIOS, MEHARI et OCTAVE.

1.3.1 EBIOS

EBIOS [36, 34] est une méthode d'analyse de risque dont l'actuelle troisième version est sortie en janvier 2010. Elle est supportée par un outil du même nom et s'aligne parfaitement avec le processus d'analyse de risque dont nous avons parlé dans la section 1.2.6.

Par ailleurs, EBIOS propose aussi une base de connaissances[35] reprenant une liste abondante illustrant les différentes sources de menaces, types d'impacts, les biens supports et les menaces. Elle récapitule les éléments principaux de la version de 2005 de l'ISO/IEC 27002 et leurs liens avec les facteurs de prévention, protection et récupération, et établit le lien entre les menaces de l'ISO/IEC 27005 et les siennes. Les menaces proposées par EBIOS sont accompagnées d'une description, des listes des vulnérabilités permettant de les concrétiser et des facteurs nécessaires à l'exploitation de ces dernières.

Comme le montre la figure 1.2, le processus proposé par EBIOS se déroule en cinq étapes distinctes, dont nous allons parler.

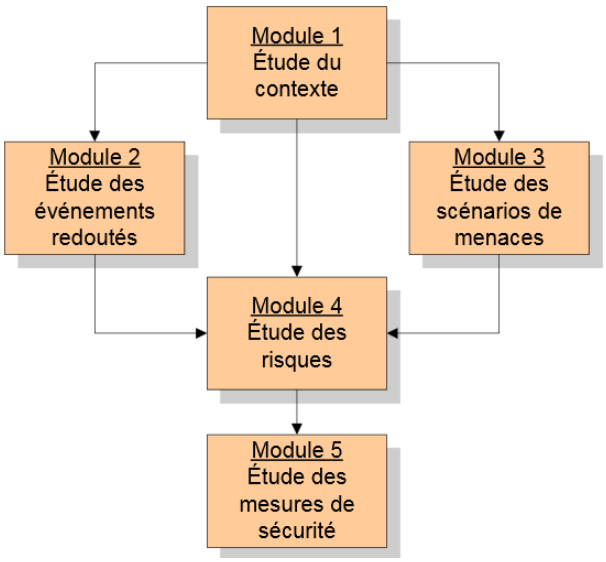


FIGURE 1.2 – Les cinq étapes de la méthode EBIOS [36]

1.3.1.1 Etude du contexte

Dans la première étape, l'utilisateur détermine le périmètre général de son étude de risque, avec les paramètres ayant un impact significatif sur cette dernière, et les sources de menaces. En second, il définit les attributs de sécurité dont l'étude tiendra compte ainsi que leur échelle de valeurs et celles des facteurs de vraisemblance et de gravité, c'est-à-dire la probabilité de concrétisation d'une menace et l'impact de l'occurrence d'une menace sur l'entreprise. Finalement, il identifie les actifs informationnels et physiques de sa société, établit les liens les unissant et détermine les actions déjà mises en place, incluant leur nature préventive, protectrice, ou récupératrice et les biens supports concernés[36, 34].

1.3.1.2 Etude des évènements redoutés

Dans cette partie du processus, focalisée sur les aspects business d'une organisation, l'utilisateur identifie et estime, en fonction des évènements qu'il craint, ses besoins de sécurité pour chacun des biens essentiels de son entreprise. Ces évènements sont ensuite classés automatiquement, selon l'échelle de gravité, du plus au moins dangereux, par l'outil[36, 34].

1.3.1.3 Etude des scénarios de menace

Dans la troisième phase, centrée sur les aspects techniques d'une organisation, l'utilisateur détermine les menaces auxquelles son entreprise est exposée, les vulnérabilités qui permettent de les réaliser et les facteurs nécessaires à l'exploitation de ces dernières. Ces menaces sont également classées automatiquement, de la plus à la moins susceptible de se produire[36, 34].

1.3.1.4 Etude des risques

Dans la quatrième partie du procédé, l'utilisateur génère automatiquement, grâce à l'outil, les risques encourus par son entreprise et peut préciser davantage leur dangerosité en fonction de différents critères comme la présence de mesures de sécurité normales et complémentaires. Ces risques sont ensuite classés en fonction de leur importance qui est déterminée par le niveau de vraisemblance et d'impact de ces derniers. Par ailleurs, l'utilisateur a aussi la possibilité de choisir sa conduite envers le risque en l'acceptant, le transférant, le réduisant ou en l'évitant et ensuite d'analyser ce qu'il en reste[36, 34].

1.3.1.5 Etude des mesures de sécurité

Dans la dernière étape, l'utilisateur définit les mesures de sécurité lui permettant d'atteindre les objectifs sélectionnés, pour les risques, dans l'étape pré-

cédente. Ensuite, il est en mesure d'analyser la dangerosité des risques résiduels après la mise en place des mesures. Enfin, il peut s'occuper du plan définissant comment instaurer et surveiller ces actions[36, 34].

1.3.2 MEHARI

MEHARI, ou MEthode Harmonisée d'Analyse des Risques, est une méthode créée par CLUSIF, le Club de la Sécurité de l'Information Français, et sa dernière version date de janvier 2010. Elle s'adresse à toute les personnes qui ont un intérêt dans la gestion et le traitement de la sécurité de l'information, comme les gestionnaires de risque et tout autre responsable ayant ces mêmes préoccupations[17].

Comme le montre la figure 1.3, MEHARI s'articule autour de trois phases afin de fournir une analyse de risque complète. Celle-ci permet de déterminer un plan d'action adressant le traitement du risque et d'obtenir ainsi une meilleure gestion de ce dernier. A cet effet, la méthode prend la forme d'une base de connaissances permettant de spécifier tous les éléments des phases concernant l'analyse de risque et la détermination d'un plan d'action. De plus, cette méthode s'aligne avec les standards ISO/IEC 27001, dont elle respecte les exigences et ainsi permet d'en obtenir la certification, ISO/IEC 27002, en établissant un lien direct entre les pratiques de ce standard et les scénarios de risque de la base de connaissances, et ISO/IEC 27005, duquel elle s'inspire afin de proposer son approche d'analyse de risque et dont on peut constater les relations avec la figure 1.1.

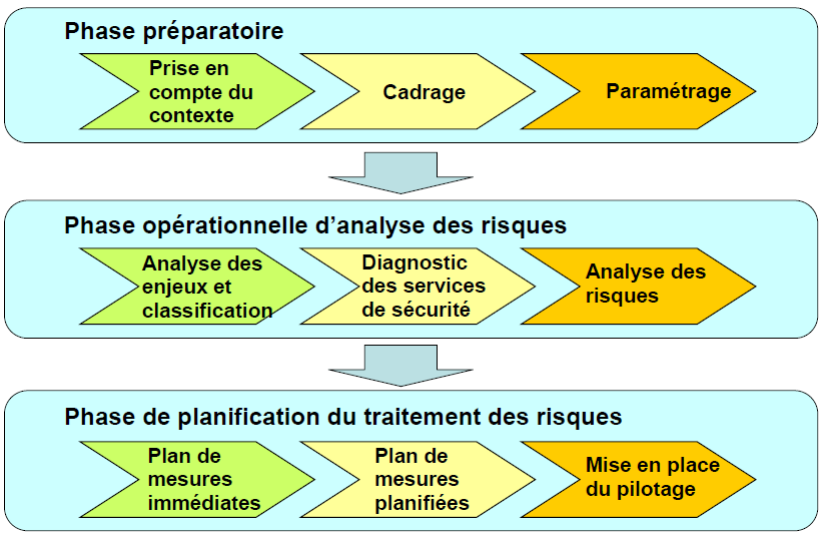


FIGURE 1.3 – Les trois phases de la méthode MEHARI [18]

Dès lors, nous allons présenter les trois phases, qui sont chacune composées de trois étapes :

1.3.2.1 Phase préparatoire

Cette phase a pour but d'aider les organisations à faire leur bilan et à déterminer leurs attentes quant à l'analyse de risque. A cet effet, elle illustre tous les objectifs à remplir avant de se lancer dans la méthode proprement dite. Ces derniers vont guider la réalisation d'une synthèse des tenants et aboutissants de l'organisation, et permettre d'établir son contexte stratégique, technique et organisationnel. Ils serviront aussi à délimiter la portée de l'analyse au niveau géographique, technique, des secteurs impliqués, à spécifier les personnes concernées et leurs rôles et, finalement, à définir les échelles de valeurs pour l'acceptation, les probabilités d'occurrence et les impacts des risques[18].
Ces informations sont importantes, mais pas obligatoires pour accomplir la phase suivante, et peuvent être utilisées afin d'améliorer sa réalisation.

1.3.2.2 Phase opérationnelle d'analyse de risque

Dans cette phase, plusieurs objectifs sont considérés. Pour commencer, le premier est d'identifier les besoins de sécurité et l'importance des actifs en définissant une nomenclature des problèmes qui peuvent les menacer. Celle-ci sert à mettre en évidence le niveau de risque inhérent aux actifs et à les classer en fonction de celui-ci. Ensuite, le second consiste à analyser les mesures de sécurité déjà présentes en définissant un plan pour identifier les mesures à considérer, et à partir de là, déterminer leur performance. Finalement, le dernier objectif est de choisir, parmi les 800 scénarios de risque de la base de connaissance, ceux menaçant les actifs les plus importants, afin de mettre l'accent sur les menaces les plus significatives, et ensuite, d'établir un compte rendu du danger réel posé par chaque scénario, grâce aux résultats de l'analyse des mesures de sécurité[18].

1.3.2.3 Phase de planification de traitement des risques

Cette phase présente plusieurs objectifs visant à organiser la gestion du risque. Tout d'abord, le premier consiste à classer les scénarios de la phase précédente par ordre décroissant de dangerosité et à présenter un ensemble d'actions directes dont le but sera de mitiger les pires d'entre eux. Ensuite, le second vise à créer un plan, définissant sur base de plusieurs critères l'ordre dans lequel les scénarios seront traités, et à présenter des initiatives illustrant comment la stratégie sera déployée et sur quelles périodes de temps. Finalement, le dernier objectif est de spécifier le rôle des parties prenantes à l'analyse de risque concer-

nant le suivi de l'application des stratégies, et de choisir et valider des métriques visant à évaluer leur efficacité et leurs résultats[18].

1.3.3 OCTAVE

La méthode OCTAVE[14, 5, 4, 34], ou Operationnally Critical Threat, Asset and Vulnerability Evaluation, est développée par le CERT, Computer Emergency Response Team, du SEI, le Software Engineering Institute, de l'université Carnegie Mellon. Les initiatives OCTAVE sont prévues pour être réalisées sans aide externe par des équipes composées de personnel appartenant aux organisations, et ayant de bonnes connaissances de son contexte, des objectifs, etc. Il s'agit pas d'une seule méthode mais en réalité de trois variantes permettant chacune de réaliser une analyse de risque. Cependant, elles diffèrent les unes des autres car elles ne s'adressent pas aux mêmes publics.

Tout d'abord, la première variante est OCTAVE, sortie en 1999 et mise à jour en septembre 2001, qui s'adresse principalement à des entreprises de plus de 300 employés. Ensuite, il y a OCTAVE-S, dont la version 0.9 date de décembre 2001, avant d'être complétée en mars 2005, et dont la population cible est l'ensemble des organisations d'au plus 100 personnes. Finalement, l'actuelle version 1.0 d'OCTAVE Allegro est apparue en juin 2007 et vise un public dont la compréhension du domaine de l'analyse de risque n'est ni complète, ni large[14].

Ces méthodes sont proches les unes des autres car il s'agit évidemment d'une analyse de risque dans tous les cas. Cependant, elles n'ont pas toutes les trois la même structure, ni ne s'appliquent dans les mêmes circonstances, c'est pourquoi elles seront toutes les trois détaillées ici. Finalement, La consultation approfondie des documents techniques, abondants pour cette méthode, aidera le lecteur à mieux se rendre compte des différences qui les séparent.

1.3.3.1 OCTAVE et OCTAVE-S

Ces deux méthodes[5, 4, 3] sont structurées de la même manière et, comme le montre la figure 1.4, se découpent en trois phases. En effet, OCTAVE-S est une adaptation de la variante principale, et ces dernières diffèrent principalement par le public auquel elles s'adressent et ainsi par les moyens qu'elles proposent pour atteindre les objectifs, identiques aux deux approches, de l'analyse de risque. De fait, les nuances entre les organisations visées par ces deux méthodes mettent en évidence des besoins, des contraintes et des niveaux de détails différents et spécifiques à leur contexte.

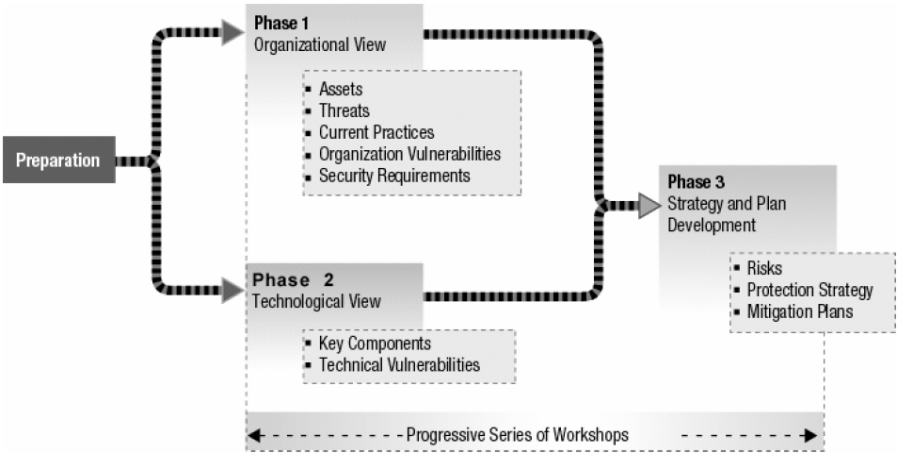


FIGURE 1.4 – Les trois phases de la méthode OCTAVE [5]

1.3.3.1.a Phase 1 - Créer des profils de menaces basés sur les actifs

Cette phase se divise en deux étapes. Tout d'abord, dans la première les utilisateurs sont amenés à définir les valeurs d'appréciation de l'impact qui serviront à estimer le risque. Ensuite, ils déterminent les actifs vitaux au fonctionnement de l'organisation et à l'accomplissement de ses objectifs, par exemple de l'information ou des services, ou encore des personnes dont les capacités sont essentielles à l'entreprise. Enfin, ils effectuent une revue des pratiques déjà existantes de gestion du risque.

Finalement, la seconde étape consiste à sélectionner, parmi les actifs identifiés précédemment, lesquels sont les plus importants pour l'organisation, c'est-à-dire ceux sur lesquels le risque aurait un impact extrêmement néfaste pour l'entreprise. Cette étape se termine avec la création, pour chacun d'eux, d'une documentation spécifiant les besoins de sécurité dont ils doivent faire l'objet et les menaces dont ils peuvent être la cible[5, 4, 3].

1.3.3.1.b Phase 2 - Identifier les vulnérabilités de l'infrastructure

Cette phase contient une seule étape. Dans celle-ci, il convient d'effectuer une revue de tous les équipements informatiques et de leur agencement dans l'organisation. Cela permet d'identifier les points d'entrée à l'infrastructure et au système, en se concentrant sur les accès des utilisateurs aux biens essentiels de l'entreprise et sur les personnes chargées de s'occuper des appareils et réseaux concernés. Enfin, elle propose de prendre l'approche inverse et de se concentrer sur les équipements. En effet, ils permettent l'accès aux biens essentiels et il convient d'identifier les processus impliqués lors de ces entrées et surtout la qualité des mesures de sécurité dont ils font l'objet[5, 4, 3].

1.3.3.1.c Phase 3 - Développer la stratégie et les plans de sécurité

Cette phase se compose de deux étapes. Pour commencer, la première consiste à déterminer l'échelle de valeurs pour le facteur de vraisemblance des menaces, c'est-à-dire la probabilité qu'elles se produisent. Ensuite, ce dernier est utilisé avec le critère d'impact précédemment défini afin d'apprécier le risque des différentes menaces, en leur attribuant des valeurs d'impact et de vraisemblance et en les combinant.

Finalement, la seconde étape sert à déterminer les nouveaux plans visant à défendre l'organisation face au risque. A cet effet, les résultats des étapes précédentes sont utilisés pour choisir les approches permettant d'améliorer la gestion du risque déjà proposée dans les plans initiaux présents avant le lancement de l'analyse. La méthode se termine avec la définition d'une démarche de mise en place effective des nouveaux plans et des résultats des conclusions de l'analyse. Cela inclut la prise en compte de la participation du corps managérial de l'entreprise, de la surveillance de l'application des plans, de refaire une analyse à une date prévue et d'en agrandir la portée[5, 4, 3].

1.3.3.2 OCTAVE Allegro

Cette méthode[14] vise l'obtention de résultats, aussi fiables que ceux des variantes précédentes, sans que les participants aient une connaissance exhaustive des concepts de l'analyse de risque. Elle s'articule autour de quatre domaines couvrant l'ensemble de ses huit étapes, comme le montre la figure 1.5.

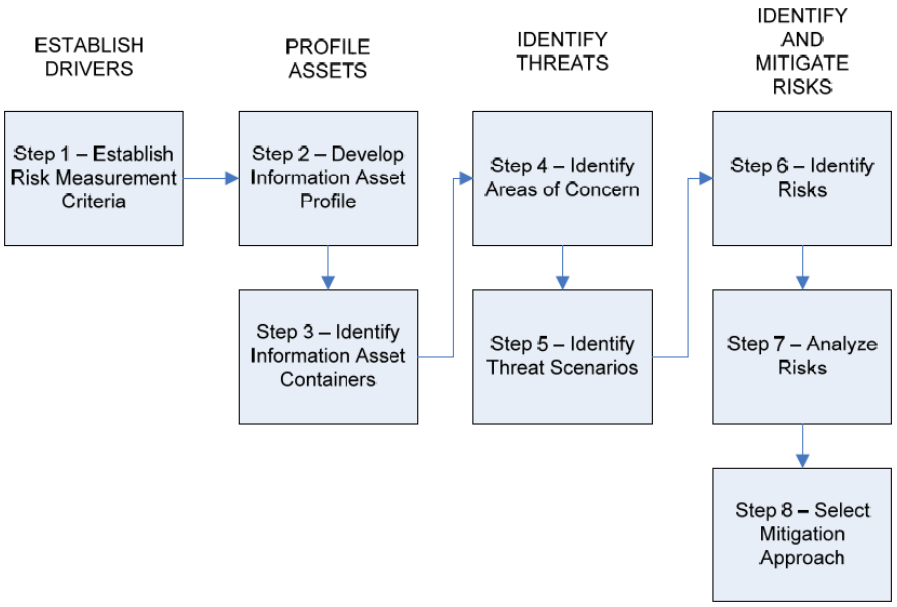


FIGURE 1.5 – Les huit étapes de la méthode OCTAVE Allegro [14]

Ces dernières sont documentées de manière extensive dans le manuel introduisant cette démarche. D'ailleurs, il fournit des canevas afin de guider les utilisateurs dans la résolution des défis proposés par chaque étape.

1.3.3.2.a Définir les paramètres

Ce domaine contient uniquement la première étape, c'est-à-dire la détermination des métriques qui vont guider l'analyse. Elle amène les utilisateurs à définir, selon leurs perceptions, les échelles de valeurs des facteurs permettant d'estimer l'impact du risque sur les biens essentiels à l'organisation. Ces facteurs doivent être pertinents et définis de manière à illustrer explicitement la vision de l'entreprise sur la gravité de la concrétisation du danger. Ceci permettra d'assurer une évaluation cohérente du risque entre les différents biens essentiels, mais aussi la pertinence et l'harmonie des mesures servant à les traiter.

Finalement, l'organisation doit déterminer l'importance des critères de mesure les uns par rapport aux autres. En effet, selon les aspects sur lesquels l'entreprise met l'accent, par exemple la protection des actifs organisationnels ou les ressources humaines, les critères les concernant doivent avoir plus de poids que ceux portant sur des aspects auxquels l'entreprise accorde moins d'importance. Cela permettra d'établir des priorités dans le traitement du risque[14].

1.3.3.2.b Définir les profils des actifs

Ce domaine contient les étapes deux et trois du processus. Tout d'abord, la deuxième étape consiste à établir le profil des actifs informationnels. Ainsi, elle propose d'identifier la liste des informations et données nécessaires au fonctionnement de l'entreprise et à la réalisation de ses objectifs.Ensuite, il convient d'en sélectionner les plus importantes et de les documenter selon plusieurs critères comme la méthode de sélection, la portée, les objectifs qu'elles supportent, leurs responsables, leurs besoins de sécurité, etc. Cette documentation servira de référentiel exhaustif, et idéalement clair et complet, pour la suite du processus d'analyse.

Finalement, la troisième étape consiste à identifier les conteneurs d'actifs informationnels. A cet effet, il convient de déterminer tous les réceptacles physiques, électroniques et humains, contenant, manipulant et véhiculant ces données vitales à l'organisation, ainsi que leur emplacement, et les personnes ou organismes les supervisant. Ceci est nécessaire pour mettre en évidence les dangers liés à ces mediums, spécifier le périmètre technique de l'analyse et les cas particuliers à considérer[14].

1.3.3.2.c Identifier les menaces

Ce domaine contient les étapes quatre et cinq de l'approche. Pour commencer, la quatrième étape consiste à identifier les zones de préoccupation. Ainsi, elle propose de déterminer des situations évidentes de la vie réelle, par exemple celles déjà vécues, capables de menacer les biens essentiels de l'organisation. Pour ce faire, il convient de partir des résultats de l'étape 3 et de les utiliser afin de discuter des éventuels circonstances pouvant constituer un danger ou une violation des besoins de sécurité, tout en prenant compte de facteurs tels que les personnes impliquées, les raisons les poussant à agir de la sorte et les conséquences.

Finalement, la cinquième étape consiste à identifier des scénarios de menace. A cet effet, elle propose d'utiliser l'étape précédente afin de dériver des scénarios approfondissant le niveau de spécification des menaces. Ensuite, ils sont analysés afin de dériver un nouvel ensemble de menaces couvrant davantage le périmètre de l'étude. Enfin, cette étape permet aussi d'établir une échelle de valeurs pour la probabilité d'occurrence des scénarios, même si elle propose la sienne par défaut[14].

1.3.3.2.d Identifier et diminuer le risque

Ce domaine contient les étapes six, sept et huit de la démarche. Pour commencer, la sixième étape consiste à identifier les risques. Ainsi, elle sert à mettre en évidence les différentes conséquences des menaces identifiées préalablement dans le but de compléter l'évaluation du risque. Ces menaces sont documentées pour chaque actif intervenant dans l'analyse de risque.

Ensuite, la septième étape consiste à analyser les risques. Pour cela, elle utilise des éléments définis lors des étapes précédentes, spécifiquement les facteurs de vraisemblance, et d'impact, afin d'effectuer le calcul du risque des actifs informationnels. Ainsi, elle affiche des résultats qui s'inscrivent dans le contexte de l'organisation.

Finalement, la dernière étape consiste à sélectionner une approche de traitement. A cet effet, les utilisateurs définissent la manière avec laquelle ils vont s'occuper du risque afin de le réduire. A cet effet, ils sélectionnent les risques qui feront l'objet d'un traitement, en s'aidant des scores de l'étape précédente comme indicateur de priorité, et définissent les plans d'action. Ceux-ci doivent observer certains critères comme l'importance des actifs, leurs besoins de sécurité, leurs réceptacles, et le contexte de l'entreprise[14].

1.4 Conception de questionnaires

La création et la conception de questionnaires[11, 31, 12] est une idée au coeur de ce travail, car il s'agit du medium au travers duquel nous souhaitons communiquer la méthodologie aux utilisateurs. Dans cette section, nous abordons les nombreux principes de ces notions car lors de la réalisation de ce genre de tâche, il convient de s'intéresser à la manière avec laquelle on construit le questionnaire, c'est-à-dire la suite logique des questions, et à la manière avec laquelle on propose les réponses à ces dernières, autant que leur qualité, leur compréhensibilité et bien d'autres aspects.

Tout d'abord, un questionnaire est un agencement de questions explorées par un répondant et pouvant être liées à plusieurs autres. Il peut être capable de ne pas afficher directement toutes les questions, mais seulement en fonction des réponses des utilisateurs, et donc être interactif[31]. Une question, ou interrogation, est une phrase en forme interrogative à laquelle il est possible de fournir des réponses. Il existe principalement deux types de questions, celles ouvertes, dont les réponses sont des associations de mots de la langue parlée, et celles fermées, pour lesquelles les réponses peuvent être binaires(Oui/Non), ternaires(Oui/Non/Je ne sais pas), à choix multiples, ou encore qualitatives ordonnées(Très souvent/Souvent/Rarement)[12].

Comme nous l'avons déjà énoncé, la conception de questions et de leurs réponses doit faire l'objet de considérations spécifiques afin d'atteindre efficacement les objectifs visés, et le principal facteur à observer est la qualité des questions. A cet effet, un questionnaire doit être accompagné d'hypothèses et d'objectifs dont les questions, qui en sont inspirés, illustrent les idées et concepts qu'ils véhiculent. Dans ce travail, ces hypothèses et ces objectifs sont déterminés dans la section 3.1. Les termes utilisés dans les questions doivent être compréhensibles et avoir le même sens pour toute personne dans la population ciblée, sans pour autant être trop longues car cela risquerait de forcer un utilisateur à abandonner. Par ailleurs, la suite des questions doit être logique afin de susciter l'intérêt des répondants, mais aussi dans le but de les aider à mieux appréhender le sujet mis en avant[12].

Dans le cadre de la création de questionnaires, il existe un procédé particulièrement intéressant à prendre en considération, il s'agit du processus cognitif de réponse à une question[11], et comme nous allons le voir, il met l'accent sur les caractéristiques dont nous venons de parler. Ce procédé se divise en cinq étapes, mais nous parlerons seulement des quatre premières car la dernière, la communication des réponses oralement ou par écrit, est suffisamment claire pour qu'il ne soit pas nécessaire de l'approfondir. Chacune des quatre étapes illustre, sous la forme d'un challenge, des bonnes pratiques à mettre en place et des problèmes

récurrents à considérer :

- Challenge 1 : Le répondant cherche à déchiffrer et à comprendre le sens de la question qui lui est posée. A cet effet, il convient d'utiliser des termes précis et compréhensibles par toute personne de la population ciblée. En effet, certains mots peuvent être interprétés différemment par certaines personnes et il est nécessaire d'éviter ce cas de figure. Par exemple, l'utilisation de la forme interrogative négative, ou doublement négative, est vivement déconseillée.
- Challenge 2 : L'utilisateur retrouve l'information qui lui est demandée par la question, soit dans sa mémoire, soit dans des documents. Les questions doivent être posées de sorte que la réponse puisse être trouvée par le répondant. Dans cette optique, il est nécessaire de considérer plusieurs facteurs. Tout d'abord, l'effet connaissance, selon lequel on présuppose qu'une personne connaît les réponses aux questions. Or, et c'est d'ailleurs une des hypothèses les plus importantes du travail, ce n'est pas toujours le cas selon les divers sujets dont la complexité varie. Ainsi, il est important de créer des questions qui s'alignent avec le niveau de connaissance requis des répondants. Ensuite, il y a l'effet mémoire, selon lequel la facilité à se souvenir d'une information est directement proportionnelle à sa récence, son importance, ou à sa nature. Ainsi, il convient d'utiliser des références temporelles courtes, ou de poser plusieurs questions liées, afin de faciliter l'exercice de la mémoire. Par la suite, le dernier effet est celui du télescopage selon lequel un répondant risque d'associer un fait à une mauvaise période. Afin d'éviter ce problème, plusieurs recommandations sont proposées, par exemple l'utilisation de repères temporels ou d'un calendrier. Finalement, il convient de dire que même si les deux derniers facteurs sont intéressants, ils ne sont pas aussi importants que le premier dans le cadre de ce mémoire.
- Challenge 3 : Il s'agit de la formulation des réponses. En effet, il est judicieux d'observer plusieurs conditions pour réaliser cette démarche. Tout d'abord, il est nécessaire de décider si la réponse sera ouverte ou fermée. Ensuite, une question et ses réponses doivent idéalement être liées par des points de références afin de réduire le temps de réponse de l'utilisateur. Par exemple, si une question parle de lieux, les réponses doivent le mettre en évidence. Par après, toute question doit véhiculer un concept unique, afin de ne pas mettre l'utilisateur dans le doute. Finalement, si la question propose des réponses prédéfinies, ces dernières doivent être compréhensibles, sans équivoque, et couvrir l'ensemble des éventualités possibles.
- Challenge 4 : Cela concerne la notion selon laquelle la manière d'écrire les

questions, ou encore les sujets qu'elles abordent, amènent les répondants à changer leur réponse afin de ne pas perdre la face ou de ne pas se faire juger. Néanmoins, il est possible de rassurer les interlocuteurs au moyen des mécanismes suivants : motiver la nécessité de poser les questions, proposer des accords de confidentialité, utiliser des réponses apparaissant vagues comme les intervalles, ou répondre anonymement aux questions. Finalement, il est important de fournir des questions qui ne présentent pas de parti pris afin de ne pas influencer la réponse de l'utilisateur et de s'assurer de son honnêteté.

La figure 1.6 représente graphiquement les étapes du processus par lequel passe un utilisateur lorsqu'il répond à une question.

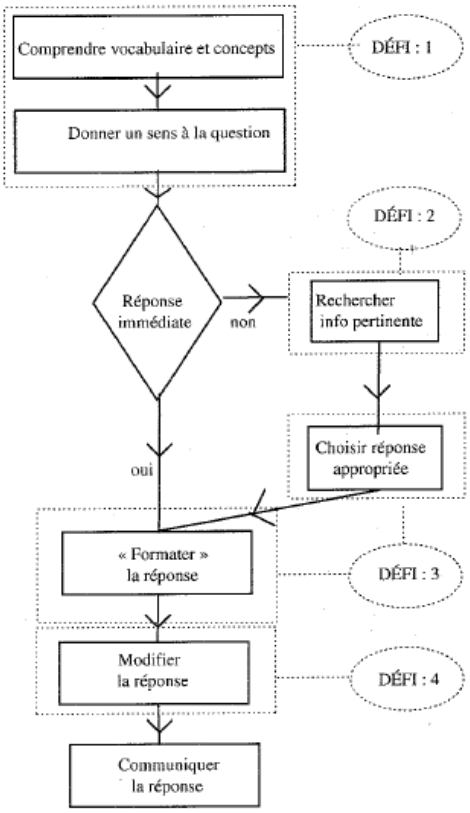


FIGURE 1.6 – Représentation graphique du processus cognitif de réponse à une question [11]

Toutefois, la conception ne s'arrête pas ici. Il reste la partie évaluation des questionnaires dont nous n'avons pas encore parlé. En effet, afin de vérifier si les hypothèses sont respectées, si les objectifs sont atteints et donc que le questionnaire est bien conçu, il convient de vérifier s'il est adéquat. A cet effet, il existe plusieurs techniques à mettre en place[11].

La première consiste à regrouper plusieurs personnes afin de dialoguer efficacement à propos d'un sujet ou concept du questionnaire. Il est ainsi possible de revoir l'ensemble de son contenu et de recueillir les avis des parties prenantes à la discussion, selon les aspects mis en évidence dans le processus cognitif. Même si les résultats ne sont pas un indicateur absolu de ce que pense ou perçoit la population cible, ils représentent néanmoins une bonne base à partir de laquelle des améliorations peuvent être envisagées.

La seconde technique propose de laisser un répondant réaliser le questionnaire au cours d'une rencontre avec un responsable. Ensuite, ce dernier pose périodiquement des questions sur les actions effectuées par l'utilisateur afin de récupérer des informations sur la qualité et la validité du questionnaire. Evidemment, ces questions mettent en évidence les points dont nous avons parlé dans le processus cognitif. Le choix des périodes d'obtention de feedback est laissé à la discrétion du responsable mais il est commun de le faire soit à la fin de la rencontre, soit après une suite significative de questions, ou encore après chacune.

La troisième manière de faire est de réaliser un pré-test. Il s'agit de mettre un échantillon réduit de répondants en situation réelle de réalisation du questionnaire, afin de mettre en évidence les problèmes posés par ce dernier.

La dernière technique est de prendre le temps de dialoguer avec les répondants au questionnaire. Idéalement, ceci s'effectue dans le cycle de vie de création du questionnaire, et surtout après un test. A cet effet, il est même suggéré de réaliser des enquêtes de satisfaction des questionnaires soumis aux utilisateurs afin de récupérer leurs opinions.

Finalement, nous terminons cette section avec une discussion sur divers outils de création de questionnaires[42]. Au cours de nos recherches, nous avons trouvé énormément de logiciels permettant de réaliser des enquêtes et des questionnaires, ainsi que des formalismes forts intéressants et complets permettant de les définir avec un grand niveau de détail et de complétude. Or, bien que nous nous soyons inspirés de ces derniers afin de créer la structure du questionnaire final et de nous assurer que nous intégrons bien certains aspects importants, comme les valeurs des réponses pour le calcul des scores de résultats, nous n'avons utilisé ni ces outils, ni ces formalismes pour la création proprement dite. En effet, la nature sensible des données, que le sujet de ce travail nous amène à manipuler, rentre en conflit avec ces logiciels qui pour la plupart sont en ligne sur internet. Cela pose un énorme risque au niveau de la confidentialité des données, et les entreprises ne souhaitent pas le courir. Le reste des outils stand-alone ne proposent pas de fonctions suffisamment poussées pour réaliser l'ensemble des tâches requises par la méthodologie. C'est pourquoi nous nous sommes tournés vers une solution alternative abordée dans l'annexe C.

1.5 Les métriques pour le calcul du risque

Dans cette section, nous présentons le concept des métriques pour le calcul du risque[43, 2, 6] du point de vue de la sécurité de l'information, mais aussi d'un point de vue plus général afin d'en avoir la vision la plus complète. Ainsi, nous pouvons mettre en évidence l'utilité et l'importance de cette notion, mais aussi les contraintes à respecter lors de son emploi dans la méthodologie.

Les métriques, rapidement survolées dans les sections 1.2.5 et 1.4, sont importantes dans le cadre de ce mémoire car elles abordent le sujet du calcul des scores de résultats. Actuellement, il s'agit encore d'un domaine relativement récent et, malgré l'existence de standards comme l'ISO/IEC 27001 et l'ISO/IEC 27004 dans lesquels ce sujet est abordé et soutenu, il est encore délicat de spécifier et d'implémenter des métriques efficaces et faciles à utiliser, surtout si l'on considère un public n'ayant pas ou peu de connaissances en la matière.

Dans le cadre de la sécurité de l'information, les métriques sont définies comme des méthodes permettant de quantifier, grâce à des échelles de valeurs prédéfinies, la performance des mesures de sécurité mises en place dans des organisations[6]. Toutefois, dans le cadre de ce travail nous nous intéressons surtout à la mise en évidence du risque afin de déterminer le niveau de maturité en termes de sécurité de l'information et ce n'est pas le but principal des métriques dans ce contexte.

Or, si l'on se rapporte à un cadre plus général, les métriques sont des méthodes utilisant des échelles de valeurs pour calculer des résultats. Ainsi, il est tout à fait possible de les adapter afin de faire sortir l'information qui nous intéresse, c'est-à-dire la valeur du risque encouru par une organisation. D'ailleurs, la formule bien connue du calcul du risque[25] : Risque = Menace $*$ Impact $*$ Vulnérabilité, dans laquelle les ensembles de valeurs spécifiés pour les trois facteurs de la formule servent à lui donner une valeur numérique indiquant son importance, en est une preuve supplémentaire.

De plus, et cela est commun aux deux notions, les métriques doivent satisfaire certaines exigences [43, 2] dont les plus importantes sont :

1. La simplicité des résultats : les résultats doivent être compréhensibles par leur public cible.
2. La reproductibilité des résultats : les résultats obtenus doivent être identiques dans des situations identiques.
3. La comparabilité des résultats : les résultats doivent pouvoir être confrontés les uns aux autres afin de mettre en évidence des améliorations ou des détériorations.
4. L'interprétabilité des résultats : les résultats doivent être accompagnés

des moyens de les interpréter, notamment en définissant des valeurs d'acceptabilité et d'inacceptabilité.

Au travers de ces deux définitions, il est facile de voir l'importance d'intégrer des métriques dans une méthode d'évaluation de la sécurité de l'information car s'il n'est pas possible de mesurer le niveau de sécurité d'une organisation alors il est invraisemblable d'imaginer mettre en évidence les problèmes de sécurité, leur sévérité et encore moins de savoir choisir les actions de traitement appropriées. Ainsi, nous nous sommes informés sur les manières d'appliquer cette idée dans le cadre de ce travail. Au cours de nos recherches, nous avons trouvés plusieurs documents qui nous ont aidés à nous familiariser avec le concept, avant de définir l'approche utilisée dans cette méthodologie.

Tout d'abord, une étude conduite par Weib, Weissman et Dressler[43], développe et décrit une métrique permettant l'évaluation de l'entièreté d'une organisation, dont les résultats sont reproductibles afin d'assurer un certain degré d'objectivité, et comparables pour établir une base et pouvoir agir dessus. La méthode est prévue pour être intégrée au cycle de gestion d'une organisation selon la démarche Plan-Do-Check-Act et elle s'articule autour de trois étapes. En premier, il y a la détermination de l'importance des actifs de l'organisation avec l'identification de scénarios de menace, vulnérabilité ou dommages, suivie de leur évaluation et de leur association à trois indicateurs pour l'organisation. Le premier donne une idée générale de la sécurité, le second illustre la distribution de la sécurité au cours du temps et le dernier propose des informations sur l'occurrence de dommages critiques.
En fait, plus qu'une métrique, cette méthode ressemble plutôt à une évaluation de la sécurité d'une organisation, intégrant la métrique décrite et développée. Cependant, elle met en évidence un argument pertinent, c'est-à-dire la communication du danger au travers de plusieurs indicateurs. Tout ceci, plus le fait que l'approche fut introduite dans l'ISO/IEC 27004 font de ce document une source d'informations intéressantes pour ce travail.

Finalement, une étude, réalisée par Ahmad, Sahib et Azuwa[2], présente une méthode d'identification et de spécification de métriques, conformément au standard 27001, visant à évaluer l'efficacité de la gestion d'un réseau. Pour ce faire, ils proposent un modèle dans lequel la mesure est basée sur la performance des moyens mis en place pour protéger un réseau et ses services. Dans leur démarche, ils utilisent l'approche "Goal-Question-Metric" afin de produire des métriques compréhensibles et respectant les critères d'efficacité mis en évidence. Parmi ces derniers, les plus importants sont toujours la simplicité, la comparabilité et l'objectivité des résultats quantitatifs.

Cette approche est utilisée afin de produire un système de mesure, hiérarchisé en trois niveaux, ciblant des problèmes particuliers. Il fonctionne selon une

approche "Top-Down" dont le but est de permettre la spécification de métriques à partir de questions et d'objectifs de mesure. Les trois niveaux sont[34] :

1. Goal : L'utilisateur y définit un objectif pour un objet tel qu'un produit, un processus ou une ressource, afin de conceptualiser son but.
2. Question : L'utilisateur crée des questions dont l'utilité est de déterminer comment la mesure de l'objectif se déroulera, afin de rendre cet objectif opérationnel.
3. Metric : L'utilisateur assigne, à chaque question, un ensemble de données de sorte à pouvoir quantifier leur résultat.

Finalement, cette notion est particulièrement intéressante, car elle propose une approche compréhensible et ne nécessitant pas de grandes connaissances, afin de déterminer des métriques pour, notamment, le calcul du risque. En se posant les bonnes questions, un utilisateur arrive facilement à raffiner l'objectif principal et à développer un ensemble de méthodes de mesures adaptées à son contexte.

1.6 Les modèles de maturité

Les modèles de maturité sont intéressants à considérer dans le cadre de ce travail car il s'agit du moyen au travers duquel nous souhaitons communiquer l'efficacité de la prise en charge de la sécurité de l'information par des organisations. De plus, ils représentent un medium compréhensible pour la visualisation du progrès, ou du déclin, au niveau de la sécurité de l'information en comparant les instances des modèles de différentes évaluations. Par ailleurs, les modèles de maturité s'inscrivent directement dans la lignée des informations illustrées par la section 1.5 sur les métriques pour le calcul du risque. En effet, les modèles de maturité peuvent en avoir l'utilité afin d'effectuer leur mission. Mais tout d'abord, débutons avec une explication du concept.

Pour commencer, d'après la définition du dictionnaire Larousse[1], la maturité d'un sujet est l'état dans lequel ses capacités et ses facultés sont à l'apogée de leur évolution. Ainsi, un modèle de maturité sert à situer un sujet d'étude, c'est-à-dire une organisation, une entreprise, un processus, ou encore leurs éléments clefs et constituants, sur une échelle qui indique sa capacité à effectuer efficacement une tâche ou un ensemble de tâches, ainsi que la pertinence et la qualité des moyens utilisés pour atteindre ce résultat[33, 37].
Il possède généralement une structure hiérarchique distribuée en un nombre variable de niveaux, fonction du désir de son créateur de détailler ou non cette structure. Chaque niveau de maturité se focalise sur certains aspects du domaine, est qualifié par des conditions d'appartenance, définit des objectifs à at-

teindre pour prétendre au niveau suivant, et souvent, fournit des conseils pour guider l'utilisateur dans la satisfaction de ceux-ci.[33, 39]
De plus, il convient de garder à l'esprit qu'étant donné la structure hiérarchique de ce genre de modèles, la validation de la maturité pour l'atteinte d'un niveau, autre que le premier, passe obligatoirement par la satisfaction de tous les précédents[32].

Ensuite, deux types d'observations sont nécessaires pour estimer la maturité :

- les observations de la satisfaction de pré-requis et d'objectifs qui dépendent du domaine considéré et du niveau de maturité,
- les observations de la conformité entre le choix des moyens, ainsi que la manière de les mettre en place, et les pratiques à émuler définies dans le modèle.

Ces éléments observés sont souvent dérivés de référentiels tels que les standards fournis par l'Organisation Internationale de Normalisation, ou de bonnes pratiques, ou obtenus à partir d'exigences et de besoins[33, 39].

De plus, les observations peuvent être réalisées quantitativement ou qualitativement. La première approche est formelle et basée sur des principes et formules mathématiques. C'est d'ailleurs sur ce point que les modèles de maturité rejoignent le concept des métriques de la section 1.5, qui permettent justement de mesurer et de mettre en place la mesure de résultats. La seconde approche est informelle et basée sur des impressions, des opinions et des expériences des utilisateurs. Cependant, aussi rigoureuse que soit cette dernière approche, sa réalisation offrira un résultat moins fiable qu'une démarche formelle, qui par contre sera beaucoup plus difficile à utiliser par des personnes n'ayant pas les connaissances requises[37].

En outre, le but d'un modèle de maturité est de donner à un utilisateur une représentation fiable, compréhensible et pondérée en fonction du contexte, afin qu'il puisse identifier directement les aspects nécessitant une intervention immédiate, mais aussi pour d'éventuelles comparaisons avec un bilan passé ou futur ou selon des statistiques extérieures.

Il est tout à fait possible pour un organisme de définir son propre modèle de maturité selon ses propres exigences. Par contre, c'est un processus assez compliqué et qui nécessite de fortes connaissances des normes, des pratiques et des règles concernant le développement de ce genre de modèles[33].

La figure ci-dessous illustre un exemple de modèle de maturité.

Generic Security Maturity Model	
Level 1	Physical security Lack of confidence Basic computer and network protection
Level 2	Critical review of organisation Appoint security team Some level of confidence Formal security policies/procedure
Level 3	Initiation of security programme Security architecture Stricter security controls Organisation-wide policies/procedures
Level 4	Security testing Mitigate security weaknesses Information management Identity security threats
Level 5	Full implementation of policies/procedures Consistent outcomes Automated security controls

Ce modèle de maturité générique fut réalisé par MM Lessing en 2006 et il est spécifié dans son article[33]. Il s'agit du résultat de la comparaison et de l'intégration de différents modèles de maturité portant sur le domaine de la sécurité de l'information. L'image présente un modèle en cinq niveaux, tous décrits dans l'article, et pour chacun d'entre eux, les éléments sur lesquels ils se concentrent et auxquels il faut donc avoir satisfait afin de prétendre à la maturité du niveau en question. Cependant, c'est une représentation assez simple, qui n'inclut pas de lignes de conduites ou de conseils pour la satisfaction des exigences.

Par après, il convient de traiter de l'applicabilité de ces modèles. Dans ce travail, nous nous intéressons surtout aux modèles de maturité qui portent sur la sécurité de l'information. Cependant, le concept est applicable à beaucoup de domaines, tels que le développement de logiciels, la fourniture de services, et même à des secteurs qui ne sont pas spécialement liés à l'informatique. Une bonne compréhension du concept de modèle de maturité permet d'expliquer cela facilement. En effet, s'ils servent à constater dans quelle mesure une organisation est capable d'effectuer une tâche, un business, c'est-à-dire ce qui fait l'objet d'une évaluation de maturité, correctement, avec efficacité, en employant les bonnes méthodes, ... , alors ils peuvent effectivement servir à mesurer la maturité de n'importe quel processus dans n'importe quel contexte, dans la mesure où un

modèle de maturité spécifique au domaine est défini, validé et utilisé.

Finalement, il est bon de garder à l'esprit qu'il s'agit ici d'un concept qui couvre une abondance de contextes, du fait que sa finalité est relative à un objectif commun à énormément de processus, c'est-à-dire la vérification qu'ils sont effectués au mieux de ce qui est possible de réaliser, en utilisant les meilleurs moyens possibles selon diverses contraintes, en prenant en compte les objectifs nécessaires, de sorte à permettre à d'autres objectifs d'être atteints de manière optimale, etc.

1.6.1 Les modèles de maturité existants

Cette section résume le résultat de la recherche dans le domaine des modèles de maturité en présentant brièvement certains d'entre eux. Ils sont intéressants dans le cadre de ce travail car ils fournissent une base de laquelle s'inspirer afin de développer un modèle de maturité propre à la méthodologie, ou pour en reprendre un et l'utiliser directement.

Le CMMI, ou "Capability Maturity Model Integration", est subdivisé en trois sous modèles qui concernent respectivement le développement de systèmes, la maîtrise des activités d'achat et la fourniture de services[8].

Le SSE-CMM ou ISO 21827 est un modèle orienté processus, cependant il est aussi strictement technique et ne couvre que des aspects basiques. De plus, il essaye surtout de fournir un bon résultat de la qualité par rapport au coût, parfois au détriment de la qualité. Tout ceci implique qu'il ne permet d'atteindre qu'un niveau de sécurité acceptable, ni insuffisant ni excellent. Par ailleurs, les effets sur le business ne sont évalués que plus tard dans le cycle, ce qui peut poser problème si ces aspects, et c'est souvent le cas pour les entreprises, sont à considérer en priorité. Néanmoins, il est équipé de métriques facilement interprétables[40].

Le modèle ISM-cubed ou ISM3, comme le précédent, est orienté processus. Son optique est que chaque mesure de sécurité nécessite son propre processus de gestion. Il se focalise cependant beaucoup plus sur l'accomplissement des objectifs business au cours de la mise en place d'un niveau acceptable de sécurité. En effet, il impose aux utilisateurs de connecter les objectifs et les cibles de sécurité aux objectifs business[40, 28].

Karakola, Kowalski et Yngström proposent un modèle de maturité pour des services sécurisés de e-Governments. Il vise autant les aspects techniques que non-techniques et permet de mieux comprendre, définir, implémenter, contrôler et améliorer continuellement les services en question[32].

Spremic et Popovic proposent un modèle de gestion des risques des technologies de l'information d'un business dont les principes sont la mise en place de politiques obligatoires, des démarches et règles pour leur implémentation, et

des contre-mesures ayant pour but d'augmenter la protection contre les menaces et attaques. L'approche de ce modèle permet d'avoir une présentation haut niveau de l'évaluation des risques ainsi que de l'implémentation des réponses aux risques[38].

Saleh propose un modèle de maturité permettant aux entreprises d'évaluer elles-même leur capacité à satisfaire les objectifs de sécurité. Il couvre différents domaines qui sont la gouvernance de l'organisation, la culture organisationnelle, l'architecture des systèmes et la gestion de services[37].

Finalement, nous terminons avec la présentation d'un article de Spruit et Roeling[39]. Par rapport aux objectifs de ce travail, cet article et les modèles qu'il présente sont plus appropriés pour répondre aux objectifs que les autres ne le sont. Ainsi, il est abordé plus en profondeur et réutilisé dans la proposition de solution illustrée dans la section 6.3. Cet article est d'autant plus intéressant car le modèle illustré est très générique, afin de s'adresser à un maximum d'organisations, et se sert notamment de l'ISO/IEC 27002, document très utilisé dans le cadre de ce travail, pour déterminer la maturité de la sécurité d'une organisation. Le modèle en question est l'ISFAM, ou Information Security Focus Area Maturity Model, et il se compose de 13 zones de focus et de 12 niveaux de maturités qui couvrent les 4 catégories de maturité suivantes : design, implémentation, efficacité opérationnelle et surveillance. Les zones de focus sont majoritairement issues de l'ISO/IEC 27002 sauf la dernière qui est issue du CISSP et du Standard of Good Pratice et elles sont réparties en 4 catégories : organisationnel, technique, organisationnel et technique, et support. Chaque zone possède son propre modèle de maturité, dont le nombre de niveaux peut varier d'une zone à l'autre, et une liste de questions liées à ces niveaux. Ainsi, l'atteinte d'un niveau de maturité dans une zone de focus dépend des réponses aux questions portant sur ce niveau et sur les niveaux qui le précèdent. De plus, certains de ces niveaux de maturité sont liés à travers les différentes zones de focus afin de mettre en évidence que l'atteinte d'un niveau de maturité dans une zone de focus peut dépendre du niveau de maturité atteint dans d'autres zones de focus. Enfin, l'ISFAM distribue les niveaux de maturité des zones de focus au travers de ses 12 niveaux et il affiche, de manière lisible et compréhensible, les niveaux de maturité de ces zones.

1.6.2 Des outils utilisant les modèles de maturité

Cette section résume le résultat de la documentation dans le domaine des outils utilisant le concept des modèles de maturité, en présentant brièvement certains d'entre eux. Ils sont intéressants dans le cadre de ce travail car ces exemples apportent des informations sur l'utilisation de modèles de maturité au

sein d'outils, c'est-à-dire, comment ils s'intègrent dans l'outil, comment ils en présentent les résultats, etc.

Taha, Trapero, Luna, Suri proposent un framework, intégré dans un outil de validation, permettant de comparer et classer le niveau de sécurité de deux, voire plus, "Cloud Service Providers", selon une technique d'évaluation "Security Cloud Service Level Agreements" qualitative et quantitative, qui permet aux utilisateurs de spécifier leurs exigences de sécurité à différents niveaux[41].

L'outil COBIT ou "Control Objectives for Information and related Technology" permet aux entreprises de satisfaire les exigences métiers et de gouvernance. A cet effet, il fournit un cadre de référence, faisant autorité, du contrôle de la gouvernance. Toutefois COBIT n'est pas uniquement orienté sur la sécurité de l'information mais bien sur tout ce qui tout touche à la gouvernance de l'information et il inclut donc la sécurité. Il reste néanmoins une référence importante, ne serait-ce que pour son utilisation de modèles de maturité, permettant aux entreprises de connaître la qualité de la gestion de leur système d'informations[29].

1.7 Mise en contexte du mémoire

Le contexte étant désormais établi, cette section situe le cadre dans lequel ce mémoire s'applique. En effet, nous le montrons dans la section 1.1, les technologies de l'information sont très présentes dans les entreprises, et cela implique que la sécurité de l'information revêt une importance primordiale pour ces dernières, même si elles l'ignorent parfois.

De nos jours, il est vraiment impossible d'avoir son entreprise sans devoir mettre en place un système d'information, ni sans devoir utiliser des données dont il est nécessaire d'assurer la protection. Cela souligne la nécessité de fournir une méthodologie permettant à des utilisateurs, particulièrement les novices, de pouvoir identifier l'origine du danger, les menaces et les risques pesant sur leur société, mais aussi leurs biens essentiels qui peuvent en être les victimes. En effet, ce n'est que par une prise de connaissance du risque, contextualisée dans le périmètre de l'organisation réalisant l'étude, qu'il sera possible à celle-ci de mieux appréhender les enjeux de la sécurité de l'information.

Dans le cadre qui nous intéresse, même si l'utilisation de standards tels que la famille des ISO/IEC 2700x, ou encore de méthodes d'analyse de risque comme EBIOS, MEHARI ou OCTAVE, permettrait de solutionner le problème, la consultation et l'emploi de leurs documents sources nous amènent à conclure que ces solutions s'adressent à un public ayant de trop bonnes connaissances techniques en sécurité de l'information, et plus de temps et d'expérience pour pouvoir mettre en place ces pratiques et réaliser des études complètes et pertinentes, par rapport au public que nous ciblons. En effet, les standards sont trop génériques pour les organisations qui souhaiteraient une méthodologie s'adressant à elles de manière claire et directe. De plus, les méthodes d'analyse de risque sont trop longues à réaliser que pour motiver ces organisations à les utiliser et trop abstraites pour leur permettre d'en comprendre facilement le fonctionnement et les résultats.

Tout cela met en évidence l'absence de méthodologies suffisamment faciles à employer par des utilisateurs novices et permettant de réaliser une évaluation de la maturité en termes de sécurité de l'information selon les contraintes auxquelles nous sommes tenus : rapidité, simplicité, auto-portance, aspect didactique de la méthodologie (voir section 3.1), etc. En effet, même si l'on considère OCTAVE Allegro comme une réponse possible à cette problématique, car cette méthode est justement prévue pour des personnes ayant très peu de connaissances dans le domaine de la sécurité de l'information, elle reste néanmoins trop complexe et ne satisfait pas les exigences de simplicité auxquelles nous sommes tenus.

Ainsi, une piste s'offre à nous pour aider les sociétés à identifier leurs besoins de sécurité et leur niveau de maturité en termes de sécurité de l'information : la

création d'une méthodologie supportée par un outil interactif et permettant, au travers de questions compréhensibles menées par l'exemple, de mettre en évidence les biens importants d'une entreprise, les besoins de sécurité liés à ceux-ci, les biens supports permettant de les soutenir, les menaces qui sont susceptibles de présenter un danger pour ces derniers, et les vulnérabilités qui rendent ces menaces possibles. Tout cela permettra de déterminer la maturité en termes de sécurité de l'information au travers de l'affichage des niveaux de risque liés aux biens essentiels de l'entreprise, dans une forme compréhensible par un utilisateur sans connaissances particulières dans le domaine de la sécurité de l'information.

Toutefois, une autre solution était envisageable. Il s'agissait de créer un questionnaire reprenant les points importants de standards tels que l'ISO/IEC 27002 afin de rapidement mettre en évidence les problèmes de sécurité d'une entreprise. Cependant, cette option était de loin impraticable si l'on considère le public cible et les contraintes auxquelles nous sommes tenus : rapidité, simplicité, auto-portance, aspect didactique de la méthodologie (voir section 3.1), etc. En effet, elle n'aurait aucunement solutionné la problématique principale, c'est-à-dire trouver un moyen de rapprocher le domaine de la sécurité de l'information des utilisateurs, et non l'inverse, et nous nous serions retrouvés avec une méthode de plus utilisable uniquement par des personnes avec des connaissances spécifiques, ou bien aidées par des experts.

Bien qu'aucun des deux choix ne soit idéal, le premier car il y a un principalement un risque de perte d'information dans le processus d'adaptation des contenus pour un public novice, et le deuxième, à cause de la probabilité non négligeable que notre public cible ne sache pas comment l'utiliser. Cependant, à nos yeux, la première proposition fournira le début d'une bonne solution permettant de familiariser les utilisateurs avec le domaine de la sécurité de l'information.

Ce mémoire est par ailleurs fort inspiré par les documents EBIOS et les ISO/IEC 27002 et 27005, entre lesquels il effectue divers croisements dont nous parlerons plus loin dans ce document. Il est impossible d'identifier des correspondances parfaites entre les éléments des différents supports, notamment entre les pratiques de l'ISO/IEC 27002 et les vulnérabilités de l'ISO/IEC 27005, la tâche étant d'une difficulté conséquente.

Néanmoins, nous nous sommes servis de ces documents, ainsi que, bien entendu, d'autres inspirations, comme base principale pour la réalisation de la méthodologie. Cela comprend la dernière version de 2010 de la méthodologie et de la base de connaissances EBIOS, ainsi que la version de 2013 et 2008 des ISO/IEC 27002 et 27005. Le but était de prendre des connaissances déjà reconnues, validées et communément acceptées par des experts afin de nous concentrer sur la création des questions, et d'établir les meilleurs liens entre les divers éléments des supports considérés. L'objectif final est de réaliser une mé-

thodologie, créée à partir d'un travail sur ces documents, dont le fonctionnement est automatisé grâce à un outil et de tester ce produit aux seins d'entreprises wallonnes ayant accepté de participer à cette expérience. Ces tests permettront aussi de mettre en évidence les forces et les faiblesses de la méthode, de l'outil, et de sa documentation, ainsi que d'éventuelles pistes d'amélioration.

Le développement de la méthodologie s'est déroulé en trois étapes qui sont abordées au cours des différents chapitres.

Le chapitre 2 présente la démarche suivie pour réaliser le développement du modèle de données et d'activités de la méthodologie et nous les illustrons en fin de chapitre.

Le chapitre 3 illustre les hypothèses de la méthodologie, les objectifs dérivés de ces dernières, mais aussi son contenu et les méthodes employées pour dériver les questions et les réponses à partir d'informations bas niveau. En outre, il présente les liens des questions avec le domaine de la sécurité et entre elles, ainsi que la création des échelles de valeurs des ensembles de réponses des questions.

Le chapitre 4 aborde le développement des formules de calculs de la méthodologie. Nous expliquons les méthodes employées, nous présentons les formules plus loin dans le chapitre et nous nous en servons afin de définir des intervalles d'inacceptabilité des scores de résultats d'une évaluation.

Le chapitre 5 présente la validation de la méthodologie. Il décrit la démarche suivie pour approcher les entreprises, le déroulement des tests et aussi les résultats obtenus.

Le chapitre 6 présente les limites de la méthodologie, mises en évidence grâce aux résultats de la validation, et les pistes de solutions visant à les adresser.

Finalement, l'outil, en automatisant la méthodologie décrite dans le document, fournira à un utilisateur les moyens de réaliser une évaluation de la maturité en termes de sécurité de l'information de son entreprise par la mise en évidence des niveaux de risque qu'encourt sa société. Ces niveaux sont calculés automatiquement et utilisent les questions, leurs liens, leurs réponses et les valeurs assignées à ces réponses afin de déterminer les scores qui sont ensuite attribués à différents graphiques. Ils s'adressent surtout aux novices utilisant la méthodologie, cependant une représentation sous la forme d'un modèle de maturité illustrera les résultats d'une évaluation pour les utilisateurs avec de meilleures connaissances. Cet outil, pour reprendre un cas vécu comme exemple, permettra au gérant d'une petite entreprise de se rendre compte que malgré des besoins de sécurité élevés, le risque auquel son entreprise est exposée n'est pas aussi important qu'il ne le pensait durant la complétion du questionnaire, ou encore, en gardant le même exemple, de se rendre compte de vulnérabilités auxquelles il ne pensait pas mais qui sont relativement faciles à résoudre.

Chapitre 2

Modélisation de la méthodologie

Dans ce chapitre, nous allons présenter les schémas de modélisation que nous avons empruntés, développés et utilisés afin de créer le modèle de données de la méthodologie, ainsi que pour illustrer son déroulement. Nous expliquerons les démarches suivies pour les réaliser, mais nous parlerons aussi de leur contenu et du rôle qu'ils jouent dans le développement de la méthodologie.

2.1 Besoin de modéliser l'approche

La méthodologie vise à réaliser une évaluation de la maturité en termes de sécurité de l'information dans une entreprise, par la mise en évidence du niveau de risque des entreprises, via un questionnaire permettant d'illustrer les concepts de la gestion du risque et de les articuler clairement et logiquement afin d'obtenir des résultats présentables selon plusieurs formats, au travers de graphiques pour les novices et d'un modèle de maturité pour les experts. Cette méthodologie doit aussi permettre de générer un rapport contenant entre autres des recommandations visant à aider les utilisateurs à traiter le risque.
Cet énoncé met en évidence plusieurs problématiques :

1. La première porte sur la forme et le contenu d'un questionnaire, ce qu'il permet de faire et quels en sont les éléments constitutifs.
2. Ensuite, il nous convient de proposer un modèle récapitulant les concepts principaux de la gestion du risque et, idéalement, intégrant le principe des métriques afin de permettre des calculs sur le niveau de risque.
3. Par après, nous devons évidemment pouvoir nous inspirer des deux schémas précédents afin de structurer notre approche, de déterminer quelle

forme prendra le questionnaire et quels éléments propres à la gestion du risque seront inclus dans le modèle.

4. Enfin, le dernier problème est d'établir un lien entre les concepts de ces deux domaines, afin de savoir quels concepts du questionnaire seront analogues à ceux de la gestion du risque et comment ces relations permettront au modèle final d'illustrer une évaluation de la maturité en termes de sécurité de l'information susceptible de permettre le calcul de son niveau dans une entreprise.

A cet effet, nous proposons plusieurs diagrammes de classes UML, qui seront abordés dans les sections suivantes et qui illustreront la démarche de construction du schéma de données final de la méthodologie.

Finalement, une fois cette étape accomplie, il sera important de considérer le déroulement de la méthodologie. En effet, avant de pouvoir commencer son développement, il est nécessaire d'avoir sa structure, mais aussi, de savoir comment la démarche se déroulera, c'est-à-dire les actions qu'elle permettra à un utilisateur de réaliser, ou celles dont elle se chargera elle-même, la suite logique du processus proposé, etc. Il est évidemment utile de déterminer toutes ces informations afin d'être sûr, à tout moment du développement, de ce qu'il se passe dans la méthodologie et surtout des informations dont on doit disposer à telle ou telle étape du parcours. A cet effet, nous proposons un diagramme d'activités UML. Nous en profiterons pour expliquer la démarche appliquée pour son développement, son utilité et les informations qu'il véhicule.

2.2 Structure de la méthodologie

La structure de la méthodologie ne s'est pas définie en une seule fois. Il s'agit d'un travail itératif appliqué en vue de produire pas à pas un modèle exprimant tous les concepts jugés utiles pour cette méthodologie.
Nous avons décidé de suivre cette démarche de construction progressive après avoir identifié les problèmes, dont nous avons parlé dans la section précédente, auxquels nous allons répondre dès maintenant.

2.2.1 Modèle générique d'un questionnaire

Dans le but de répondre à la première problématique de ce chapitre, nous proposons un modèle générique et aussi complet que possible de la structure d'un questionnaire. Afin de le réaliser, nous nous sommes inspirés d'un formalisme[31], abordé dans la section 1.4, décrivant l'agencement de tels formulaires, sous la forme d'un schéma DTD, mais aussi les attributs caractéristiques qui les constituent.

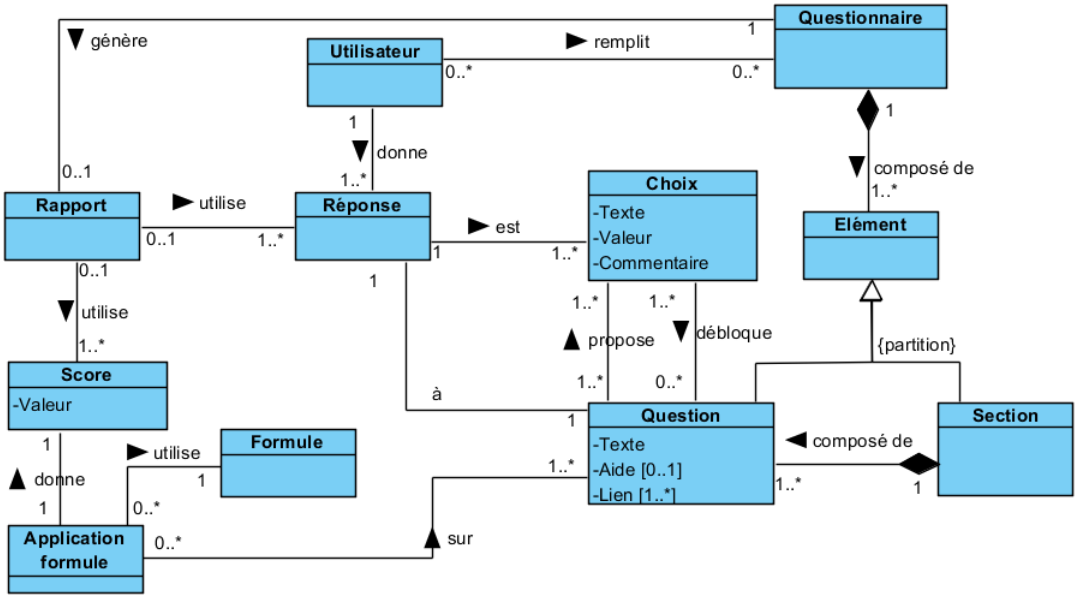


FIGURE 2.1 – Modèle générique d'un questionnaire

Nous sommes ainsi partis de cette base afin de créer un premier schéma, et nous l'avons enrichi de concepts complémentaires soit issus du bon sens, soit mis en évidence lors de discussions avec des experts du domaine.
La figure 2.1, dont nous allons vous présenter le contenu, montre le diagramme de classes UML illustrant les concepts d'un questionnaire.

Comme ce diagramme le montre, un questionnaire est un objet composite fait d'éléments qui sont soit des sections, soit des questions, soit un mélange des deux. Chaque section est elle-même composée de questions. Nous avons choisis d'utiliser la relation de composition, c'est-à-dire la variante plus contraignante de l'agrégation, afin de souligner deux informations. La première est que les concepts de Questionnaire et de Section n'ont de sens qu'à partir du moment où leurs composés existent car il est évident, par exemple, qu'un questionnaire doit contenir des questions pour recevoir cette qualification, et ensuite, pour appuyer sur le fait que la destruction d'une instance de ces concepts implique la destruction de leurs composés, qu'ils contiennent.

Ensuite, une question est un un objet possédant un texte, proposant une aide pouvant prendre la forme, par exemple, d'une documentation ou d'un texte explicatif, et cet objet peut être lié à d'autres questions. En effet, chaque interrogation propose plusieurs choix et ces derniers peuvent débloquer d'autres questions grâce aux liens existants entre elles. Un choix est composé d'un texte, c'est-à-dire la proposition de solution, d'une valeur, une appréciation de son importance afin de réaliser des calculs, et d'un commentaire, présenté à l'utilisateur

dès la sélection de l'alternative. Par ailleurs, certains choix sont communs à plusieurs questions, par exemple, le choix binaire oui/non est très commun comme réponse à une question.

Notons également qu'un questionnaire est un objet auquel plusieurs utilisateurs peuvent répondre et réalisable plusieurs fois. Chaque personne en faisant l'usage peut sélectionner plusieurs réponses, chacune propre au répondant et associée à une question spécifique. Chaque question ne possède qu'une seule réponse, cependant, celle-ci peut être soit un choix unique, soit un ensemble de choix, et toute réponse peut être utilisée pour la génération d'un rapport unique au questionnaire. Nous avons choisi de rendre facultative la relation de Questionnaire vers Rapport car ils n'en proposent pas tous.

Finalement, un questionnaire est souvent accompagné de formules de calculs, ces dernières s'appliquent aux questions afin de calculer des scores qui seront eux-mêmes employés pour la génération du rapport. Une formule peut être appliquée à une ou plusieurs questions à la fois et les questions peuvent faire l'objet de calculs différents. Par transition, on peut voir que les formules utilisent les valeurs des choix qui correspondent à la réponse d'un utilisateur à une question.

2.2.2 Modèle de gestion du risque enrichi avec des métriques

Ce modèle présente le domaine de la gestion du risque pour la sécurité des systèmes d'information. Ainsi, il comprend tous les concepts nécessaires à une évaluation complète du risque.

Ce schéma n'est pas le nôtre et nous l'avons repris du livre de M. Nicolas Mayer[34] car il est complet, illustre clairement les liens entre les divers éléments nécessaires à la gestion du risque et intègre des métriques pour justement mesurer le niveau de risque.

Ce modèle est très intéressant pour cette méthodologie car il répond à la deuxième problématique de ce chapitre en nous donnant une base complète des concepts de l'évaluation du risque. De plus, cette dernière, couplée avec les concepts de la section précédente, nous servira pour la problématique suivante car leur étude nous permettra de déterminer les éléments dont nous souhaitons tenir compte dans la méthodologie et illustrer au travers de son questionnaire. La figure 2.2, dont nous allons parler, montre le diagramme de classes UML des concepts du domaine de la gestion du risque. Nous n'en décrivons pas tous les détails car ces informations sont disponibles dans le livre dont nous nous inspirons.

Il y a dans ce diagramme de classes deux parties qui nous intéressent particulièrement. La première est la description du risque et la seconde est sa relation

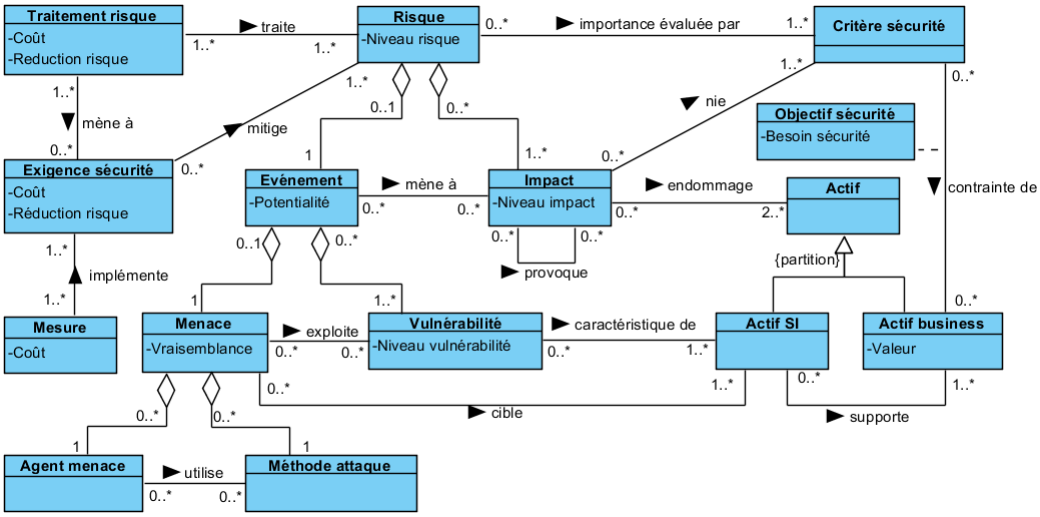


FIGURE 2.2 – Modèle du domaine ISSRM enrichi avec des métriques [34]

avec les actifs organisationnels.

Tout d'abord, le modèle présente le risque selon une structure hiérarchisée de plusieurs agrégations. Selon celle-ci, le risque est le résultat de la combinaison d'un événement et de ses impacts, eux-mêmes capables d'en causer d'autres, sur les actifs d'une organisation. Son niveau est déterminé en fonction des caractéristiques de ces deux concepts, respectivement la potentialité et le niveau d'impact. Ensuite, un évènement est la concrétisation d'une menace au travers des vulnérabilités qu'elle peut exploiter et son ampleur dépend des caractéristiques de vraisemblance de la menace et des niveaux d'exploitabilité des vulnérabilités. Enfin, les menaces sont identifiées via les agents menaçants et spécifiées par la détermination de la méthode d'attaque employée. Etant donné qu'un agent est capable de menacer une organisation en utilisant diverses tactiques, chaque couple attaquant-méthode identifiable définira une nouvelle menace.

Ensuite, il convient de parler des liens entre risque et actifs, qui sont au nombre de trois. Le premier spécifie que l'ampleur du risque dépend des critères de sécurité identifiés pour les actifs business concernés, car chacun d'eux définit un besoin de sécurité propre au bien. Il s'agit ici d'attributs tels que la confidentialité, l'intégrité et la disponibilité. Ceci implique que les impacts du risque sur les actifs business sont déterminés par leurs besoins de sécurité. Le second lien se trouve au niveau des impacts. En effet, chaque menace concrétisée a un impact sur au minimum deux actifs d'une société, un actif business et celui de support auquel il est fatalement lié. Le dernier lien se trouve au niveau des menaces. De fait, elles ciblent des actifs supports spécifiques, qui eux-mêmes possèdent des vulnérabilités particulières. Ainsi, une menace qui vise un support, exploite les

vulnérabilités de ce dernier et provoque un impact à la fois sur le support et le business, au travers du lien illustré ci-dessus.

Finalement, à partir d'un tel modèle, il nous est désormais plus facile de faire une analyse dans le but de déterminer quels sont les concepts dont nous avons besoin pour l'évaluation du niveau de risque. Ainsi, nous sommes plus à même d'en produire une version simplifiée, toujours cohérente et de la lier ensuite aux concepts d'un questionnaire, comme nous le montrons dans les sections suivantes.

2.2.3 Structuration de la méthodologie : Modèle de gestion du risque et Questionnaire

Dans les deux sections précédentes, nous avons illustré un modèle générique pour les questionnaires et un modèle complet pour la gestion du risque. Dès lors, afin de répondre à la troisième problématique, nous allons nous en inspirer dans le but de développer la structure finale de la méthodologie.
A cet effet, nous débutons avec la gestion du risque en proposant un modèle synthétique et nous finissons avec le questionnaire dont le modèle est modifié et enrichi afin de mieux répondre à nos attentes.

Tout d'abord, la figure 2.3 montre notre vision de la gestion du risque. Il s'agit d'une version réduite de la figure 2.2 car la méthodologie développée dans ce document propose une vision simplifiée visant à faciliter l'appréhension de ce domaine par les utilisateurs.

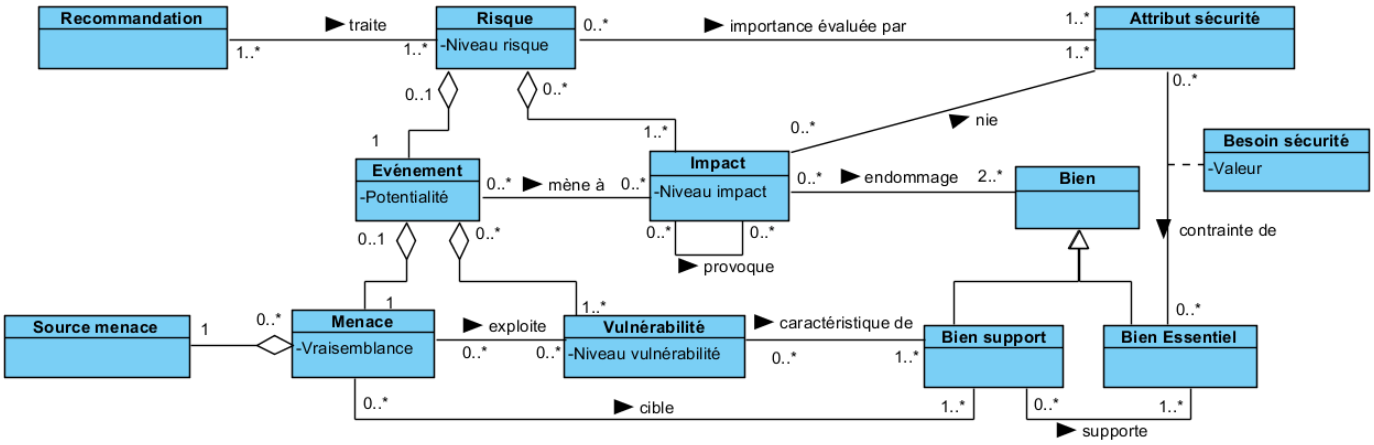


FIGURE 2.3 – Modèle de gestion du risque

Afin de la développer, nous avons sélectionné les concepts nécessaires et suffisants à une analyse de risque, ainsi que ceux nécessaires au calcul de sa valeur et le concept de traitement du risque. Cela inclut les éléments suivants : les

agents menaçants, les menaces, les vulnérabilités, les événements, les impacts, le risque, les actifs, les attributs, les besoins de sécurité et les mesures de sécurité.

Par après, nous avons renommé certains de ces concepts selon les termes EBIOS pour les rendre plus compréhensibles, sans pour autant perdre leur sens premier, par exemple, Actif business devient Bien essentiel et Agent menaçant devient Source de menace. Les objectifs de sécurité ont été retirés car nous préférons déterminer les besoins de sécurité directement à partir des valeurs d'importance des attributs de sécurité pour les biens essentiels sur lesquels ils portent. Nous rajoutons le concept de Recommandation, représentant celui de Mesure dans la figure 2.2, car le but de la méthodologie est aussi de fournir des conseils aux utilisateurs afin de mitiger le risque.

Enfin, nous retirons l'attribut valeur pour les biens essentiels car une fois identifiés, il n'est pas nécessaire de les classer selon leur importance, ce que les utilisateurs sont tout à fait capables de déterminer par eux-mêmes, mais selon leur niveau de risque. De plus, l'importance des biens essentiels n'entre pas en compte pour le calcul de leur niveau de risque. Pour ces deux raisons, elle n'est donc pas nécessaire à la méthodologie.

Ensuite, la figure 2.4 est une version enrichie de la figure 2.1, dans laquelle nous avons effectué plusieurs modifications.

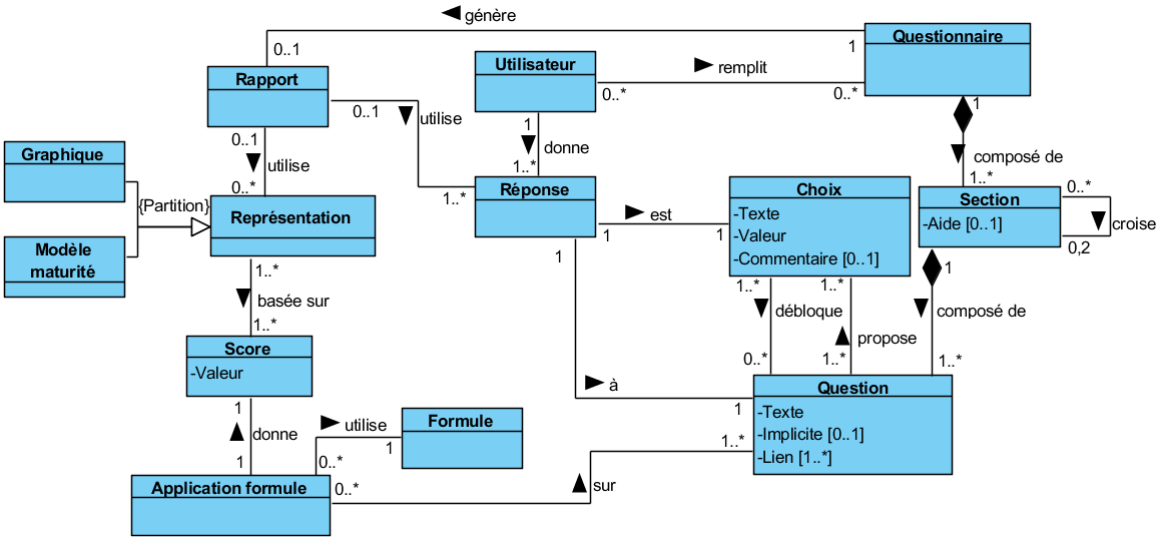


FIGURE 2.4 – Modèle du questionnaire

Tout d'abord, nous simplifions la structure d'un questionnaire en retirant le concept Element, afin de ne plus avoir de questions qui n'appartiennent à aucune section. Cela permettra de clarifier la séparation des contenus des dif-

férentes sections, mais aussi de faciliter l'attribution des résultats des calculs. Nous transformons l'attribut Commentaire du concept de Choix en un attribut facultatif car il alourdit le questionnaire mais il est intéressant de le garder afin de proposer des messages pour mieux guider l'utilisateur, si cela s'avère nécessaire. Nous gardons l'attribut facultatif Aide mais nous le déplaçons au niveau du concept de Section. En effet, les questions de la méthodologie sont prévues pour être aussi simples et compréhensibles que possible, ainsi il n'est pas forcément nécessaire de fournir une mise en contexte ou des explications, mais le cas échéant, il est plus léger pour la méthodologie de proposer cette aide au niveau de la section tout entière plutôt que question par question.

Par après, nous introduisons la relation de croisement de sections. Ainsi, une section peut faire le lien entre 0 ou deux autres sections du questionnaire, il s'agit alors d'une section de croisement, mais elle peut aussi faire l'objet d'un croisement dans 0 à plusieurs sections de croisement, il s'agit alors d'une section normale. Nous modélisons le croisement de sections afin de pouvoir établir des liens entre plusieurs concepts de la gestion du risque, notamment les biens supports et les biens essentiels. En effet, nous avons mis en évidence précédemment qu'un impact s'applique au moins à deux actifs, un de support et un essentiel, et cela souligne le fait que le calcul du niveau de risque doit avoir connaissance de ces relations afin de s'effectuer correctement. Par ailleurs, il est important de noter qu'une section de croisement, à l'inverse d'une section normale, est uniquement composée de questions implicites, c'est-à-dire qu'elle contiendra les description des questions à croiser, et non des questions telles que : "Tel élément est-il supporté par tel autre?". A cet effet, nous avons rajouté l'attribut facultatif Implicite dans le concept de Question pour illustrer que les questions des sections de croisement sont sous-entendues par les descriptions des questions à croiser.

Ensuite, nous avons modifié la cardinalité du lien entre les concepts de Réponse et de Choix, car même si le questionnaire proposera toujours des choix multiples de solution, une réponse correspondra à un et un seul choix, pour chaque question. De plus, nous rajoutons le concept de Représentation, qui comprend deux manières de communiquer les scores d'évaluation du risque, soit sous la forme de graphiques pour les novices, soit sous la forme de modèles de maturité pour les experts, et nous le lions au concept de Rapport car il pourra en faire partie.

Finalement, dans cette section nous avons créé, et enrichi selon nos besoins, la structure d'une approche de l'évaluation du risque au travers d'un questionnaire. Cependant, il reste encore à faire le lien entre ces deux domaines de manière à comprendre comment la méthodologie permettra d'illustrer les concepts du risque et de réaliser des calculs de scores pour donner une valeur au risque.

2.2.4 Identification des liens entre la structure du questionnaire et celle du modèle de gestion du risque

Maintenant que nous avons la structure finale des deux domaines principaux de la méthodologie, il convient d'établir les liens qui les unissent, afin de déterminer quelle partie du questionnaire s'occupera de quelle partie de l'évaluation du risque et de savoir quelles données seront utilisées dans ces différentes parties. Une fois ces liens mis en évidence et expliqués, nous serons plus à même de déterminer les étapes de cette méthodologie et leur enchaînement.

La figure 2.5 présente le diagramme de classes UML final de la méthodologie. Dans celui-ci, nous réalisons un lien malheureusement vague entre ce que nous appelons des thèmes de sécurité et les deux concepts principaux d'un questionnaire, soit Section et Question. Cependant, voici l'information que nous souhaitons véhiculer au travers de ces relations.

Tout d'abord, chaque thème sera illustré par au moins une section et les questions de cette section seront inspirées de ce même thème, ou de ses attributs. Cela implique des questions sur, par exemple, les menaces et leur vraisemblance.

Ensuite, le lien entre Bien essentiel et Attribut sécurité met en évidence plusieurs éléments. Le premier est l'existence de questions permettant d'identifier, pour chaque bien, quels sont les attributs à considérer pour leur évaluation et l'importance de leur besoin de sécurité. Le second est que la section regroupant ces diverses questions sera celle qui illustre le concept de Bien essentiel. En effet, leurs liens impliquent la nécessité de les rassembler afin d'avoir un questionnaire cohérent. Le dernier est que les thèmes sont accompagnés de métriques, de telle manière que les choix de solution des questions inspirées de ces thèmes, par exemple celles portant sur la vraisemblance ou les besoins de sécurité, devront refléter les échelles de valeurs correspondantes. Ainsi, il y aura des questions sur l'importance des besoins de sécurités pour les différents attributs et les choix possibles correspondront aux diverses valeurs des échelles analogues.

Finalement, le concept de Section et les liens avec le concept de Thème sécurité et les concepts de la gestion du risque nous permettent de justifier la mise en place des étapes du questionnaire méthodologique sous la forme de sections. La partie gestion du risque de la figure 2.5, combinée avec les connaissances acquises dans les documents des méthodes illustrées dans la section 1.3 et de l'ISO/IEC 27005 dans la section 1.2.6, nous permet de déterminer les étapes suivantes de la méthodologie : l'identification des sources de menaces, des biens essentiels avec leurs besoins de sécurité, des biens supports, des menaces avec leur vraisemblance, et des vulnérabilités. Les liens entre sources de menaces, biens essentiels et biens supports varient d'une évaluation à l'autre. Ainsi, il est nécessaire de prévoir un moyen manuel de croiser les éléments de ces étapes.

L'existence de sections qui peuvent en croiser deux autres permet justement de mettre en place ces liens. Ainsi, nous identifions deux nouvelles étapes : l'établissement des liens entre les sources de menaces et les biens essentiels et entre les biens supports et essentiels. Les deux dernières étapes sont issues de la partie questionnaire du modèle mais leur lien avec le concept de Section les rattache de manière évidente aux concepts de la gestion du risque du modèle. Il s'agit des étapes de calcul des scores, c'est-à-dire les valeurs numériques des réponses aux questions des sections mises en évidence ci-dessus, et la génération d'un rapport utilisant les données de toutes les étapes précédentes pour se construire.

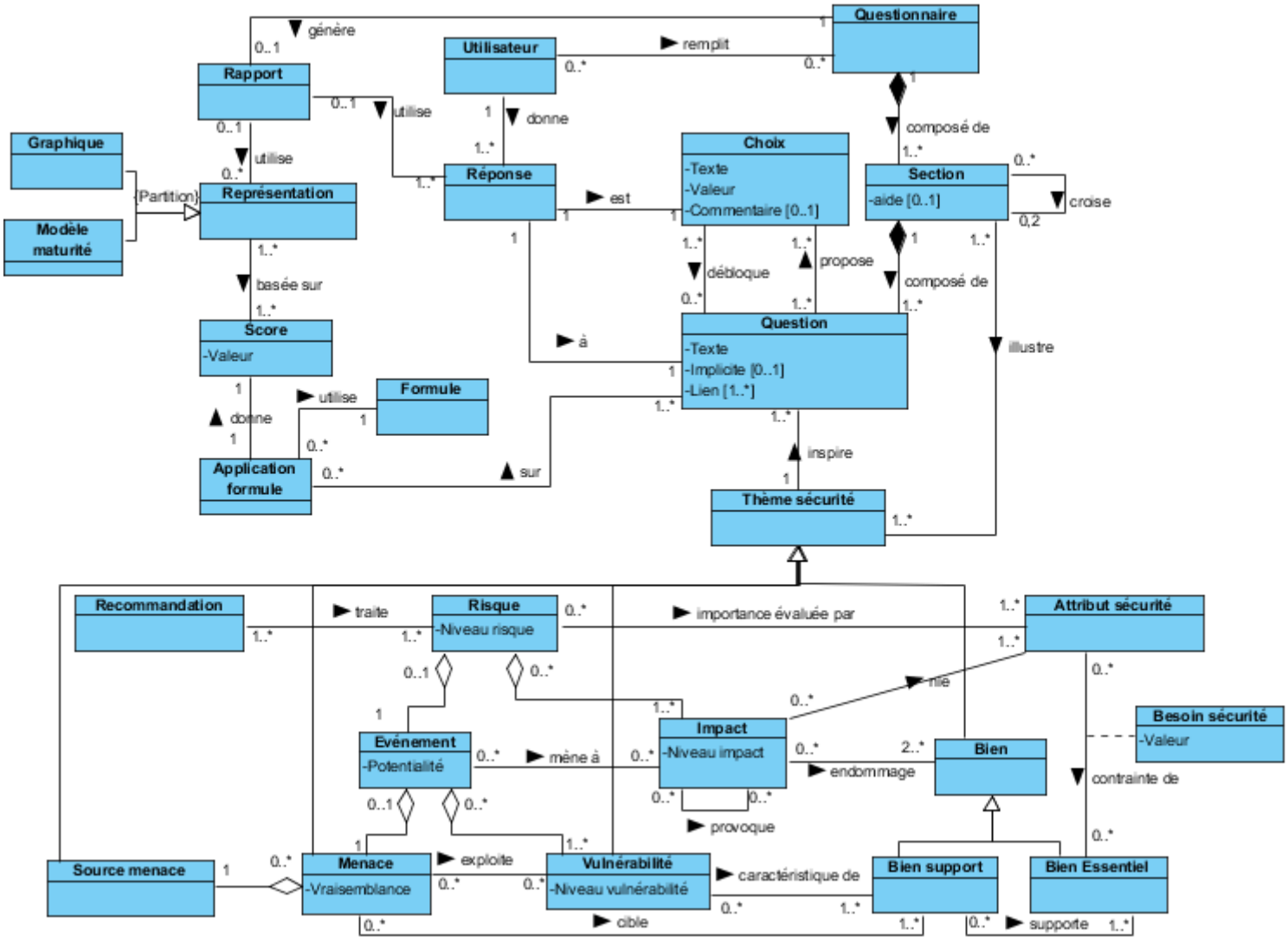


FIGURE 2.5 – Modèle final de la méthodologie

2.3 Déroulement des étapes de la méthodologie

Maintenant que les étapes de la méthodologie sont identifiées, il reste seulement à définir l'ordre dans lequel elles se dérouleront, ainsi que leurs activités, et le rôle des acteurs prenant part au processus. Ceci nous permettra d'avoir une meilleure compréhension des liens entre les diverses étapes.
Afin de réaliser cette tâche, nous nous sommes inspirés de la figure 1.1 présentant le processus de gestion du risque et nous avons développé un processus illustré à la figure 2.6 sous la forme d'un diagramme d'activités.

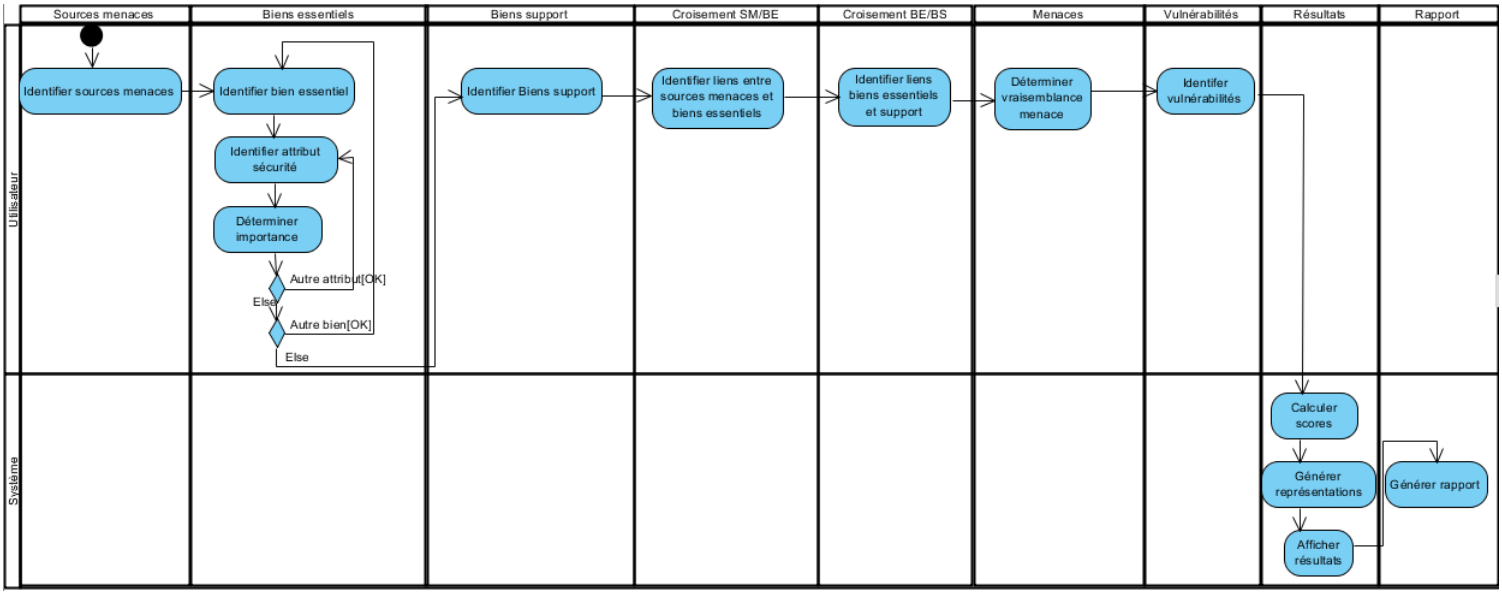


FIGURE 2.6 – Diagramme d'activités de la méthodologie

Le processus de gestion du risque commence avec l'établissement du contexte, et ainsi, nous avons décidé de mettre les étapes illustrant ce principe en premier, c'est-à-dire les parties sources de menaces, biens essentiels et biens supports, contenant chacune des questions servant à les identifier, mais aussi les deux matrices de croisement permettant de faire le lien entre les sources de menaces et les biens essentiels et entre ces derniers et les biens supports. Il est important de noter que l'identification des biens essentiels passe par la détermination des besoins de sécurité de ces derniers qui, comme le montre le modèle de données de la méthodologie à la figure 2.5, permettront de pondérer l'importance du risque.

Ensuite, nous avons la partie analyse de risque, couverte par les étapes d'identification des menaces avec leur vraisemblance, et des vulnérabilités.
Par après, il y a l'évaluation du risque illustrée par l'étape de calcul des scores

qui se charge aussi de les afficher. Bien évidemment, ces derniers sont calculés selon les réponses aux questions des étapes précédentes, qui attribuent des valeurs aux facteurs de vraisemblance, des besoins de sécurité et d'exploitabilité des vulnérabilités.

Finalement, la dernière partie du processus, c'est-à-dire le traitement du risque avec sa communication et sa surveillance, est permise grâce à l'étape finale qui se charge de générer le rapport pour faire la synthèse de l'évaluation et de proposer des recommandations afin de mitiger le risque.

2.4 Conclusion

Au cours de ce chapitre, nous avons décrit la démarche employée dans la création d'un modèle de données et suivit sa construction au cours de quatre étapes. Ensuite, ayant identifié les principales étapes de la méthodologie, nous avons développé un diagramme d'activités décrivant le déroulement de cette dernière et mettant en évidence les acteurs et leurs rôles dans les différentes étapes de la méthodologie. L'analyse de ces résultats nous permet de tirer plusieurs conclusions.

Tout d'abord, la création de ces diagrammes nous permet d'avoir une meilleure idée de la structure de la proposition de solution mais aussi du contenu de chaque étape, par exemple, la partie sur les biens essentiels contiendra des questions pour identifier ces derniers, mais aussi et surtout leurs besoins de sécurité.

De plus, l'étude des diagrammes nous permet de mettre en évidence des informations utiles pour les étapes suivantes. En effet, grâce aux modèles, nous sommes en mesure de déterminer que les sources de menaces et les biens supports pourront être utilisés afin de proposer des menaces spécifiques au contexte de l'entreprise et de même pour les vulnérabilités qui sont déterminées en fonction des menaces et des biens supports. En outre, les matrices de croisement devront utiliser les données du contexte, soit sources de menaces, biens essentiels et biens supports, afin de lier ces différents concepts. Enfin, la génération des rapports nécessitera les données de tout le questionnaire afin d'être complet, précis et d'intégrer par ailleurs les calculs des scores, nécessitant eux-mêmes les informations des étapes qui les précèdent.

Finalement, la structure et le déroulement de la méthodologie établis, il convient de développer son contenu. Le chapitre suivant en présentera la construction, étape par étape.

Chapitre 3

Développement de la méthodologie

Dans ce chapitre nous allons présenter la teneur de la méthodologie. En effet, après avoir mis en évidence sa structure de données et son enchaînement, il convient de passer à la phase de développement du contenu : les questions des différentes étapes, leurs réponses et les échelles de valeurs correspondantes. A cet effet, nous débuterons avec les hypothèses et les objectifs de la méthodologie et nous continuerons avec la présentation, pour chaque étape identifiée dans le chapitre précédent, des objectifs visés par les questions, des démarches employées afin de les créer, et finalement, des résultats obtenus. Ensuite, nous expliquerons la méthode de création des échelles de valeurs des différents ensembles de réponses du questionnaire. Finalement, nous terminerons avec une rapide présentation de l'outil implémentant le questionnaire méthodologique.

3.1 Objectifs de la méthodologie

Avant de développer le contenu du questionnaire méthodologique, il est nécessaire d'établir les hypothèses et les objectifs. En effet, les hypothèses guident la création des objectifs et ces derniers orientent la construction des questions en définissant les besoins à satisfaire.

Toutefois, bien qu'il n'y ait qu'un seul ensemble d'hypothèses, nous identifions deux séries d'objectifs : la première contient ceux liés à la méthodologie et la seconde contient ceux liés à la conception de questionnaires. Les objectifs des deux séries ont été identifiés après plusieurs discussions avec les parties prenantes à ce projet et suite à la consultation de documents sur la conception de questionnaires, dont nous parlons dans la section 1.4. Il est important de noter

que la compréhension du processus cognitif de réponse à une question[11] a été d'une aide significative dans la spécification de ces objectifs, mais aussi lors de la construction des questions et des réponses.

Tout d'abord, voici la liste des hypothèses sur lesquelles nous nous appuyons :

1. Nous nous adressons aux petites et moyennes entreprises.
2. Le public cible souhaite connaître son niveau de maturité en termes de sécurité de l'information.
3. Le public cible n'a pas ou peu de connaissances dans le domaine de la sécurité de l'information.
4. Le public cible ne connaît pas ses besoins en termes de sécurité de l'information.
5. Le public cible souhaite réaliser une évaluation rapide.
6. Le public cible désire une méthodologie contenant toutes les informations nécessaires à la réalisation d'une évaluation.

Ces dernières permettent de dériver les objectifs, spécifiques à la méthodologie, dont voici la liste :

1. Proposer une méthodologie d'évaluation de la maturité en termes de sécurité de l'information dans une organisation.
2. Proposer des questions et des réponses à la portée de personnes sans connaissances particulières dans le domaine de la sécurité de l'information, et dont la seule lecture suffit à la compréhension des idées véhiculées.
3. Proposer des questions menées par l'exemple.
4. Intégrer une vocation didactique en permettant, au fur et à mesure de son utilisation, à un utilisateur d'améliorer sa familiarité avec le domaine de la sécurité, de comprendre ses besoins de sécurité et les faiblesses de son entreprise.
5. Proposer un nombre limité de questions et intégrer une fonction dynamique à la méthodologie, afin de ne pas surcharger l'utilisateur avec des questions qui ne le concernent pas.
6. Représenter les résultats sous forme de graphiques pour les novices et d'un modèle de maturité pour des personnes plus expertes.
7. Calculer des scores liés aux domaines de l'ISO/IEC 27002.
8. Permettre la génération d'un rapport contenant notamment des recommandations pour traiter le risque.
9. Automatiser la méthodologie grâce à un outil de support facile d'utilisation, d'installation et d'exploitation.

De plus, nous devons considérer les objectifs propres à la conception de questionnaires, dont voici la liste :

1. La formulation des questions et des réponses proposées par le questionnaire doit illustrer les concepts des objectifs des diverses étapes. Par exemple, les questions sur les biens supports devront mettre en évidence des biens supports.
2. Les termes employés doivent être compréhensibles et avoir le même sens pour tous.
3. Les questions et les réponses ne doivent pas être trop longues.
4. La formulation des questions et des réponses proposées par le questionnaire ne doit pas induire en erreur le répondant.
5. La formulation des questions et des réponses proposées par le questionnaire ne doit pas afficher de parti pris afin de ne pas influencer l'utilisateur dans sa réponse.
6. Les réponses doivent couvrir l'ensemble des possibilités.

Ces listes, bien que redondantes, déterminent la marche à suivre pour le développement des questions et des réponses. Dans cette optique, nous les gardons à l'esprit, ainsi que le processus cognitif de réponse à une question, afin de nous rappeler à tout moment ce que nous souhaitons accomplir, les raisons motivant les choix de développement, mais aussi les contraintes à respecter.
Il est important de noter que nous réalisons, dans le chapitre 5 de ce document, une validation de la méthodologie afin de vérifier la satisfaction de ces objectifs.

Finalement, les hypothèses et les objectifs définis, nous pouvons débuter la construction du contenu du questionnaire. Chacune des sections suivantes adressera une étape de la méthodologie, dont nous présenterons la description et les objectifs, la méthode employée pour créer les questions et les réponses, et nous terminerons par leur illustration.

3.2 Sources de menaces

3.2.1 Description et objectifs

Tout d'abord, les sources de menaces représentent l'origine des menaces qui pourraient cibler une entreprise. Bien que l'on puisse considérer un large panel de sources, il convient néanmoins de réfléchir et considérer celles qui représentent réellement un danger pour l'entreprise. Il est possible de les distinguer selon différents critères définis par EBIOS, dont voici la liste :

1. Humain ou Non-Humain.
2. Interne ou Externe, c'est-à-dire la facilité d'accès aux biens menacés.
3. Délibéré ou accidentel, si la source de menace est humaine.
4. La capacité à causer des dégâts, si la source de menace est humaine.
5. Son type, si la source de menace est non-humaine. Il définit la source à l'origine de la menace, dans notre cas, soit code malveillant ou événement interne.

Finalement, les questions de cette étape servent à déterminer l'origine des menaces pertinentes lors d'une évaluation, indépendamment du type de menace considéré. Il s'agit de permettre à l'utilisateur d'établir qui ou quoi pourrait représenter un danger à son entreprise au travers d'une suite de questions améliorant son appréhension du sujet. En effet, la structure de cette partie du questionnaire permet de raffiner les types et l'importance des sources de menaces au fur et à mesure de son déploiement. Mais nous reviendrons sur ce point dans l'illustration des questions de cette étape.

3.2.2 Méthode de création

Afin de créer ces questions, nous nous sommes intéressés à la base de connaissances EBIOS dont nous parlons dans la section 1.3.1. En effet, cette dernière contient une documentation complète et structurée des différents types de sources de menaces, accompagnées de leur définition, à considérer lors d'une analyse de risque.

Tout d'abord, nous avons séparé les deux ensembles principaux de sources de menaces, c'est-à-dire les sources humaines d'un côté et les non-humaines de l'autre. Ensuite, nous avons ajouté deux niveaux de profondeur au type humain, le premier permettant de déterminer les caractères délibéré ou accidentel, et interne ou externe des sources, et le second, permettant de définir la capacité à infliger des dommages.

Par après, les sources non-humaines proposent cinq sous-types et nous avons sélectionné les deux les plus susceptibles de représenter des sources de menaces

pertinentes dans le cadre de ce travail. Les codes malveillants car ils peuvent causer des dommages à tout type d'infrastructure informatique, et les événements internes, étant donné que nous nous intéressons aux entreprises et implicitement à leur fonctionnement interne. Toutefois, il est important de noter que les phénomènes et catastrophes naturels sont intégrés aux sources de menaces sous le terme "événements environnementaux" au niveau de la question racine. Cependant, il s'agit de situations extrêmes et nous préférons inclure des exemples de celles-ci directement au niveau des menaces, dans la section 3.6, afin de simplifier la tâche aux utilisateurs.

Finalement, comme nous le montrons dans la section suivante, nous avons lié ces questions ensemble, au travers des choix de réponses qu'elles proposent. Ainsi, une réponse à "Oui" débloquera des questions dépendantes si elles existent, tandis qu'un "Non" ne le fera pas.

3.2.3 Illustration des résultats

Les tableaux 3.1 et 3.2 présentent les résultats du travail d'analyse sur les sources de menaces. Dans chacun, la première colonne présente les questions, ordonnées, et montre visuellement leurs liens de dépendance. Par exemple, la question 1 permet de débloquer les questions 1.1, 1.2, 1.3 et 1.4, ou encore, la question 1.1 permet de débloquer les questions 1.1.1 et 1.1.2. Ces liens sont mis en évidence au niveau des relations entre les concepts de Choix et de Question du modèle de données dans la figure 2.5. La seconde colonne montre le ou les critères de distinction des sources de menaces.

Tout d'abord, il est intéressant de noter que la structure de cette partie du questionnaire et le fonctionnement des critères, analogue aux relations d'héritage, permettent de mieux appréhender les différentes sortes de sources. En effet, l'utilisateur commence par déterminer si elles sont humaines ou non et en suivant l'ordre des questions, et parcourant ainsi les critères de distinction des sources qu'elles illustrent, il finira par en obtenir une meilleure compréhension, et les exemples lui donneront des cas concrets auxquels associer ce qu'il aura appris. Par exemple, s'il identifie les sources de menaces 1.1.2 et 1.2.2, il saura que des personnes telles que des managers, des développeurs et des administrateurs sont des sources de menaces humaines, internes, à la fois accidentelles et délibérées, et dont la capacité à infliger des dégâts est importante.

Question	Critère
1. Pensez-vous que votre entreprise puisse être menacée par des personnes?	Humain
1.1. Pensez-vous que des personnes au sein de votre entreprise, c'est-à-dire qui collaborent avec elle et ont accès à ses bâtiments, à ses locaux et à son système informatique, puissent intentionnellement lui nuire, par vengeance, cupidité, idéologie, ego ou pour d'autres raisons?	Interne délibéré
1.1.1. Pourrait-il s'agir de stagiaires, de clients, de personnel d'entretien ou de toute autre personne n'ayant que des moyens limités pour accéder et agir sur le système, et des connaissances limitées de celui-ci?	Capacité faible
1.1.2. Pourrait-il s'agir de managers, de développeurs, d'actionnaires, de sous-traitants, de personnel de maintenance ou d'assistance à distance, d'administrateurs système ou réseau, ou d'autres personnes ayant des moyens importants pour accéder et agir sur le système, et des connaissances importantes de celui-ci?	Capacité forte
1.2. Pensez-vous que des personnes au sein de votre entreprise puissent accidentellement lui nuire, par maladresse, faute d'attention, manque d'information, malchance ou pour d'autres raisons ?	Interne accidentel
1.2.1. Pourrait-il s'agir de collaborateurs maladroits, ou mal informés sur ce que leur accès limité au système permet de faire, ou peu impliqués par leur travail et leurs responsabilités, de sous-traitants, de personnel d'entretien, de stagiaires, d'intérimaires, d'utilisateurs, ou de toute autre personne n'ayant que des moyens limités pour accéder et agir sur le système, et des connaissances limitées de celui-ci?	Capacité faible
1.2.2. Pourrait-il s'agir de managers, de développeurs, d'administrateurs, système ou réseau, de directeurs, ou de toute autre personne ayant des moyens importants pour accéder et agir sur le système, et une connaissance importante de celui-ci?	Capacité forte
1.3. Pensez-vous que des personnes extérieures à votre entreprise, c'est-à-dire qui n'ont pas ou plus de rapports professionnels avec elle, et ne sont pas sensés pouvoir accéder à ses bâtiments ni à ses locaux ni à son système informatique, puissent intentionnellement chercher à lui nuire?	Externe délibéré
1.3.1. Pourrait-il s'agir de vandales, ou de pirates du dimanche(script-kiddies) ou de toute autre personne capable d'occasionner des dégâts minimes à votre entreprise ou à son image?	Capacité faible
1.3.2. Pourrait-il s'agir de militants, de pirates expérimentés, de fraudeurs, d'anciens employés en colère, de concurrents, de journalistes ou de toute autre personne capable d'occasionner des dégâts importants à votre entreprise ou à son image?	Capacité forte
1.4. Pensez-vous que des personnes extérieures à votre entreprise puissent accidentellement lui nuire?	Externe accidentel
1.4.1. Pourrait-il s'agir des familles de votre personnel, de travailleurs dans la proximité de votre entreprise, de manifestants, de visiteurs, ou de toute autre personne capable d'occasionner des dégâts minimes à votre entreprise ou à son image?	Capacité faible
1.4.2. Pourrait-il s'agir de vos hébergeurs de données, ou de votre fournisseur d'accès internet, ou d'activités industrielles susceptibles de provoquer des catastrophes, ou d'explosions, ou d'impulsions électromagnétiques, d'équipements dangereux pour votre matériel, ou de toute autre personne ou nuisances qu'elles provoquent capables d'occasionner des dégâts importants à votre entreprise ou à son image?	Capacité forte

TABLE 3.1 – Tableau des sources de menaces - partie 1

Question	Critère
2. Pensez-vous que votre entreprise puisse être menacée par des événements environnementaux et/ou imprévisibles?	Non-humain
2.1. Pensez-vous que votre entreprise puisse être victime de codes malveillants d'origine inconnue, tels que des virus de fichiers, du secteur d'amorçage, multipartites, compagnons, ou des chevaux de troie, backdoors, adwares, spywares, vers, ... ?	Code malveillant
2.2. Pensez-vous que votre entreprise puisse être victime d'événements internes imprévisibles tels que des incendies, fuites de canalisation, accidents de travail, pannes de courant, une réorganisation, un changement de forme ou de type du réseau, ... ?	Evènement interne

TABLE 3.2 – Tableau des sources de menaces - partie 2

Ensuite, nous pouvons constater que les questions de second niveau vont en se simplifiant. En effet, elles illustrent deux critères à chaque fois. Ainsi, dès que l'un d'eux est défini dans une question, il n'est plus nécessaire de le répéter dans une autre. Par exemple, la question 1.4 ne définit pas les termes "extérieur" et "accidentel" car ils l'ont déjà été plus tôt dans le questionnaire. Il s'agit d'une tactique permettant de soulager la lecture et d'amener l'utilisateur à améliorer sa compréhension des concepts de ce sujet.

Finalement, les liens entre les sources de menaces et les menaces, modélisés dans la figure 2.5, sont placés au niveau des racines de cette étape. Ainsi, la première question de chaque tableau permettra d'affiner la sélection des menaces plus loin dans la méthodologie. Ce choix sera expliqué dans la section 3.6.

3.3 Biens essentiels

3.3.1 Description et objectifs

Tout d'abord, les biens essentiels sont le patrimoine informationnel d'une entreprise et certains les appellent actifs informationnels ou encore actifs business. Ils ne sont ni monétaires ni physiques mais sont constitués d'informations ou de connaissances.

Ensuite, nous avons décidé d'élargir la portée de la définition précédente en incluant des éléments tels que les services. En effet, ces derniers s'apparentent plus à des concepts qu'à des structures physiques véritables et font intervenir des connaissances et des informations potentiellement importantes à la société. Ce choix sera expliqué en même temps que la méthode employée pour créer les questions.

Finalement, les questions de cette étapes ont pour objectif de permettre l'identification des biens essentiels pertinents pour une évaluation, et pour chacun, de déterminer quels sont les besoins de sécurité dont ils doivent faire l'objet, mais aussi leur importance. Ces besoins, déterminés dans la section suivante, sont analogues aux attributs de sécurité traités dans le questionnaire et ils représentent l'ampleur des impacts des menaces sur les biens essentiels de l'entreprise.

3.3.2 Méthode de création

Afin de créer ces questions, nous avons suivi deux approches, la première afin d'identifier les biens essentiels, la seconde afin de savoir quels attributs de sécurité adresser en priorité.

Tout d'abord, nous avons développé un questionnaire, disponible dans l'annexe J servant de support pour des interviews réalisées en décembre 2014 auprès d'entreprises wallonnes. Elles avaient pour but de nous aider à établir le contexte des entreprises auxquelles nous nous intéressons. Parmi toutes les informations collectées, une des plus intéressantes concerne la mise en évidence des données, informations et autres biens essentiels aux organisations, dont nous nous sommes servis afin d'établir une liste de questions les reprenant.

Par ailleurs, c'est aussi à ce moment que nous avons décidé d'inclure l'élément "service" en tant que bien essentiel de cette méthodologie. En effet, les interviews ont mis en évidence l'existence de tels biens, sans pour autant nous permettre d'identifier les actifs informationnels utilisés en leur sein, à cause notamment de problèmes de confidentialité. De plus, chaque entreprise étant libre de mener ses affaires comme bon lui semble, un même service peut faire intervenir des actifs informationnels différents d'un contexte à l'autre. Ainsi, nous

avons choisi de nous servir de l'élément "service" comme bien essentiel regroupant les vrais biens essentiels propres à chaque entreprise, comme les questions 2 et 7 du tableau 3.3 le montrent.

Ensuite, après une révision des différents documents et des discussions, notamment avec les entreprises, nous avons choisi les attributs de sécurité les plus importants dans le cadre de ce travail, c'est-à-dire les attributs principaux du domaine de la sécurité de l'information : la confidentialité, l'intégrité et la disponibilité.

Finalement, nous avons créé des réponses spécifiques à la détermination de l'importance des besoins de sécurité. A cet effet, nous nous sommes inspirés des échelles par défaut proposées dans la méthode EBIOS et nous en avons dérivé des phrases compréhensibles et exploitables par les utilisateurs. Il est intéressant de noter que nous avons ajouté une réponse pour l'échelle de valeurs de l'intégrité. Elle représente l'absence d'un besoin de sécurité au niveau de cet attribut. Quant aux autres questions, elles proposent un choix binaire de réponses.

3.3.3 Illustration des résultats

Les tableaux 3.3 et 3.4 illustrent les résultats du travail d'analyse sur les biens essentiels et les besoins de sécurité.

Tout d'abord, le premier montre les biens essentiels et les questions qu'ils permettent de débloquer afin de déterminer l'importance des besoins de sécurité. Il est important de noter que les sous-questions du premier bien essentiel du tableau 3.3 seront disponibles pour les autres biens.

Ensuite, le second tableau montre les réponses aux questions servant à déterminer l'importance des besoins et chaque ensemble de réponses représente l'échelle de valeurs pour le besoin de sécurité de l'attribut associé.

Finalement, la structure de cette partie du questionnaire définit une hiérarchie de questions dont le parcours permet à l'utilisateur d'identifier aisément ses besoins de sécurité et de mieux comprendre les concepts de cette étape. En effet, elle le guide pas à pas en suivant le schéma suivant : identification du bien, identification de l'attribut et identification du besoin, avec l'identification implicite d'un impact de la concrétisation de menaces ciblant ce bien essentiel et cet attribut. De plus, ces questions sont formulées de manière à véhiculer clairement ces concepts afin d'aider davantage l'utilisateur.

Question	Type
1. Possédez-vous des données sur vos clients et/ou vos employés, par exemple des données à caractère personnel, telles que leurs habitudes commerciales, leur adresse, leurs fiches de salaire, leur numéro privé, ... ?	Bien essentiel
1.1. Serait-ce un problème si ces données étaient rendues publiques?	Confidentialité
1.1.1. Quelles sont les personnes qui devraient pouvoir accéder à ces données?	Importance
1.2. Serait-ce un problème si ces données étaient altérées, par des personnes autorisées ou non, de sorte à ne plus être vraie, à ne plus être comme elles sont supposées l'être, par exemple si les prix de vos articles étaient modifiés à votre insu pour que chaque valeur soit égale à 0, ou bien si les adresses de vos clients étaient altérées avant l'expédition de factures, ... ?	Intégrité
1.2.1. Jusqu'à quel point acceptez-vous que vos données soient altérées?	Importance
1.3. Serait-ce un problème si, durant vos activités, ces données étaient subitement inaccessibles, par exemple le support les contenants venait à disparaître, ou devenait inutilisable(cassé, abîmé, ...), ou encore si les données étaient supprimées, ou déplacées dans un emplacement inconnu, ... ?	Disponibilité
1.3.1. Pendant combien de temps pouvez-vous vous en passer?	Importance
2. Avez-vous un service de production des biens et services?	Bien essentiel
3. Possédez-vous des données sur les commandes de produits par vos clients?	Bien essentiel
4. Possédez-vous des données de facturation?	Bien essentiel
5. Possédez-vous des données de comptabilité?	Bien essentiel
6. Possédez-vous des données en rapport avec la recherche et le développement, que ce soit l'acquisition de connaissances, le développement de nouveaux produits, ou encore l'amélioration de produits existants?	Bien essentiel
7. Avez-vous un service après-vente?	Bien essentiel

TABLE 3.3 – Tableau des biens essentiels et des attributs de sécurité

Type	Réponse	Valeur
Confidentialité	Uniquement les personnes qui en ont besoin et possèdent les autorisations nécessaires	1
Confidentialité	Uniquement le personnel interne de l'entreprise qui est concerné par sa gestion, son utilisation, son exploitation, ...	0.666
Confidentialité	Le personnel de l'entreprise, les partenaires et les personnes en relation professionnelle avec l'entreprise	0.333
Confidentialité	N'importe qui	0
Intégrité	Les données ne peuvent absolument pas être altérées	1
Intégrité	Les données peuvent être altérées mais on doit pouvoir identifier celles qui l'ont été et on doit pouvoir revenir en arrière	0.666
Intégrité	Les données peuvent être altérées mais on doit pouvoir identifier celles qui l'ont été	0.333
Intégrité	Les données peuvent être altérées sans causer de problèmes	0
Disponibilité	Moins de 4 heures	1
Disponibilité	Entre 4 et 24 heures	0.666
Disponibilité	Entre 24 et 72 heures	0.333
Disponibilité	Plus de 72 heures	0

TABLE 3.4 – Tableau des réponses pour les besoins de sécurité

3.4 Biens supports

3.4.1 Description et objectifs

Tout d'abord, les biens supports sont les biens physiques de l'entreprise. Ils peuvent être techniques, par exemple des ordinateurs, ou non-techniques, par exemple des employés. Leur utilité principale est de supporter le fonctionnement et de permettre l'exploitation des biens essentiels et du système d'information de l'entreprise. Chaque bien support peut être la cible de menaces exploitées au travers de vulnérabilités. Certaines de ces menaces et vulnérabilités lui sont propres mais d'autres sont communes à différents biens supports.

Finalement, les questions de cette étape servent à déterminer quels sont les biens supports utilisés dans le cadre des activités de l'entreprise et pertinents à une évaluation. Cette sélection se fait indépendamment de toute considération pour les biens essentiels car le lien entre ces deux concepts se fait plus loin dans la méthodologie.

3.4.2 Méthode de création

Afin de créer ces questions nous nous sommes inspirés encore une fois de la base de connaissances EBIOS. En effet, cette dernière contient aussi une docu-

mentation conséquente des différentes catégories de biens supports et de leurs sous-catégories. Par ailleurs, nous avons croisé cette documentation avec le standard ISO/IEC 27005, illustrant aussi différentes catégories de biens supports, afin de considérer l'ensemble des biens supports.

Tout d'abord, nous avons regroupé les deux documents dans le but de sélectionner les catégories principales. Celles-ci sont les biens matériels et logiciels, les canaux de communications, les personnes, les supports papiers, les canaux interpersonnels et les locaux. Or, les trois premières catégories présentent une quantité non négligeable de sous-éléments plus spécifiques : par exemple, le matériel comprend les ordinateurs, les périphériques informatiques et de téléphonie, les relais de communication et les supports électroniques. Ainsi, il est nécessaire de réduire le nombre de ces biens afin de ne pas avoir trop de questions.

A cet effet, nous avons décidé de fusionner diverses sous-catégories sur base du critère suivant : les biens sont suffisamment semblables pour être associés. Ainsi, pour les matériels, nous assemblons les supports physiques avec les périphériques informatiques car tous deux sont des périphériques à connecter à des ordinateurs. Toutefois, nous n'y mettons pas les périphériques de téléphonie car cela représente un tout autre type de bien support.

Ensuite, nous fusionnons les deux premières sous-catégories des logiciels, car dans le cadre des applications et des systèmes de bases de données, ce qui menace l'un risque fort de menacer l'autre. De plus, nous choisissons de ne pas tenir compte des middlewares, firmwares et systèmes d'exploitation afin de diminuer le nombre final de questions. De plus, ils feront souvent partie intégrante des équipements électroniques et des systèmes informatiques sans pour autant faire l'objet de suffisamment de menaces et vulnérabilités spécifiques afin de justifier la création de questions les mettant en évidence.

Par ailleurs, nous ne prenons que les canaux de communication numérique et non ceux de téléphonie. En effet, ces derniers représentent surtout les lignes téléphoniques et nous les incluons implicitement dans la partie matériels de téléphonie.

En outre, les dernières catégories, c'est-à-dire le personnel, les supports papiers, les canaux interpersonnels et l'infrastructure, font l'objet d'une question chacune. En effet, il s'agit de biens forts différents, avec des menaces et des vulnérabilités spécifiques, et cela implique la nécessité de les mettre en évidence séparément avec leur propre question.

Finalement, chaque question propose un choix binaire de réponses pour inclure ou non les biens supports dans l'évaluation.

3.4.3 Illustration des résultats

Le tableau 3.5 montre les résultats du travail d'analyse sur les biens supports. La première colonne montre les questions permettant d'identifier les biens et la seconde spécifie la catégorie à laquelle ils appartiennent. Il est important de noter que chaque catégorie de biens supports est liée à des menaces qui la ciblent spécifiquement et à des vulnérabilités qui lui sont propres, comme nous le modélisons dans la figure 2.5. L'établissement de ces références sera expliqué dans les sections 3.6 pour les menaces et 3.7 pour les vulnérabilités.

Question	Catégorie
1. Utilisez-vous des appareils de traitement des données, tels que des ordinateurs, des serveurs, des tablettes, des PDA, des centres multimédia, des ordinateurs centraux, des smartphones, ... ?	Matériel
2. Utilisez-vous des périphériques, d'interaction ou de stockage, tels que des imprimantes, souris, claviers, scanners, lecteurs de disques ou disquettes, tablettes graphiques, webcams, microphones, clef USB, CDROM, DVD-ROM, disques durs portables, cartouches de sauvegardes, cartes mémoire, disquettes, cassettes, bandes magnétiques, ... ?	Matériel
3. Utilisez-vous des appareils de téléphonie, tels que des téléphones fixes, PSTN, IP, mobiles, satellites, des fax, ... ?	Matériel
4. Utilisez-vous des relais de communication tels que des routeurs, modems, hubs, bridges, switches, gateways, proxies, ... ?	Matériel
5. Utilisez-vous des logiciels tels que des navigateurs web(Firefox, Chrome), portails web(Europa,Skynet), clients de messagerie électronique(Outlook, Thunderbird), suites bureautiques(Excel, Word, OpenOffice), logiciels réseaux(Network Manager), logiciels de comptabilité, ou spécifiques à votre activité, des gestionnaires de bases de données(Oracle Database, Microsoft Access, MySQL), ... ?	Logiciel
6. Utilisez-vous des moyens de communication de données numériques, tels que des câbles RJ45, de la fibre optique, le wifi, le bluetooth, l'infrarouge, ... ?	Canaux informatiques
7. Cela concerne-t-il vos employés, tels que les développeurs, managers, directeurs, chefs de projets, helpdesk, des utilisateurs, ou des personnes sous la responsabilité de votre entreprise tels que des stagiaires, thésards, ... ?	Personnel
8. Utilisez-vous des supports papier, tels que des documents manuscrits ou imprimés, des transparents, des archives papier, des documentations, des rapports, ... ?	Support papier
9. Avez-vous des canaux interpersonnels, tels que des circuits de validation par parapheur, des processus de décisions, des circuits courrier, des réunions, des échanges verbaux, ... ?	Canaux interpersonnels
10. Avez-vous une infrastructure immobilière hébergeant votre personnel et matériel, tel qu'un un siège social, des bureaux, des entrepôts, ... ?	Infrastructure

TABLE 3.5 – Tableau des biens supports

3.5 Matrices de croisement

Les matrices de croisement prennent la forme de grilles et nous les utilisons afin de mettre en relation deux concepts différents grâce à la création de liens entre eux. Afin de développer ces dernières, nous nous sommes inspirés de la méthodologie EBIOS implémentant cette formule. De fait, elle est à la fois efficace et simple car elle permet de rapidement relier différentes informations sans surcharger le questionnaire avec des questions inutiles et répétitives. En effet, si nous considérons deux familles de données, il suffit de placer les éléments de la première en ligne, ceux de la seconde en colonne, et de spécifier les liens aux intersections de ces divers éléments.

Dans le cadre de cette méthodologie, nous proposons deux matrices de croisement. Une pour les sources de menaces et les biens essentiels et l'autre pour les biens supports et les biens essentiels.

Tout d'abord, la première joue un rôle important dans la création du rapport final car elle permet à l'utilisateur de déterminer pour chaque source de menace le ou les biens qu'elle met en danger. En effet, il établit ainsi un lien direct entre les deux et saura quels sont les éléments, ou personnes auxquels il doit faire attention afin de mieux protéger ses biens.

Toutefois, nous avions d'abord pensé à réaliser un lien entre les biens supports et les sources de menaces, comme les relations de la figure 2.5 nous le laissent penser. Cependant, la première alternative ne viole pas le modèle et n'est pas beaucoup plus difficile à exécuter, mais surtout apporte des informations plus intéressantes. De manière évidente, il est de grandes chances que la plupart des biens supports repris dans la méthodologie soient inclus dans une évaluation et qu'ils supportent la plupart des biens essentiels, ainsi cette proposition permet de gagner du temps en sautant l'étape intermédiaire et elle aide l'utilisateur à mieux comprendre le danger d'une source de menace sur ses biens essentiels.

Ensuite, la seconde matrice permet d'établir un lien dont l'existence est nécessaire au calcul des scores de résultats pour les biens essentiels. En effet, la dépendance existant entre ces deux concepts rend cette opération nécessaire pour toute évaluation.

Finalement, dans ces matrices, les éléments à croiser sont des résumés des sujets des questions analogues, accompagnés du numéro de leur question. En effet, il n'est pas possible d'inclure ces dernières entièrement dans une grille sans que celle-ci n'en devienne inexploitable du fait de sa taille. Ces descriptions ont été développées avec l'objectif d'évoquer au mieux leur sujet et l'ajout d'un identifiant permet d'assurer qu'en cas d'ambiguïté l'utilisateur puisse retrouver l'information d'origine.

3.6 Menaces

3.6.1 Description et objectifs

Tout d'abord, une menace est un événement néfaste pouvant se réaliser sur un bien support, si une vulnérabilité permettant de la concrétiser venait à être exploitée. Si une menace est reconnue comme vraisemblable, c'est-à-dire si elle a une chance de se réaliser, alors son impact risquera de causer des dégâts aux biens supports visés, mais aussi aux biens essentiels supportés par ces derniers.

De plus, l'impact de chaque menace porte sur les attributs de sécurité de l'information : la confidentialité, l'intégrité et la disponibilité.

Finalement, l'objectif des questions de cette étape est de mettre en évidence les menaces susceptibles de mettre en danger une entreprise en déterminant directement si elles ont une chance de se produire où non, c'est-à-dire leur vraisemblance.

3.6.2 Méthode de création

Afin de créer ces questions, nous nous inspirons des documents ISO/IEC 27005 et de la base de connaissances EBIOS, abordés respectivement dans les sections 1.2.6 et 1.3.1. En effet, ces derniers proposent chacun une liste de menaces génériques représentant un danger pour le fonctionnement des organisations. Il est d'ailleurs intéressant de noter que EBIOS propose une série de menaces qui couvrent l'ensemble de celles de l'ISO/IEC 27005.

Ainsi, deux questions se posent à nous : quelle liste choisir et comment faire en sorte que le nombre de questions illustrant ces menaces ne soit pas trop important au cours d'une évaluation. Dans le but de trouver une solution à ces questions, nous observons la démarche suivante.

Tout d'abord, pour chacun des deux documents, nous réalisons un résumé des menaces, sous la forme d'une série de tableaux disponibles dans les annexes D et E. Ils mettent en évidence les critères pouvant servir de filtres afin de réduire le nombre de menaces d'une évaluation. Parmi ces derniers, nous avons les facteurs humain/non-humain, interne/externe, délibéré/accidentel, le type du bien support ciblé par la menace, c'est-à-dire matériel, logiciel, canaux informatiques, personnes, support papier, canaux interpersonnels, infrastructure et les attributs de sécurité de l'information, soit confidentialité, intégrité et disponibilité.

En premier lieu, nous remplissons les tableaux EBIOS grâce au raisonnement suivant. Etant donné que chaque menace est issue de la base de connaissances EBIOS, les différents attributs de sécurité et les biens supports y sont déjà déterminés. Ensuite, nous consultons l'ISO/IEC 27005 et avec l'aide des tableaux

de croisements dans la base de connaissances EBIOS, nous identifions les liens entre les menaces des deux documents. Ceci nous permet de déterminer si elles sont causées par des sources de menaces d'origine humaine, non-humaine, délibérée, et/ou accidentelle.

En deuxième lieu, nous complétons les tableaux ISO/IEC 27005, de l'annexe E, par la méthode suivante. Chaque menace est issue du standard ISO/IEC 27005, ainsi les critères humain, non-humain, délibéré et accidentel y sont déterminés. Ensuite, nous reprenons les tableaux de croisements et de manière analogue au raisonnement précédent, nous retrouvons les attributs de sécurité concernés et les biens supports ciblés. De plus, nous réalisons un lien trivial entre ces menaces et le bien support infrastructure. Par exemple, il est évident qu'un incendie peut détruire ou abîmer un bâtiment, le rendant indisponible; et en suivant ce même ordre d'idées pour le reste des menaces, nous réussissons à identifier les liens et les attributs concernés.

En dernier lieu, comme une menace ciblant un bien support peut avoir un impact sur plusieurs attributs de sécurité. Nous les indiquons dans les tableaux directement au croisement des menaces et des biens supports afin d'améliorer la lisibilité.

Ensuite, nous analysons ces tableaux afin de déterminer l'efficacité de l'application de filtres pour cibler les menaces pertinentes à une évaluation. Il apparaît que ces derniers perdent leur efficacité au fur et à mesure qu'un utilisateur inclus de nouveaux éléments dans une évaluation. Ceci est une conséquence des faits suivants :

1. Dans les séries de tableaux des annexes D et E, bien que les combinaisons des filtres humain/non-humain, interne/externe et délibéré/accidentel permettent de réduire le nombre de menaces d'une évaluation, cette réduction n'est pas significative car beaucoup de menaces partagent les éléments de ces filtres. De plus, comme plusieurs combinaisons peuvent être identifiées au cours d'une évaluation, par exemple humain-interne-délibéré et humain-externe-accidentel, les ensembles de menaces en résultant sont unis et non croisés car l'utilisateur se soucie des deux sortes de menaces et non de celles communes à ces combinaisons.

2. Dans ces mêmes tableaux, le filtre utilisant les attributs de sécurité permet de réduire significativement le nombre de menaces. Cependant, il n'y a que trois attributs et il y a une forte probabilité qu'ils soient tous inclus dans une évaluation à cause des biens essentiels et de leurs besoins de sécurité. De cette manière, le filtre perd son efficacité car toute menace ayant un impact sur au moins de ces attributs sera inclue dans l'évaluation.

3. Dans les tableaux de l'annexe D, EBIOS sépare efficacement les menaces portant sur les différents biens. Cependant, dès que plusieurs sont sélectionnés, les ensembles résultants sont unis car il n'existe pas de menaces portant sur différents biens supports et surtout car l'utilisateur s'intéresse au menaces ciblant ces biens et pas uniquement à celles ciblant les deux à la fois.

4. Dans les tableaux de l'annexe E, chaque bien support est lié à un nombre conséquent de menaces, certaines communes à différents biens. De ce fait, ils ne les filtrent pas efficacement initialement et cela se détériore au fur et à mesure que de nouveaux biens sont inclus dans une évaluation.

Ceci nous amène à la conclusion qu'il est nécessaire de fusionner les menaces afin de présenter un nombre limité de questions aux utilisateurs et ensuite d'appliquer les filtres les plus efficaces pour réduire au mieux ce nombre durant une évaluation.

A cet effet, nous choisissons de fusionner directement les menaces EBIOS, car elles incluent toutes celles de l'ISO/IEC 27005, mais aussi d'utiliser ces dernières pour enrichir la création de questions s'il est opportun de le faire. Afin de réaliser cette tâche, nous utilisons les tableaux EBIOS, complétés avec les informations sur les infrastructures identifiées dans les tableaux ISO/IEC 27005. Ensuite, nous prenons les attributs de sécurité comme critère principal de fusion, car il s'agit de l'information la plus importante à maintenir, alors que les autres moins essentielles représentent les critères secondaires, c'est-à-dire les biens supports et les facteurs humain/non-humain et délibéré/accidentel, utilisés afin de respecter une certaine cohérence entre les menaces. Au cours de cette fusion, nous utilisons les menaces EBIOS et leurs liens avec les biens supports afin de lier les nouvelles menaces aux biens supports de la méthodologie. Le tableau de fusion est disponible dans l'annexe F et le tableau des critères de filtrage pour les nouvelles menaces l'est dans l'annexe G.

Dès lors, nous avons les liens entre les menaces d'EBIOS et nous nous servons des descriptions de ces dernières, complétées avec les menaces de l'ISO/IEC 27005 qu'elles couvrent, afin de développer les questions et d'y introduire des exemples améliorant leur compréhensibilité.

Par après, une révision des tableaux de l'annexe G, résumant les nouvelles menaces, montre que les seuls filtres utilisables sont le critère humain/non-humain, même s'il n'est pas très puissant, avec celui des biens supports. Ils permettront une meilleure sélection, surtout des menaces non-humaines, alors que leur combinaison avec le critère délibéré/accidentel n'affinera pas davantage l'ensemble final des menaces.

Finalement, nous créons les réponses à ces questions. Nous proposons un

ensemble de réponses, pour la vraisemblance, assigné directement aux questions sur les menaces afin de diminuer le nombre de questions de cette étape. Ces réponses sont inspirées de l'échelle par défaut proposée dans la méthode EBIOS et nous en avons dérivé des phrases compréhensibles et exploitables par les utilisateurs.

3.6.3 Illustration des résultats

Les tableaux 3.6 et 3.7 illustrent les résultats du travail d'analyse sur les menaces. Tout d'abord, la première colonne montre les questions identifiant les menaces et la seconde le type de la question. Le tableau 3.8 illustre les réponses à ces questions, la première colonne montre le type des réponses, la seconde contient la réponse et la dernière contient sa valeur numérique.

Ensuite, les menaces sont générées grâce aux liens entre les sources de menaces et les menaces et entre les biens supports et les menaces, expliqués dans la section précédente, des sources de menaces et des biens supports sélectionnés au cours d'une évaluation.

Finalement, de par la fusion, il est important de noter que la sélection d'un bien support peut provoquer la génération de menaces en ciblant plusieurs. Or, le modèle de données de la figure 2.5 montre aussi un lien entre biens supports et vulnérabilités, utilisé pour ne pas perdre d'information, ou à l'inverse, éviter d'en inclure de trop. De fait, grâce à ces dépendances, la sélection d'un bien support et d'une menace, le ciblant parmi d'autres, générera uniquement les vulnérabilités propres au bien de départ.

Question	Type
1. Craignez-vous que vos équipements ou vos logiciels soient utilisés de manière inappropriée, par exemple si une personne utilise la puissance de traitement d'un ordinateur pour des activités personnelles, stocke des données personnelles, utilise un téléphone pour des appels privés, installe des logiciels piratés ou distribue des logiciels dont il n'est pas propriétaire, utilise le réseaux et le service mail pour spammer des collègues, ... ?	Menace
2. Craignez-vous que vos équipements perturbent le fonctionnement les uns des autres ou que vos logiciels soient altérés, résultant en une panne ou un dysfonctionnement, par exemple si un périphérique incompatible est branché, une clef USB infectée est branchée, une maintenance a été mal effectuée, une mise à jour échoue, un virus provoque des altérations, ... ?	Menace
3. Craignez-vous que vos équipements, vos logiciels, vos moyens de communication numérique, vos téléphones, vos supports papier ou vos interactions interpersonnelles soient espionnées, par exemple par une personne non-autorisée qui observe, écoute ou cherche à vous géolocaliser, essaye de collecter des données stockées dans votre système ou les intercepte via votre réseau ou met vos téléphones sur écoute, copie vos données papier, écoute vos conversations de couloir, vos réunions, via microphone, ... ?	Menace
4. Craignez-vous que vos équipements, vos moyens de communication numérique, ou vos téléphones soient exploités au point de lâcher, par exemple s'ils sont utilisés en permanence, alimentés incorrectement ou déchargés, mal ventilés, les conditions d'emploi ignorées, les périphériques remplis à fond, s'il y a beaucoup de téléchargement illégal, si votre internet est accessible à tous, si la météo perturbe ou empêche les communications, provoque des pannes de courant, ... ?	Menace
5. Craignez-vous que vos équipements, vos logiciels, vos moyens de communication numérique, vos téléphones, votre personnel, ou vos supports papier soient endommagés au point de ne plus pouvoir effectuer leurs fonctions, à cause par exemple de l'usure, de virus informatiques, d'effacement de données ou codes avec des méthodes agressives telles que les aimants, de destruction ou torsion de câbles et fibre optique, d'accidents de travail, de maladies, de décès, d'incendies , de l'humidité, d'inondations, de séismes, ... ?	Menace
6. Craignez-vous que vos équipements, vos logiciels, vos téléphones ou vos supports papier soient indisponibles, à cause par exemple de vols, de pertes, de dons, de mises au rébus, de reventes, de non renouvellement ou cessions des licences d'utilisation, ... ?	Menace
7. Craignez-vous que vos logiciels ou vos procédures de communication interpersonnelle soient surchargées, par exemple à cause d'un manque de vérification des données saisissables, d'une sollicitation forte et constante de vos logiciels, ou si vos logiciels ralentissent voire ne répondent pas, d'une surcharge de vos réunions, de bruits limitant l'audibilité, ... ?	Menace
8. Craignez-vous que vos moyens de communication numérique, vos supports papier ou vos procédures de communication interpersonnelle soient utilisées de manière inappropriée, à cause par exemple d'attaques de votre réseau, telles qu'une personne qui intercepte ou modifie vos messages, falsifie ou efface vos documents papier, s'en sert comme brouillon, modifie ou détruit des notes ou parapheurs, fait courir des rumeurs, utilise les réunions à des fins personnelles, ... ?	Menace

TABLE 3.6 – Tableau des menaces - partie 1

Question	Type
9. Craignez-vous que le fonctionnement vos moyens de communication numérique soit ralentit ou bloqué, à cause par exemple du remplacement d'un câble par un incompatible, ou qui n'a pas la même capacité de transfert, d'un vol, d'une perte, d'un changement non-communiqué de mot passe du wifi, d'une coupure des lignes téléphoniques ... ?	Menace
10. Craignez-vous votre personnel soit distrait au point que ses performances diminuent, à cause par exemple de distractions telles que des spams, canulars, escroqueries par mail, un supérieur qui assigne un job en dehors du contrat, ou de blocages tels que des grèves, inondations, météo, séismes, maladies, ... ?	Menace
11. Craignez-vous que votre personnel soit espionné, par exemple qu'il soit, avec ou sans équipement spécialisé, épié dans la rue, au travail ou chez lui, amené à divulguer des informations confidentielles, mit sur écoute, ... ?	Menace
12. Craignez-vous que votre personnel soit surchargé au point de ne plus travailler correctement, à cause par exemple de surmenage, de travail excessif ou dans de mauvaises conditions, de stress, de manque de maîtrise de son travail, de manque d'adaptabilité, d'incapacité à gérer la pression, de la météo, ... ?	Menace
13. Craignez-vous que votre personnel soit influencé au point de divulguer des informations ou de mal travailler, à cause par exemple de pressions personnelles, politiques, ou encore hiérarchiques, de corruption, de manipulation, de harcellement, lors d'une conversation anodine par accident, ... ?	Menace
14. Craignez-vous que votre personnel soit indisponible, que ce soit à cause d'un départ, d'un licenciement, d'une réaffectation, d'un kidnapping, ... ?	Menace
15. Craignez-vous que la communication interpersonnelle soit ralentie ou bloquée, par exemple si vos courriers sont perdus ou ouverts, vos réunions de communication et de prise de décisions mal organisées ou supprimées indéfiniment ou les gens conviés ne viennent pas, vos employés ne communiquent pas, une mauvaise atmosphère règne, ... ?	Menace

Table 3.7 – Tableau des menaces - partie 2

Type	Réponse	Valeur
Vraisemblance	Ces scénarios vont se (re)produire dans un délai relativement bref	1
Vraisemblance	Ces scénarios pourraient clairement se (re)produire un jour ou l'autre	0.666
Vraisemblance	Ces scénarios pourraient bien se (re)produire	0.333
Vraisemblance	Ces scénarios sont improbables et ne nous concernent pas	0

Table 3.8 – Tableau des réponses pour la vraisemblance des menaces

3.7 Vulnérabilités

3.7.1 Description et objectifs

Tout d'abord, les vulnérabilités sont des brèches de sécurité sur les biens supports et leur exploitation permet de concrétiser des menaces ciblant ces biens supports. Ainsi, elles sont liées à ces deux concepts, en respectant la contrainte suivante : une vulnérabilité d'un bien support est obligatoirement une vulnérabilité concrétisant une menace portant sur ce même bien support. Ces brèches peuvent être techniques, comme un antivirus qui n'est pas à jour, ou encore non-techniques, par exemple un employé démontrant un comportement à risque comme ouvrir des e-mails douteux ou aborder des sujets confidentiels avec des personnes n'ayant pas les autorisations nécessaires.

Finalement, l'objectif des questions de cette étape est de mettre en évidence les brèches de l'entreprise, exploitables ou ayant déjà été exploitées, au travers de questions mettant en évidence des mauvaises pratiques.

3.7.2 Méthode de création

Afin de développer ces questions, nous nous inspirons de la base de connaissances EBIOS et de l'ISO/IEC 27005 car ces deux documents contiennent chacun une liste bien remplie de vulnérabilités, mais aussi de l'ISO/IEC 27002 car il contient de nombreuses mesures visant à améliorer la sécurité de l'information.

Tout d'abord, nous avons rassemblé pour chaque bien support les différentes vulnérabilités les concernant. A cet effet, nous reprenons toutes celles des menaces EBIOS dont le lien avec les biens supports est directement présenté dans la base de connaissances. Ensuite, nous utilisons le tableau de croisement entre les menaces EBIOS et de l'ISO/IEC 27005 afin de lier les vulnérabilités de ce document aux biens supports de la méthodologie.

Par après, nous établissons le ou les liens entre chaque vulnérabilité et les mesures de sécurités de l'ISO/IEC 27002. La réflexion est menée de la manière suivante : "Si cette vulnérabilité était exploitée, quels seraient les conseils que nous donnerions aux victimes afin d'améliorer leur situation?". Par exemple, si un employé quitte son entreprise et va révéler des secrets, la vulnérabilité pourrait être l'absence de contraintes contractuelles l'empêchant légalement de révéler des informations confidentielles. Les conseils, permettant d'apporter des éléments de solution à ce problème, seraient d'assurer la signature par l'employé d'un accord de confidentialité en entrant dans l'entreprise et d'un nouveau en terminaison de contrat. Ces mesures correspondent aux sections 7.1.2 et 7.3.1 de l'ISO/IEC 27002.

Ensuite, nous utilisons ces informations sur les vulnérabilités afin d'en dériver

des questions permettant aux utilisateurs de cette méthodologie de comprendre les problèmes évoqués par les énoncés originaux. Nous avons choisi de présenter ces questions selon le format suivant : une question met en évidence une ou plusieurs mauvaises pratiques à ne pas appliquer ni laisser appliquer. En effet, nous partons du postulat qu'il est plus facile de se rappeler de mauvaises expériences, dans le cas où ces vulnérabilités auraient déjà été exploitées, mais aussi que la mise en évidence d'un problème ou d'une faiblesse véhicule plus d'information que l'approche inverse. De plus, il convient de noter que cette manière d'aborder les vulnérabilités permet à un utilisateur de prendre conscience de certaines actions à réaliser afin d'améliorer la maturité en termes de sécurité de l'information de son entreprise.

Par la suite, nous lions ces vulnérabilités aux diverses menaces EBIOS et implicitement aux nouvelles menaces définies dans cette méthodologie, mais aussi aux biens supports. Dans cette optique, les vulnérabilités empruntées à EBIOS et les vulnérabilités de l'ISO/IEC 27005 sont rattachées aux menaces et aux biens supports de la méthodologie grâce, respectivement, à la base de connaissances EBIOS et au tableau de croisement des menaces des deux documents. En effet, la base de connaissances EBIOS contient les liens explicites entre les vulnérabilités et les menaces et entre les menaces et les biens supports. De plus, l'ISO/IEC 27005 illustre des liens explicites entre les biens supports et les vulnérabilités et entre les vulnérabilités et les menaces. Ces derniers, combinés avec le tableau de croisement des menaces EBIOS et de l'ISO/IEC 27005, permettent de rattacher les vulnérabilités aux menaces de la méthodologie, en passant par les menaces EBIOS.

Finalement, chaque question est pourvue d'un choix binaire de réponses présenté dans le tableau 3.9. "Oui" indique que la ou les mauvaises pratiques illustrées par la questions ont été appliquées ou exploitées, "Non" indique qu'elles ne le sont pas, ou bien que l'utilisateur n'est pas concerné par ce problème. Il est important de noter que la formulation de ces questions admet difficilement d'autres ensembles des réponses. Cependant, cette formulation est nécessaire afin d'améliorer la compréhensibilité des questions par les utilisateurs. De plus, le nombre de questions étant conséquent, cet ensemble facilite la prise de décision par l'utilisateur car il est restreint, et il augmente la rapidité de complétion de cette partie du questionnaire en offrant une uniformité des réponses aux travers des questions.

Réponse	Valeur
Oui	1
Non	0

TABLE 3.9 – Tableau des réponses pour les vulnérabilités

3.7.3 Illustration des résultats

Les résultats du travail d'analyse sur les vulnérabilités sont illustrés dans les annexes H et I. Tout d'abord, les vulnérabilités sont générées grâce aux liens entre les biens supports et les vulnérabilités et entre les menaces et les vulnérabilités. Ces liens ont été expliqués dans la section précédente et seuls ceux des biens supports et de menaces sélectionnés au cours d'une évaluation sont pris en compte pour la génération.

Finalement, Il est intéressant de noter que les liens entre les vulnérabilités et l'ISO/IEC 27002 agissent en tant que valeur pondératrice du résultat final du calcul, présenté dans la section 4.3.5, des scores liés aux domaines de ce document. En effet, plus une question est liée à un même domaine en portant sur différentes mesures de sécurité de ce dernier, plus son importance est grande car elle représente un danger à la réalisation de plusieurs objectifs de sécurité.

3.8 Résultats

3.8.1 Description et objectifs

Tout d'abord, les résultats sont la représentation des scores obtenus après la réalisation d'une évaluation proposée par le questionnaire méthodologique. Actuellement, nous présentons un ensemble de plusieurs graphiques illustrant les scores des différentes étapes significatives de l'évaluation : les biens essentiels, les biens supports et les menaces. En effet, il est plus facile d'afficher des résultats selon le contexte défini par l'utilisateur. Par ailleurs, nous y ajoutons deux diagrammes supplémentaires pour les scores associés aux domaines de l'ISO/IEC 27002. De fait, il s'agit d'une référence importante dans le domaine de la sécurité de l'information et elle véhicule des renseignements relatifs à l'amélioration de la maturité en termes de sécurité de l'information.

Finalement, l'objectif de cette étape est de permettre à un utilisateur novice de prendre un premier constat, facile à interpréter, des résultats d'une évaluation conduite grâce à la méthodologie.

3.8.2 Méthode de création

Afin de créer cette représentation des résultats, nous nous sommes posés une simple question : Quelle est la manière la plus simple et compréhensible de présenter visuellement des valeurs numériques?

Pour commencer, il est évident, bien que nous en ayons discuté avec diverses personnes ayant de l'expérience en ce domaine, que l'utilisation de graphiques est sans doute le procédé le plus communément accepté pour représenter des

résultats quantifiables. En effet, la méthode est facile à mettre en place et ce genre de présentation très simple améliore la compréhensibilité des données.

Ensuite, nous proposons deux types de graphiques pour l'ensemble des scores obtenus à la fin d'une évaluation. Le premier est un graphique en histogramme empilé car nous représentons la valeur finale des scores mais aussi la proportion de chaque attribut de sécurité dans ces totaux. Or, ce genre d'image permet de faire comprendre ces deux informations au premier coup d'oeil. Le second est un graphique en étoile, utilisé pour l'affichage des scores associés aux domaines de l'ISO/IEC 27002. Le choix de changer la manière de représenter ces données nous permet d'attirer l'attention de l'utilisateur sur ce sujet, différent de ceux mis en évidence dans les autres graphiques.

Finalement, chaque graphique affichera des scores dont les valeurs sont comprises dans l'intervalle $[0, 1]$ car il s'agit d'une représentation commune et sans équivoque des résultats, rapidement transformable en pourcentage.

3.8.3 Illustration des résultats

La figure 3.1 montre un exemple des différents graphiques de résultats d'une évaluation.

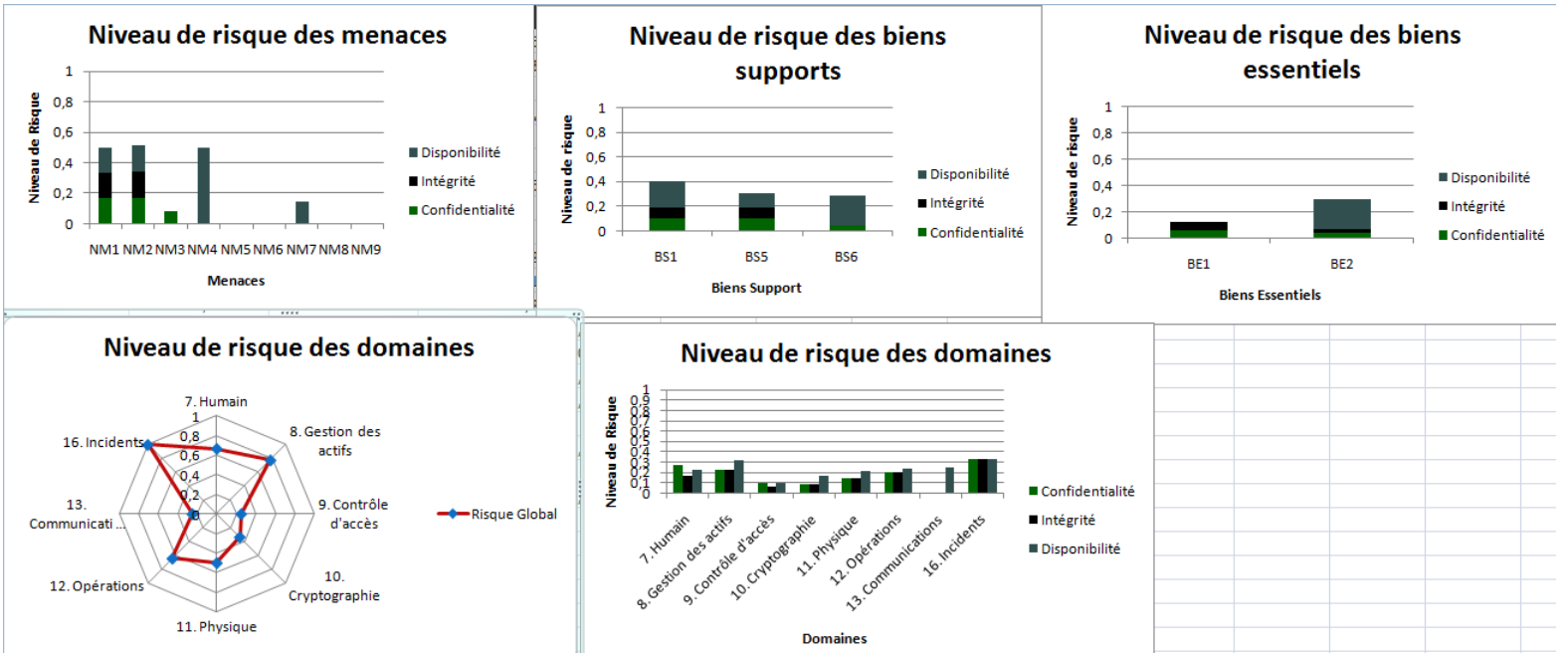


FIGURE 3.1 – Exemple des résultats d'une évaluation

Il est important de noter la présence d'un histogramme empilé pour les scores des domaines de l'ISO/IEC 27002. Ce choix découle de l'impossibilité de représenter dans le diagramme en étoiles les proportions des scores associées aux attributs de sécurité, sans rendre ce dernier illisible.

Finalement, le chapitre 4 approfondira le sens véhiculé par ces graphiques en présentant les formules développées pour les calculer et leur utilité.

3.9 Création des échelles de valeurs pour les réponses

Afin de calculer les niveaux de risque, dont les formules sont présentées dans le chapitre 4, il est nécessaire d'assigner des valeurs aux divers choix de réponses des questions de la méthodologie. Dans ce chapitre, nous avons identifiés cinq ensembles de réponses : trois pour les besoins de sécurité, un pour le facteur de vraisemblance des menaces et le dernier pour le reste des questions, mais dont les valeurs sont utilisées uniquement dans le cadre des vulnérabilités.

Tout d'abord, les échelles de valeurs, illustrées dans les tableaux 3.4, 3.8 et 3.9, sont reprises du livre de Nicolas Mayer[34]. Il est important de noter que nous avons une valeur nulle pour l'échelle de valeurs du facteur de vraisemblance. En effet, l'approche de M. Mayer fait abstraction des menaces invraisemblables, contrairement à la méthodologie présentée dans ce document.

Finalement, les valeurs de ces échelles appartiennent à l'ensemble {0;1;2;3} mais comme nous présentons des niveaux de risque compris dans l'intervalle $[0, 1]$, nous divisons chaque valeur de l'ensemble par trois et nous obtenons l'ensemble {0;0.333;0.666;1}.

3.10 Outil implémenté

Dans le but de simplifier l'emploi de cette méthodologie par les utilisateurs, nous avons développé un outil de support permettant de l'automatiser.

Ce dernier prend la forme d'un classeur Excel 2007 en deux parties. Ce choix est inspiré de la méthode MEHARI, abordée dans la section 1.3.2, qui implémente une méthode de gestion du risque utilisant ce format; et il est motivé par les avantages, abordés dans l'annexe C, que l'utilisation d'Excel permet d'obtenir.

Tout d'abord, nous avons la partie invisible, contenant la base de données de toutes les questions du questionnaire méthodologique, de leurs dépendances entre elles, mais aussi avec les attributs de sécurité de l'information. Cette partie couvre aussi toute la programmation permettant d'assurer le dynamisme de l'outil. En effet, des fonctions ont été implémentées afin d'assurer la génération des questions, les questionnaires de croisement inclus, sur base des réponses aux questions des diverses étapes, mais aussi pour effectuer les calculs de scores sur base de ces réponses.

Ensuite, nous avons la partie visible de l'outil, c'est-à-dire les différentes étapes présentées dans la figure 2.6 et abordées tout au long de ce chapitre. Chaque étape prend la forme d'une feuille Excel. L'utilisateur peut passer des unes aux autres afin de réaliser une évaluation et décider de naviguer en arrière afin de modifier des éléments de réponse. A cet effet, le code de l'outil assure les modifications en temps réel des contenus des étapes, selon les modifications apportées par l'utilisateur. Ainsi, la sélection d'une menace, après l'affichage des résultats, provoquera l'apparition des vulnérabilités permettant de la concrétiser dans l'étape analogue, et une fois complétées, les résultats seront recalculés lors du retour sur la page contenant les graphiques.

Finalement, ce logiciel est un outil stand-alone ne nécessitant pas d'installation, hormis celle d'une version d'Office datant de ou postérieure à 2007. Ainsi, il est facile à prendre en main, à utiliser et ne communique pas les résultats via internet pour d'évidentes raisons de confidentialité, ni ne nécessite un ordinateur performant pour être exploité. La figure 3.2 montre une capture d'écran de l'outil et illustre la première étape de la méthodologie.

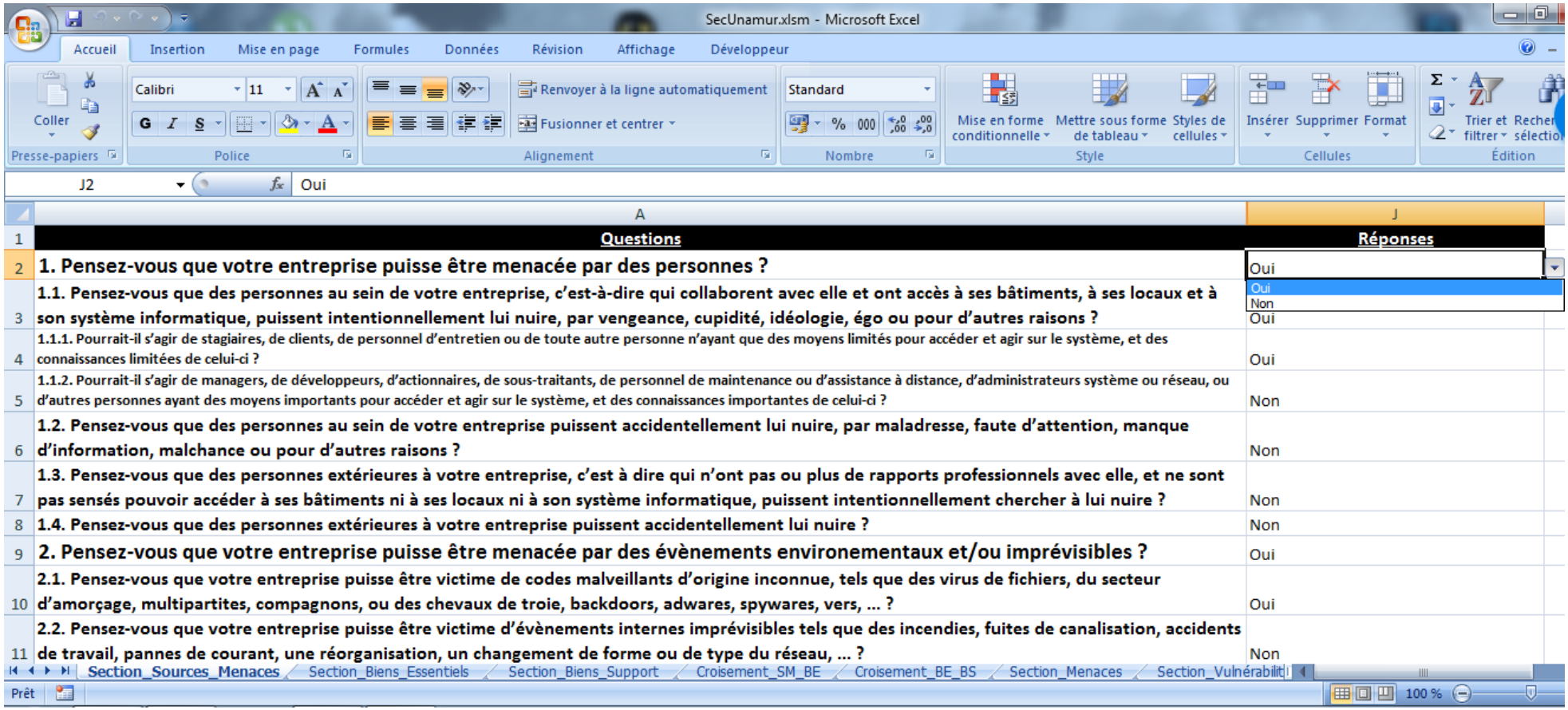


FIGURE 3.2 – Capture d'écran de l'outil

3.11 Conclusion

Dans ce chapitre, nous avons suivi le procédé de développement des questions et des réponses du questionnaire méthodologique. En commençant par la définition des hypothèses permettant d'inférer les objectifs spécifiques à la méthodologie et complétés par ceux propres à la conception de questionnaires, nous avons déterminé les contraintes générales à prendre en considération lors du développement du contenu de la méthodologie.

Ensuite, pour chaque étape de la proposition de solution, nous avons défini des objectifs spécifiques et, tout en gardant à l'esprit les contraintes générales, nous avons développé des questions et leurs réponses. Cette démarche est accomplie en utilisant des méthodes visant à transformer des données brutes ou de bas niveau en information compréhensible et toujours en prenant la perspective des utilisateurs au travers de l'étude du processus cognitif de réponse à une question pour les divers éléments créés.

Par après, nous avons illustré la méthode de création des échelles de valeurs pour les ensembles de réponses de la méthodologie et nous avons avons terminé le chapitre par un résumé de l'outil de support et de son implémentation.

Finalement, il reste à créer les formules de calcul qui utiliseront le contenu de la méthodologie et les réponses des utilisateurs afin de calculer des scores de résultats, comme ceux présentés dans la section 3.8. Le chapitre 4 présentera ces formules et les méthodes employées pour les concevoir.

Chapitre 4

Calcul des scores de résultats

Dans ce chapitre, nous allons présenter les formules mathématiques qui permettent de calculer les scores de résultats d'une évaluation de la maturité en termes de sécurité de l'information dans une entreprise et de définir des intervalles d'inacceptabilité pour ces scores. A cet effet, nous parlerons de la méthode employée afin de développer ces formules et nous les présenterons ensuite. Enfin, nous terminerons avec la définition des intervalles.

4.1 Besoin de calculer des scores

Un des objectifs principaux de cette méthodologie est de proposer les résultats d'une évaluation à un utilisateur. Il s'agit d'un pré-requis de toute initiative de gestion du risque, à ceci près que nous devons assurer une haute compréhensibilité de ces résultats. Par ailleurs, comme la section 1.5 l'illustre, il est nécessaire d'assurer leur reproductibilité, leur comparabilité, leur simplicité et de définir leurs valeurs d'inacceptabilité afin d'obtenir une méthodologie exploitable. En effet, sans ces propriétés, les résultats d'une évaluation à l'autre n'auront aucun sens, ni ne seront utilisables pour tirer des conclusions pertinentes.

Afin de résoudre ce problème, nous proposons d'appliquer à la méthodologie, des métriques utilisant les échelles de valeurs définies et décrites dans le chapitre 3. Ensuite, ces métriques seront utilisées dans des formules de calcul qui permettront d'obtenir des données quantifiables mesurant le niveau de maturité en termes de sécurité de l'information dans les entreprises.

Par ailleurs, la nature de ces résultats, soit des données quantifiables sous la forme de valeurs numériques, assurera la satisfaction des pré-requis énoncés préalablement. En effet, ces résultats seront simples à lire et à comprendre, trivialement comparables car il suffira de mettre deux scores portant sur le même sujet en vis-à-vis pour se rendre compte d'une amélioration ou d'une détério-

ration, reproductibles grâce aux formules prédéfinies dont l'application donnera toujours des résultats semblables, et facilement interprétables une fois comparés avec les valeurs d'inacceptabilité.

Toutefois, la réalisation de cette étape met en lumière plusieurs problématiques. Nous les illustrons au travers des questions suivantes :

1. Comment représenter la maturité de la sécurité de l'information?
2. Comment identifier les différents scores à présenter?
3. Quelles sont les métriques servant à les calculer?
4. Comment construire les formules de calcul?
5. Quelles sont les intervalles d'inacceptabilité des résultats?

Afin d'y répondre, nous utilisons une méthode provenant d'un article de Ahmad, Sahib et Azuwa[2], présenté dans la section 1.5, dont le concept adresse directement les trois premières questions.

Ensuite, une fois les métriques déterminées, elles seront utilisées afin de répondre à la quatrième question et de créer les formules de calcul.

Finalement, ces formules seront utilisées afin d'adresser la dernière problématique.

4.2 Méthode d'identification des formules

Afin de créer les formules de cette méthodologie et donc de répondre au quatre premières problématiques posées dans ce chapitre, nous employons le concept GQM[34], ou "Goal-Question-Metric" abordé dans la section 1.5. Grâce à ce dernier, nous pouvons adresser les trois premiers problèmes l'un après l'autre, en commençant par la manière avec laquelle nous présentons les résultats d'une évaluation de la maturité en termes de sécurité de l'information dans une organisation. En effet, la partie "Goal" répond à la première problématique en nous donnant l'opportunité de définir la manière de représenter la maturité. Ensuite, les questions nous serviront de base de réflexion sur les différentes étapes de la méthodologie, identifiées dans le chapitre 2, dans le but de finalement identifier les métriques intervenant dans les réponses à ces questions. Cette méthode peut sembler simpliste, mais ces métriques vont guider efficacement la création de formules adéquates et donnant les résultats visés.

Par ailleurs, une fois le plan GQM établi, il reste à créer les formules au moyen des métriques identifiées. Cependant, il n'existe pas de procédé absolu pour construire des formules de calcul. Ainsi, nous utilisons la démarche suivante : au travers d'observations sur la structure de la méthodologie, sur les données qu'elle contient et sur les liens entre ces données et implicitement entre les étapes, nous établissons des formules tirant parti des métriques identifiées.

En outre, il est évident que cette construction est le résultat d'un processus itératif visant à raffiner la forme des formules au cours de son cycle et selon les résultats de leurs tests et applications à des sous-ensembles des données de la méthodologie. Ces formules sont décrites dans la section suivante de ce chapitre et suivent l'ordre établi dans la table 4.1.

Finalement, elles sont utilisées afin de répondre à la dernière problématique de ce chapitre.

La table 4.1 présente le plan GQM que nous avons développé et sur lequel nous nous sommes basés afin de construire les formules de la méthodologie. Il est intéressant de noter que ces questions fonctionnent par paires car il s'agit à chaque fois de deux représentations d'un score. Ainsi, notamment pour les biens supports et les biens essentiels, bien que les questions soient différentes, les métriques sont identiques, comme il est possible de le constater avec les biens supports dont la formule 4.3 utilise les résultats de la formule 4.4. Toutefois, il est pertinent de garder les deux questions afin de montrer clairement que deux scores différents sont calculés, même si l'un dépend de l'autre.

GQM	Numérotation	Définition
Goal	G1	Illustrer la maturité de la sécurité de l'information au travers du calcul du risque auquel les entreprises sont exposées.
Question	Q1	Quel est le niveau de risque représenté par une menace?
Métriques	M1.1	Vraisemblance, Nombre de vulnérabilités, Niveaux d'exploitabilité des vulnérabilités
Question	Q2	Quelle est la répartition de ce risque selon les attributs de sécurité?
Métriques	M2.1	Nombre d'attributs, M1.1
Question	Q3	Quel est le niveau de risque associé à un bien support?
Métriques	M3.1	Nombre de menaces liées à ce bien support, M2.1 de ces menaces
Question	Q4	Quelle est la répartition de ce risque selon les attributs de sécurité?
Métriques	M4.1	Nombre de menaces liées à ce bien support, M2.1 de ces menaces
Question	Q5	Quel le niveau de risque associé à un bien essentiel?
Métriques	M5.1	Nombre de biens supports liés à ce bien essentiel, M4.1 de ces biens, besoins de sécurité
Question	Q6	Quelle est la répartition de ce risque selon les attributs de sécurité?
Métrique	M6.1	Nombre de biens supports liés à ce bien essentiel, M4.1 de ces biens, besoins de sécurité
Question	Q7	Quel est le niveau de risque associé à un domaine de l'ISO/IEC 27002?
Métriques	M7.1	Nombre de vulnérabilité du domaine, Niveaux d'exploitabilité des vulnérabilités, Importance des vulnérabilités dans ce domaine
Question	Q8	Quelle est la répartition de ce risque selon les attributs de sécurité?
Métriques	M8.1	M7.1, Nombre de menaces liées à chaque vulnérabilité, Nombre d'attributs de ces menaces

TABLE 4.1 – Tableau GQM de définition des métriques de la méthodologie

4.3 Formules de calcul

Nous allons maintenant présenter les formules de calcul développées pour cette méthodologie, suivant l'ordre des énoncés de la table 4.1. Mais tout d'abord, commençons par énoncer les notions nécessaires à leur compréhension.

4.3.1 Notions

Soit D l'ensemble des domaines de sécurité de l'ISO 27002.

Soit SM l'ensemble des sources de menaces de la méthodologie.

Soit BE l'ensemble des biens essentiels de la méthodologie.
Soit $AS = \{\text{Confidentialité ; Intégrité ; Disponibilité}\}$ l'ensemble des attributs de sécurité traités dans la méthodologie, tel que $\#AS = 3$.

Soit BS l'ensemble des biens supports de la méthodologie.

Soit M l'ensemble des menaces de la méthodologie.

Soit V l'ensemble des vulnérabilités de la méthodologie.

Soient $\begin{array}{rcccl} Val_{SM} & : & SM & \rightarrow & \{0;1\} \\ Val_{BE} & : & BE & \rightarrow & \{0;1\} \\ Val_{BS} & : & BS & \rightarrow & \{0;1\} \end{array}$ des fonctions telles que $Val(x) = 1 \Rightarrow x$ est inclus dans une évaluation par un utilisateur.

Soit $Val_M : M \rightarrow \{0; \frac{1}{3}; \frac{2}{3}; 1\}$ une fonction telle que $Val_M(x)$ est le niveau de vraisemblance d'une menace quelconque de M et telle que $Val_M(x) > 0 \Rightarrow x$ est inclus dans une évaluation par un utilisateur.

Soit $Val_V : V \rightarrow \{0;1\}$ une fonction qui donne le niveau d'exploitabilité d'une vulnérabilité.

Soit $BE \times BS = \{\ (x,y) \mid x \in BE \text{ et } y \in BS\ \}$ le produit cartésien des ensembles BE et BS.

Soit $\begin{array}{rcccl} Crois & : & (BE \times BS) & \rightarrow & \{0;1\} \\ & & (x,y) & \rightarrow & Crois(x,y) \end{array}$ tel que $Crois(x,y) = \begin{cases} 1 & \text{si x et y sont liés} \\ 0 & \text{sinon} \end{cases}$ indique si un bien essentiel x est supporté par un bien support y.

Soit $V \times D = \{\ (x,y) \mid x \in V \text{ et } y \in D\ \}$ le produit cartésien des ensembles V et D.

Soit $\begin{array}{rcccl} Refs & : & (V \times D) & \rightarrow & \mathbb{N}^+ \\ & & (x,y) & \rightarrow & Refs(x,y) \end{array}$ tel que $Refs(x,y)$ donne le nombre de références de x vers y.

Soit $BE \times AS = \{ (x, y) \mid x \in BE \text{ et } y \in AS \}$ le produit cartésien des ensembles BE et AS.

Soit $\begin{array}{rccc} Besoin & : & (BE \times AS) & \rightarrow & \{0; \frac{1}{3}; \frac{2}{3}; 1\} \\ & & (x, y) & \rightarrow & Besoin(x, y) \end{array}$ tel que $Besoin(x, y)$ donne le besoin de sécurité de l'attribut y pour le bien essentiel x.

Soit $M \times AS = \{ (x, y) \mid x \in M \text{ et } y \in AS\}$ le produit cartésien des ensembles M et AS.

Soit $\begin{array}{rccc} MenaceAS & : & (M \times AS) & \rightarrow & \{0; 1\} \\ & & (x, y) & \rightarrow & MenaceAS(x, y) \end{array}$ tel que $MenaceAS(x, y) = \begin{cases} 1 & \text{si } y \in AS_x \\ 0 & \text{sinon} \end{cases}$ indique si une menace x a un impact sur l'attribut de sécurité y.

Soit $V \times M = \{ (x, y) \mid x \in V \text{ et } y \in M\}$ le produit cartésien des ensembles V et M.

Soit $\begin{array}{rccc} Concret & : & (V \times M) & \rightarrow & \{0; 1\} \\ & & (x, y) & \rightarrow & Concret(x, y) \end{array}$ tel que $Concret(x, y, z) = \begin{cases} 1 & \text{si } x \in V_y \\ 0 & \text{sinon} \end{cases}$ indique si une menace y est concrétisable par la vulnérabilité x.

Soit $V \times M = \{ (x, y) \mid x \in V \text{ et } y \in M\}$ le produit cartésien des ensembles V et M.

Soit $\begin{array}{rccc} NBAttributs & : & (V \times M) & \rightarrow & \{0; 1; 2; 3\} \\ & & (x, y) & \rightarrow & NBAttributs(x, y) \end{array}$ tel que $NBAttributs(x, y) = \begin{cases} \#AS_y & \text{si } x \in V_y \\ 0 & \text{sinon} \end{cases}$ donne le nombre d'attributs de sécurité sur lesquels la menace y a un impact, si elle est concrétisable par la vulnérabilité x.

4.3.2 Calcul du risque pour les menaces

Le niveau de risque d'une menace est la valeur du risque qu'elle représente pour le ou les biens supports auxquels elle est liée dans la méthodologie. Ce niveau est présenté selon deux formes :

1. La forme normale est associée à la question 1 du tableau 4.1 et illustrée par la formule 4.1. Elle donne la valeur totale du risque représenté par une menace. Cette formule est inspirée du calcul du risque[25], c'est-à-dire Menace × Impact × Vulnérabilité, et elle utilise les liens entre les menaces et les vulnérabilités afin de calculer un score. Ces liens sont définis dans la section 3.7 et disponibles dans l'annexe I.

Soient $V_{M_x} \subset V$ l'ensemble des vulnérabilités permettant de concrétiser une menace quelconque de M et $V_{BS_x} \subset V$ l'ensemble des vulnérabilités spécifiques à un bien support quelconque de BS,
alors le risque R_{M_i} représenté par une menace $M_i \in M$ est défini selon la formule :

$$R_{M_i} = Val_M(M_i) \times \frac{\sum_{j=1}^{n} Val_V(V'_j)}{n} \tag{4.1}$$

où $m = \#V$, $n = \#V'$, $V'_j \in V'$ et $V' = \{V_k \mid V_k \in (V_{M_i} \cap V_{BS}), \forall k \in \{1;..;m\}\} \subset V$
avec $V_{BS} = \bigcup_{l=1}^{o} \{V_{BS_l} \mid Val_{BS}(BS_l) = 1\}$ et $o = \#BS$

Cette formule calcule la moyenne de la somme des niveaux d'exploitabilité des vulnérabilités de V' et multiplie ce résultat par la valeur de vraisemblance de la menace M_i, soit $Val_M(M_i)$. Les résultats de cette formule permettent de classer les menaces en fonction du danger qu'elles représentent.

Il est important de noter que cette formule tient uniquement compte des vulnérabilités débloquées par les biens supports inclus dans l'évaluation en cours et qui permettent de concrétiser la menace M_i. Ainsi, l'ensemble V' contient uniquement les vulnérabilités de V qui sont à la fois dans l'ensemble des vulnérabilités spécifiques à l'ensemble des biens supports inclus dans l'évaluation en cours, soit V_{BS}, et dans l'ensemble des vulnérabilités qui permettent de concrétiser la menace M_i, soit V_{M_i}.

2. La forme avancée est associée à la question 2 du tableau 4.1 et illustrée par la formule 4.2. Elle donne la répartition du niveau de risque d'une menace selon les attributs de sécurité sur lesquels elle a un impact. Afin de créer cette formule, les liens entre menaces et attributs de sécurité ont été observés. Ces liens sont définis dans la section 3.6 et disponibles dans l'annexe G.

Soit $AS_{M_x} \subseteq AS$ l'ensemble des attributs de sécurité sur lesquels une menace quelconque de M a un impact, alors la part de risque $R_{AS_j\,M_i}$ associée à un attribut de sécurité $AS_j \in AS$, sur lequel une menace $M_i \in M$ a un impact, est définie selon la formule :

$$R_{AS_j\,M_i} = \begin{cases} \frac{R_{M_i}}{\#AS_{M_i}} & \text{si } AS_j \in AS_{M_i} \\ 0 & \text{sinon} \end{cases} \tag{4.2}$$

où $1 \leq \#AS_{M_i} \leq 3$.

Cette formule divise le résultat de la formule 4.1 par le nombre d'attributs de sécurité sur lesquels elle a un impact, soit $\#AS_{M_i}$. Si AS_j n'appartient pas à AS_{M_i} alors le résultat vaut 0. Les résultats de cette formule ont une vocation didactique car ils permettent de visualiser les attributs de sécurité mis en danger par les menaces. Cette dernière information fournit un critère supplémentaire pour classer les menaces.

Il est important de noter que chaque menace possède un nombre prédéterminé d'attributs de sécurité, comme cela est expliqué dans la section 3.6. Ainsi, les parts de risque associées aux différents attributs d'une même menace sont identiques.

4.3.3 Calcul du risque pour les biens supports

Le niveau de risque d'un bien support est la valeur du risque que les menaces dont il est la cible lui font courir. Ce niveau est présenté sous deux formes :

1. La forme normale est associée à la question 3 du tableau 4.1 et illustrée par la formule 4.3. Elle donne la valeur totale du risque encouru par le bien support.

Le risque R_{BS_i} associé au bien support $BS_i \in BS$ est défini selon la formule :

$$R_{BS_i} = \frac{\sum_{j=1}^{n} R_{AS_j\,BS_i}}{n} \tag{4.3}$$

où $AS_j \in AS$ et $n = \#AS$

Cette formule calcule la somme des résultats obtenus grâce à la formule 4.4. Les résultats de cette formule permettent de classer les biens supports en fonction du risque qu'ils encourent.

Il est important de noter que nous avons décidé de présenter ces formules dans cet ordre afin de respecter le tableau 4.1 selon lequel il est plus logique de déterminer le niveau de risque d'un bien support avant

de déterminer la répartition de ce risque selon les attributs de sécurité. Cependant, dans les faits, le calcul est réalisé dans l'autre sens.

2. La forme avancée est associée à la question 4 du tableau 4.1 et illustrée par la formule 4.4. Elle donne la répartition du niveau de risque d'un bien support selon les attributs de sécurité sur lesquels les menaces dont il est la cible ont un impact. Afin de créer cette formule, les formules 4.1 et 4.2 ont été réutilisées et les liens entre les sources de menaces et les menaces, entre les biens supports et les menaces et entre les attributs de sécurité et les menaces ont été observés afin de déterminer quelles menaces inclure dans le calcul. Ces liens sont définis dans la section 3.6 et disponibles dans l'annexe G.

Soient $M_{SM_x} \subset M$ l'ensemble des menaces provoquées par une source de menace quelconque de SM et
$M_{BS_x} \subset M$ l'ensemble des menaces ciblant un bien support quelconque de BS,
$V_{BS_x} \subset V$ l'ensemble des vulnérabilités spécifiques à un bien support quelconque de BS,
V_{M_x} l'ensemble des vulnérabilités spécifique à une menace quelconque de M et
AS_{M_x} l'ensemble des attributs de sécurité sur lesquels une menace quelconque de M a un impact, alors la part de risque $R_{AS_j\,BS_i}$ associée à un attribut de sécurité $AS_j \in AS$, pour un bien support $BS_i \in BS$, est définie par la formule :

$$R_{AS_j\,BS_i} = \frac{\sum_{k=1}^{n} MenaceAS(M'_k, AS_j) \times Val_M(M'_k) \times \frac{\sum_{l=1}^{m} Val_V(V'_l)}{m \times \#AS_{M'_k}}}{n} \tag{4.4}$$

où $q = \#M$, $M'_k \in M'$ et $M' = \{M_a \mid (M_a \in (M_{SM} \cap M_{BS_i})) \wedge (Val_M(M_a) > 0), \forall a \in \{1; ..; q\}\} \subset M$,
$r = \#V$, $V'_l \in V'$ et $V' = \{V_b \mid (V_b \in (V_{BS_i} \cap V_{M'_k})), \forall b \in \{1; ..; r\}\} \subset V$,
avec $M_{SM} = \bigcup_{c=1}^{o} \{M_{SM_c} \mid Val_{SM}(SM_c) = 1\}$ et $o = \#SM$.

Cette formule calcule la moyenne de la somme des niveaux d'exploitabilité des vulnérabilités de V', multiplie ce résultat par la vraisemblance de la menace M'_k, divise cela par le nombre d'attributs sur lesquels la menace M'_k a un impact, et divise la somme de ces résultats pour chaque menace par le nombre de menaces de M'. Ceci donne un résultat du type de celui calculé dans la formule 4.2. La fonction $MenaceAS$ permet d'assurer que seuls les résultats des menaces ayant un impact sur l'attribut AS_j sont inclus dans le calcul. Les résultats de cette formule ont une vocation didactique car ils montrent au niveau des biens supports les attributs de sécurité mis en danger par les menaces, mais aussi l'ampleur de ce danger sur les différents attributs de sécurité. Cette dernière information fournit un critère supplémentaire pour classer les biens supports.

Il est important de noter que cette formule tient uniquement compte des menaces vraisemblables ciblant le bien support BS_i, parmi celles débloquées par les sources de menaces inclues dans l'évaluation en cours.

Cela signifie que M' ne contient que les menaces de M dont $Val_M > 0$ et appartenant à la fois à M_{BS_i} et à M_{SM} . De plus, l'ensemble V' change avec chaque menace de M'. En effet, la formule ne tient compte que des vulnérabilités spécifiques à BS_i et permettant de concrétiser la menace M'_k. Cela signifie que V' est le résultat de l'intersection entre l'ensemble des vulnérabilités spécifiques au bien support BS_i, soit V_{BS_i}, et permettant de concrétiser la menace M'_k, soit $V_{M'_k}$. Or, comme il y a plusieurs menaces dans M', V' changera à chaque nouvelle menace.

Il est intéressant de noter que, pour chaque menace, la formule 4.4 travaille sur un ensemble de vulnérabilités plus réduit que celui sur lequel la formule 4.1 travaille. En effet, cette dernière ne fait pas la différence entre les vulnérabilités des différents biens supports. Ce choix a été fait pour des raisons de simplicité car il n'est pas envisageable de proposer différents scores, pour une même menace, sans compliquer l'affichage des résultats. De ce fait, réutiliser directement les résultats des formules 4.1 et 4.2 n'est pas possible sans fausser le calcul des formules 4.3 et 4.4.

4.3.4 Calcul du risque pour les biens essentiels

Le niveau de risque d'un bien essentiel donne la valeur du risque que les menaces, dont il est la cible au travers des biens supports auxquels il est lié, lui font courir. Ce niveau est présenté sous deux formes :

1. La forme normale est associée à la question 5 du tableau 4.1 et illustrée par la formule 4.5. Elle donne la valeur totale du risque encouru par le bien essentiel.

Le risque R_{BE_i} associé à un bien essentiel $BE_i \in BE$ est défini selon la formule :

$$R_{BE_i} = \sum_{j=1}^{n} R_{AS_j\, BE_i} \tag{4.5}$$

où $AS_j \in AS$ et $n = \#AS$

Cette formule calcule la somme des résultats obtenus grâce à la formule 4.6. Les résultats de cette formule permettent de classer les biens essentiels en fonction du risque qu'ils encourent.

Il est important de noter que nous avons décidé de présenter ces formules dans cet ordre afin de respecter le tableau 4.1 selon lequel il est plus logique de déterminer le niveau de risque d'un bien essentiel avant de déterminer la répartition de ce risque selon les attributs de sécurité. Cependant, dans les faits, le calcul est réalisé dans l'autre sens.

2. La forme avancée est associée à la question 6 du tableau 4.1 et illustrée par la formule 4.6. Elle donne la répartition du niveau de risque d'un bien essentiel selon les attributs de sécurité sur lesquels les menaces, ciblant les biens supports liés au bien essentiel, ont un impact. Afin de construire cette formule, nous avons observé les liens entre biens essentiels et biens supports.

La part de risque $R_{AS_j\,BE_i}$ associée à un attribut de sécurité $AS_j \in AS$ pour un bien essentiel $BE_i \in BE$ est définie selon la formule :

$$R_{AS_j\,BE_i} = Besoin(BE_i, AS_j) \times \frac{\sum_{k=1}^{n} R_{AS_j\,BS'_k}}{n} \tag{4.6}$$

où $BS'_k \in BS'$, $n = \#BS'$, $BS' = \{BS_l \mid ((Val_{BS}(BS_l) = 1) \wedge (Crois(BE_i, BS_l) = 1)), \forall l \in \{1; ..; m\}\} \subseteq BS$ et $m = \#BS$

Cette formule calcule la moyenne de la somme des parts de risque, associées à l'attribut AS_j, des biens supports liés au bien essentiel BE_i, et la multiplie par le besoin de sécurité de cet attribut. Les résultats de cette formule donnent l'ampleur de l'impact du risque sur les différents attributs de sécurité d'un bien essentiel. Cette dernière information fournit un critère supplémentaire pour classer les biens essentiels.

Il est important de noter que les biens supports intervenant dans le calcul sont identifiés grâce à la matrice de croisement entre biens essentiels et biens supports, présentée dans la section 3.5. Cela signifie que BS' ne contient que les biens supports de BS inclus dans l'évaluation en cours, soit dont $Val_{BS} = 1$, et liés au bien essentiel BE_i, soit dont $Crois(BE_i, BS_l) = 1$.

La fonction $Besoin(BE_i, AS_j)$ donne la valeur du besoin de sécurité exprimé pour l'attribut AS_j du bien essentiel BE_i.

4.3.5 Calcul du risque selon les domaines

Le niveau de risque d'un domaine de l'ISO/IEC 27002 donne l'ampleur de la vulnérabilité d'une entreprise du point de vue de ce domaine. Ce risque représente le danger que le non respect des mesures de sécurité, du domaine en question, pose à la sécurité de l'information d'une entreprise. Ce niveau est représenté sous deux formes :

1. La forme normale est associée à la question 7 du tableau 4.1 et illustrée par la formule 4.7. Elle donne la valeur globale de la vulnérabilité d'une entreprise du point de vue du domaine en question. Afin de développer cette formule, nous avons observé les liens entre les vulnérabilités et les domaines de l'ISO/IEC 27002. Ces liens sont définis dans la section 3.7 et disponibles dans l'annexe H.

Soient $M_{SM_x} \subset M$ l'ensemble des menaces provoquées par une source de menace quelconque de SM,
$M_{BS_x} \subset M$ l'ensemble des menaces ciblant un bien support quelconque de BS,
$V_{BS_x} \subset V$ l'ensemble des vulnérabilités spécifiques à un bien support quelconque de BS et
V_{M_x} l'ensemble des vulnérabilités spécifique à une menace quelconque de M,
alors l'indice de risque global associé à un domaine $D_i \in D$ de l'ISO/IEC 27002 est défini selon la formule :

$$IGR_{D_i} = \sum_{j=1}^{n} \left(Val_V(V'_j) \times \frac{Refs(V'_j, D_i)}{\sum_{j=1}^{n} Refs(V'_j, D_i)} \right) \tag{4.7}$$

où $V' = \{V_l \mid (V_l \in (V_{BS} \cap V_{M'})) \wedge (Refs(V_l, D_i) > 0), \forall l \in \{1; ..; o\}\} \subset V$ et $o = \#V$
$M' = \{M_k \mid (M_k \in (M_{SM} \cap M_{BS})) \wedge (Val_M(M_k) > 0), \forall k \in \{1; ..; m\}\} \subset M$ et $m = \#M$
$M_{SM} = \bigcup_{a=1}^{p} \{M_{SM_a} \mid Val_{SM}(SM_a) = 1\}$ et $p = \#SM$, $M_{BS} = \bigcup_{b=1}^{q} \{M_{BS_b} \mid Val_{BS}(BS_b) = 1\}$ et
$q = \#BS$, $V_{BS} = \bigcup_{c=1}^{q} \{V_{BS_c} \mid Val_{BS}(BS_c) = 1\}$, $V_{M'} = \bigcup_{d=1}^{r} \{V_{M'_d}\}$ et $r = \#M'$.

Cette formule calcule la somme du produit des niveaux de vulnérabilité des vulnérabilités de V' par leur pondération. Le nombre de références de la vulnérabilité V'_j vers le domaine D_i, divisé par la somme des références des vulnérabilités de V' vers le domaine D_i, donne la pondération V'_j. les résultats de cette formule mettent en évidence l'ampleur de la vulnérabilité d'une entreprise du point de vue des domaines de l'ISO/IEC 27002 et ils indiquent implicitement quels domaines sont à observer en priorité afin de diminuer globalement le risque.

Il est important de noter que cette formule tient uniquement compte des vulnérabilités débloquées au cours d'une évaluation et ayant des références vers le domaine D_i. Cela signifie que V' contient uniquement les vulnérabilités de V dont $Refs(V_l, D_i) > 0$ et qui sont à la fois dans l'ensemble des vulnérabilités débloquées par les biens supports inclus dans l'évaluation en cours, soit V_{BS}, et dans l'ensemble des vulnérabilités permettant de concrétiser les menaces inclues dans cette même évaluation, soit V'_M.

Pour rappel, M' est l'ensemble des menaces vraisemblables de M, soit dont $Val_M > 0$, appartenant à l'ensemble des menaces débloquées par les sources de menaces inclues dans l'évaluation, soit M_{SM}, et à celui des menaces ciblant les biens supports dans cette même évaluation, soit M_{BS}.

Il est intéressant de noter que les pondérations dépendent du nombre de vulnérabilités dans V'. Ainsi, elles peuvent varier d'une évaluation à l'autre ou même au cours d'une même évaluation, si la taille de V' change.

2. La forme avancée est associée à la question 8 du tableau 4.1 et illustrée par la formule 4.8. Elle donne la répartition du niveau de risque du domaine D_i selon les attributs de sécurité sur lesquels les menaces de M', que les vulnérabilités de V' permettent de concrétiser, ont un impact. Afin de créer cette formule, nous avons réutilisé la précédente, mais nous avons aussi tenu compte des liens entre menaces et vulnérabilités et des liens entre menaces et attributs de sécurité.Ces liens sont définis dans les sections 3.7 et 3.6 et disponibles dans les annexes I et G.

La part de risque $IGR_{AS_l\,D_i}$ associée à un attribut de sécurité $AS_l \in AS$, pour un domaine $D_i \in D$ de l'ISO/IEC 27002, est définie selon la formule :

$$IGR_{AS_l\,D_i} = \sum_{i=1}^{n} IRG_{D_i} \times \frac{\sum_{j=1}^{m}\left(\sum_{k=1}^{n}\left(MenaceAS(M'_k, AS_l) \times Concret(V'_j, M'_k)\right)\right)}{\sum_{j=1}^{m}\left(\sum_{k=1}^{n} NBAttributs(V'_j, M'_k)\right)} \tag{4.8}$$

où M' et V' sont les mêmes ensembles que dans la formule précédente, $n = \#M'$ et $m = \#V'$

Cette formule pondère le résultat de la formule 4.7 par l'importance de l'attribut AS_j par rapport aux autres attributs. Il s'agit d'une pondération obtenue en additionnant, pour chaque vulnérabilité de V', le nombre de fois qu'elle provoque un impact sur cet attribut, via les menaces de M' qu'elle permet de concrétiser, et en divisant ce résultat par le nombre d'impacts total sur tous les attributs. Les résultats de cette formule mettent en évidence, pour chaque domaine, les attributs menacés par les vulnérabilités qui lui sont liées, ainsi que l'ampleur de cette menace. Ces informations fournissent un critère supplémentaire pour classer les domaines.

Pour rappel, les ensembles M' et V' sont les mêmes que dans la formule 4.7.

Il est important de noter que la fonction $MenaceAS$ vérifie que la menace M'_k a bien un impact sur l'attribut AS_j et la fonction $Concret$ vérifie que la vulnérabilité V'_j peut concrétiser la menace M'_k. Leur combinaison permet d'assurer que le bon nombre d'impacts sur l'attribut AS_j est comptabilisé. La fonction $NBAttributs$ se charge de récupérer le nombre d'attributs sur lesquels les menaces ont un impact afin de calculer le nombre d'impacts total pour tous les attributs.

4.4 Définition des intervalles d'inacceptabilité des scores

Cette section présente la définition des intervalles contenant les valeurs d'inacceptabilité des scores de résultats. Comme ce chapitre le montre, ces scores sont les niveaux de risque calculés à partir des formules de la section précédente. Ces intervalles indiquent à partir de quelle valeur un niveau de risque est trop important pour être ignoré. Par exemple, si le score d'un bien support appartient à l'intervalle défini pour les biens supports, cela signifie qu'il court un risque trop grand et que ce dernier doit être réduit.

Comme cette méthodologie est prévue pour des utilisateurs sans grandes connaissances dans le domaine de la sécurité de l'information et afin de les aider à identifier les niveaux de risque inacceptable dans les différents graphiques de résultats, nous définissons des intervalles par défaut pour les menaces, les biens supports, les biens essentiels et les domaines de l'ISO/IEC 27002. De manière évidente, comme les scores de résultats sont des valeurs $\in [0, 1]$ la borne supérieure de ces intervalles est 1 à chaque fois. Toutefois, les bornes inférieures sont déterminées grâce aux formules de la section précédente :

1. Une menace représente un risque inacceptable à partir du moment où sa vraisemblance est significative, $\geq \frac{2}{3}$, et où la moyenne des niveaux d'exploitabilité de ses vulnérabilités est significative, $\geq \frac{2}{3}$. Ainsi, dès que le score d'une menace $\in [\frac{4}{9}, 1]$, le risque qu'elle représente est considéré inacceptable.
2. L'intervalle pour les biens supports est le même que pour les menaces car la formule fait une moyenne des valeurs de risque des menaces qui le visent.
3. Un bien essentiel fait l'objet d'un risque inacceptable à partir du moment où la moyenne de ses besoins de sécurité est significative, $\geq \frac{2}{3}$, et que la moyenne du risque encouru par ses biens supports est inacceptable, $\geq \frac{4}{9}$. Ainsi, dès que le score d'un bien essentiel $\in [\frac{8}{27}, 1]$, le risque qu'il encourt est considéré inacceptable.
4. La définition de l'intervalle pour les domaines de l'ISO/IEC 27002 est plus arbitraire que pour les autres. En effet, le score d'un domaine dépend du nombre de vulnérabilités exploitables et de leur importance pour le domaine. De plus, comme l'importance d'une vulnérabilité peut changer d'une évaluation à l'autre car l'ensemble de vulnérabilités est lui-même variable d'une évaluation à l'autre, il est difficile de tenir compte de ce facteur. Ainsi, nous choisissons de placer la borne inférieure de cet intervalle à la valeur 0.4. Cela signifie qu'un domaine représente un risque

inacceptable à partir du moment où la moyenne des niveaux d'exploitabilité des vulnérabilités de V' $\in [0.4, 1]$.

Finalement, il est important de noter qu'une version ultérieure de la méthodologie permettra aux utilisateurs de définir eux-mêmes ces intervalles en sélectionnant une réponse dans chaque ensemble de réponses. Ces dernières seront automatiquement combinées de la manière décrite dans cette section afin de déterminer des intervalles propres aux besoins des utilisateurs.

4.5 Conclusion

Dans ce chapitre, nous avons suivi le processus de construction des formules de calcul et de définition des intervalles d'inacceptabilité des scores, pour cette méthodologie, au travers de trois étapes répondant aux cinq problématiques identifiées. En premier lieu, nous avons défini un plan "GQM" d'identification des métriques. En second lieu, nous avons utilisé les informations de ce tableau afin de construire les formules. En dernier lieu, ces formules nous ont servis à définir les bornes inférieures et supérieures des intervalles d'inacceptabilité des scores. L'analyse des résultats obtenus nous permet de tirer quelques conclusions présentées ci-dessous.

Tout d'abord, le calcul du niveau de risque dans les différentes étapes significatives de la méthodologie permet de donner une vue globale du risque à l'utilisateur et de lui montrer les résultats de son cheminement tout au long d'une évaluation.

Ensuite, de par leur nature et grâce à l'utilisation des formules, les scores sont à la fois simples, reproductibles et comparables. Ainsi, les évaluations pourront être confrontées avec un bon degré d'objectivité et de validité des résultats afin de tirer des conclusions sur l'amélioration ou la détérioration des niveaux de risque.

De plus, les intervalles d'inacceptabilité des scores de résultats permettent aux utilisateurs d'identifier facilement les éléments d'une évaluation pour lesquels le niveau de risque est trop important.

Finalement, les formules de calcul désormais établies, la méthodologie est prête à l'emploi. Ainsi, le chapitre suivant en présentera la validation.

Chapitre 5

Validation de la méthodologie

Dans ce chapitre, nous allons présenter la validation de la méthodologie. A cet effet, nous aborderons les objectifs visés par cette action, mais aussi sa préparation, son déroulement et nous terminerons avec la présentation des résultats obtenus.

5.1 Besoin de valider la méthodologie

Le questionnaire méthodologique propose une évaluation de la maturité en termes de sécurité de l'information proche des utilisateurs et facile à utiliser. Afin de la développer, nous avons défini dans la section 3.1 des hypothèses et, sur base de celles-ci, des objectifs à atteindre. Or, dans le but de déterminer s'ils sont satisfaits et donc si le questionnaire est bien conçu et s'il répond aux attentes du public cible, nous devons vérifier s'il est adéquat. A cet effet, nous réalisons une tâche de validation de cette méthodologie, pour laquelle nous identifions plusieurs problématiques.

Tout d'abord, nous devons déterminer les objectifs de cette initiative de validation, afin de guider et donner du sens à cette approche, mais aussi dans le but d'informer les futurs testeurs des tenants et aboutissants de cette action et des éléments auxquels ils devront porter attention lors des tests de validation.

Ensuite, nous déterminons le procédé employé pour réaliser la validation. En effet, comme cela est abordé dans la section 1.4, il existe plusieurs méthodes et il est nécessaire d'en choisir une à la fois adéquate et efficace pour obtenir un maximum de résultats significatifs.

Finalement, une fois le cadre complet de l'initiative de validation défini, il nous reste à l'appliquer. Dans cette optique, nous sélectionnons plusieurs entreprises et nous décrivons le déroulement des tests de validation, ainsi que les interactions avec ces parties prenantes.

5.2 Préparation de la validation

Afin de développer une approche de validation, nous avons suivi un processus en plusieurs étapes. Tout d'abord, nous avons commencé par la création d'un document présentant le cadre de l'initiative de validation et spécifiant les éléments que nous souhaitons vérifier au travers d'objectifs à atteindre. Ces derniers servent à guider cette approche et sont inférés des objectifs de la méthodologie dans la section 3.1. Les objectifs des tests de validation sont les suivants :

1. Déterminer la facilité d'utilisation du questionnaire.
2. Déterminer la clarté et la qualité des questions et des réponses.
3. Déterminer la complétude du contenu du questionnaire.
4. Déterminer si le questionnaire permet d'identifier et comprendre les besoins de sécurité.
5. Déterminer si le questionnaire aide à se familiariser avec le domaine de la sécurité de l'information.
6. Déterminer la clarté des graphiques et la compréhensibilité des résultats qu'ils affichent.
7. Déterminer l'utilité des graphiques.
8. Déterminer la clarté et l'utilité des documents fournis avec l'outil.
9. Déterminer l'existence de bugs dans l'outil.

Ensuite, nous avons créé la documentation de la méthodologie, afin de fournir un produit aussi complet que possible. Cette dernière permet aux utilisateurs souhaitant se renseigner de trouver les réponses à leurs questions sur son fonctionnement et son emploi. Toutefois, nous avons aussi développé un résumé de cette documentation dans le but d'adresser directement l'utilisation de la méthodologie sans surcharger les utilisateurs avec un document trop lourd.

Par après, nous avons choisi la méthode de validation à employer pour tester la méthodologie auprès de différentes entreprises. En effet, il en existe plusieurs et au lieu de n'en choisir qu'une seule, nous avons préféré utiliser une combinaison des variantes présentées dans la section 1.4, afin d'obtenir une méthode de validation aussi complète et efficace que possible. Ainsi, elle est réalisable avec ou sans supervision et elle permet de récupérer un maximum d'informations.

Dans cette optique, nous avons décidé d'organiser des rencontres avec les entreprises, durant lesquelles nous avons réalisé une revue des objectifs du test et du résumé du fonctionnement de la méthodologie. Ensuite, nous avons accompagné le répondant dans la complétion d'un sous-ensemble des données, par

exemple les trois biens essentiels les plus importants et les trois menaces les plus vraisemblables, afin de ne pas prendre trop de temps aux entreprises. Ces sous-ensembles ont été déterminés au moment des tests et selon les désirs du répondant. De plus, au début de chaque étape, nous avons fourni des explications complémentaires à la personne de contact. Une fois l'étape complétée, nous en avons discuté afin d'obtenir les opinions de cette personne et d'estimer sa compréhension des informations parcourues. Il est important de noter que nous n'avions pas l'intention de réaliser des pré-tests, c'est-à-dire de laisser des utilisateurs remplir le questionnaire sans notre aide. Toutefois, l'existence des trois documents accompagnant la réalisation des tests de validation couvre cette éventualité, si elle s'avère nécessaire.

Par la suite, nous avons créé une enquête de satisfaction, disponible dans l'annexe K, à soumettre aux participants en fin de test. Cette technique de récupération d'information vient en complément des interactions avec les participants. A cet effet, nous avons construit, avec "Google Form", un questionnaire en ligne dont les questions adressent les objectifs de l'initiative de validation. Bien que nous ayons l'intention de directement poser certaines de ces questions au cours des discussions avec les répondants, nous avons préféré les garder dans l'enquête, par soucis de complétude et dans l'éventualité où un testeur souhaiterait rajouter des informations.

Finalement, nous avons sélectionné des entreprises auprès desquelles exécuter les tests. Ce choix s'est porté sur les entreprises interviewées durant le mois de décembre 2014 et dont voici la liste :

1. Finomat, une agence immobilière de quatre employés implantée à Namur.
2. Au Plus Net, entreprise/coopérative d'insertion à finalité sociale située à Namur. Elle propose des services de nettoyage et se compose de deux gestionnaires et de 30 travailleurs.
3. Bibliopolis, une entreprise de vente de livres dont le siège social est à Bruxelles. Elle se compose de deux responsables achats qui sont les patrons, d'un comptable et des gérants des sept implantations au travers de la Belgique, pour un total d'environ 15 travailleurs.
4. Priminfo, une entreprise d'assemblage, de livraison et d'installation d'ordinateurs, située à Novilles-les-Bois. Elle se compose d'environ 50 travailleurs en comptant ses deux sous-traitants.

Il est important de noter que Bibliopolis n'a pas participé à ces tests. En effet, malgré de nombreuses tentatives, il n'a pas été possible d'obtenir un rendez-vous. Nous avons aussi tenté de réaliser un pré-test en leur envoyant l'outil méthodologique et les documents. Cependant, bien qu'ils aient confirmé leur désir de le remplir, nous n'avons jamais reçu le questionnaire complété.

5.3 Déroulement

Afin de lancer les tests, nous avons pris contact avec ces quatre entreprises wallonnes, par e-mail et par téléphone, pour fixer des rendez-vous.

Tout d'abord, nous leur avons envoyé le document des objectifs du test, la documentation de la méthodologie et son résumé afin de leur donner le moyen, si elles le désiraient, de prendre connaissance de la teneur du test et du fonctionnement de la méthodologie.

Ensuite, nous nous sommes rendus sur place et nous avons suivi la démarche définie dans la section 5.2. De plus, durant les interactions avec les répondants nous avons posé de nombreuses questions, notamment sur la qualité et la clarté des questions, la compréhension des concepts et des idées véhiculées dans les différentes étapes, ou encore sur la compréhension des graphiques de résultats, afin d'obtenir des réactions spontanées.

Par la suite, nous avons supervisé la complétion de l'enquête de satisfaction, notamment en indiquant les questions devenues inutiles suite aux informations récupérées lors des interactions.

Finalement, parmi les trois entreprises que nous avons assistées dans la réalisation du test, aucune n'avait eu le temps de lire les documents avant notre rencontre. Ainsi, nous leur avons proposé de le faire à leur convenance et de nous contacter avec les réponses à plusieurs questions supplémentaires. En premier lieu, nous leur avons demandé dans quelle mesure les documents avaient répondus à leurs questions sur la méthodologie et son fonctionnement. En deuxième lieu, nous leur avons demandé d'estimer la clarté et la compréhensibilité de ces documents et, en cas d'insatisfaction, de proposer des recommandations pour les améliorer. En dernier lieu, nous leur avons demandé de nous dire s'ils auraient été capables de réaliser le test sans aide extérieure.

5.4 Résultats

Cette section est l'aboutissement de ce travail. La méthodologie, développée au fil des chapitres, propose une évaluation aisée et autonome de la maturité en termes de sécurité de l'information dans une organisation, au travers de la présentation des niveaux de risque encourus par une entreprise.

Nous présentons, dans la figure 5.1, les résultats de la satisfaction des objectifs de la méthodologie, au travers des réponses aux questions à choix multiple de l'enquête de satisfaction et de celles à réponse ouverte abordées de manière globale juste après. Cette enquête est disponible dans l'annexe K. Pour rappel, les choix de réponses pour Q4 sont "Très facile", "Facile", "Difficile", "Très difficile", pour Q8 ces choix sont "Très complet", "Suffisamment complet", "Incomplet", "Très incomplet", et pour toutes les autre questions ces choix sont "Très satisfait", "Satisfait", "Insatisfait", "Très insatisfait".

Il est important de noter que les tests de la méthodologie nous ont permis de couvrir l'ensemble des questions des différentes étapes, à part celles de l'étape des vulnérabilités dont 70% des questions ont été parcourues sur l'ensemble des trois tests. En effet, comme nous l'expliquons dans la section précédente, la portée des tests a été réduite et ainsi, toutes les questions sur les vulnérabilités n'ont pas pu être explorées.

	Réponses des entreprises		
Questions	Finomat	Au Plus Net	Priminfo
Q4	Facile	Facile	Difficile
Q6	Très satisfait	Très satisfait	Satisfait
Q8	Très complet	Très complet	Suffisamment complet
Q10	Très satisfait	Très satisfait	Satisfait
Q12	Très satisfait	Très satisfait	Satisfait
Q14	Très satisfait	Très satisfait	Satisfait
Q16	Satisfait	Très satisfait	Satisfait

TABLE 5.1 – Tableau des résultats de l'enquête de satisfaction

	Finomat	Au Plus Net	Priminfo
Durée	53'	65'	85'

TABLE 5.2 – Tableau des durées des tests

Bien que les résultats de la figure 5.1 sont très positifs, nous avons noté différents éléments intéressants durant les tests.

Tout d'abord, nous avons tenu compte des durées de complétion, disponibles dans la figure 5.2. Elles se situent aux environs d'une heure et sont fortement dépendantes de la vitesse de lecture et de compréhension du questionnaire par les utilisateurs, mais aussi du nombre et de la longueur des questions. La plupart des utilisateurs ont considéré que la complétion du questionnaire prenait beaucoup de temps, même s'ils n'ont pas été gênés par la longueur des questions.

Ensuite, nous avons noté quelques difficultés lors de la sélection des réponses aux questions sur les besoins de sécurité. En effet, certaines réponses demandaient un peu plus de temps de lecture que d'autres afin d'être comprises par les utilisateurs. Ainsi, bien qu'ils ont estimé que les choix disponibles permettaient d'exprimer leurs besoins de sécurité, nous en venons à penser que les réponses associées aux échelles de valeurs pour les attributs d'intégrité et de confidentialité pourraient être reformulées afin d'en faciliter la compréhension.

En outre, Au plus Net et Priminfo nous ont confirmé que la documentation leur aurait permis d'utiliser l'outil sans notre aide, contrairement à Finomat. Toutefois, cette dernière nous a confié qu'il ne s'agissait pas d'un problème venant des documents, dont elle a reconnu la complétude et la clarté, tout comme Au Plus Net et Priminfo. Il est intéressant de noter que Priminfo a émis un doute quant à l'accessibilité du vocabulaire de la documentation par des personnes sans aucune notion de la sécurité de l'information. Toutefois, il ne s'agit pas d'un réel problème car Priminfo est globalement "Satisfait" de la qualité de la documentation. De plus, le doute qu'elle a émis est minimisé par le fait que Finomat et Au Plus Net n'ont pas eu de problème avec ce même vocabulaire.

De plus, nous n'avons rencontré que deux bugs durant les tests. En effet, contrairement à ce que nous pensions, l'outil ne fonctionne pas sur Excel 2013 et lors du test auprès de Priminfo, nous avons eu un problème de calculs des scores qui n'ont ainsi pas pu être affichés. Toutefois, il est important de noter que ce problème a été réglé le jour même et les résultats ont été envoyés par e-mail à la société.

Finalement, nous avons aussi identifié des problèmes au niveau de la facilité d'utilisation du questionnaire. De fait, la police d'écriture de certaines questions est trop petite et cela cause des difficultés de lecture et parfois des oublis car la question passe inaperçue. De plus, les couleurs utilisées dans certains graphiques de résultats ont été jugées trop ternes et similaire, et dans certains cas, l'échelle statique a posé problème pour la lecture des valeurs numériques des différents niveaux de risque. Le dernier problème est l'absence d'une documentation directement intégrée à l'outil. En effet, bien que les entreprises sont en général très satisfaites par la clarté des concepts véhiculés dans les questions, Priminfo a estimé qu'il est nécessaire de fournir cet aspect.

5.5 Conclusion

Dans ce chapitre, nous avons suivi les processus de construction et d'application d'une démarche de validation de la méthodologie, au travers de deux étapes répondant aux problématiques identifiées. En premier lieu, nous avons défini les objectifs, les documents de support de la méthodologie et la méthode de validation. Enfin, nous avons réalisé des tests auprès d'entreprises de la région wallonne, afin de récupérer leurs opinions et leur ressenti. L'analyse des résultats obtenus nous permet de tirer quelques conclusions présentées ci-dessous.

Tout d'abord, le questionnaire a été globalement bien reçu et apprécié par les testeurs. En effet, les données des enquêtes de satisfaction abondent dans ce sens, notamment au niveau de la compréhensibilité des questions et des concepts qu'elles véhiculent. Il est de leur opinion que la méthodologie et assez facile à utiliser et qu'elle permet de se rendre compte des enjeux de la sécurité de l'information, de se familiariser avec les concepts de ce domaine et surtout de comprendre le danger.

Ensuite, la méthodologie n'est pas parfaite et présente plusieurs limites pour lesquelles il est nécessaire de proposer des pistes de solution. De fait, nous avons tout de même noté des hésitations au cours de certaines étapes et quelques difficultés à compléter le questionnaire. Il ne s'agit pas de problèmes majeurs mais il est cependant possible d'améliorer ces aspects.

Finalement, le chapitre suivant présentera ces limites et proposera des améliorations afin de les adresser.

Chapitre 6

Limites de la méthodologie et pistes d'amélioration

Dans ce chapitre, nous allons présenter des pistes d'amélioration pour la méthodologie. En effet, il reste encore une grande quantité de travail à réaliser afin d'améliorer son utilisabilité et son exploitabilité. A cet effet, nous aborderons, section par section, les différentes limites et, pour chacune, la proposition de solution l'adressant.

6.1 Valider les liens entre les vulnérabilités et l'ISO/IEC 27002

A ce stade du mémoire, les liens entre l'ISO/IEC 27002 et les vulnérabilités n'ont pas été validés par un expert. Il s'agit d'une limite importante car elle nous empêche d'assurer les utilisateurs de l'efficacité de la méthodologie au niveau du calcul du risque selon les domaines et aussi de la présentation des recommandations. Dans le but d'adresser ce problème, nous proposons la démarche suivante.

Tout d'abord, nous ferons appel à un expert du domaine de la sécurité de l'information et formé à l'utilisation et à l'application des pratiques et des lignes de conduites du référentiel.

Ensuite, nous emploierons ses connaissances afin de revoir et de vérifier les liens déjà établis. En effet, cela nous permettra de mettre en évidence s'ils sont corrects, incorrects et/ou incomplets.

Finalement, nous en profiterons pour lui demander de nous former afin de pouvoir continuer cette tâche, sans son aide, en cas d'expansion du nombre de vulnérabilités de la méthodologie.

6.2 Proposer des recommandations

A ce stade du mémoire, bien que les vulnérabilités de la méthodologie soient développées de sorte à sous-entendre des recommandations, nous n'en proposons pas, à proprement parler, en fin d'évaluation. Or, ces conseils permettraient aux utilisateurs d'orienter leur démarche d'amélioration de la maturité de la sécurité de l'information. Cette limite est particulièrement importante car elle correspond à la non-satisfaction d'un des objectifs de cette méthodologie et nous proposons de l'adresser de la manière suivante.

Tout d'abord, nous utiliserons la base de connaissances EBIOS, en conjonction avec la dernière version des ISO/IEC 27001 et 27002, afin de créer une base de données des différentes mesures de sécurité applicables.

Ensuite, nous ajouterons une nouvelle étape à la méthodologie, pour afficher les recommandations. Afin de faciliter la tâche à l'utilisateur, nous proposerons trois filtres, pour un total de 19 critères, à cette liste. Le premier filtre permettra de sélectionner le ou les types des mesures : préventives, protectrices et/ou récupératrices. Le second servira à définir la portée de l'ensemble : intersection ou union des critères précédents. Le troisième proposera de sélectionner un ou plusieurs domaines parmi les 14 de l'ISO/IEC 27002 dont l'utilisateur souhaite voir les recommandations. Bien entendu, s'il en choisit plusieurs, le filtre fera une union des ensembles. La combinaison de ces trois filtres permettra d'affiner la sélection des mesures de sécurité.

En outre, les recommandations seront déterminées en fonction des vulnérabilités exploitables de l'évaluation en cours et, implicitement, de leurs liens avec l'ISO/IEC 27002. De plus, les recommandations seront reliées aux menaces grâce aux liens entre les menaces et les vulnérabilités, définis dans la section 3.7 et disponibles dans l'annexe I.

Finalement, les résultats de cette étape seront intégrés au rapport final de l'évaluation.

6.3 Créer une représentation des résultats sous la forme d'un modèle de maturité

A ce stade du mémoire, nous ne produisons pas de représentation des résultats sous la forme d'un modèle de maturité. Bien que les informations sur le risque et la maturité soient analogues, car il est évident qu'un risque élevé est indicateur d'un faible niveau de maturité de la sécurité de l'information, nous ne

pouvons pas simplement réaliser le calcul $M = 1 - R$ où M est la maturité et R le risque, et avancer qu'il s'agit là d'un score de maturité fiable. En effet, comme nous l'abordons dans la section 1.6, la représentation de la maturité nécessite des traitements particuliers comparativement au calcul des scores basé sur des données fournies par les utilisateurs. Il s'agit d'une limite importante car elle correspond à la non-satisfaction d'un objectif de ce travail et nous proposons de l'adresser de la manière suivante.

Tout d'abord, nous réutiliserons l'idée de Spruit et Röling [39] dont le modèle de maturité est présenté dans la section 1.6. Comme dans cet article, les zones de focus du modèle que nous proposons seront les domaines de l'ISO/IEC 27002 et chacune aura ses propres niveaux de maturité, distribués sur un modèle global.

Ensuite, chaque domaine de l'ISO/IEC 27002 présente plusieurs objectifs illustrant eux-mêmes des mesures afin de les satisfaire. Ainsi, pour chaque objectif, les mesures de sécurité et implicitement les vulnérabilités, seront associées aux différents niveaux de maturité. Ce procédé nécessitera la mise en place des dépendances entre les vulnérabilités d'un même niveau de maturité. En effet, si la vulnérabilité associée à la première mesure de sécurité nécessaire à l'atteinte d'un niveau de maturité est exploitable, cela devra se ressentir dans l'affichage du niveau de maturité.

De plus, il sera nécessaire de mettre en évidence les dépendances entre les niveaux de maturité des différentes zones de focus afin de savoir quelles mesures de sécurité, et implicitement quelles vulnérabilités, ont une influence sur l'atteinte de niveaux de maturité en dehors de leur zone de focus.

Par après, beaucoup d'informations sur ces dépendances sont disponibles dans le modèle ISFAM. Cependant, des travaux d'adaptations seront nécessaires afin de faire correspondre les données issues de la version 2005 de l'ISO/IEC 27002 avec celles issues de la version de 2013 et pour inclure les nouveaux domaines apparaissant dans cette version.

Par ailleurs, nous utiliserons un deuxième modèle de maturité, le modèle final. Il présentera le niveau de maturité global d'une entreprise. Ce dernier sera déterminé sur base des niveaux de maturité atteints dans les zones de focus.

Finalement, il convient de dire que cette tâche représente une charge de travail très lourde, mais surtout, à réaliser uniquement après avoir développé une base de connaissances des vulnérabilités suffisamment étendue et dont les liens avec l'ISO/IEC 27002 sont validés.

6.4 Générer automatiquement le rapport d'une évaluation

A ce stade du mémoire, nous ne produisons pas de rapport. Or, la génération automatique d'un compte rendu complet améliorerait l'exploitabilité de la méthodologie et permettrait aux utilisateurs de bénéficier de l'application périodique de cette dernière, afin de se rendre compte plus facilement de l'amélioration ou de la détérioration de la situation de leur entreprise. Il s'agit d'une limite majeure car elle correspond à la non-satisfaction d'un des objectifs de la méthodologie et nous proposons de l'adresser des deux manières suivantes.

6.4.1 Aspect méthodologique

L'aspect méthodologique correspond au contenu du rapport et comment il sera proposé. Tout d'abord, dans cette proposition d'amélioration, la génération du rapport utilisera le contenu des différentes sections du questionnaire et leurs liens afin d'établir des récapitulatifs selon la structure suivante : Bien essentiel - Sources de menaces - Biens supports - Menaces. Nous choisissons d'utiliser le concept de bien essentiel comme racine car il s'agit de l'élément suscitant le plus d'intérêt pour l'utilisateur et à propos duquel il est nécessaire de fournir un maximum d'informations.

Ensuite, ces récapitulatifs seront accompagnés de nouveaux graphiques pour chacun des éléments cités, sauf les sources de menaces. Il est intéressant de noter que pour chaque récapitulatif, le graphique des menaces ne sera pas celui présenté actuellement dans les résultats, mais une version ne contenant que les menaces correspondant aux biens supports de ce bien essentiel, et dont les scores auront été recalculés.

En effet, comme nous l'expliquons dans le chapitre 4, le graphique des menaces actuel ne fait pas la différences entre les vulnérabilités des différents biens supports pour des raisons de simplicité d'affichage des résultats. Cependant, le rapport permettra de passer au delà de ce problème et de proposer des graphiques où le score de chaque menace est bien la valeur qui intervient dans le calcul du score d'un bien support, comme c'est le cas dans les formules 4.3 et 4.4.

Par après, chaque bien essentiel se fera assigner une liste de recommandations afin d'adresser son niveau de risque. Ces dernières seront issues de la liste de recommandations proposée en fin d'évaluation et éventuellement filtrée par l'utilisateur, comme nous l'expliquons dans la section 6.2. De plus, chaque bien essentiel sera classé selon son score de risque dans la catégorie correspondante parmi les suivantes : risque inacceptable et risque acceptable.

Finalement, ce rapport contiendra aussi les graphiques des scores des domaines et les modèles de maturité présentant les résultats de l'évaluation.

6.4.2 Aspect technique

L'aspect technique correspond aux propositions de solutions visant à automatiser la génération du rapport :

1. La première solution consiste à créer un parseur et un générateur de fichier pdf en Java. Le parseur récupérera les informations d'une évaluation et les donnera au générateur dont le but sera de produire un rapport structuré.
2. La seconde solution consiste à utiliser le logiciel Adobe Pro et le langage Javascript. Le logiciel servira à créer un document pdf modifiable, dont les champs seront remplis grâce aux commandes Javascript dont le but sera de récupérer les données d'une évaluation.

De plus, dans le but de simplifier la réalisation de ces solutions, il est possible de créer un tableau, dans l'outil, regroupant les données du rapport et sur lequel le parseur ou les commandes javascript travailleront directement.

Finalement, la première solution sera plus facile à mettre en oeuvre, mais compliquera l'utilisation de la méthodologie à cause de l'apparition d'un nouvel exécutable. A l'inverse, la seconde solution proposera un outil intégré, mais sa mise en oeuvre sera bien plus complexe.

6.5 Améliorer la complétude et la compréhensibilité des réponses

Plusieurs étapes du questionnaire posent des questions dont les réponses sont issues d'échelles de valeurs, par exemple les besoins de sécurité et la vraisemblance. Or, comme nous en parlons dans la section 5.4, certains utilisateurs ont rencontré des difficultés lors du choix de leur réponse pour les besoins de sécurité d'intégrité et de confidentialité. Bien qu'il s'agisse d'un problème mineur, nous le considérons comme une limite et nous proposons d'y remédier de la manière suivante.

Tout d'abord, il est possible de reformuler ces réponses afin de les rendre encore plus accessibles aux utilisateurs. Toutefois, une autre solution est d'ajouter, à l'image de la méthode Octave Allegro abordée dans la section 1.3.3.2, une nouvelle étape au début de la méthodologie. Cette dernière permettra aux utilisateurs de définir des échelles de valeurs qualitatives pour certains paramètres d'une évaluation, comme la vraisemblance ou les besoins de sécurité. Toutefois,

il est important de noter que les réponses actuelles seront toujours disponibles, si l'utilisateur choisit de ne pas créer les siennes.

Ensuite, un calcul s'effectuera sur ces échelles afin d'assurer une correspondance entre une réponse et une valeur quantifiable, pour les calculs des scores. Simplement, un algorithme parcourra chaque ensemble de réponses et appliquera la formule de calcul suivante :

Soit R un ensemble de réponses pour un paramètre d'une évaluation, comme la vraisemblance. La valeur associée à une réponse $R_i \in R$ est définie selon la formule :

$$R_i = \frac{n-i}{n-1} \tag{6.1}$$

où $n = \#R$, $i <= n$ et $R_i > R_{i+1}$ car les réponses sont classées par ordre décroissant d'importance.

Finalement, cette amélioration apportera plusieurs avantages. En premier lieu, le processus de réponse de l'utilisateur sera facilité, grâce à sa familiarité avec les choix. En deuxième lieu, les réponses correspondront mieux au contexte de l'entreprise, par rapport à celles prédéfinies. En dernier lieu, chaque ensemble de réponses, s'il est correctement réalisé, sera plus complet que ceux proposés par défaut et leur combinaison permettra des calculs plus précis. Cependant, il est important de noter que cette solution pourrait avoir des conséquences négatives sur la complétion du questionnaire méthodologique. En effet, les réponses actuelles sont alignées avec leurs questions. Ainsi, si un utilisateur crée son propre ensemble de réponses, pour des questions dont il ne connaît pas la formulation, ces réponses risquent d'être incohérentes avec les questions. Cela lui compliquera la tâche lors de la complétion du questionnaire.

6.6 Pondérer les menaces

A ce stade du mémoire, les menaces ne sont pas pondérées les unes par rapport aux autres, bien que la démarche de fusion mette en évidence cette problématique. Il s'agit d'une limite mineure car la présence du facteur de vraisemblance permet déjà de pondérer le danger que représente chaque menace. Toutefois, nous proposons d'y remédier de la manière suivante.

Tout d'abord, nous compléterons la base de données des menaces de la méthodologie en ajoutant pour chacune les différentes menaces EBIOS dont elles sont la fusion.

Ensuite, au cours d'une évaluation, un algorithme prenant en compte cette information consultera les menaces et réalisera les opérations suivantes pour chacune :

1. Vérifier si la menace est vraisemblable, c'est-à-dire dont $Val_M > 0$.
2. Si elle l'est, récupérer, dans la base de données, le nombre de menaces EBIOS dont la menace est la fusion.
3. Calculer la somme du nombre de menaces EBIOS dont les menaces vraisemblables de cette évaluation sont la fusion.
4. Diviser le résultat du point 2 par celui du point 3 donne la pondération de la menace.

En outre, il est intéressant de noter que ces pondérations ne seront pas des valeurs statiques. En effet, elles seront calculées selon le nombre de menaces vraisemblables et ce nombre peut changer en cours d'évaluation, ou d'une évaluation à l'autre.

De plus, l'application de cette nouvelle formule nous obligera à modifier la formule 4.4, afin de tenir compte de ces nouvelles pondérations.

Finalement, cette amélioration permettra d'améliorer la précision des calculs des scores en valorisant l'importance des nouvelles menaces les unes par rapport aux autres.

6.7 Pondérer les vulnérabilités

A ce stade du mémoire, les vulnérabilités sont uniquement pondérées pour le calcul des scores associés aux domaines de l'ISO/IEC 27002. Il s'agit d'une limite mineure car la formule de calcul du risque ne tient pas compte de cette information. Toutefois, nous proposons trois manières d'y remédier.

Tout d'abord, la première approche tient compte du nombre de références des vulnérabilités vers les domaines de l'ISO/IEC 27002, indicateur de l'importance de ces vulnérabilités pour ces domaines et du danger qu'elles représentent pour la sécurité de l'information en général. Ainsi, un algorithme parcourra les vulnérabilités d'une évaluation et réalisera les opérations suivantes pour chacune :

1. Récupérer, dans la base de données, le nombre de références vers les domaines de D que possède cette vulnérabilité.
2. Calculer la somme du nombre de références que possèdent les vulnérabilités de l'évaluation en cours.
3. Diviser le résultat du point 1 par celui du point 2 donne la pondération de la vulnérabilité.

Ensuite, la seconde approche tient compte du nombre de menaces que chaque vulnérabilité permet de concrétiser. Ainsi, un algorithme parcourra les vulnérabilités d'une évaluation et réalisera les opérations suivantes pour chacune :

1. Calculer le nombre de menaces vraisemblables de l'évaluation en cours, c'est-à-dire dont $Val_M > 0$, que la vulnérabilité permet de concrétiser.
2. Calculer la somme du nombre de menaces vraisemblables de l'évaluation que toutes les vulnérabilités de cette même évaluation permettent de concrétiser.
3. Diviser le résultat du point 1 par celui du point 2 donne la pondération de la vulnérabilité.

Par la suite, la dernière approche consiste à combiner les deux précédentes afin d'obtenir une pondération, spécifique à la démarche de fusion et prenant en compte le domaine de la sécurité de l'information. Les pondérations seront obtenues en réalisant une moyenne des pondérations des approches précédentes.

En outre, l'application de n'importe laquelle de ces alternatives nous obligera à modifier les formules 4.1 et 4.4. En effet, ces dernières calculent une moyenne, désormais inutile grâce aux nouvelles pondérations.

Finalement, cette amélioration permettra d'améliorer la précision des calculs de scores en valorisant l'importance des vulnérabilités.

6.8 Diminuer la longueur du questionnaire

Dans son état actuel, cette méthodologie demande au moins une heure pour être complétée, même si l'on réduit la portée d'une évaluation. Ce problème est principalement une conséquence du nombre de questions et de la longueur de certaines d'entre elles. Bien que les testeurs n'ont pas manifesté de mécontentement concernant la longueur des questions, ils reconnaissent tout de même que la complétion est trop longue. Il s'agit d'une limite importante de cette proposition de solution, prévue pour être rapidement réalisée, mais il est nécessaire de mettre ce problème en perspective notamment vis-à-vis des objectifs de ce travail, dont certains entrent en conflit.

Tout d'abord, il est difficile de proposer une évaluation de la maturité en termes de sécurité de l'information complète et valide en un nombre réduit de questions. En effet, le domaine de la sécurité de l'information est trop vaste et trop complexe pour espérer l'illustrer et le faire comprendre à des novices en seulement quelques questions. Par exemple, si nous prenons simplement les vulnérabilités comme exemple indicateur, nous en proposons une centaine et cela ne couvre toujours pas l'ensemble de celles proposées dans l'ISO/IEC 27005 et encore moins celles de la base de connaissances MEHARI qui en compte environ 800.

De plus, les tentatives de réduction du nombre de questions n'ont pas porté de bons résultats. En effet, l'application des filtres n'est pas aussi efficace que

l'on pourrait l'espérer et la fusion des éléments, bien que réduisant le nombre de questions, augmente leur longueur.

Ensuite, le besoin de créer des questions menées par l'exemple, afin de permettre une évaluation autonome, nous oblige à proposer suffisamment d'exemples afin d'assurer la compréhension des questions par les utilisateurs et cela en augmente la longueur.

Cependant, il est important de noter que la méthodologie prend tout de même moins de temps à réaliser qu'une étude EBIOS, OCTAVE, ou encore MEHARI. Toutefois, nous souhaitons proposer une piste afin de diminuer le nombre de questions.

A cet effet, nous proposons de modifier l'étape d'identification des biens essentiels en la transformant en une matrice de croisement. Ses lignes seront les trois questions permettant d'estimer l'importance des besoins de sécurité, fusionnées avec les questions permettant d'identifier les attributs de sécurité. Ses colonnes seront les descriptions des biens essentiels, impliquant la disparition des questions explicites sur les biens essentiels, en faveur de questions implicites.
Afin de ne pas inclure des biens essentiels dans une évaluation, l'utilisateur pourra soit mettre la réponse équivalente à la valeur nulle pour chacun de leurs besoins de sécurité, soit les laisser vides auquel cas l'outil se chargera automatiquement de les ignorer.

Finalement, ces changements amélioreront la rapidité de complétion du questionnaire, notamment en réduisant le nombre de questions, sans pour autant lui faire perdre son côté didactique et d'aide à la compréhension des enjeux de la sécurité.

6.9 Amélioration de la lisibilité des questions

Dans son état actuel, l'outil ne gère pas automatiquement la taille de la police d'écriture des questions et des réponses. Ainsi, certaines sont trop petites pour certains utilisateurs. Cela peut poser des problèmes de lecture, ou d'oubli des questions car elles passent inaperçu durant une évaluation. De plus, si l'utilisateur se sert d'une résolution d'écran particulièrement grande, la lecture des questions et des réponses n'en sera que plus difficile. Il s'agit d'une limite mineure mais nous proposons de l'adresser en créeant un algorithme capable de définir la taille de la police d'écriture de ces éléments en fonction de la résolution de l'écran.

6.10 Améliorer la lisibilité des graphiques

Dans son état actuel, l'outil propose une échelle et des couleurs prédéterminées pour l'affichage des résultats. Ceci peut compliquer leur lecture, surtout si les scores sont petits. Il s'agit d'une limite vraiment mineure, mais nous proposons de l'adresser de la manière suivante.

Tout d'abord, nous modifierons le code de génération des graphiques, afin que l'échelle soit gérée automatiquement par l'outil. Ainsi, même si les scores sont petits, les graphiques resterons lisibles. Toutefois, il conviendra de rappeler à l'utilisateur que les valeurs restent comprises entre 0 et 1.

Ensuite, nous utiliserons des nouvelles couleurs plus intenses, telles que le jaune, le rouge et le bleu, pour améliorer la lisibilité des résultats.

Finalement, il permettront aux utilisateurs de déterminer eux-mêmes les paramètres précédents. Nous proposerons aussi un ensemble de plusieurs couleurs vives à sélectionner.

6.11 Intégrer la documentation dans l'outil

Dans son état actuel, l'outil ne propose pas de documentation en son sein car il s'agit d'un document extérieur. Cette limite est mineure mais nous proposons de l'adresser de la manière suivante.

Tout d'abord, nous créerons dans l'outil plusieurs points d'accès affichant un formulaire Excel composé de plusieurs pages. Ces dernières contiendront la documentation des différentes étapes de la méthodologie.

Ensuite, nous paramétrerons ce formulaire afin qu'il s'ouvre directement à la page contenant les informations de l'étape depuis laquelle il est ouvert.

Finalement, ce formulaire contiendra les liens vers les documents originaux de la documentation et de son résumé afin de les ouvrir facilement depuis l'outil.

6.12 Continuation du projet

Cette limite est la plus évidente, il s'agit de continuer le travail en proposant une nouvelle version de la méthodologie mais aussi en la testant davantage.

Tout d'abord, la méthodologie devra tenir compte des propositions de solutions présentées dans ce chapitre et voir sa base de connaissances complétées, notamment au niveau des vulnérabilités dont nous ne traitons qu'une partie.

Ensuite, il est important de noter que certaines de ces pistes de solutions, telles que les pondérations pour les vulnérabilités et les menaces, devront faire l'objet d'une validation par des experts afin de nous assurer de leur adéquation et efficacité.

De plus, nous devrons identifier et idéalement solutionner le problème du fonctionnement de l'outil méthodologique sur Excel 2013, tout en conservant la compatibilité avec les autres versions à partir de 2007.

Par après, la nouvelle version devra aussi faire l'objet d'une validation par les utilisateurs. Dans l'idéal, nous commencerons avec les entreprises déjà contactées afin d'obtenir leur opinion sur les modifications apportées et nous continuerons avec de nouveaux contacts dans le but de récolter un maximum d'informations. Celles-ci permettront d'obtenir davantage de données, issues de milieux encore plus variés, sur l'efficacité de la méthodologie.

Finalement, les tests de validation devront inclure des pré-tests afin de déterminer la faisabilité d'une évaluation avec seulement la documentation, son résumé et sans aide externe. En effet, bien que nous ayons déjà des données sur le sujet, des mises en situation réelle permettront d'obtenir des informations plus précises.

Chapitre 7

Conclusion

Tout au long de ce mémoire, nous avons décrit le développement et la validation d'une méthodologie d'évaluation de la maturité en termes de sécurité de l'information dans les petites et moyennes entreprises, au travers des diverses étapes de sa création : la conception de sa structure et de son déroulement, la création de son contenu, de son outil de support et des formules de calcul, et finalement, le développement et l'application d'une méthode de validation.

La conceptualisation de cette méthodologie nous a permis d'identifier les concepts à intégrer et leurs liens, pour ensuite nous guider dans le développement du contenu et des formules l'utilisant pour calculer les résultats d'une évaluation.

En effet, nous avons ainsi déterminé la structure du questionnaire méthodologique, composé de sections de questions proposant des réponses prédéfinies qui possèdent des valeurs numériques, les liens entre ces questions et le domaine de la gestion du risque, mais aussi les liens entre les questions de différentes sections. Nous avons également identifié les données sur lesquelles appliquer des formules de calcul afin d'obtenir des scores de résultats et nous avons utilisé ces formules afin de déterminer des niveaux de risque inacceptable.

Ensuite, la validation de la méthodologie, au travers de tests effectués auprès d'entreprises de la région wallonne, nous a permis de vérifier la satisfaction des objectifs de la méthodologie et de récupérer les opinions des participants. Ces informations nous ont permis de poser un regard critique et objectif sur la méthodologie afin de déterminer les limites de cette dernière et elles nous ont donné une base de réflexion afin de proposer des pistes de solutions les adressant.

Bien que la construction de la méthodologie fut difficile et nous ait imposé de nombreuses remises en question, elle représente un bon point de départ pour l'évaluation de la maturité en termes de sécurité de l'information. De plus, elle

est facile à utiliser, didactique et plus accessible par rapport aux standards et aux méthodes actuellement disponibles, tels que les ISO/IEC de la famille 2700x et les méthodes EBIOS, MEHARI, OCTAVE, OCTAVE-S et même OCTAVE Allegro.

Nous avons bon espoir, d'ailleurs les résultats de la validation vont dans ce sens, qu'elle permettra d'aider à la compréhension du domaine de la sécurité de l'information, de ses enjeux et des besoins de sécurité des entreprises, tout en amenant les utilisateurs à considérer leurs vulnérabilités et les moyens de les adresser.

Actuellement, la sécurité de l'information est vraiment au coeur de l'actualité et, de plus en plus, les entreprises se retrouveront dans l'obligation d'en considérer les tenants et les aboutissants afin de rester crédibles, fonctionnelles et de garder la confiance de leur clientèle. Ce travail apporte une bonne contribution à la réalisation de cette opération. Toutefois, la sécurité de l'information est un domaine tellement évolutif, complexe et large que la difficulté à l'appréhender posera encore des problèmes, et il sera nécessaire de continuer à sensibiliser les utilisateurs.

Ainsi, il convient de pousser encore plus loin la méthodologie développée dans ce document afin de continuer d'abonder dans le sens des utilisateurs en allant à la rencontre de leurs besoins d'une manière toujours simple mais encore plus complète et efficace, tout en leur assurant un meilleur niveau de qualité et de fiabilité des résultats fournis.

Pour l'instant, nous pouvons nous réjouir de l'importance que prend la sécurité de l'information dans l'actualité des médias. En effet, cet essor amènera les entreprises à s'intéresser davantage à ce domaine et ses concepts. Cela les motivera à utiliser la méthodologie développée dans ce mémoire et éventuellement, au fur et à mesure que leurs connaissances s'améliorent, d'autres plus compliquées telles qu'EBIOS, OCTAVE ou MEHARI.

Annexe A

Contenu du CD-ROM

Cette annexe liste le contenu du disque optique rendu avec le mémoire.

1. L'outil méthodologique SecUnamur sous la forme d'un classer Excel.
2. La documentation de la méthodologie et de l'outil en version PDF.
3. Le résumé de cette documentation en version PDF.
4. Le document des objectifs de la validation de la méthodologie, en version PDF. Il comprend le lien vers l'enquête de satisfaction.
5. La seconde version de SecUnamur contenant plusieurs améliorations.
6. La seconde version de la documentation de la méthodologie et de l'outil en version PDF.
7. La seconde version du résumé de cette documentation en version PDF.
8. Le mémoire en version PDF.

Annexe B

Le langage UML

Ce langage de modélisation intervient dans le cadre de ce travail car il est utilisé pour modéliser la structure et le comportement de la proposition de solution. A cet effet, nous allons brièvement en parler et présenter les deux types de diagrammes qui nous intéressent principalement : les diagrammes de classes et d'activités.

Tout d'abord, le langage UML, ou Unified Modeling Language, apparaît en 1996 avec sa version 0.9 . Il est issu du désir d'unir les différents langages de modélisation populaires à l'époque, soit BOOCH, OMT et OOSE. Actuellement, UML en est officiellement à la version 2.4.1 datant d'août 2011. Cependant, il existe une version 2.5 d'octobre 2012 mais elle est toujours en bêta test.

De plus, ce formalisme permet de modéliser, grâce à des images au sens prédéfini et communément accepté, des systèmes logiciels, des structures, des comportements, des architectures, des structures de données et des processus business. Actuellement il existe environ 13 sortes de diagrammes différents, chacun permettant de modéliser des concepts et véhiculer des informations spécifiques à leur famille et leur type.

Finalement, il existe trois famille de diagrammes dans UML. La première contient les diagrammes de structure, soit ceux de classes, d'objets, de composants, de structure composite, de package et de déploiement. La seconde contient les diagrammes de comportements, soit ceux de cas d'utilisation, d'activité et de machine à état. La dernière famille contient les diagrammes d'interactions, soit ceux de séquences, de communication, de synchronisation et d'aperçu des interactions.

B.1 Diagrammes de classes

Les diagrammes de classes[10, 27] permettent de créer des entités, sous la forme de classes, représentant les concepts d'un système. Typiquement, une classe se divise en trois parties horizontales, la première contient le nom, la seconde, contient les attributs avec leur type et éventuellement leur multiplicité et la dernière contient les opérations à implémenter pour la classe.

Bien souvent, ce genre de diagramme sert à représenter la structure d'un système. Ainsi, les utilisateurs ne s'occupent pas toujours de définir les attributs, sauf ceux vraiment importants, ni les opérations, mais se concentrent principalement sur les classes et leurs relations. En effet, les entités peuvent être connectées les unes aux autres grâce à des liens prenant la forme de traits, orientés ou non. Cette orientation indique le sens obligatoire de lecture de la liaison. De plus, à moins que la relation ne soit bi-directionnelle, l'entité ciblée n'a pas connaissance de son lien avec l'entité la ciblant.

Comme le montre la table B.1, il existe plusieurs manières d'établir des connexions entre les concepts d'un diagramme de classes. Parmi celles-ci, nous avons la relation d'association. Elle permet de réaliser une liaison entre deux classes et de spécifier ce lien en nommant explicitement la relation. Comme le montre la table B.2, chaque extrémité possède une cardinalité indiquant le nombre de relations possibles entre les entités liées.

Ensuite, nous avons la relation d'héritage, permettant de généraliser des concepts du diagramme en créant des sur-types et des sous-types. Un sur-type contient tous les attributs et opérations communes à ses sous-types, en ayant eux-mêmes des spécifiques au concept qu'ils illustrent. Les relations d'héritage n'admettent pas la détermination de cardinalités, car elles sont implicites. Toutefois, il est possible spécifier des contraintes sur les ensembles de population des sous-types afin de mettre en évidence si elles sont disjointes, couvrent totalement ou partiellement la population du sur-type et sont partitionnées.

Par après, nous avons la relation d'agrégation qui représente une relation, entre deux entités, selon laquelle l'entité ciblée par le lien est une partie de celle qui la cible. Dans ce cas de figure, l'entité composante, soit la cible, ne nécessite pas la présence de l'entité composite pour exister.

Enfin, la dernière est la relation de composition. Il s'agit d'une version plus contraignante de la dépendance précédente. En effet, elle exprime que l'entité composite est composée d'un ensemble d'instances de l'entité pointée par le lien. Ce lien est plus fort que le précédent car l'entité composante ne peut pas exister sans l'entité composée dont elle est une partie intégrante.

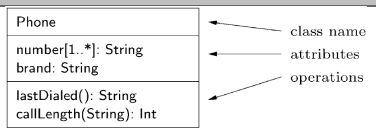
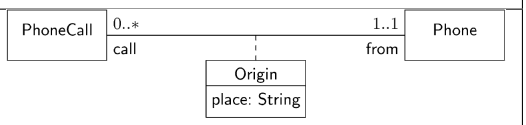
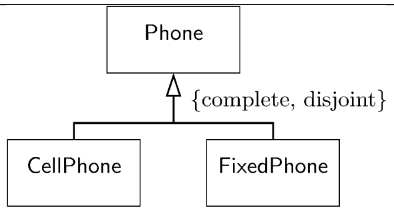
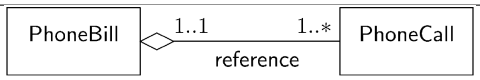
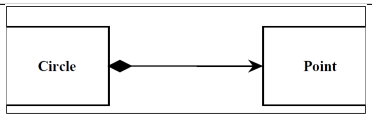
Concepts	Représentation
Classe	
Relation d'association	
Relation d'héritage	
Relation d'agrégation	
Relation de composition	

TABLE B.1 – Tableau illustrant les principaux concepts des diagrammes de classes

Cardinalité	Explication
$m_l..m_u$	Forme des cardinalités exprimant le nombre d'association entre des entités, dont m_l est La borne inférieure et m_u la borne supérieure.
0..1	Relation facultative, 0 ou 1.
1	Relation obligatoire, 1.
0..* ou *	Relation facultative, 0 à plusieurs.
1..*	Relation obligatoire, 1 à plusieurs.

TABLE B.2 – Tableau illustrant les principales cardinalités UML des diagrammes de classes

B.2 Diagrammes d'activités

Les diagrammes d'activités[9, 27] permettent de représenter graphiquement le comportement d'un flux de données dans un système, ainsi que les acteurs impliqué dans son déroulement et les activités qui les concernent. Ils sont notamment utilisés pour représenter le déroulement de méthodes et pratiques, en étayant leurs activités, les relations entre elles, leur ordre, etc.
Les concepts principaux de ce type de diagramme sont présentés dans la table B.3.

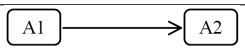
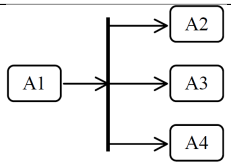
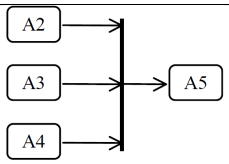
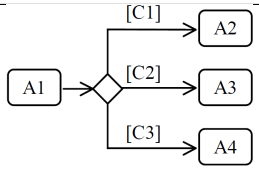
Concepts	Représentation	Explication
Noeud initial		Le noeud marquant le début d'une activité.
Noeud final		Le noeud marquant la fin d'activité. Ce noeud marque la fin de tous les flux d'une activité.
Noeud final		Le noeud marquant la fin du flux. La terminaison d'un flux n'a aucune influence sur les autres toujours en cours.
Noeud action		Une activité dont l'exécution change l'état du système.
Noeud objet		Activité abstraite pouvant résulter de l'exécution d'un noeud action, et servir d'input à un autre.
Transition		Les activités s'exécutent les unes après les autres.
Noeud Fork		Une processus peut être séparé en plusieurs. Cela permet à plusieurs activités d'être réalisées en même temps.
Noeud Join		Il permet de synchroniser plusieurs flux, en les fusionnant, avant de continuer.
Noeud de décision		Il propose plusieurs options d'exécution du flux, chacune dépendant d'une condition.

TABLE B.3 – Tableau illustrant les principaux concepts des diagrammes d'activités

Annexe C

Excel et le langage VBA

Cette annexe aborde le fonctionnement de Microsoft Excel 2007 et de son langage VBA, Visual Basic for Applications [15]. Nous considérons que le lecteur possède un savoir basique de cet outil et du langage de programmation qu'il propose, ainsi nous en parlerons brièvement.

Il s'agit d'un logiciel supportant une implémentation orientée objet du Visual Basic de Microsoft. Il est capable de gérer des classeurs aux formats XLSM ou XLS, soit avec ou sans l'activation des macro-commandes. Ces dernières sont des ensembles d'instructions, soit des procédures, des fonctions ou des événements, s'exécutant à l'aide d'une commande unique, venant du clavier ou de la souris. Toutefois, il est possible de les créer soi-même dans l'environnement de développement qui accompagne Excel, ou via l'enregistreur de macro-commandes disponible dans l'interface de l'outil. Une fois lancé, les actions de l'utilisateur sont enregistrées jusqu'à ce qu'il l'arrête, néanmoins cette option est limitée et ne remplace pas la programmation directe dans l'IDE. Ces commandes servent à automatiser ou à déclencher des comportements spécifiques aux manipulations des utilisateurs ou aux changements réalisés sur les feuilles.

Tout classeur est constitué d'une à plusieurs feuilles, chacune faite d'un ensemble de cellules arrangées en lignes et en colonnes, et dont le contenu apparaît en clair. Cet outil possède aussi des fonctionnalités déjà implémentées et permettant de faire appel à des fonctions communes, de créer des graphiques ou des tableaux, de protéger l'accès au code des fonctions, etc.

Ces classeurs permettent de réaliser des tâches de calcul, de comptabilité, ou encore de base de données, mais ils ne se limitent pas à cela. Grâce au langage VBA, Excel donne les moyens de créer toutes sortes d'outils, tels que des questionnaires, des agendas intelligents, etc.

Voici un exemple simple et explicite d'une procédure provenant de l'outil de support de la méthodologie, elle effectue un triage sur un "Field of integer", un type de donnée plus performant qu'un tableau d'entiers :

```
1  Sub QuickSort(Field() As Integer,ByVal LB As Long,ByVal
       UB As Long)
2  Dim P1 As Long, P2 As Long, Ref As String, Temp As String
3  P1 = LB
4  P2 = UB
5  Ref = Field((P1 + P2) / 2)
6       Do
7            Do While (Field(P1) < Ref)
8                 P1 = P1 + 1
9            Loop
10           Do While (Field(P2) > Ref)
11                P2 = P2 - 1
12           Loop
13           If P1 <= P2 Then
14                Temp = Field(P1)
15                Field(P1) = Field(P2)
16                Field(P2) = Temp
17                P1 = P1 + 1
18                P2 = P2 - 1
19           End If
20      Loop Until (P1 > P2)
21 If LB < P2 Then Call QuickSort(Field, LB, P2)
22      If P1 < UB Then Call QuickSort(Field, P1, UB)
23 End Sub
```

Cette section ne présente qu'une introduction à l'outil Excel et son langage, et il reste encore beaucoup de fonctions dont nous n'avons pas parlé pas, par exemple le "Select Case" ou encore les fonctions de manipulation des cellules des feuilles.

Par ailleurs, cette version du programme n'est pas très récente, cependant, elle présente plusieurs avantages qui nous conviennent. En effet, les classeurs qui fonctionnent sur cette version fonctionneront aussi sur des versions plus récentes. De fait, Office 2013 et les versions précédentes supportent les classeurs utilisant des macro-commandes implémentées sous Office 2007.

De plus, nous avons constaté que beaucoup de personnes utilisent encore Windows Vista, et Windows Seven, rendant le choix de ce logiciel pratique car utilisable par plus de personnes, même si plus tard elles décident de migrer vers

un système d'exploitation plus récent, ainsi qu'une version d'Office plus récente.

Finalement, étant donné que la suite Office est très populaire et répandue sur plusieurs systèmes d'exploitation tels que Windows et Mac, le choix de ce logiciel pour supporter la méthodologie n'en n'est que plus pertinent. Le tableau C.1 illustre et explique les concepts les plus importants de ce langage.

Concepts VBA	Explication
[Private | Public | Friend] [Static] Sub name [(arglist)] [statements] End Sub	Permet de définir une procédure avec ses arguments.
[Public | Private | Friend] [Static] Function name [(arglist)] [As type] [statements] [name = expression] End Function	Permet de définir une fonction avec ses arguments, et le type de la valeur retournée.
Do [While | Until condition] [statements] Loop	Permet d'itérer tant que la condition n'est pas remplie ou jusqu'à ce qu'elle le soit.

If condition Then
[statements]
[ElseIf condition-n Then
[elseifstatements]
[Else
[elsestatements]]
End If
	Exécute les instructions selon la valeur de l'expression.

For Each element In group [statements] Next [element]	Répète des instructions pour chaque élément d'un tableau ou d'une collection.
[Public | Private | Dim] varName [As type]	Permet de déclarer des variables et leur type.
Exit [Sub | Function | Property | For | Do]	Permet de sortir directement d'un des concepts listés.

TABLE C.1 – Tableau explicatif des principaux concepts du langage VBA [15]

Annexe D

Résumé des menaces EBIOS

Cette annexe contient les tableaux des menaces EBIOS et des caractéristiques permettant de les filtrer. Ils sont créés à partir de la base de connaissances EBIOS et de l'ISO/IEC 27005. Cette annexe contient aussi une légende des termes utilisés dans les tableaux.

De plus, ces tableaux permettent de savoir quelles menaces visent quels biens supports et les attributs de sécurité sur lesquels ces menaces ont un impact, mais aussi, si elles sont humaines, non-humaines, accidentelles et/ou délibérées.

Finalement, nous fournissons aussi les justifications à plusieurs décisions, concernant ces menaces et leurs filtres, basées sur des informations inférées de ces mêmes documents, et dont voici la liste :

1. M5 peut être d'origine non-humaine au sens EBIOS. En effet, selon la définition et les exemples fournis dans la base de connaissances, la modification du matériel peut être due au piégeage de matériel. Or, un virus peut provoquer des changements dans le fonctionnement des diverses machines, tels que des postes de travail ou des smartphones, et un cheval de troie peut être utilisé pour récupérer des informations via keylogger.

2. M9 n'est pas d'origine non-humaine au sens EBIOS. En effet, dans sa base de connaissances, pour cette menace, les virus, bombes logiques et autres sources non-humaines ne sont pas inclues, mais le sont dans M10 et M11. Par ailleurs, le tableau de croisement EBIOS montre que M9 ne couvre pas le piégeage de logiciel. On peut en déduire que la méthode EBIOS cherche à mettre en évidence les dépassement des limites d'un logiciel causés par des actions humaines.

3. M12 peut être d'origine accidentelle au sens EBIOS. En effet, selon la définition et les exemples fournis dans la base de connaissances, la disparition d'un logiciel peut être due à une perte. Or, la perte peut être

accidentelle et il tout a fait raisonnable de supposer qu'une personne puisse, par exemple, égarer le CD d'un logiciel.

4. M25 peut être d'origine accidentelle au sens EBIOS. En effet, selon la définition et les exemples fournis dans la base de connaissances, le détournement de l'usage d'un support papier comprend l"utilisation de ce dernier comme brouillon. Or, il est tout à fait raisonnable de supposer qu'une personne peu organisée utilise par erreur un document officiel afin de prendre des notes, avant de se rendre compte de son erreur.
5. M24 n'est pas d'origine accidentelle au sens EBIOS. En effet, selon la définition et les exemples fournis dans la base de connaissances, le départ d'une personne est un acte volontaire. Que ce soit si elle décide de quitter l'entreprise, acte volontaire de l'employé, ou si elle est enlevée, acte volontaire des kidnappeurs, ou encore si l'organisation est rachetée, acte volontaire de l'acheteur. Par ailleurs, l'idée qu'une entreprise puisse être privée d'une personne par accident est comprise dans la menace M22 sur la détérioration des personnes.

Légende :

1. MAT signifie Matériel. Il caractérise les menaces portant sur le matériel d'une organisation.
2. LOG signifie Logiciel. Il caractérise les menaces portant sur les logiciels d'une organisation.
3. RSX signifie Canaux Réseaux informatiques et de téléphonie. Il caractérise les menaces portant sur ces canaux dans une organisation.
4. PER signifie Personnes. Il caractérise les menaces portant sur le personnel d'une organisation.
5. PAP signifie Papier. Il caractérise les menaces portant sur les supports papier d'une organisation.
6. CAN signifie Canaux Interpersonnels. Il caractérise les menaces portant sur ces canaux dans une organisation.
7. USG signifie Détournement de l'usage prévu. Il détermine, comme les suivants, le type de la menace.
8. ESP signifie Espionnage.
9. DEP signifie Dépassement des limites de fonctionnement.
10. DET signifie Détérioration.
11. MOD signifie Modification.
12. PTE signifie Perte.
13. I,C,D signifie Intégrité, Confidentialité et Disponibilité. Il s'agit des principaux attributs de sécurité.

Filtres \ Menaces	M1.MAT-USG	M2.MAT-ESP	M3.MAT-DEP	M4.MAT-DET	M5.MAT-MOD	M6.MAT-PTE	M7.LOG-USG	M8.LOG-ESP	M9.LOG-DEP	M10.LOG-DET	M11.LOG-MOD	M12.LOG-PTE	M13.RSX-USG
1. Humain(H)/ Non-Humain(NH)	H	H	H/NH	H/NH	H/NH	H	H	H	H	H/NH	H/NH	H	H
2. Interne(In)/ Externe(Ex)	In	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex
3. Délibéré(D)/ Accidentel(A)	D/A	D	D/A	D/A	D/A	D/A	D/A	D	D/A	D/A	D/A	D/A	D/A
4. Matériel	C/I/D	C	D	D	C/I/D	C/D							
5. Logiciel							C/I/D	C	D	D	C/I/D	C/D	
6. Canaux Informatiques													I/D
7. Personnes													
8. Support Papier													
9. Canaux Interpersonnels													
10. Infrastructure													

TABLE D.1 – Tableau des correspondances entre filtres et menaces EBIOS - partie 1

Menaces / Filtres	M14.RSX-ESP	M15.RSX-DEP	M16.RSX-DET	M17.RSX-MOD	M18.RSX-PTE	M19.PER-USG	M20.PER-ESP	M21.PER-DEP	M22.PER-DET	M23.PER-MOD	M24.PER-PTE	M25.PAP-USG	M26.PAP-ESP
1. Humain(H)/ Non-Humain(NH)	H	H/NH	H/NH	H	H	H/NH	H	H/NH	H/NH	H	H	H	H
2. Interne(In)/ Externe(Ex)	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In	In/Ex
3. Délibéré(D)/ Accidentel(A)	D	D/A	D/A	D/A	D/A	D/A	D/A	D/A	D/A	D/A	D	D/A	D
4. Matériel													
5. Logiciel													
6. Canaux Informatiques	C	D	D	D	D								
7. Personnes						D	C	I/D	D	C/I	C/D		
8. Support Papier												I/D	C
9. Canaux Interpersonnels													
10. Infrastructure													

TABLE D.2 – Tableau des correspondances entre filtres et menaces EBIOS - partie 2

Menaces / Filtres	M27.PAP-DET	M28.PAP-PTE	M29.CAN-USG	M30.CAN-ESP	M31.CAN-DEP	M32.CAN-DET	M33.CAN-MOD	M34.CAN-PTE
1. Humain(H)/ Non-Humain(NH)	H/NH	H	H	H	H	H	H	H
2. Interne(In)/ Externe(Ex)	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In	In	In
3. Délibéré(D)/ Accidentel(A)	D/A	D/A	D/A	D	D/A	D	D	D
4. Matériel								
5. Logiciel								
6. Canaux Informatiques								
7. Personnes								
8. Support Papier	D	C/D						
9. Canaux Interpersonnels			I/D	C	D	D	D	D
10. Infrastructure								

TABLE D.3 – Tableau des correspondances entre filtres et menaces EBIOS - partie 3

Annexe E

Résumé des menaces de l'ISO/IEC 27005

Cette annexe contient les tableaux des menaces des l'ISO/IEC 27005 et des caractéristiques permettant de les filtrer.

Tout d'abord, ces tableaux permettent de savoir quelles menaces visent quels biens supports, et les attributs de sécurité sur lesquels elles ont un impact, mais aussi, si elles sont humaines, non-humaines, accidentelles et/ou délibérées.

Finalement, ces tableaux font les liens, entre menaces et attributs de sécurité, et le bien support infrastructure, contrairement à la méthode EBIOS.

Menaces / Filtres	M1.Incendie	M2.Dégâts des eaux	M3.Pollution	M4.Sinistre Majeur	M5.Destruction de matériels ou de supports	M6.Phénomène climatique	M7.Phénomène sismique	M8.Phénomène volcanique	M9.Phénomène météorologique	M10.Crue	M11.Défaillance de la climatisation	M12.Perte d'alimentation énergétique
1. Humain(H)/ Non-Humain(NH)	H/NH	H/NH	H/NH	H/NH	H/NH	NH	NH	NH	NH	NH	H	H/NH
2. Interne(In)/ Externe(Ex)	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex						In/Ex	In/Ex
3. Délibéré(D)/ Accidentel(A)	D/A	D/A	D/A	D/A	D/A						D/A	D/A
4. Matériel	D	D	D	D	D	D	D	D	D	D	D	D
5. Logiciel												
6. Canaux Informatique	D	D		D		D	D	D	D	D		
7. Personnes	D		D	D		I/D	D	D	I/D	D	I/D	
8. Support Papier	D	D	D	D	D	D	D	D	D	D		
9. Canaux Interpersonnel												
10. Infrastructure	D	D		D		D	D	D	D	D		D

TABLE E.1 – Tableau des correspondances entre filtres et menaces de l'ISO/IEC 27005 - partie 1

Menaces / Filtres	M13.Perte des moyens de télécommunication	M14.Rayonnement électromagnétiques	M15.Rayonnement thermiques	M16.Impulsions électromagnétiques	M17.Interception de signaux parasites compromettants	M18.Espionnage à distance	M19.Ecoute passive	M20.Vol de supports ou de documents	M21.Vol de matériels	M22.Récupération de supports recyclés ou mis au rebut	M23.Divulgation
1. Humain(H)/ Non-Humain(NH)	H	H/NH	H/NH	H/NH	H	H	H	H	H	H	H
2. Interne(In)/ Externe(Ex)	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex
3. Délibéré(D)/ Accidentel(A)	D/A	D/A	D/A	D/A	D	D	D	D	D	D	D/A
4. Matériel		D	D	D	C	C		C/D	C/D	C/D	
5. Logiciel											
6. Canaux Informatique	I/D				C	C	C				
7. Personnes			I/D			C					C/I
8. Support Papier						C		C/D		C/D	
9. Canaux Interpersonnel						C	C				I/D
10. Infrastructure				D							C

TABLE E.2 – Tableau des correspondances entre filtres et menaces de l'ISO/IEC 27005 - partie 2

Filtres \ Menaces	M24.Informations sans garantie de l'origine	M25.Piégeage du matériel	M26.Piégeage du logiciel	M27.Géolocalisation	M28.Panne matérielle	M29.Dysfonctionnement du matériel	M30.Saturation du système d'information	M31.Dysfonctionnement logiciel	M32.Atteinte à la maintenabilité du système	M33.Utilisation illicite des matériels	M34.Copie frauduleuse de logiciels
1. Humain(H)/ Non-Humain(NH)	H	H	H	H	H	H	H	H	H	H	H
2. Interne(In)/ Externe(Ex)	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In/Ex	In	In/Ex
3. Délibéré(D)/ Accidentel(A)	D/A	D	D/A	D	A	A	D/A	A	D/A	D	D
4. Matériel		C/I/D		C	C/I/D	C/I/D	D		C/I/D	C/I/D	
5. Logiciel	C/I/D		C/I/D				D	C/I/D	C/I/D		C/I/D
6. Canaux Informatique							D		I/D		
7. Personnes C/I							I/D				
8. Support Papier											
9. Canaux Interpersonnel	I/D						D				
10. Infrastructure				C							

TABLE E.3 – Tableau des correspondances entre filtres et menaces de l'ISO/IEC 27005 - partie 3

Filtres \ Menaces	M35.Utilisation de logiciels contrefaits ou copiés	M36.Altération des données	M37.Traitement illicite des données	M38.Erreur d'utilisation	M39.Abus de droits	M40.Usurpation de droits	M41.Reniement d'actions	M42.Atteinte à la disponibilité du personnel
1. Humain(H)/ Non-Humain(NH)	H	H	H	H	H	H	H	H/NH
2. Interne(In)/ Externe(Ex)	In/Ex	In/Ex	In	In/Ex	In	In/Ex	In/Ex	In/Ex
3. Délibéré(D)/ Accidentel(A)	D/A	D	D	A	D/A	D	D	D/A
4. Matériel				C/I/D	C/I/D	C/I/D	C/I/D	
5. Logiciel	C/I/D	C/I/D		C/I/D	C/I/D	C/I/D	C/I/D	
6. Canaux Informatique		I/D		I/D	I/D		C/I/D	
7. Personnes		C/I/D			D	C/I/D	C/I/D	C/I/D
8. Support Papier			I/D				C/I/D	
9. Canaux Interpersonnel		I/D	I/D		I/D	I/D	C/I/D	
10. Infrastructure								

TABLE E.4 – Tableau des correspondances entre filtres et menaces de l'ISO/IEC 27005 - partie 4

Annexe F

Résumé des fusions des menaces

Cette annexe contient le tableau présentant les fusions des menaces EBIOS, sous la forme d'unions. Les critères employés pour réaliser cette tâche sont dans les tableaux des annexes D et E.

Nouvelles Menaces	Fusion
NM1	M1.MAT-USG ∨ M7.LOG-USG
NM2	M5.MAT-MOD ∨ M11.LOG-MOD
NM3	M2.MAT-ESP ∨ M8.LOG-ESP ∨ M14.RSX-ESP ∨ M26.PAP-ESP ∨ M30.CAN-ESP
NM4	M3.MAT-DEP ∨ M15.RSX-DEP
NM5	M4.MAT-DET ∨ M10.LOG-DET ∨ M16.RSX-DET ∨ M22.PER-DET ∨ M27.PAP-DET
NM6	M6.MAT-PTE ∨ M12.LOG-PTE ∨28.PAP-PTE
NM7	M9.LOG-DEP ∨ M31.CAN-DEP
NM8	M13.RSX-USG ∨ M25.PAP-USG ∨ M29.CAN-USG
NM9	M17.RSX-MOD ∨ M18.RSX-PTE
NM10	M19.PER-USG
NM11	M20.PER-ESP
NM12	M21.PER-DEP
NM13	M23.PER-MOD
NM14	M24.PER-PTE
NM15	M32.CAN-DET ∨ M33.CAN-MOD ∨ M34.CAN-PTE

Table F.1 – Tableau de fusion des menaces EBIOS

Légende :

1. NM signifie Nouvelle Menace. Il s'agit des menaces de la méthodologie.
2. MAT signifie Matériel. Il caractérise les menaces portant sur le matériel d'une organisation.
3. LOG signifie Logiciel. Il caractérise les menaces portant sur les logiciels d'une organisation.
4. RSX signifie Canaux Réseaux informatiques et de téléphonie. Il caractérise les menaces portant sur ces canaux dans une organisation.
5. PER signifie Personnes. Il caractérise les menaces portant sur le personnel d'une organisation.
6. PAP signifie Papier. Il caractérise les menaces portant sur les supports papier d'une organisation.
7. CAN signifie Canaux Interpersonnels. Il caractérise les menaces portant sur ces canaux dans une organisation.
8. USG signifie Détournement de l'usage prévu. Il détermine, comme les suivants, le type de la menace.
9. ESP signifie Espionnage.
10. DEP signifie Dépassement des limites de fonctionnement.
11. DET signifie Détérioration.
12. MOD signifie Modification.
13. PTE signifie Perte.

Annexe G

Résumé des nouvelles menaces

Cette annexe contient les tableaux des nouvelles menaces et des caractéristiques permettant de les filtrer. Ils sont crées à partir des tableaux des annexes D, E et F.

Tout d'abord, nous rappelons que les seuls filtres utilisables pour ces menaces sont les critères humain/non-humain et bien support.

Finalement, ce tableau permet de savoir quelles menaces visent quels biens supports et les attributs de sécurité sur lesquels elles ont un impact.

Nouvelle Menace / Filtres	NM1.MAT/LOG-USG	NM2.MAT/LOG-MOD	NM3.MAT/LOG/RSX/PAP/CAN-ESP	NM4.MAT/RSX-DEP	NM5.MAT/LOG/RSX/PER/PAP-DET	NM6.MAT/LOG/PAP-PTE	NM7.LOG/CAN-DEP	NM8.RSX/PAP/CAN-USG	NM9.RSX-MOD-PTE
1. Humain(H)/ Non-Humain(NH)	H	H/NH	H	H/NH	H/NH	H	H	H	H
2. Délibéré(D)/ Accidentel(A)	D/A	D/A	D	D/A	D/A	D/A	D/A	D/A	D/A
3. Matériel	C/I/D	C/I/D	C	D	D	C/D			
4. Logiciel	C/I/D	C/I/D	C		D	C/D	D		
5. Canaux Informatiques			C	D	D			I/D	D
6. Personnes					D				
7. Support Papier			C		D	C/D		I/D	
8. Canaux Interpersonnels			C				D	I/D	
9. Infrastructure			C	D	D				

TABLE G.1 – Tableau des correspondances entre filtres et nouvelles menaces - partie 1

Nouvelles Menaces / Filtres	NM10.PER-USG	NM11.PER-ESP	NM12.PER-DEP	NM13.PER-MOD	B-NM14.PER-PTE	NM15.CAN-DET-MOD-PTE
1. Humain(H)/ Non-Humain(NH)	H/NH	H	H/NH	H	H	H
2. Délibéré(D)/ Accidentel(A)	D/A	D/A	D/A	D/A	D	D
3. Matériel						
4. Logiciel						
5. Canaux Informatiques						
6. Personnes	D	C	I/D	C/I	C/D	
7. Support Papier						
8. Canaux Interpersonnels						D
9. Infrastructure	D	C		C		

TABLE G.2 – Tableau des correspondances entre filtres et nouvelles menaces - partie 2

Annexe H

Tableau des vulnérabilités

Cette annexe contient les tableaux des vulnérabilités de la méthodologie. La première colonne donne le type de bien support sur lequel porte la vulnérabilité. La seconde colonne indique le document dans lequel nous avons récupéré la vulnérabilité. La troisième colonne présente la question illustrant la vulnérabilité. La dernière colonne montre le ou les liens entre une vulnérabilité et l'ISO/IEC 27002.

H.1 Tableau

Type	Origine	Vulnérabilité	Vulnérabilité dérivée	ISO 27002
MATERIEL	EBIOS	Connaissance de l'existence et de la localisation du matériel	V1. Vos employés parlent-ils parfois des endroits dans lesquels votre entreprise stocke, par exemple, ses équipements de remplacement, ou ses serveurs, ou d'autres équipement qui lui sont importants?	7.1.1, 7.1.2
		Utilisable en dehors de l'usage prévu	V2. Vos équipements ont-ils déjà été utilisés à d'autres fins que celles que vous aviez prévues, par exemple un ordinateur utilisé pour aller sur facebook au lieu de travailler, ou une clef USB utilisée pour stocker un film au lieu de documents de travail, ...?	8.1.2, 8.1.3
		N'est pas approprié aux conditions d'utilisation	V3. Avez-vous déjà placés vos équipements dans des situations violant les conditions d'utilisation, par exemple une salle fort humide ou trop chaude, ou branché à une prise défectueuse, ...?	8.1.2, 8.1.3
	ISO 27005	Manque de soin lors de la mise au rébus	V4. Avez-vous déjà oublié de supprimer définitivement des données confidentielles stockées sur un équipement amovible dont vous souhaitiez vous débarrasser?	8.1.1, 8.1.2, 8.3.1
		Manque de soin lors de la mise au rébus	V5. Avez-vous déjà jeté à la poubelle ou laissé traîner une clef USB ou un disque dur externe ou autre, contenant ou ayant contenu des informations confidentielles, dont vous souhaitiez vous débarrasser, plutôt que de les détruire?	8.1.1, 8.1.2, 8.3.2

TABLE H.1 – Tableaux des vulnérabilités - partie 1

MATERIEL	ISO 27005	Manque de soin lors de la mise au rébus	V6. Avez-vous déjà réutilisé ou donné une clef USB ou un disque dur externe, ou autre, ayant contenu des données confidentielles sans vous assurer que les données avaient été définitivement supprimées?	8.1.2, 11.2.7
	EBIOS	Permet d'ajouter/retirer ou substituer des éléments via des connecteurs	V7. Quand vous laissez un équipement sans supervision, est-il encore possible d'utiliser ses différents connecteurs, USB, Ethernet, VGA, DVI, ou lecteurs, ..., car vous ne les bloquez pas avec des outils tels que des USB blocker ou Diskey IV, ...?	11.2.1
		Accès physique non protégé / Utilisable en dehors de l'usage prévu	V8. Vos équipements se sont-ils déjà retrouvés hors du site de votre entreprise?	11.2.1
	ISO 27005	Sensibilité aux radiations électromagnétiques/Sensibilité aux variations de tension/Sensibilité aux variations de température	V9. Avez-vous des équipements, qui selon les notices des fournisseurs, sont sensibles aux variations de températures, à l'exposition à de fortes lumières ou encore aux variations de tensions, ...?	11.2.2
	EBIOS	Requiert de l'électricité en permanence	V10. Avez-vous des équipements qui requièrent une alimentation permanente?	11.2.2
	ISO 27005	Maintenance Insuffisante	V11. Vos équipements ont-ils déjà montré des signes de ralentissement, de dysfonctionnement, de baisse de performance ou de panne?	11.2.4
		Mauvaise installation d'un médium de stockage	V12. L'installation de nouveaux périphériques ou composants, tel un disque dur ou un clef USB, ou une nouvelle carte réseau, ... , a-t-elle déjà posé problème ou échoué?	11.2.4
		Absence de backup matériel	V13. Vous êtes vous déjà retrouvé dans l'incapacité de remplacer un équipement à cause d'un manque de pièces de remplacement?	11.2.4

TABLE H.2 – Tableaux des vulnérabilités - partie 2

MATERIEL	EBIOS	Portable	V14. Vos équipements ont-ils déjà été retirés du lieu de travail sans votre autorisation?	11.2.5
		Utilisable en dehors de l'usage prévu / Permet d'observer des données interprétables	V15. Avez-vous déjà oublié de protéger vos équipements avec par exemple avec un écran de veille protégé par un mot de passe, la déconnexion d'une session, verrouillage du clavier, ...?	11.2.8, 11.2.9
		Accès physique non protégé / Absence de contrôle sur le copiage	V16. Avez-vous déjà laissé des équipements amovibles en vue dans vos bureaux?	11.2.9(clear desk)
	ISO 27005	Absence de contrôle efficace de changement de configuration	V17. Contrôlez-vous les changements importants que vous apportez à vos équipements et aux systèmes qu'ils supportent, par exemple en les documentant, les planifiant, les testant, ...?	12.1.2
	EBIOS	Dimensionnement inapproprié des capacités de stockage / Dimensionnement inapproprié des capacités de stockages	V18. Utilisez-vous des équipements trop ou pas assez puissant ou avec trop ou pas assez d'espace de stockage pour effectuer votre travail, par exemple des ordinateurs dernier cri pour faire du traitement de texte ou des vieux ordinateurs pour faire du graphisme, une clef USB pour stocker de fichiers trop volumineux, ...?	12.1.3
LOGICIEL	EBIOS	Connaissance de l'existence et de la localisation du matériel	V19. Vos employés parlent-ils parfois des logiciels que vous utilisez et des machines dans lesquelles ils se trouvent?	7.1.1, 7.1.2
		Utilisable en dehors de l'usage prévu	V20. Vos logiciels ont-ils déjà été utilisés en dehors de leur usage prévu, par exemple pour réaliser des tâches personnelles?	8.1.3
	ISO 27005	Mise au rébus ou réutilisation de médium de stockage sans effacement efficace	V21. Avez-vous déjà jeté ou réutilisé des équipements de stockage sans vous assurer que les données contenues étaient complètement effacées?	8.1.1, 8.1.2, 8.3.1, 8.3.2, 11.2.7
		Accès Logique / Manque de mécanismes d'identification	V22. Permettez-vous à des personnes d'utiliser votre système sans devoir s'inscrire?	9.2.1

TABLE H.3 – Tableaux des vulnérabilités - partie 3

LOGICIEL	ISO 27005	Accès Logique / Mauvaise gestion des mots de passes	V23. Permettez-vous aux futurs inscrits de choisir n'importe quel mot de passe?	9.2.1
		Accès Logique / Manque de mécanismes d'identification	V24. Permettez-vous à des personnes d'utiliser votre système sans devoir entrer un identifiant et un mot de passe?	9.4.2, 9.4.3
		Accès Logique / Mauvaise allocation des droits d'accès	V25. Toute personne utilisant votre système peut-elle librement voyager dans celui-ci sans devoir lui confirmer qu'elle a le droit d'aller dans ses différents dossiers ou d'effectuer certaines actions?	9.2.2, 9.2.3
		Accès Logique / Pas de log-out aux postes de travail	V26. Avez-vous des postes de travail qui ne permettent pas de se déconnecter d'une session?	9.4.2
	EBIOS	Code source accessible et compréhensible	V27. Est-il possible d'accéder au code des logiciels, c'est-à-dire les instructions qui dictent son fonctionnement, que vous utilisez ou développez?	9.4.5
		Possibilité d'effacer ou de supprimer des programmes	V28. Un de vos logiciels a-t-il déjà été effacé ou supprimé alors que vous en aviez encore l'utilité?	9.4.5
	ISO 27005	Table des mots de passe non protégée	V29. Stockez-vous les mots de passe des utilisateurs sans les rendre illisibles grâce à des outils de chiffrement tels GPG, ...?	10
	EBIOS	Modifiable, améliorable, paramétrable	V30. Vos logiciels ont-ils déjà été reconfigurés, ou modifiés, après par exemple une maintenance, ou une mise à jour?	9.4.5, 12.1.2
	ISO 27005	Manque de contrôle efficace de changement	V31. Avez-vous déjà effectué des reconfigurations, mises à jours ou autres modifications de vos logiciels sans les documenter, ni prévoir de mécanisme de retour en arrière, ...?	12.1.2

Table H.4 – Tableaux des vulnérabilités - partie 4

LOGICIEL	ISO 27005	Absence de backup logiciel	V32. Utilisez-vous des logiciels ou des données dont vous n'avez qu'une seule copie?	12.3.1
		Absence de surveillance des téléchargements et utilisation de logiciels	V33. Les utilisateurs de votre système peuvent-ils télécharger ou encore installer des logiciels en toute impunité?	12.2.1, 12.4.1, 12.5.1
		Manque de documentation	V34. Avez-vous déjà utilisé des logiciels ne fournissant pas leur documentation, ou encore sans documenter la manière avec laquelle vous les utilisez?	12.1.1, 12.5.1
		Logiciels nouveaux ou immatures	V35. Utilisez-vous des logiciels qui viennent de sortir et/ou n'ont pas été suffisamment testés?	12.5.1
		Interface compliquée	V36. Utilisez-vous des logiciels dont l'interface vous semble compliquée?	12.5.1
		Vulnérabilités bien connues	V37. Avez-vous déjà utilisé des logiciels sans vérifier s'ils étaient considérés comme sécurisés?	12.6.1
		Services inutiles activés	V38. Les services, de vos logiciels, que vous n'utilisez pas, restent-ils activés, comme par exemple ceux de Windows?	12.2.1, 12.6.1
		Manque de traces d'audit	V39. Permettez-vous que vos logiciels soient utilisés sans qu'il y ait des enregistrements des actions effectuées par les utilisateurs, comme le permettent des logiciels tels que NetOrbit?	12.4.1, 12.4.2, 12.4.3, 12.4.4
		Mauvaise date	V40. Le calendrier d'un de vos "operating system" a-t-il déjà été mis à une mauvaise date?	12.4.4
		Incapacité à produire des rapports de management	V41. Vous êtes-vous déjà retrouvé incapable de produire un rapport sur un incident de sécurité, à cause de manque de traces, ou preuves, ou de procédures adéquates pour créer et soumettre un tel rapport?	12.1.3, 12.4.1, 12.4.3, 12.4.4, 16
	EBIOS	Permet de saisir n'importe quelle donnée / quantité de données	V42. Dans les logiciels que vous utilisez ou développez, est-il possible d'entrer n'importe quelles données ou quantités de données sans que ceux-ci n'interviennent pour prévenir un problème?	12.6.1

TABLE H.5 – Tableaux des vulnérabilités - partie 5

PAPIER	EBIOS	Connaissance de l'existence et de la localisation du matériel	V43. Vos employés parlent-ils parfois des endroits dans lesquels votre entreprise stocke, les documents papiers qui lui sont importants?	7.1.1, 7.1.2
		Utilisable en dehors de l'usage prévu	V44. Vos documents papier ont-ils déjà été utilisés à d'autres fins que celle que vous aviez prévues, par exemple comme brouillon, ou feuille d'impression, ...?	8.1.2, 8.1.3
		N'est pas approprié aux conditions de travail	V45. Avez-vous déjà placé vos documents papier dans des conditions violant les conditions d'utilisation, par exemple une salle trop humide, ...?	8.1.2, 8.1.3
	ISO 27005	Manque de soin lors de la mise au rébus	V46. Avez-vous déjà jeté des documents papier sans les détruire auparavant?	8.1.1, 8.1.2, 8.3.2
	EBIOS	Accès physique non protégé	V47. Vos documents papiers important se sont-ils déjà retrouvés hors du site de votre entreprise?	8.1.2, 11.2.1
		Portable	V48. Vos documents papiers ont-ils déjà été retirés de vos bureaux sans votre autorisation?	8.1.2, 11.2.5, 11.2.9
	ISO 27005	Manque de soin lors de la mise au rébus	V49. Avez-vous déjà réutilisé des documents papier importants, par exemple comme brouillon?	8.1.2, 11.2.7
	EBIOS / ISO 27005	Utilisable en dehors de l'usage prévu / Accès physique non protégé /Absence de contrôle sur le copiage	V50. Avez-vous déjà laissé des documents papier importants en vue dans vos bureaux?	11.2.9(clear desk)
	EBIOS	Falsifiable	V51. Vos documents papier peuvent-ils être falsifiés?	11.2.9 (clear desk)

TABLE H.6 – Tableaux des vulnérabilités - partie 6

PAPIER	EBIOS	Permet d'observer des données interprétables	V52. Les données écrites sur vos documents papier sont-elles lisibles?	11.2.9 (clear desk)
		Absence de backup	V53. Avez-vous des documents papier importants pour lesquels il n'existe qu'un seul exemplaire?	12.3.1
INFRASTRUCTURE	ISO 27005	Absence de protection physique des bâtiments, portes et fenêtres	V54. Des individus se sont-ils déjà introduits sans autorisation dans les locaux de votre entreprise sans que personne ne s'en rende compte?	11.1.1, 11.1.2
		Absence de protection physique des bâtiments, portes et fenêtres	V55. Des personnes non autorisées ont-elles déjà eu accès à des endroits à l'accès réservé de votre entreprise?	11.1.1, 11.1.2, 11.1.3
		Absence de protection physique des bâtiments, portes et fenêtres	V56. Placez-vous d'importantes informations, équipement, équipes de travail, ... dans des pièces faciles d'accès, ou très visibles, ou encore dont les murs sont fins au point que l'on entende des conversations, ...?	11.1.3
		Utilisation inadéquate ou imprudente de contrôle d'accès physique aux bâtiment et pièces	V57. D'autres personnes que celles autorisées ont-elles déjà eu connaissance de l'existence de zones de votre entreprise qui devaient être gardées secrètes?	7.1.2, 11.1.5
		Utilisation inadéquate ou imprudente de contrôle d'accès physique aux bâtiment et pièces	V58. Le travail dans ces zones secrètes s'effectue-t-il sans supervision?	11.1.5
		Utilisation inadéquate ou imprudente de contrôle d'accès physique aux bâtiment et pièces	V59. Vos zones de chargement et livraison, ou autres points d'accès de l'extérieur vers l'intérieur du bâtiment sont-ils surveillés?	11.1.6
		Réseau énergétique instable / Emplacement susceptible à une inondation, incendie, ...	V60. Êtes-vous implantés dans une zone à risque d'incendie, d'inondation, de séisme, ... ou dont le réseau électrique est instable?	11.1.4

TABLE H.7 – Tableaux des vulnérabilités - partie 7

PERSONNEL	EBIOS	Connaissance de l'existence et de la localisation	V61. Vos employés, et surtout ceux travaillant à des tâches vitales ou dans des secteurs vitaux, sont-ils autorisés à parler publiquement de leur emploi?	7.1.1, 7.1.2
		Ressources insuffisantes pour les tâches assignées	V62. Avez-vous déjà assigné des tâches à vos employés sans leur donner tous les moyens nécessaires à leur accomplissement, que ce soit en équipements, logiciels, ou même lignes de conduites, ...?	7.2.1
		Compétences inappropriées à l'exercice des fonction	V63. Avez-vous des employés qui n'ont pas les bonnes compétences pour le travail qu'il leur est demandé de réaliser?	7.1.1, 7.1.2
		Incapacité à s'adapter au changement	V64. Avez-vous des employés qui n'arrivent pas à s'adapter aux changements de leurs fonctions, que ce soit en termes d'équipements ou logiciels manipulés, ou de responsabilités, ...?	7.2.1, 7.2.2
	ISO 27005	Absence du personnel	V65. Certains de vos employés ont-ils déjà été absent sans vous avoir notifié suffisamment à l'avance?	7.1.1, 7.1.2
		Procédures de recrutement inadéquates	V66. Certains de vos employés ont-ils déjà causés des dégâts matériels ou à la rentabilité de l'entreprise?	7.1.1, 7.1.2
		Procédures de recrutement inadéquates	V67. Certains de vos employés ont-ils déjà eu accès à des données confidentielles sans devoir signer d'accord de confidentialité?	7.1.2
		Manque d'entraînement en sécurité	V68. Certains de vos employés ont-il déjà causés des problèmes de sécurité à cause d'un manque de prise de conscience des enjeux et des besoins de sécurité de votre entreprise, ainsi que de l'évolution des procédures et responsabilités qui les concernent?	5.1.1, 7.2.2
		Utilisation incorrecte de logiciels et équipements	V69. Certains de vos employés se sont-ils déjà retrouvé dans l'incapacité d'utiliser correctement des logiciels ou des équipements, ...?	7.2.1, 7.2.3

TABLE H.8 – Tableaux des vulnérabilités - partie 8

PERSONNEL	ISO 27005	Retourner actifs si terminaison contrat	V70. Certains de vos employé ont-ils déjà emporté du matériel ou des logiciels de votre entreprise alors qu'ils quittaient son service?	8.1.1, 8.1.2, 8.1.4
		Manque de mécanismes de surveillance	V71. Laissez-vous vos employés utiliser les logiciels et les équipements sans enregistrer leurs actions dans des logs?	12.4.1, 12.4.2, 12.4.3, 12.4.4
			V72. Ces enregistrements ont-ils déjà été altérés, modifiés, rendus douteux, ...?	12.4.2
			V73. Vos administrateurs système, et autres personnes du même grade peuvent-elles agir sur le système sans que leurs actions soient enregistrées?	12.4.3
			V74. Avez-vous déjà eu des imprécisions sur la précision du moment auquel des enregistrements auraient été faits?	12.4.4
		Absence de supervision des travailleurs venant de l'extérieur ou de nettoyage	V75. Les travailleurs venant de l'extérieur ou encore le personnel de nettoyage travaillent-ils sans supervision?	11.1.1, 11.1.2, 11.1.3
		Manque de politiques pour l'utilisation correcte de médium de télécommunications et de messagerie	V76. Vos employés ont-ils déjà utilisés internet pour aller sur des réseaux sociaux, ou utilisé leur messagerie professionnelle pour envoyer des e-mails personnels, ...?	8.1.3, 13.2.1
	EBIOS	Sujet à la dissipation	V77. Avez-vous des employés distraits pendant les heures de travail, au point de ralentir votre entreprise?	7.1.1, 7.1.2
		Peu discret	V78. Un de vos employés a-t-il déjà, indépendamment des circonstances, divulgué des informations confidentielles?	5.1.1, 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.2.3

TABLE H.9 – Tableaux des vulnérabilités - partie 9

PERSONNEL	EBIOS	Influençable / Manipulable	V79. Avez-vous des employés naïfs, crédules, ou autrement influençables, qui gèrent difficilement la pression, ou autrement manipulables, ...?	7.1.1, 7.2.2, 7.2.3
		Faible loyauté	V80. Un de vos employés a-t-il déjà quitté votre entreprise du jour au lendemain, à cause d'intérêts personnels, ou de manque de satisfaction, ...?	7.1.1, 7.1.2, 7.3.1
CANAUX RESEAUX	EBIOS	Connaissance de l'existence et de la localisation du matériel	V81. Vos employés parlent-ils parfois des endroits dans lesquels votre entreprise place, par exemple, ses modems, ou routeurs ou câbles réseaux?	7.1.1, 7.1.2
	ISO 27005	Transfert de mots de passe non chiffrés	V82. Avez-vous déjà transféré des mots de passe sur votre réseau?	9.3.1, 10
	EBIOS	Remplaçable	V83. Quelqu'un a-t-il déjà remplacé un de vos modems, ou routeurs, ou câbles réseau, à votre insu, par des modèles incompatibles ou de capacité de transfert moindre, ...?	11.2.1
		Peu visible	V84. Avez-vous déjà oublié, au moment de quitter vos locaux, de vérifier si vos modems, routeurs, ou câbles réseaux sont toujours à leur place?	11.2.1
	EBIOS / ISO 27005	Observable / Lignes de communications non protégées	V85. Votre wifi a-t-il déjà été utilisé par des personnes qui ne font pas partie de votre entreprise?	9.3.1, 9.4.2
	EBIOS	Portable	V86. Quelqu'un a-t-il déjà retiré sans votre autorisation un modem, ou routeur, ou câble réseau des prémisses de votre entreprise?	11.2.5
	ISO 27005	Câbles en mauvais état	V87. Avez-vous des câbles réseau vieux ou en mauvais état?	11.2.3, 11.2.4

TABLE H.10 – Tableaux des vulnérabilités - partie 10

CANAUX RESAUX	EBIOS	Dimensionnement insuffisant	V88. Le débit de votre connexion internet encore ou la capacité de vos câbles réseau ne sont-elles pas trop grandes ou petites par rapport à l'utilisation que vous en faites?	12.1.3
	ISO 27005	Architecture réseau non sécurisée	V89. Utilisez-vous des ordinateurs ou autres postes de travail sans antivirus maintenus à jour?	12.2.1
		Single point of failure	V90. Ne possédez-vous certains équipements réseaux tels que les modems ou routeurs, ou câbles réseaux, ... qu'en un seul exemplaire?	12.6.1 & 13.1.2
	EBIOS / ISO 27005	Permet d'observer des données interprétables / Trafic confidentiel/sensible non protégé	V91. Transférez-vous des données confidentielles ou sensibles sans préalablement les rendre incompréhensibles, avec des logiciels tels que GPG, ...?	10, 13.2.1, 13.2.3
	ISO 27005	Absence de preuves d'envoi et de réception de messages	V92. Avez-vous, ou un de vos correspondant a-t-il, déjà oublié de donner une preuve de l'envoi et/ou de la réception de messages, tels que des e-mails, ...?	13.2.2
	EBIOS / ISO 27005	Permet d'altérer les flux communiqués / Absence d'identification et authentification de l'envoyeur ou récepteur	V93. Avez-vous déjà reçu des données, au travers d'e-mails ou autres canaux de communications, dont vous ne pouviez confirmer qu'il s'agissait du bon envoyeur?	10, 13.1.1, 13.2.1, 13.2.2
		Permet d'altérer les flux communiqués / Absence d'identification et authentification de l'envoyeur ou récepteur	V94. Avez-vous déjà envoyé ou reçu des données confidentielles, par e-mail ou autres canaux de communications, dont le contenu n'était rendu illisible, par des mécanismes de cryptographie par exemple?	10, 13.1.1, 13.2.1, 13.2.2
	ISO 27005	Connections à des réseaux publics non protégés	V95. Vous êtes-vous déjà connectés à des réseaux publics dans le cadre de votre travail?	13.1.1, 14.1.2, 14.1.3

TABLE H.11 – Tableaux des vulnérabilités - partie 11

CANAUX RESEAUX	EBIOS	Modifiable / Remplaçable	V96. Un de vos câbles réseaux, modems, routeurs, ou autre équipement de la sorte a-t-il déjà été remplacé sans que vous en soyez informé?	11.2.3, 11.2.8
CANAUX PERSONNElS	EBIOS	Permet d'altérer les flux communiqués	V97. Avez-vous des canaux interpersonnels qui sont altérables, par exemple, des notes d'un circuit courrier dont on peut changer le contenu, des lettres qui sont modifiées, ou des parapheurs interchangeables, ou des réunions qui s'éloignent des sujets à discuter, ...?	8.1.1, 8.1.2, 8.1.3, 11.1.1, 11.1.2, 11.1.3
		Seule ressource de transmission pour le flux / Unique	V98. Avez-vous des canaux interpersonnels à exemplaire unique, c'est-à-dire, un seul circuit courrier, ou une seule réunion périodique d'information ou de prise de décision, ou une seule note importante laissée pour informer quelqu'un, ...?	5.1.1, 6.1.1, 7.2.1, 7.2.2
		Permet la modification du circuit organisationnel	V99. Un de vos circuits organisationnel a-t-il déjà été altéré, par exemple, une réunion périodique qui ne se fait pas le même jour de chaque mois, un circuit courrier qui ne suit jamais deux fois le même parcours, ...?	5.1.1
		Connaissance de l'existence et de la localisation du canal interpersonnel	V100. D'une manière ou d'une autre, l'existence de réunions importantes, ou d'un circuit courrier, ou de tout autre circuit organisationnel, a-t-elle déjà été divulguée à des personnes qui n'ont pas besoin de le savoir?	5.1.1, 6.1.1, 7.1.2, 7.2.1, 7.2.2

TABLE H.12 – Tableaux des vulnérabilités - partie 12

CANAUX PERSONNElS	EBIOS	Observable	V101. Vos circuits organisationnels se déroulent-ils à la vue de tous, par exemple, donnez-vous du courrier ou des notes importantes devant tout le monde, faites-vous des réunions dans des salles observables depuis l'extérieur, ou dans lesquelles on peut cacher des appareils d'écoute, ...?	5.1.1, 11.1.1, 11.1.3
		Existence de limites quantitatives ou qualitatives	V102. Avez-vous déjà effectué des réunions durant lesquelles la charge de travail s'est avéré trop importante, ou dans une ambiance trop bruyante, ...?	5.1.1, 7.2.2
		Instable / Modifiable	V103. Permettez-vous aux acteurs de vos réunions, de vos circuits courriers, ou autres circuits organisationnels, à effectuer leur tâche ou leur participation sans respecter des règles préétablies?	5.1.1, 7.2.2

TABLE H.13 – Tableaux des vulnérabilités - partie 13

Annexe I

Tableau des liens entre menaces et vulnérabilités

Cette annexe contient le tableau montrant les liens entre les menaces et les vulnérabilités de la méthodologie. Ces liens ont été identifiés au cours d'une analyse de la base de connaissances EBIOS et de l'ISO/IEC 27005.

Nouvelles menaces	Vulnérabilités de la méthodologie
NM 1	V1, V2, V8, V11, V12, V13, V15, V17, V19, V20, V21, V22, V23, V24, V25, V26, V31, V32, V33, V34, V35, V36, V37, V38, V39, V40, V41, V68, V69, V71, V72, V73, V74, V76
NM 2	V1, V7, V8, V11, V12, V13, V17, V22, V23, V24, V29, V30, V31, V32, V33, V34, V35, V36, V40, V68, V69, V71, V72, V73, V74
NM 3	V1, V8, V15, V19, V22, V23, V24, V25, V26, V27, V43, V50, V52, V56, V81, V82, V85, V89, V90, V91, V98, V100, V101
NM 4	V3, V9, V10, V11, V12, V13, V18, V60, V68, V69, V71, V72, V73, V74, V81, V87, V88, V90, V92
NM 5	V9, V11, V12, V13, V17, V19, V28, V30, V31, V32, V34, V35, V36, V43, V45, V47, V50, V54, V55, V57, V58, V59, V60, V65, V66, V68, V69, V81, V87, V90
NM 6	V1, V4, V5, V6, V8, V14, V16, V19, V32, V43, V46, V47, V48, V49, V50, V53, V54, V55, V56, V57, V58, V59, V70, V75
NM 7	V19, V22, V23, V24, V25, V26, V29, V31, V34, V35, V36, V40, V42, V68, V69, V71, V72, V73, V74, V100, V102
NM 8	V43, V44, V47, V50, V51, V68, V69, V71, V72, V73, V74, V81, V87, V90, V91, V93, V94, V95, V97, V98, V99, V100
NM 9	V68, V69, V81, V83, V84, V86, V87, V90, V96
NM 10	V60, V61, V65, V77
NM 11	V56, V61, V67, V78
NM 12	V61, V62, V63, V64
NM 13	V61, V67, V79
NM 14	V61, V80
NM 15	V98, V100, V103

TABLE I.1 – Tableau des vulnérabilités spécifiques aux menaces de la méthodologie

Annexe J

Questionnaire d'interview des entreprises

Cette annexe contient le questionnaire utilisé comme support des interviews réalisées auprès des entreprises. Nous leur avons posé les questions et rempli le questionnaire nous-même sur base de leurs réponses afin de diminuer la charge de travail des répondants.

1 Introduction

1.1 Contexte

Dans le but d'aider les entreprises wallonnes à évaluer leur capacité à protéger l'information, il nous faut d'abord comprendre ces dernières. Ainsi, ce questionnaire sert de guide pour réaliser des interviews auprès des entreprises. Il nous servira à comprendre comment elles fonctionnent, quels sont leurs activités principales, de quoi ces activités dépendent, de quoi l'entreprise dépend,etc, dans le but d'identifier les aspects de la sécurité de l'information sur lesquels il convient de mettre l'accent.

1.2 Hypothèses

1. Le degré de maturité des entreprises vis à vis de la sécurité de l'information varie fortement.
2. Les entreprises ont des secteurs d'activités forts variés.
3. Les entreprises n'ont pas les même besoins en matière de sécurité de l'information.
4. Les entreprises font face à des menaces et problèmes propres à leur secteur d'activité.
5. Les entreprises utilisent des équipements différents.

1.3 Objectifs

1. Obtenir une description de l'entreprise, de ses objectifs et de son organisation.
2. Identifier les mesures en place pour assurer la disponibilité, l'intégrité, et la confidentialité des données.
3. Identifier les activités de l'entreprise, et leur importance.
4. Identifier les problèmes pouvant empêcher l'entreprise de fonctionner correctement.
5. Identifier les éléments, logiciels ou matériels, que l'entreprise utilise dans ses activités, et leur importance.
6. Identifier les sources de dépendance de l'entreprise.

1.4 Aspects légaux

Les informations contenues dans ce questionnaire sont considérées confidentielles sauf mention contraire de votre part.

Ce questionnaire peut être rempli anonymement, sauf mention contraire de votre part. Nous utiliserons de notre côté des acronymes pour identifier les questionnaires sans pour autant divulguer leur provenance.

Concernant une éventuelle publication des résultats, nous vous contacterons ultérieurement et nous conviendrons avec vous des modalités.

Nous vous remercions pour votre aide et pour le temps que vous prenez pour répondre à ce questionnaire.

2 Questionnaire

1. **Nom :** _____ **Prénom :** _____ **Age :** ___ **Entreprise :**_____

2. **Combien de salariés votre entreprise compte-t-elle ?** _____

3. **Combien d'implantations votre entreprise possède-t-elle ?** _____

4. **Décrivez brièvement votre entreprise ?**

5. **Citez les objectifs de votre entreprise ?**

6. **Décrivez l'organisation de votre entreprise ? Qui s'occupe de quoi ?**

7. **A quelle fréquence votre entreprise engage-t-elle du personnel ?**

8. **Traitez-vous avec :**
   - ☐ Des fournisseurs
   - ☐ Des partenaires
   - ☐ Personne
   - ☐ Je ne sais pas

   Que vous apportent-ils ?

9. **Qu'est-ce qui s'occupe de la gestion des technologies informatiques dans votre entreprise ?**

Avez-vous un département, un service ou une personne qui s'occupe de gérer la sécurité de l'information ?

10. **Possédez-vous des données qu'il vous faut protéger ?**
    - ☐ Oui
    - ☐ Non
    - ☐ Je ne sais pas

Quelle est la nature de ces données ? Et leur importance vis à vis de vos activités ?

Contre quoi est-il nécessaire de protéger ces données ?

Quelles services/tâches vous aident-elles à accomplir ?

Qui a accès a ces données ?

Comment vous assurez-vous que seules les personnes autorisées peuvent y accéder ?

Quelles sont les mesures de sécurité qui existent ?

11. Avez-vous des moyens pour vous assurer de l'intégrité des données que vous manipulez ?

- ☐ Oui
- ☐ Non
- ☐ Je ne sais pas

Comment vous assurez-vous qu'à tout moment il n'y a pas de perte des données ?

Comment vous assurez-vous qu'à tout moment il n'y a pas de modification des données ?

Comment vérifiez-vous que vos données sont authentiques ?

Comment vérifiez-vous que vos données sont valides/utilisables ?

12. Par quels moyens communiquez-vous vos données aux entités ou personnes qui en ont besoin ?

Quelles sont les mesures de sécurité mise en place pour ces moyens ?

Quels problèmes une perturbation de vos moyens de communication provoquerait-elle ?

13. Avez-vous des services et données qui doivent être disponibles à tout moment ?

- ☐ Oui
- ☐ Non
- ☐ Je ne sais pas

Quels sont-ils/elles ?

A quel point leur indisponibilité vous serait-elle dommageable ?

Comment assurez-vous leur disponibilité ?

14. Citez les activités principales et/ou services de votre entreprise. Classez-les de la plus à la moins importante.

15. **Décrivez en quelques lignes votre journée de travail type.**

16. **Décrivez les éléments matériels et/ou équipements qui sont vitaux au fonctionnement de votre entreprise.**
Classez-les du plus au moins important.

17. **Décrivez les instruments et logiciels que vous utilisez au cours de vos journées de travail.**

18. **Décrivez les problèmes qui ont déjà bloqué le fonctionnement de votre entreprise, ou menacé son existence.**
Classez-les selon leur fréquence d'apparition.

Comment les avez-vous surmontés ?

19. **Décrivez les évènements dont vous redoutez la réalisation car vous supposez ou savez qu'ils ont la capacité de menacer l'existence de votre entreprise.**

Savez-vous quoi faire s'ils se produisent ?

- ☐ Oui
- ☐ Non
- ☐ Vaguement
- ☐ Je ne sais pas

Comment ?

3 Feedback du questionnaire

20. Qu'avez-vous pensé des questions ?

21. Avez-vous aimé réaliser cette interview ? ☐ Oui ☐ Non

Pourquoi ?

22. Avez-vous pu bien illustrer votre entreprise ? ☐ Oui ☐ Non

Pourquoi ?

23. Avez-vous pu communiquer les enjeux de sécurité de l'information qui vous concernent ?

☐ Oui

☐ Non

Pourquoi ?

Annexe K

Enquête de satisfaction de l'étape de validation

Cette annexe contient l'enquête de satisfaction proposée aux entreprises après la réalisation des tests de validation. Certaines des questions à réponse ouverte ont été ignorées par les répondants, sur nos recommandations, car nous les leur avons posées au cours des tests.

Enquête de satisfaction sur l'utilisation de SecUNamur

Cette enquête a pour but de nous permettre d'estimer votre niveau de satisfaction quant à l'utilisation de l'outil SecUNamur d'évaluation de la sécurité des PME. Nous souhaitons vous rappeler que les trois premières questions sont tout à fait facultatives.

*Obligatoire

1. **Quels sont vos nom et prénom ?**

   _____

2. **Quel est le nom de votre entreprise ?**

   _____

3. **Quel est votre fonction ?**

   _____

4. **Trouvez-vous que l'outil soit facile à utiliser ?** *

   ☐ Très facile
   ☐ Facile
   ☐ Difficile
   ☐ Très difficile

5. **Quelles sont vos suggestions pour améliorer son utilisabilité ?**

   _____

   _____

   _____

6. **Les questions et les réponses véhiculent-elles clairement les concepts, sujets et informations sur la sécurité et les entreprises ?** *

   Il s'agit de la clarté, lisibilité et compréhensibilité des questions et de leurs réponses.

   ☐ Très satisfait
   ☐ Satisfait
   ☐ Insatisfait
   ☐ Très insatisfait

7. **Pourriez-vous nous indiquer les questions et les réponses qui n'ont pas satisfait à cette exigence ?**

   Pour une question veuillez indiquer la section, et le numéro de la question. Pour une réponse, veuillez indiquer la section, le numéro de la question, et la réponse. N'hésitez pas à ajouter vos commentaires et suggestions.

   _____

   _____

   _____

8. **Le questionnaire était-il complet, en terme de sujets abordés par les questions, et de réponses sélectionnables ?** *

   ☐ Très complet
   ☐ Suffisamment complet
   ☐ Incomplet
   ☐ Très incomplet

9. Quels sont les éléments manquants que vous suggéreriez ?

Pour une question, veuillez indiquer la section, et le sujet ou l'élément que vous souhaiteriez ajouter. Pour une réponse, veuillez indiquer la section, la question à laquelle elle devrait s'appliquer, et la réponse que souhaiteriez voir ajoutée.

10. Le questionnaire vous a-t-il permis de comprendre vos besoins en terme de sécurité de l'information ? *

- ☐ Très satisfait
- ☐ Satisfait
- ☐ Insatisfait
- ☐ Très insatisfait

11. Si non, pour quelles raisons ?

12. Les graphiques de résultats vous ont-ils permis de mieux appréhender votre niveau de gestion de la sécurité ? *

Ils sont affichés dans "Section Résultats".

- ☐ Très satisfait
- ☐ Satisfait
- ☐ Insatisfait
- ☐ Très insatisfait

13. Pourriez-vous nous donner les raisons de cette insatisfaction ?

14. L'information véhiculée par les graphiques de résultats est-elle compréhensible ? *

Ils sont affichés dans "Section Résultats". Vous ont-ils aidés à situer votre niveau de sécurité de l'information ?

- ☐ Très satisfait
- ☐ Satisfait
- ☐ Insatisfait
- ☐ Très insatisfait

15. Que suggéreriez-vous pour améliorer la compréhensibilité des résultats ?

16. La documentation fournie avec l'outil a-t-elle répondu à vos questions sur outil et la méthodologie derrière celui-ci ? *

- ☐ Très satisfait
- ☐ Satisfait
- ☐ Insatisfait
- ☐ Très insatisfait

17. Que suggéreriez-vous pour améliorer cette documentation ?

_____

_____

_____

18. Quels sont les bugs que vous avez rencontrés lors de l'utilisation de l'outil ?

_____

_____

_____

Bibliographie

[1] Larousse (2014). Définitions : maturité - Dictionnaire de français Larousse. `http://www.larousse.fr/dictionnaires/francais/maturit%C3%A9/49925?q=maturit%C3%A9#49824`. Consultation : 2015-07-22.

[2] Rabiah Ahmad, Shahrin Sahib, and Muhamad Pahri Nor'Azuwa. Effective measurement requirements for network security management. *International Journal of Computer Science and Information Security*, 12(4), Avril 2014.

[3] Cecilia Albert and Audrey J Dorofee. Octave criteria, version 2.0. 2001.

[4] Christopher Alberts, Audrey Dorofee, James Stevens, and Carol Woody. Octave-s implementation guide, version 1. Technical report, Janvier 2005.

[5] Christopher J Alberts, Audrey J Dorofee, and Julia H Allen. Octave^{SM} : Catalog of practices, version 2.0. Technical report, DTIC Document, Octobre 2001.

[6] M Azuwa, Rabiah Ahmad, Shahrin Sahib, and Solahuddin Shamsuddin. Technical security metrics model in compliance with ISO/IEC 27001 standard. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1(4):280–288, 2012.

[7] Hanane Bahtit and Boubker Regragui. Risk management for ISO 27005 decision support. *Risk Management*, 2(3), Mars 2013.

[8] Richard Basque. *CMMI 1.3 - Guide complet de CMMI-DEV*. Dunod, 2011.

[9] Ricardo M Bastos and Duncan Dubugras A Ruiz. Extending uml activity diagram for workflow modeling in production systems. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 3786–3795. IEEE, 2002.

[10] Daniela Berardi, Diego Calvanese, and Giuseppe De Giacomo. Reasoning on UML class diagrams. *Artificial Intelligence*, 168(1):70–118, 2005.

[11] France Bilocq. Conception et évaluation de questionnaires. *Actes des journées de méthodologie statistique*, 69:70–71, 1996.

[12] Agnès Bouletreau, Dominique Chouanïère, et al. Concevoir, traduire et valider un questionnaire. A propos d'un exemple, EUROQUEST. 1999.

[13] Canal-U. Les enjeux de sécurité de l'information dans le monde économique. `https://www.canal-u.tv/video/canal_aunege/les_enjeux_de_securite_de_l_information_dans_le_monde_economique.12920`. Consultation : 2015-07-19.

[14] Richard A Caralli, James F Stevens, Lisa R Young, and William R Wilson. Introducing octave allegro: Improving the information security risk assessment process. Technical report, DTIC Document, 2007.

[15] Microsoft Corporation. Office 2013 release. `https://msdn.microsoft.com/en-us/library/office/jj162978.aspx`, Janvier 2013. Dernière modification : 2015-06-02. Consultation : 2015-06-10.

[16] Commission de la protection de la vie privée. Aperçu - sécurité de l'information. `http://www.privacycommission.be/fr/securite-information`. Consultation : 2015-07-19.

[17] Club de la Sécurité de l'Information Français. Mehari 2010 : Présentation générale. `https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduction.pdf`, Janvier 2010. Consultation : 2015-06-10.

[18] Club de la Sécurité de l'Information Français. Mehari 2010: Guide de la démarche d'analyse et de traitement de risque. `https://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2010-Guide-demarche.pdf`, Avril 2011. Consultation : 2015-06-10.

[19] Georg Disterer. ISO/IEC 27000,27001 and 27002 for information security management. *Journal of Information Security*, 2013-04-16.

[20] Agence du Numérique. Problèmes et solutions de sécurité informatique. `http://www.awt.be/web/dem/index.aspx?page=dem,fr,020,020,018`. Consultation : 2015-07-19.

[21] International Organization for Standardization. ISO/IEC *27002:2013 - Information technology - Security techniques - Code of practice for information security controls*, second edition, 2013-10-01.

[22] International Organization for Standardization. ISO/IEC *27003:2010 - Information technology - Security techniques - Information security management system implementation guidance*, first edition, 2010-02-01.

[23] International Organization for Standardization. ISO/IEC *27004:2009 - Information technology - Security techniques - Information security management - Measurement*, first edition, 2008-06-15.

[24] International Organization for Standardization. ISO/IEC *27005:2008 - Information technology - Security techniques - Information security risk management*, first edition, 2009-12-15.

[25] International Organization for Standardization. ISO/IEC *27000:2009 - Information technology - Security techniques - Information security management systems - Overview and vocabulary*, first edition, 2009-05-01.

[26] International Organization for Standardization. ISO/IEC *27001:2013 - Information technology - Security techniques - Information security management systems - Requirements*, second edition, 2013-10-01.

[27] Object Management Group. Unified modeling language (UML). `http://www.uml.org/`, 1997-2015. Consultation : 2015-06-10.

[28] The Open Group. *Open Information Security Management Maturity Model (O-ISM3)*. Van Haren Publishing, first edition, Mai 2005.

[29] IT Governance Institute, editor. *CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. IT Governance Institute, Rolling Meadows, 2007.

[30] Organisation internationale de normalisation. ISO - Organisation internationale de normalisation. `http://www.iso.org/iso/fr/home.htm?=`. Consultation : 2015-07-22.

[31] Fabrice Issac and Olivier Hû. Un formalisme de description de questionnaires pour l'évaluation. *TICE'2000, Technologie de l'Information et de la Communication dans l'Enseignement*, pages 18–20, 2000.

[32] Geoffrey Karokola, Stewart Kowalski, and Louise Yngström. Towards an information security maturity model for secure e-government services: A stakeholders view. In *HAISA*, pages 58–73, 2011.

[33] MM Lessing. Best practices show the way to information security maturity. 2008.

[34] Nicolas Mayer. *Model-based management of information system security risk*. PhD thesis, University of Namur, April 2009.

[35] Agence nationale de la sécurité des systèmes d'information. Ebios : Bases de connaissances. `http://www.ssi.gouv.fr/uploads/IMG/pdf/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf`, Janvier 2010. Consultation : 2015-06-10.

[36] Agence nationale de la sécurité des systèmes d'information. Ebios : Guide methodologique. `http://www.ssi.gouv.fr/uploads/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf`, Janvier 2010. Consultation : 2015-06-10.

[37] Malik F Saleh. Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, 5(3):316–337, 2011.

[38] Mario Spremic and Matija Popovic. Towards a corporate it risk management model. In *Proceedings of the 6th WSEAS international conference*

on Information security and privacy, pages 111–116. World Scientific and Engineering Academy and Society (WSEAS), 2007.

[39] Marco Spruit and Martijn Röling. Isfam: The information security focus area maturity model. 2014.

[40] Boris Stevanović. Maturity models in information security. *International Journal of Information*, 1(2), Juin 2011.

[41] Ahmed Taha, Ruben Trapero, Jesus Luna, and Neeraj Suri. Ahp-based quantitative approach for assessing and comparing cloud security. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*, pages 284–291. IEEE, 2014.

[42] Jernej Berzelak Vasja Vehovar, Katja Lozar Manfreda. Software - websm, web survey methodology. `http://www.websm.org/c/1283/Software/?preid=1283`. Consultation : 2015-07-22.

[43] Steffen Weiß, Oliver Weissmann, and Falko Dressler. A comprehensive and comparative metric for information security. In *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2005)*, pages 1–10, 2005.