REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Ecole Nationale Polytechnique

Département de Génie Industriel

Mémoire de Magister

Présenté par :

SI AHMED Boualem
Ingénieur d'Etat en Recherche opérationnelle USTHB

Thème

Système de Management de la Sécurité Informatique:

Norme ISO27000

Membre du jury

Président : BALI Abderrahim, Prof ENP

Examinateurs : HAMAMI Latifa, Prof ENP

Belmokhtar Oumhani, prof ENP

Directeur de mémoire : Mme BENCHERIF Houria, MC ENP Alger

Invitée: BENMEZIANE Souad, chargée de recherche CERIST

Année universitaire 2010/2011

ملخص

البنية التحتية لتقنية لتكنولوجيا المعلومات و الويب وأهميتها في ازدياد مستمر لتلبية احتياجات الاتصال وتبادل متطلبات الاتصال والتشارك في المعلومات.البنيات التحتية لتكنولوجيا المعلومات والشبكات ذات الأهمية المتزايدة يستوفون كلا من ا نظام المعلومات، ونبحث ايضا لمخاطر التي يتعرض لها ، حالة فن المهنة إلى ا(SI)يتمثل هدف هذه الدراسة في أمن أنظمة المعلومات في نهاية المطاف يسمح لنا هذا إلى اقتراح أداة تدقيق وفقا .طرق تحليل و معالجة المخاطر والمعايير التي تحكم سلامة هذه الأنظمة وفقا للمعايير.مع نموذج رياضي يهدف الى مساعدة مستشار في اختيار التدابير التي وضعت لتغطية نظام معل لالمعيار

أمن نظم المعلومات، معيار :كلمات رئيسية ISO27001, معيار ISO27002 , التدقيق.

Résumé:

Les infrastructures informatiques, et Web dont l'importance ne cesse de croitre répondent à la fois à des besoins de communication et de partage d'information. La présente étude a pour objet la sécurité des systèmes d'information, l'état de l'art nous introduit aux risques auxquels un système d'information est exposé, nous y traitons également des méthodes d'analyse des risques et des normes qui régissent la sécurité. Ceci nous a permis, par la suite, de proposer un outil d'audit selon la norme 27001. Pour terminer par une modélisation mathématique qui se propose d'aider un conseiller dans le choix des mesures à mettre en place pour couvrir un système d'information, toujours selon les normes.

Mots clé : Sécurité des systèmes d'information, Norme 27001, Norme 27002, Audit.

Abstract:

IT infrastructure and Web meet both the needs of communication and information sharing. This study is aimed at the security of information systems (IS), the state of the art introduces us to the risk that an SI is exposed, we also discuss methods of risk analysis and standards governing security. This allowed us later to propose an audit tool according to the ISO27001 standard. To end with a mathematical model that aims to assist counsel in the selection of measures to cover an information system, according to ISO standards

.

Keywords: Information Systems Security, ISO27001, ISO27002 standard, Audit.

Remerciements

Le travail présenté dans ce mémoire a été réalisé conjointement au sein du département Génie industriel à l'Ecole Nationale Polytechnique (ENP) et Le Centre de Recherche sur l'information scientifique et technique (CERIST).

Je remercie madame H.BENCHERIF, maitre de conférences au Département Génie industriel à l'Ecole nationale polytechnique, pour son encadrement sa patience et ses conseils tout au long de la période de travail.

Je remercie Monsieur NOUALI, Directeur de recherche pour m'avoir encadré, pour sa gentillesse pour laquelle je serais toujours reconnaissant.

Je remercie madame S.BENMEZIANE chargée de recherche au niveau du CERIST, pour les heures passées ensemble à travailler, mais surtout de m'avoir encouragé dans les moments les plus difficiles, sans elle je n'aurais surement pas terminé ce travail.

Je remercie tous mes professeurs à L'Ecole polytechnique d'Alger pour leurs enseignements tout au long de ce cursus ainsi qu'à leurs conseils.

Je remercie mes Amis Meriem, Hayet, Abdou, Allel et Tarek pour leur aide, moral et leur contribution à différents niveaux de mon travail.

Je remercie mes parents pour leur soutien tout au long de cette période, sans eux je n'aurais jamais pu trouver la force et les ressources d'aller jusqu'au bout.

Dédicace

A mes parents

Sommaire

Liste des figures :

Liste des tableaux

Liste des Abréviations :

ISO	International Organization for Standardization
SI	Système d'Information
TCP/SYN	*Transmission Control Protocol*/
IP	Internet Protocol
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
MEHARI	Méthode Harmonisée d'Analyse de Risques
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
SMSI	Système de Management de la Securite Informatique
PDCA	Planifier Déployer Contrôler Agir
IT	Information technology
IANOR	Institut Algérien de Normalisation
PCA	plans de continuité d'activité
OWL	Ontology Web *Language*
SPARQL	Simple Protocol and RDF (Resource Description Framework) Query Language
SQL	Structured query language
OCMO	Optimisation Combinatoire Multi Objectif
IEEE	Institute of Electrical and Electronic Engineers
Dda	Déclaration d'Applicabilité

Introduction Générale:

I. Problématique

Toute entreprise, quelque soit son secteur d'activité et sa taille, a recours au service de l'informatique et des télécommunications pour construire, développer et défendre sa compétitivité et sa position sur le marché. Ainsi, grâce aux nouvelles technologies de l'informatique, l'entreprise peut développer de nouveaux services permettant de la rendre plus compétitive et plus efficace. Notons que même si les nouvelles technologies apportent plus de flexibilité, de mobilité et d'évolutivité, elles introduisent aussi une dimension de complexité et de gestion sans précédent.
Le passage à l'ère informationnelle de notre société révèle l'importance des technologies de l'information et de leur maîtrise. En considérant les dimensions nouvelles qu'elles introduisent sur les plans techniques, la nécessité d'assurer la sécurité des systèmes d'information est devenue fondamentale et soulignent le caractère stratégique de la gestion et de la mise en œuvre de la sécurité informatique.
L'objectif de la sécurité des systèmes d'information est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Cela consiste à diminuer la probabilité de voir les menaces se concrétiser, à en limiter les atteintes ou tout type de dysfonctionnement et surtout permettre le retour à un fonctionnement normal à des coûts et des délais acceptables en cas d'incident.
Néanmoins, l'efficacité de la sécurité ne repose pas seulement sur les outils de sécurité, une vision stratégique de la sécurité globale de l'entreprise est nécessaire. Le choix des mesures à mettre en place résulte généralement d'un compromis entre le coût du risque et celui de sa réduction. En effet, avant tout, une analyse des différents risques est réalisée. Celle-ci passe par l'identification des valeurs de l'entreprise, leurs niveaux de vulnérabilité en fonction des menaces particulières. En fait, il s'agit de répondre aux questions : quoi protéger ? Contre qui ? Et enfin, pourquoi ?
La sécurité de l'information est obtenue en appliquant un ensemble de mesures de contrôle, qui peuvent prendre la forme de politiques, de pratiques, de procédures, de structures organisationnelles et de fonctions de logiciels. Ces mesures de contrôle ont besoin d'être établies afin que les objectifs de sécurité spécifiques de l'organisation soient atteints.
Pour contrôler la sécurité, les entreprises ont souvent recours à de nombreux audits techniques. Cependant, ces derniers conduisent généralement aux deux constatations suivantes :

1) Nécessité d'avoir une vision de la sécurité sur le long terme : les audits techniques produisent une photo instantanée de l'état de la sécurité des plates-formes et infrastructures. Ils ont l'avantage de donner un point de vue factuel et indépendant de la situation.

2) Fossé entre la direction et l'exploitation : il y a un écart chronique entre ces deux entités. Il n'est pas rare que les directions disposent de documents répartissant de façon formelle les responsabilités des uns et des autres en matière de sécurité ou définissant les politiques à respecter. Tout en bas de la pyramide, force est de constater que la sécurité repose essentiellement sur la conscience professionnelle des exploitants. Les procédures relatives à la sécurité étant souvent transmises oralement plutôt que formalisées dans des documents, avec tous les risques que cela comporte en cas de problème. Il y a donc un lien rompu entre le haut et le bas de la pyramide.

Objectifs du travail

Dans ce contexte, l'objectif de ce projet est de définir une méthodologie de gestion de la sécurité de l'information en incluant la gestion du risque. Le recours aux normes internationales semble être une réponse aux attentes des entreprises en matière de sécurité.

La conformité par rapport à la norme ISO 27001 permet de garantir aux entreprises d'atteindre un niveau de sécurité appréciable. Néanmoins, ceci nécessite un travail fastidieux vu la consistance de la norme d'une part et les relations de chevauchement qui existent entre les différentes mesures préconisées par la norme d'autre part. Ainsi, deux problèmes se posent :

1. Tester la conformité d'une entreprise donnée par rapport à cette norme : en général, ce type de test est réalisé par une personne experte dans le domaine que nous qualifierons par Auditeur sécurité. Son rôle est de valider si le système de management de la sécurité de l'information répond aux exigences de la norme ISO 27001.
2. Aider l'entreprise à choisir les meilleures mesures de sécurité préconisées par la norme.

Ainsi, notre objectif est d'offrir à l'auditeur un outil automatique permettant de collecter les différentes réponses aux interrogations posées par la norme, d'analyser ces réponses et enfin rédiger un rapport d'audit.

Disposer d'un rapport d'audit ne suffit pas pour répondre aux différentes attentes de l'entreprise. En effet, l'auditeur sécurité, en appliquant la norme, ne tient pas compte des spécificités de l'entreprise, à savoir le budget d'investissement et les coûts des mesures à adopter. Il est donc

utile de se doter d'un outil d'aide à la décision qui permet de prendre en considération des critères adéquats pour répondre aux besoins de l'entreprise.

Dans cette partie, nous proposons une approche basée sur l'ontologie et sur l'utilisation d'un algorithme génétique. Notre approche utilise des données d'entrée d'une ontologie/sémantique de sécurité qui permet l'intégration standardisée de règles qui sont nécessaires pour modéliser les combinaisons de mesures possibles en adéquation avec la norme ISO 27001. Cette ontologie transformée permettra d'établir les relations entre mesures-vulnérabilités-coûts. Une modélisation multi objectifs et multi critères est également proposée. Pour sa résolution, nous optons pour l'utilisation d'un algorithme génétique.

Organisation du document

Ce mémoire est structuré en deux parties:

La première partie, qui fait un état de l'art de la sécurité informatique, comprend trois chapitres :

Le chapitre 1 introduit les notions de base de la sécurité informatique : menace, vulnérabilité, contre-mesure ; il effectue un premier parcours de l'ensemble du domaine, de ses aspects humains, techniques et organisationnels, sans en donner de description technique détaillée ; Il est vital de bien appréhender la relation qui unit les menaces, les expositions, les vulnérabilités et les contre-mesures afin de pouvoir appliquer des mesures de sécurité efficaces dans toute entreprise.

Puis au **chapitre 2**, nous nous sommes intéressés à la gestion du risque, où dans un premier temps, nous faisons une introduction au management du risque, Ce domaine est si vaste que nous nous sommes contentés de définitions, et de typologie de risque. Dans un second temps, des méthodes d'analyse du risque informatique sont introduites afin de relier la gestion du risque en général au domaine des systèmes d'information et de la sécurité informatique.

Pour normaliser la pratique de la gestion du risque en système d'information, la famille de normes ISO27K est apparue, c'est ainsi que **le chapitre 3** en fait une description, il aura pour objectif d'introduire les normes ISO27001 et ISO27002, et d'en faire une comparaison. C'est sur la base de ces deux normes que sera développé le programme d'audit dans **le chapitre 4.**

La deuxième partie qui constitue une proposition d'audit et une autre d'aide à la décision, comporte deux chapitres :

Le premier chapitre intitulé 'Outil d'audit de sécurité', présente un système d'audit automatisé développé au sein du CERIST, basé sur les normes ISO27001 et 27002.

Le second et dernier chapitre intitulé ‘Une approche de gestion de la sécurité de l’information’ propose un processus et une modélisation mathématique pour aider un conseiller à mettre en place des mesures de contrôle de sécurité au sein d’une organisation.

Nous achèverons cette thèse par une conclusion évoquant les principales perspectives de ce travail.

Chapitre 1

Introduction à la sécurité des SI

I.1 Introduction

Le dilemme majeur de la sécurité des systèmes d'information est qu'aucune garantie absolue ne peut être donnée. La seule manière totalement efficace de protéger un système consiste à ne pas y concéder l'accès de quelque manière que ce soit.

Tout accès au système peut potentiellement devenir une porte d'accès non autorisée. Il est clair qu'un système auquel nul n'a accès n'a que peu d'utilité. Toute la difficulté de la notion de sécurité consiste donc à autoriser l'accès à un système aux ayants droits de la manière la moins désagréable possible, tout en empêchant l'accès aux personnes non autorisées de la manière la plus efficace possible. Les deux objectifs sont souvent antinomiques.

Ce chapitre introduit les notions de base de la sécurité informatique : menace, vulnérabilité, contre-mesure ; il effectue un premier parcours de l'ensemble du domaine, de ses aspects humains, techniques et organisationnels, sans en donner de description technique détaillée ; Il est important de bien appréhender la relation qui unit les menaces, les expositions, les vulnérabilités et les contre-mesures, afin de pouvoir appliquer des mesures de sécurité efficaces dans toute entreprise.

2 Quelle est la valeur de l'Information ?

Les japonais ont coutume de dire que l'information est le sang de l'entreprise. Si l'information a une valeur intrinsèque, c'est surtout **dans son échange et son partage** qu'elle développe de la valeur [Akio, 1986].

On peut dire que l'information **acquiert de la valeur** quand elle aide les collaborateurs à agir plus efficacement lorsqu'ils cherchent à réaliser les objectifs qui leur sont assignés par l'entreprise.

Cette valeur de l'information peut prendre diverses formes :

- la connaissance des clients ou les informations partagées avec les fournisseurs et partenaires.
- Les bases de données de l'entreprise.
- Les connaissances (ou savoirs) du personnel de l'entreprise, soit le capital humain.
- Les brevets.
- les méthodes, …etc.

Bien qu'il soit difficile d'attribuer à ces éléments une valeur comptable ou les évaluer en fonction de paramètres comptables normalisés, la perte, la manipulation ou le vol d'informations peuvent considérablement affaiblir une entreprise et remettre en question ses perspectives d'avenir.

Il est toujours plus onéreux de produire de l'information que de la copier. Ainsi, l'information contenue dans la fabrication d'un nouveau produit est toujours coûteuse, en termes de temps et de budgets consacrés à la recherche et aux essais.

3 La sécurité de l'Information

L'information représente un actif aussi important que les actifs liés au système de production classique (actifs physiques, actifs humains, actifs financiers, actifs sociaux).

Et si de multiples protections ont été développées vis à vis des actifs, que l'on pourrait appeler traditionnels » : protection des infrastructures, dommages aux biens, protection sociale, en revanche, la **sécurité de l'information** n'est généralement garantie que de manière partielle et peu coordonnée dans les entreprises et organismes.

La sécurité de l'Information peut être définie comme un **dispositif global** dont la mise en œuvre assure que l'Information **peut être partagée** d'une façon qui garantit **un niveau approprié** de protection dans le but d'assurer : la confidentialité, l'intégrité et la disponibilité [ISO7493, 1989].

La sécurité est également définie dans l'ISO7498 comme suit [ISO7498, 2000]:

Le terme « sécurité » est utilisé dans le sens de minimiser les vulnérabilités d'actifs et de ressources. Un actif est tout élément de valeur. Une vulnérabilité est toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient. Une menace est une violation potentielle de la sécurité.

La sécurité doit garantir les trois propriétés de base, à savoir : la confidentialité, l'intégrité et la disponibilité.

3.1 Confidentialité

La confidentialité peut être définie comme la propriété d'une information de ne pas être révélée à des utilisateurs non autorisés. Assurer la confidentialité, c'est faire en sorte que les informations soient inaccessibles ou incompréhensibles pour des utilisateurs désignés comme non autorisés à y accéder [Deswarte, 2003]. Ceci correspond à empêcher un utilisateur de lire une information confidentielle qu'il n'est pas autorisé à connaître mais aussi à empêcher un utilisateur autorisé à lire une information et de la divulguer à d'autres utilisateurs non autorisés à y accéder. Garantir la confidentialité revient à assurer que tous les canaux d'informations sont sécurisés, c'est-à-dire que tous les chemins que peut prendre l'information pour circuler dans le

système ou vers l'extérieur sont contrôlés. Ceci entraîne des contraintes fortes et des coûts souvent incompatibles avec les besoins réels ; dans la plupart des cas, on ne s'occupera que de sécuriser un certain nombre de ces canaux.

3.2 Intégrité

L'intégrité est la garantie qu'à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité, la précision et l'authenticité.

Pour assurer cette propriété, le système doit mettre en œuvre des mécanismes garantissant :

- La création légitime de l'information,
- La vérification que les mises à jour effectuées sont autorisées et valides,
- La réalisation des mises à jour devant être effectuées ainsi qu'éventuellement des mécanismes vérifiant la correspondance entre l'information et ce qu'elle représente.

3.3 Disponibilité

La disponibilité est la propriété d'une information d'être accessible lorsqu'un utilisateur autorisé en a besoin. Cela signifie que le système informatique doit :

- Fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier
- Faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information.

4. Vulnérabilités

Les vulnérabilités sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non. [Turki, 2005]

On trouve dans la littérature plusieurs définitions de ce concept, dont certaines sont présentées ci-dessous.

Une vulnérabilité se définit en la rattachant au concept de faute qui exploitée risquerait d'endommager le système. [Avizienis et al, 2004]

Une autre définition qui la rattache au même terme est une faute accidentelle ou intentionnelle, malveillante ou non, dans les spécifications, la conception ou la configuration du système qui peut être exploitée pour créer une intrusion. [MAF, 2001], Cette définition rejoint la précédente et définit la vulnérabilité comme une entrave à la sécurité.

Dans la norme ISO:27002, nous trouvons la définition suivante : une vulnérabilité est une faiblesse d'un bien (quelque chose ayant de la valeur pour l'organisation, ses opérations et leur continuité) ou groupe de biens qui peut être exploitée par un attaquant [ISO27002, 2008]
Une vulnérabilité est également définie comme une erreur ou une faiblesse dans la conception, l'implémentation ou le fonctionnement du système. [Whitson, 2003]. [NRC, 2002]

Ces définitions sont en accord avec l'une des premières définitions connues dans [Anderson, 1980], dans laquelle l'auteur définit une vulnérabilité comme une faille connue ou suspectée, issue de la conception ou l'opération, du matériel ou du logiciel qui expose le système à une intrusion ou qui permet l'exposition accidentelle d'informations.

4.2 Les types de vulnérabilités

La vulnérabilité au sein d'une entreprise peut être catégorisée en trois groupes différents que sont : managériales, physique ou technologique.

4.1.1 Les vulnérabilités managériales

La gestion du système d'information d'une organisation peut conduire dans des cas extrêmes à la faillite : souvent dans une organisation les premières personnes à en être responsables sont les managers, dans ce cas, les vulnérabilités sont multiples :

- Pas de politique sécuritaire au sein de l'entreprise : les règles à respecter sont rarement énoncées de façon claire.
- Non maîtrise de la sécurité des systèmes d'information et de communication : L'affectation de ressources non qualifiées, mais également dans certains cas la non affectation de ressources à la surveillance des systèmes d'information et de communication.
- Manque d'information des utilisateurs : même si des procédures de sécurité des systèmes d'information et de communication existent, souvent les utilisateurs et les gestionnaires des systèmes semblent ne pas en avoir connaissance.
- Inadéquation entre la politique de sécurité et les risques : l'évaluation réelle des risques encourus n'est réalisée que rarement et donc les mesures de sécurité mises en place ne sont souvent pas en adéquation avec les risques encourus.
- Mauvaise utilisation des moyens en place : même si des règles ont été mises en place au niveau de la gestion des accès (mot de passe), l'absence de contrôles effectifs a pour

conséquence que certains utilisateurs ont tendance à ne pas changer leur mot de passe et à en utiliser certains de type « faibles».

- Organisation interne : la multiplication des pôles informatiques avec leurs solutions dédiées entraîne une complexité voire une impossibilité à gérer la sécurité des systèmes d'informations et de communication de façon centralisée.

4.1.2 Les vulnérabilités au niveau physique

Cette catégorie de vulnérabilité comprend des évènements imprévisibles comme les pannes, les accidents ou encore les atteintes intentionnelles aux matériels.

Il s'agit principalement des vulnérabilités suivantes:

- Non-redondance : que ce soit pour des raisons liées aux systèmes informatiques, logiciels ou conditions physiques (température, courant...), l'indisponibilité d'un serveur ou d'une base de données peut entraîner la rupture de services.
- Manque de contrôle d'accès aux éléments physiques : l'accès aux salles informatiques, connectiques ou autres doit être limité de manière à éviter des manipulations volontaires ou non, mais pouvant causer la perte globale de la salle informatique ou de la connectique d'une partie des utilisateurs.
- Mauvaise conservation de supports de sauvegarde : les supports de sauvegarde sont souvent stockés dans la salle informatique ce qui les rend inopérants en cas de sinistre.
- Mauvaise gestion des ressources : les ressources doivent être dimensionnées de façon correcte et doivent être surveillées de près.
- Absence de gestion du câblage : l'absence de documentation du câblage peut entraîner des déconnexions intempestives voire la mise à disposition de ressources sur des réseaux publics.

4.1.3 Les vulnérabilités au niveau technologique

Cette famille de vulnérabilités comprend toutes les vulnérabilités liées à l'utilisation de technologies ou solution (hardware, software).

Les problèmes techniques actuels de sécurité informatique peuvent, au moins provisoirement, être classés en deux grandes catégories :

1 ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite ;

2 ceux qui découlent directement ou indirectement de l'essor des réseaux qui multiplie la quantité et la gravité des menaces.

Si les problèmes de la première catégorie citée existent depuis la naissance de l'informatique, il est clair que l'essor des réseaux, puis de l'Internet, en a démultiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.

Beaucoup de personnes sont actives dans la recherche des vulnérabilités et ainsi de nouvelles failles apparaissent quotidiennement.

5. Actif, Menace et Contre-mesure

Dans ce qui suit, nous allons définir certains concepts clés de la sécurité de l'information :

5.1 Définition

Actif : est un élément de l'environnement qui peut nécessiter un certain niveau de protection. Il peut s'agir d'éléments tels que des logiciels ou du matériel – ou d'autres valeurs moins mesurables comme des données ou des personnes.

Menace : Tout danger potentiel pour les informations ou les systèmes.

Agent de Menace : Personne ou processus qui attaque le réseau via un port vulnérable du pare-feu ; processus qui accède à des données de manière à enfreindre la stratégie de sécurité.

Risque : Probabilité qu'un agent de menace exploite une vulnérabilité.

Exposition : Situation dans laquelle un agent de menace expose une ressource de la société à une perte potentielle et, partant de là, à des dommages éventuels.

Contre-mesure : Mesure de protection qui atténue ou limite un risque. Il peut s'agir de configurations logicielles, de matériel ou de procédures visant à éliminer une vulnérabilité ou à limiter le risque d'exploitation d'une vulnérabilité par un agent de menace.

5.1.1 Relations entre menaces, expositions, vulnérabilités et contre-mesures

Si un **agent de menace** engendre une **menace** et exploite une **vulnérabilité**, la sécurité peut être compromise suite à l'attaque. Cette dernière peut alors endommager un **actif** en termes de confidentialité, d'intégrité ou de disponibilité. Par conséquent, elle entraîne une **exposition** de l'entreprise à des pertes potentielles. Toutefois, il est possible de minimiser ces expositions par l'application de **contre-mesures**.

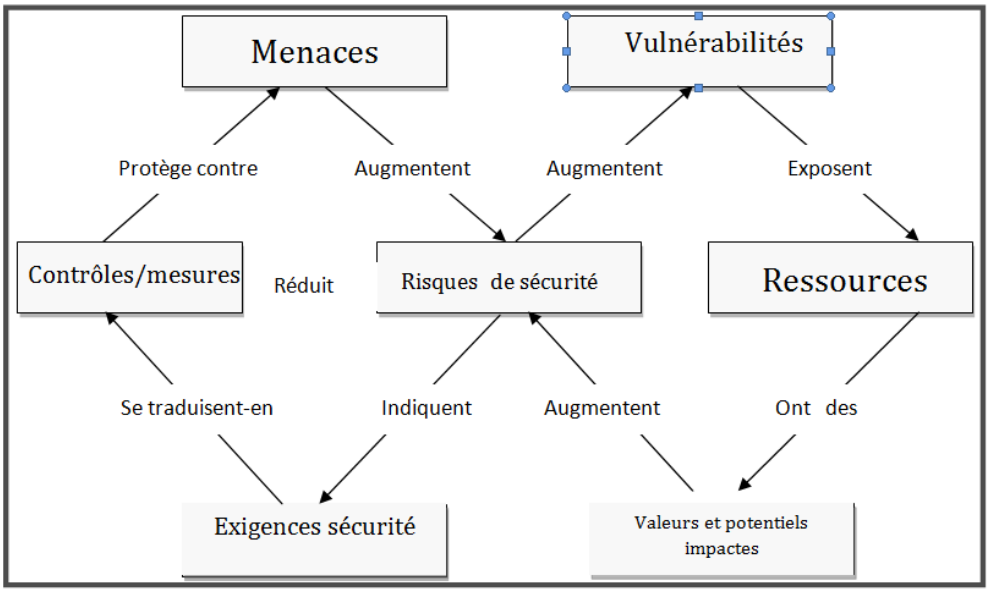


Figure 1 Relation entre menaces, expositions, vulnérabilités et contre-mesure

Exemple : Une vulnérabilité surgit si une société a installé des logiciels antivirus sur ses serveurs et que les signatures de virus ne sont pas à jour. La société devient ainsi vulnérable à d'éventuelles attaques virales dont le risque est représenté par la probabilité d'infection et de dommages causés à l'environnement. La contre-mesure nécessite donc l'installation d'un logiciel antivirus sur chacun des ordinateurs de l'environnement et à y mettre à jour les signatures de virus. La figure ci-dessous illustre les différentes relations entre les concepts :

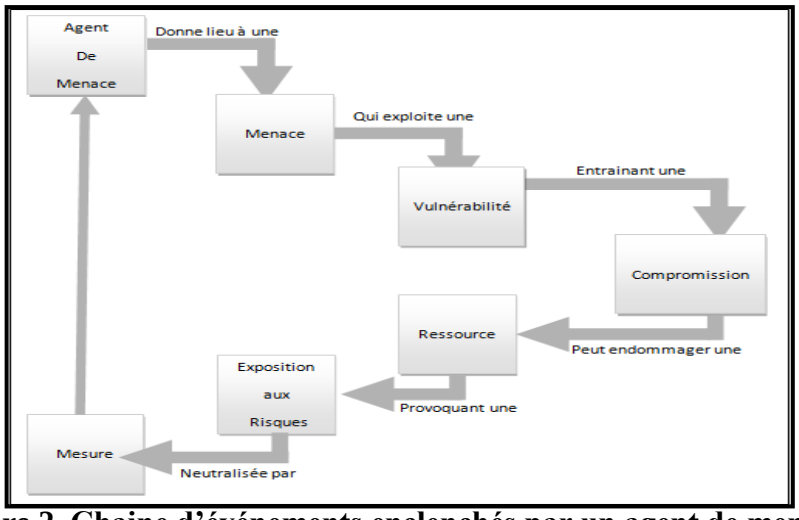


Figure 2 Chaine d'événements enclenchés par un agent de menace

6. Les attaques informatiques

Les attaques représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

Dans [MAF 2001, MAF 2003], une **attaque** est définie comme faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire, y compris les attaques lancées par des outils automatiques : vers, virus, zombies, etc. La notion d'attaque ne doit pas être confondue avec la notion d'intrusion. il est précisé également qu'un système peut être attaqué sans que cette attaque soit couronnée de succès. Dans ce cas de figure, il n'y a pas eu d'intrusion.

Une **intrusion** est donc définie comme une malveillance résultant d'une attaque qui a réussi à exploiter une vulnérabilité. Elle est susceptible de produire des erreurs pouvant provoquer une défaillance vis-à-vis de la sécurité, c'est-à-dire une violation de la politique de sécurité du système ; le terme intrusion sera employé dans le cas où l'attaque est menée avec succès et où l'attaquant a réussi à introduire et/ou compromettre le système. [MAF 2001, MAF 2003],

Il existe quatre catégories principales d'attaque :

· L'accès.

· La modification.

· Le déni de service.

· La répudiation.

6.1 Les attaques d'accès

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

- **Le sniffing**

Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe. Grâce à un logiciel appelé renifleur de paquets (sniffer), on peut intercepter tous les paquets qui circulent sur un réseau Par exemple, lors d'une connexion grâce à « telnet » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Il est aussi possible de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Cette technologie n'est pas forcement illégale car elle permet aussi de détecter des failles sur un système.

- **Les chevaux de Troie**

Les chevaux de Troie sont des programmes informatiques cachés dans d'autres programmes.
Ce nom vient de la légende grecque de la prise de Troie à l'aide d'un cheval en bois rempli de soldats qui attaquèrent la ville une fois à l'intérieur.
En général, le but d'un cheval de Troie est de créer une porte dérobée (backdoor) pour qu'un pirate informatique puisse ensuite accéder facilement l'ordinateur ou le réseau informatique. Il peut aussi voler des mots de passe, copier des données, exécuter des actions nuisibles.

- **Porte dérobée**

Lorsqu'un pirate informatique arrive à accéder à un serveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir à tout recommencer. Pour cela, il laisse donc des portes dérobées (backdoor) qui lui permettront de reprendre facilement le contrôle du système informatique.
Il existe différents types de portes dérobées :

- Création d'un nouveau compte administrateur avec un mot de passe choisi par le pirate.
- Création de compte ftp
- Modification des règles du pare-feu pour qu'il accepte des connections externes.

Dans tous les cas, l'administrateur perd le contrôle total du système informatique. Le pirate peut alors récupérer les données qu'il souhaite, voler des mots de passe ou même détruire des données.

- **L'ingénierie sociale**

L'ingénierie sociale (social engineering en anglais) n'est pas vraiment une attaque informatique, c'est plutôt une méthode pour obtenir des informations sur un système ou des mots de passe.
Elle consiste surtout à se faire passer pour quelqu'un que l'on est pas (en général un des administrateurs du serveur que l'on veut pirater) et de demander des informations personnelles (login, mots de passe, accès, numéros, données…) en inventant un quelconque motif (plantage du réseau, modification de celui-ci…). Elle se fait soit au moyen d'une simple communication téléphonique ou par mail.

- **Le craquage de mots de passe**

Le craquage consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe. Il existe deux grandes méthodes :

- L'utilisation de dictionnaires : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec

un chiffre à la fin…). Les dictionnaires actuels contiennent dans les 50 000 mots et sont capables de faire une grande partie des variantes.

- La méthode brute : toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution.

6.2 Les attaques de modification :

Une attaque de type « modification » consiste pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.

➢ **Virus, vers et chevaux de Troie**

Il existe une grande variété de virus. On peut cependant définir un virus comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.

Les dégâts causés vont du simple programme qui affiche un message à l'écran au programme qui formate le disque dur après s'être multiplié.

On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication :

- Les vers capables de se propager dans le réseau.
- Les « chevaux de Troie » créant des failles dans un système.
- Les bombes logiques se lançant suite à un événement du système.
- Les canulars envoyés par mail.

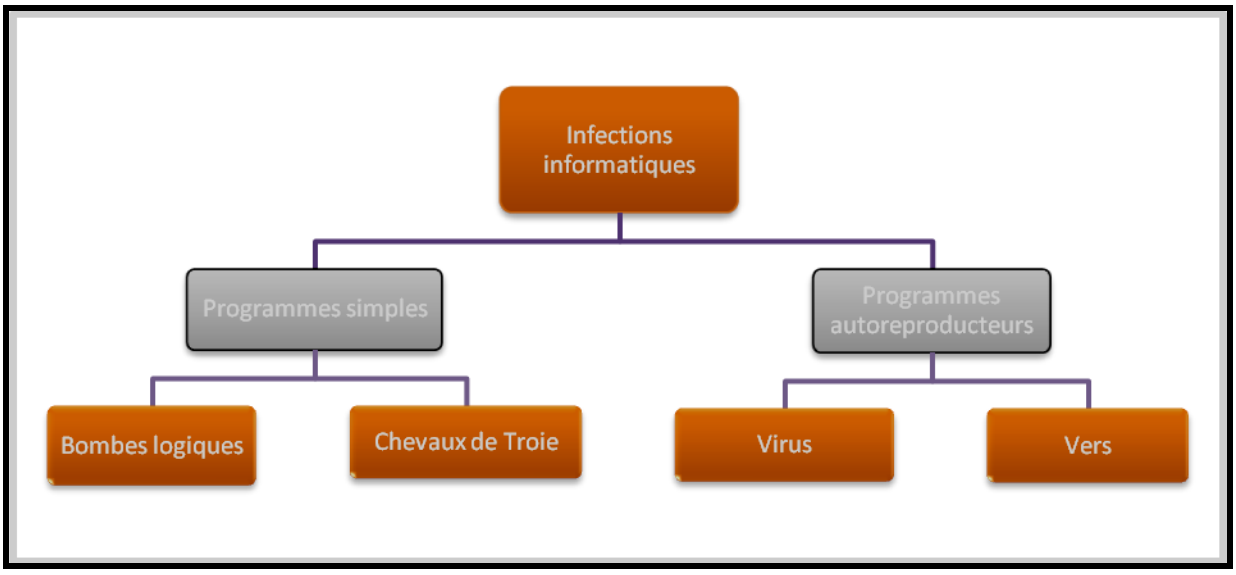


Figure 3 les infections informatiques

6.3 Les attaques par saturation (déni de service)

Les attaques par saturation sont des attaques informatiques qui consistent à envoyer des milliers de messages depuis des dizaines d'ordinateurs dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.
Cette technique de piratage assez simple à réaliser est jugée comme de la pure malveillance.
Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.
Il existe différentes attaques par saturation :

- Le flooding
- Le TCP-SYN flooding
- Le smurf
- Le débordement de tampon

- **Le flooding**

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

- **Le TCP-SYN flooding**

Le TCP-SYN flooding est une variante du flooding qui s'appuie sur une faille du protocole TCP. En effet, on envoie un grand nombre de demande de connexions au serveur (SYN) à partir de plusieurs machines. Le serveur va envoyer un grand nombre de paquet SYN-ACK et attendre en réponse un paquet ACK qui ne viendra jamais. Si on envoie les paquets plus vite que le timeout des « demi-connexions » (connexions autorisées mais non terminé), le serveur sature et finit par se déconnecter.

- **Le smurf**

Le smurf est une attaque qui s'appuie sur le ping et les serveurs de broadcast . On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune un « pong » au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.

- **Le débordement de tampon**

Cette attaque se base sur une faille du protocole IP. On envoie à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes.

Suite à ce débordement, plusieurs cas se présentent : la machine se bloque, redémarre ou ce qui est plus grave, écrit sur le code en mémoire.

6.4 Les attaques de répudiation

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soit réellement passé.

- **Le 'IP spoofing'**

Cette attaque consiste à se faire passer pour une autre machine en falsifiant son adresse IP. Elle est en fait assez complexe.

Il existe des variantes car on peut spoofer aussi des adresses e-mail, des serveurs DNS ou NFS.

7. Conclusion :

Les caractéristiques de sécurité augmentent généralement le coût d'un système et peuvent le rendre plus difficile à utiliser. Avant de concevoir un système sûr, il convient donc d'identifier les menaces spécifiques contre lesquelles une protection est nécessaire. C'est ce que l'on appelle « évaluation de la menace ». Un système est vulnérable de plusieurs façons, mais seules certaines de ces façons sont exploitables parce que l'attaquant n'a pas l'occasion d'intervenir, ou parce que le résultat ne justifie ni l'effort, ni le risque de se faire détecter. Cette évaluation porte en gros sur :

a. L'identification des vulnérabilités du système ;
b. L'analyse de la probabilité des menaces visant à exploiter ces vulnérabilités ;
c. L'évaluation des conséquences qu'aurai la réalisation de chaque menace ;
d. L'évaluation du coût de chaque attaque ;
e. L'établissement du prix de revient d'éventuelles contre-mesures ;
f. Le choix des mécanismes de sécurité qui sont justifiées.

D'où la nécessité d'accorder une importance particulière à la gestion du risque en général et du risque informatique en particulier, thème qui sera développé dans le chapitre suivant.

Chapitre II

La gestion du risque

1. Introduction :

Peu importe si un système d'information est prévu et utilisé pour le vote électronique, les ventes via le e-commerce ou des services bancaires en ligne, avec tous les avantages qu'il procure, il comporte également des risques inhérents.

La sécurité de l'information a retenu l'attention d'un certain nombre d'organisations, que ce soit dans l'industrie ou les gouvernements. Arief et Besnard [Arief et Besnard, 2003] ont souligné que les vulnérabilités logicielles et les attaques de virus ne sont que deux des menaces de sécurité classiques et qu'il était nécessaire de traiter avec des employés mécontents, des attaques d'ingénierie sociale et l'espionnage industriel pour n'en nommer que quelques-uns.

Parce que la sécurité est comme une chaîne, aussi forte que son maillon le plus faible, un système de gestion de sécurité de l'information exige une approche holistique si l'on veut s'assurer de son efficacité.

2. Gestion du risque

2.1 Définition du risque

Le risque comporte plusieurs définitions présentées ci-dessous :

- Un événement redouté auquel sera attribuée une fréquence de réalisation et une conséquence [Dacier, 1994]. Les risques sont donc évalués à partir d'une estimation de la fréquence de réalisation des menaces et des conséquences [Abghoul, 2004]
- Une situation (ensemble d'événements simultanés ou consécutifs) dont l'occurrence est incertaine et dont la réalisation affecte les objectifs de l'entreprise. [Barthélémy et Quibel, 2000]
- La c**o**mbinaison de la probabilité et de la (des) conséquence(s) de la survenue d'un événement dangereux spécifié.
- La probabilité qu'un agent de menace exploite une vulnérabilité.

2.2 Typologie du risque

Il existe plusieurs types de risques :

2.2.1 Risque positif et risque négatif

Certains risques pourront avoir des **effets positifs**, ce sont des risques que l'entreprise recherche. D'autres au contraire auront des **effets négatifs** que craint l'entreprise.

Les risques positifs sont parfois **spéculatifs** ou risque d'entreprise car ils résultent d'un choix de l'entreprise dans l'espoir d'un gain.

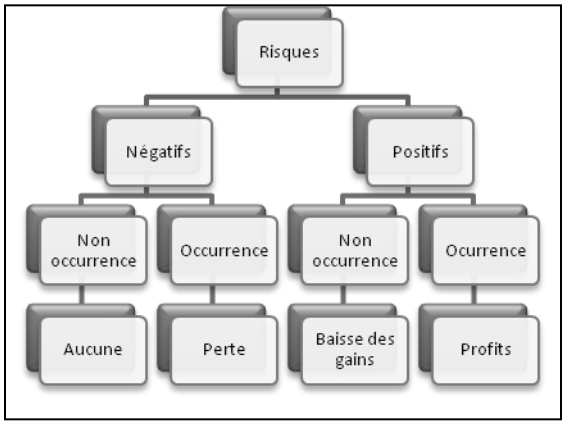


Figure 4 négatifs ou positifs

Les risques négatifs parfois qualifiés de **risques purs** par les assureurs, ce sont par exemple les catastrophes naturelles, technologiques et humaines.

Ce sont aussi des risques auxquels on pense moins, tels que par exemple :

- Les pertes du personnel et de savoir faire.
- Les conséquences de l'absence de veille technologique, commerciale ou réglementaire.
- Les défaillances de la logistique et du transport.
- La contre façon.
- Les risques sociaux.
- L'espionnage industriel.
- Les engagements de responsabilité civile ou pénale de l'entreprise.
- La défaillance des fournisseurs ou des clients.
- La malveillance, sabotage, chantage.

2.2.2 Typologie basée sur les ressources

L'entreprise a des ressources de gestion limitées, avec lesquelles elle doit composer pour atteindre les objectifs fixés par la direction ; ses risques seront analysés sur la base de la combinaison dynamique de ses ressources humaines, techniques, informationnelles, financières et partenariales.

Les risques liés aux ressources humaines :

- L'indisponibilité d'un dirigeant ou d'une personne-clef.
- Les accidents, la maladie et la formation professionnelle.
- L'inadéquation entre le recrutement, la carrière et les besoins de l'entreprise.
- La représentation du personnel, le droit du travail.
- L'intérim, la sous-traitance.

Les risques liés aux ressources techniques :

- La spécification
- L'achat
- Le contrôle qualité.
- Le stockage.
- Le site et sa sécurité.
- Les équipements et leur entretien.
- Le leasing.
- L'acquisition et la construction d'immobilisations.

Les risques liés aux ressources informationnelles

- Le savoir faire des procédés et de la main d'œuvre.
- L'indisponibilité suite à un accident.
- L'atteinte à la réputation de l'entreprise.
- La perte de crédibilité.
- La perte du capital confiance du client.
- L'atteinte au système informationnel/ comptable.
- La logistique.

Les risques liés aux ressources financières.

- La trésorerie.
- Le besoin en fonds de roulement.
- La capacité d'autofinancement.
- Les provisions diverses (dégradations des stocks etc.)

Les risques liés aux ressources partenariales :

- La responsabilité civile.
- Les contrats d'assurance
- Le respect des normes.
- Le lien avec les administrations.

2.2.3 Typologie par fonction de l'entreprise

Cette approche étudie les risques avec une vision basée sur les différentes fonctions de l'entreprise.

Risques opérationnels :

- Risque de matière première.
- Risque de stocks.
- Risque incendie, risque de dégâts des eaux.
- Risque de pollution.
- Risque de dommages matériels.

Risques Marketing :

- Risque de marché.
- Risque de concurrence.
- Risque de force de vente.
- Risque après vente.
- Risque d'image de l'entreprise.
- Risque de prospection.

Risques juridiques

- Risque lié à la responsabilité civile.
- Risque d'évolution des règlements.
- Risque de contractualisation (par exemple, la perte d'un fournisseur)

Risques financiers

- Risque de liquidité.
- Risque de solvabilité.

- Risque de rentabilité.
- Risque de taux de change.
- Risque de taux d'intérêt.

Risques de ressource humaine

- Risque lié à l'effectif.
- Risque de carrières.
- Risque d'adéquation des embauches par rapport aux postes.
- Risque de compétence.
- Risque social, risque de harcèlement.
- Risque lié à une personne-chef (responsable).

Risques informatiques

- Risque de malveillance.
- Risque de fraude.
- Risque d'incident (bug), risque de virus.
- Risque de gestion de l'information.

Risques organisationnels.

- Risque d'organigramme.
- Risque de responsabilités.
- Risque de délégations et mandats.
- Risque de prise de décision.
- Risque lié à une personne chef (responsable).

Dans le management du risque lié aux systèmes d'informations, nous nous intéresserons principalement aux risques liés aux deux fonctions précédentes à savoir les risques informatiques et les risques organisationnels.

Il existe d'autres typologies telles que la typologie basée sur le modèle d'entreprise, sur les processus, ou encore une typologie basée sur les documents financiers ; pour plus de détails, on peut se référer à l'ouvrage de Barthélémy : gestion des risques, méthode d'optimisation globale [Barthélemy et Quibel, 2000]

2.3 Caractéristiques d'un risque :

Un risque donné est caractérisé par :

La fréquence F qui mesure la probabilité d'occurrence du risque.

La gravité G qui mesure les conséquences du sinistre, généralement exprimées en unités monétaires.

Le point F x G représente l'espérance mathématique de la gravité. C'est un indicateur de l'acuité du risque souvent appelé criticité. L'unité de criticité est la même que celle de la gravité.

Criticité = fréquence x gravité [Barthélémy et Quibel, 2000]

La littérature introduit une formulation semblable, avec l'apparition de **la probabilité de non détection des causes de défaillance D**, exemple la formule que l'on trouve dans certains documents de la méthode AMDEC ou la criticité.

Criticité : C = F x D x G [Zwingeslstein, 2009]

Selon ces deux caractéristiques, nous pouvons définir :

Les risques dits **de fréquence caractérisés** par une fréquence assez élevée et une gravité relativement faible ;

Les risques dits **de gravité** qui au contraire auront une gravité forte mais une probabilité d'occurrence faible.

Les **risques négligeables** sont ceux dont la fréquence et la gravité sont faibles.

Les **risques inacceptables** sont ceux dont la fréquence et la gravité sont élevées, pour lesquels le seul traitement est l'évitement ou la suppression de l'activité risque.

Enfin **les risques à fréquence et gravité moyennes** constituent le vaste champ d'application de la gestion des risques. Le schéma suivant est une représentation de ces différents types de risques :

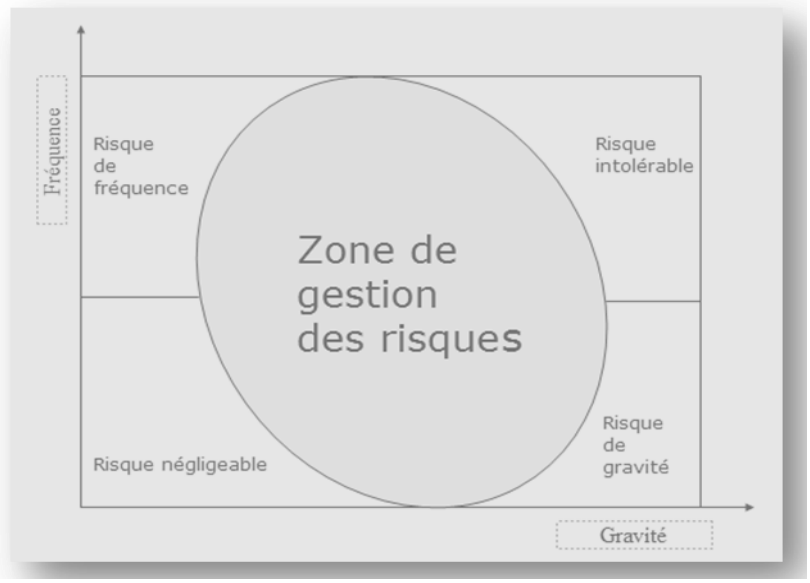


Figure 5 Types de risques et zone de gestion du risque

Remarque :

La fréquence et la gravité déterminent le risque, mais devant le même risque la personnalité du décideur et donc sa perception de la prise de risque fait qu'il ne prendra pas forcément la même décision qu'un autre décideur dans la même situation.

2.4 Définition du management des risques :

Le dispositif de management des risques est un processus permanent qui irrigue toute l'organisation, il est mis en œuvre par l'ensemble des collaborateurs à tous les niveaux de l'organisation, pris en compte dans l'élaboration de la stratégie et permet d'obtenir une vision globale de son exposition aux risques.

2.5 Les étapes du management du risque :

Nous pouvons schématiser la gestion des risques en trois étapes :

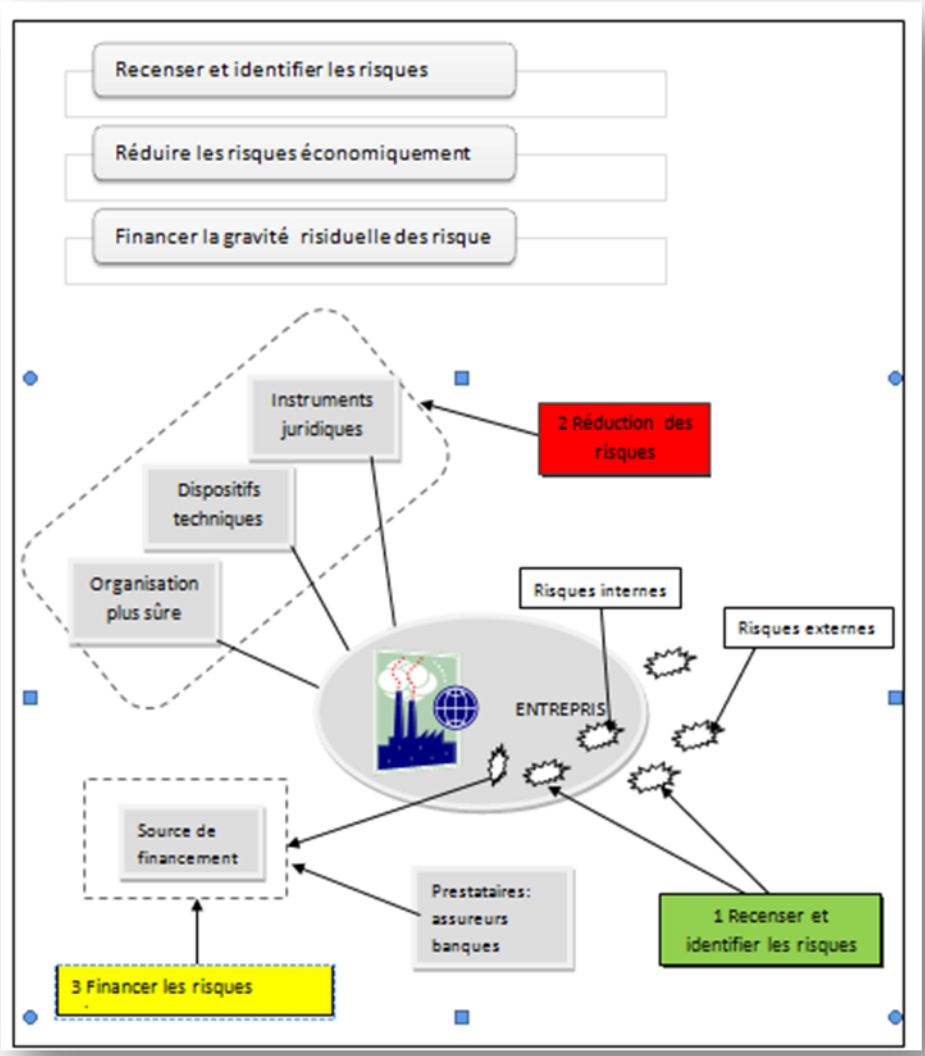


Figure 6 les étapes du management du risque [Nguéna, 2008]

2.5.1 L'identification des risques :

L'identification des risques vise à identifier l'exposition d'une organisation à l'incertitude. Elle requiert une connaissance précise de l'organisation, des marchés où celle-ci opère, de son environnement juridique, social, politique et culturel.

Elle requiert également de développer une solide compréhension de ses objectifs stratégiques et opérationnels, des facteurs critiques de succès et des menaces et opportunités qui s'y rapportent. L'identification des risques exige une approche méthodique pour garantir que chaque activité significative de l'organisation a été identifiée et que chaque risque potentiel qui en découle a bien reçu une définition.

Toute volatilité associée à ces activités sera identifiée et classée dans une catégorie.

2.5.2 La quantification des risques

a) Appréciation du risque

L'appréciation du risque est définie par le Guide ISO/IEC 73 [ISOEC73, 2002] comme le processus général d'analyse du risque et d'évaluation du risque.

b) Description des Risques

La description des risques consiste à présenter les risques identifiés dans un format structuré comme par exemple un tableau. Le tableau de description des risques peut faciliter la description et l'évaluation de certains risques. La structure de ce format sera conçue avec soin pour s'assurer que les risques sont bien identifiés, décrits et appréciés exhaustivement et avec précision.

En examinant les conséquences et la probabilité de chaque risque présenté dans le tableau, il devrait être possible de déterminer les risques clefs qui doivent être analysés plus en détail. L'identification des risques liés aux activités économiques et à la prise de décision peut recourir à des catégories comme "stratégique", "projet/tactique" ou encore "opérationnel". Il est important d'intégrer la gestion des risques dans chaque projet spécifique dès sa conception et pendant toute sa durée de vie.

c) Estimation du risque

L'évaluation du risque peut être quantitative, semi-quantitative ou qualitative en termes de probabilité d'occurrence et de conséquences possibles. Par exemple, les conséquences à la fois en terme de menaces (aléa négatif) et d'opportunités (aléa positif) peuvent être qualifiées de fortes, moyennes ou faibles. La probabilité peut se qualifier de haute, moyenne ou faible mais exige différentes définitions selon qu'il s'agit de menace ou d'opportunité.

Les mesures les plus adaptées pour les conséquences et les probabilités peuvent varier d'une organisation à une autre. Par exemple, beaucoup d'organisations jugent qu'évaluer les conséquences et les probabilités comme fortes, moyennes ou faibles selon une matrice 3x3 répond tout à fait leurs besoins. D'autres organisations préfèreront une matrice 5x5.

FORT	Impact financier sur l'organisation susceptible d'excéder x$. Impact significatif sur la stratégie ou les activités opérationnelles de l'organisation. Parties prenantes fortement préoccupées.
MOYEN	Impact financier sur l'organisation compris entre y$ et x$ Impact modéré sur la stratégie ou les activités opérationnelles de l'organisation.

	Parties prenantes modérément préoccupées.
FAIBLE	Impact financier sur l'organisation susceptible inférieur à x$. Faible impact sur la stratégie ou les activités opérationnelles de l'organisation. Parties prenantes faiblement préoccupées.

Tableau 1: exemple d'évaluation quantitative

d) Profil de risque

Le résultat de l'analyse du risque peut servir à produire un profil de risque qui donne une note d'importance à chaque risque. Il permet ainsi de déterminer les risques qui demandent un effort de traitement prioritaire. Un tel profil classe les risques identifiés et met ainsi en évidence leurs importances relatives.

Ce processus fournit la correspondance entre les risques et les secteurs d'activités, décrit les principaux moyens de maîtrise des risques en place et indique les secteurs où le niveau d'investissement dans la maîtrise du risque pourrait être réajusté.

Une bonne définition des responsabilités aide à faire reconnaître clairement le/la "propriétaire" de chaque risque et à assurer que les ressources de gestion appropriées sont correctement allouées.

e) Evaluation du risque

Après avoir analysé les risques, il est nécessaire de comparer les risques estimés aux critères de risque que l'organisation a établis. Les critères de risque peuvent comprendre les coûts et bénéfices associés, les contraintes juridiques, les facteurs socioéconomiques et environnementaux, les préoccupations des parties prenantes, etc.

Par conséquent l'évaluation du risque aide à décider de l'importance de chaque risque spécifique pour l'organisation et à déterminer s'il convient d'accepter ce risque en l'état ou bien de le traiter.

2.5.3 Traitement du risque

Le processus de traitement du risque consiste à sélectionner et mettre en place des mesures propres à modifier le risque. Le traitement du risque a pour principales composantes la maîtrise et l'atténuation du risque, mais il ne s'y limite pas et s'étend entre autres à l'évitement, au transfert et à son financement, etc.

Remarque :

- le financement du risque fait référence à des mécanismes tels que les programmes d'assurance. (financement des conséquences du risque)

- En général, le terme de financement du risque ne se rapporte pas au financement de la mise en place du traitement du risque [ISOEC73, 2002]

Tout système de traitement de risque doit assurer au minimum:

• le bon fonctionnement de l'organisation,

• l'efficacité du système de contrôle interne,

• la conformité avec les lois et la règlementation.

Le processus d'analyse de risque aide au bon fonctionnement de l'organisation en identifiant les risques qui exigent l'attention des responsables. Ceux-ci devront déterminer les actions de maîtrise du risque qui sont prioritaires en termes de bénéfice potentiel pour l'organisation.

L'efficacité du système de contrôle interne se mesure au degré d'élimination ou de réduction du risque que procurent les mesures de maîtrise proposées.

L'efficacité économique du système de contrôle interne dépend du rapport entre les coûts d'implémentation de celui-ci et les bénéfices attendus de la réduction du risque.

Pour évaluer un projet de dispositif de maîtrise des risques, il convient de mesurer et de comparer l'effet économique potentiel si aucune mesure de prévention n'est prise d'une part et le coût de l'action proposée d'autre part.

La figure suivante récapitule les différentes étapes précédemment énumérées.

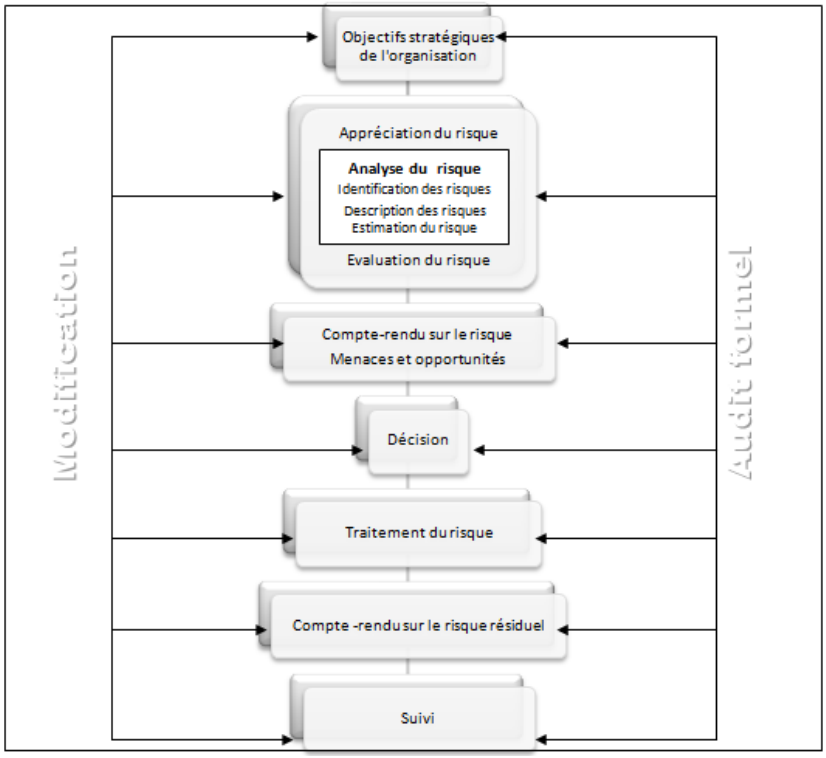


Figure 7 Les étapes du management du risque

3. Les Méthodes d'analyse du risque informatique

Même après en avoir dégrossi les fondements, la notion de risque reste un concept difficile à appréhender. La complexité des organisations actuelles associées aux enjeux business forcent à ne pas s'en remettre exclusivement à ses subjectivités, en résumé à sa perception « intellectuelle », mais plutôt à faire confiance à des méthodes formelles éprouvées. En un mot : « Nul besoin de réinventer la roue en matière d'analyse des risques ». Mieux vaut plutôt profiter du travail effectué et des guides à disposition.

Les méthodes les plus connues sont :

• OCTAVE (méthode américaine issue de l'université de Carnegie Mellon), [OCTAVE, 2007]

• MEHARI (méthode française issue du CLUSIF),

• EBIOS (méthode française créée par la DCSSI).

3.1 La méthode OCTAVE : (Operationally Critical Threat, Asset, and Vulnerability Evaluation) est la méthode de sécurisation américaine en partie basée sur les critères communs [OCTAVE, 2003]. A l'origine, OCTAVE était une méthode de sécurisation orientée vers les grandes entreprises. Comme cette version d'OCTAVE ne convenait pas trop aux petites entreprises, la version OCATVE-S a vu le jour. Il existe aussi la version OCTAVE Allegro qui est basée essentiellement sur la sécurité de l'information. OCTAVE est une méthode de sécurisation qui se différencie des autres méthodes dans la mesure où elle privilégie l'étude organisationnelle de la sécurité et propose des solutions stratégiques alors que les autres méthodes sont orientées vers les technologies de sécurisation et proposent des solutions tactiques. De plus, c'est une méthode qui peut être conduite depuis l'intérieur de l'entreprise, elle ne nécessite pas l'intervention d'experts externes.

La méthode OCTAVE se décompose en 3 phases :

• Phase 1 : Construction de profils de menaces basés sur les actifs.

• Phase 2 : Identification des vulnérabilités de l'infrastructure.

• Phase 3 : Développement d'une stratégie de sécurité et de plans.

Voici un schéma détaillant les phases de la méthode OCTAVE :

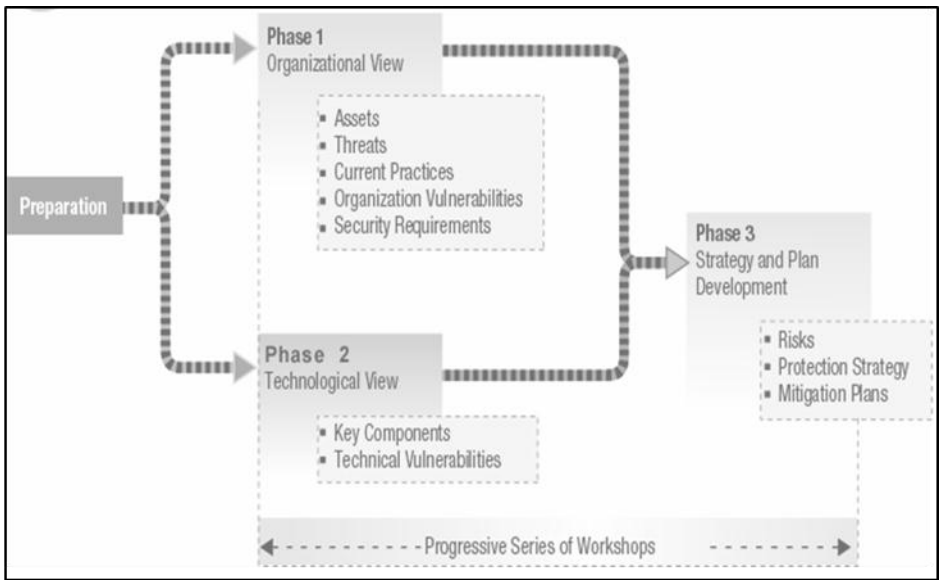


Figure 8 Les phases d'OCTAVE [OCTAVE, 2003]

La phase 1 est une évaluation organisationnelle. Elle consiste en l'identification des actifs de l'entreprise (information, ressources, etc...) et à la description de ce qui est fait pour protéger ces actifs. Par la suite, l'équipe en charge de l'évaluation va identifier les actifs qui sont importants pour l'entreprise (en faisant un classement par exemple) et décrire quel est le niveau de sécurité requis pour chacun de ces actifs. Enfin, il ne restera plus à l'équipe qu'à identifier les menaces de chaque actif pour pouvoir établir un profil de menace.

La phase 2 quant à elle est une évaluation de l'infrastructure informatique de l'entreprise. Au cours de cette évaluation, l'équipe en charge de cette opération identifiera les vulnérabilités de l'infrastructure.

Enfin, **la phase 3** permet une évaluation du risque pour chaque actif à partir des résultats de la phase 1 et 2. Sur la base de cette analyse de risque, l'équipe en charge de cette phase pourra établir une stratégie et des plans de sécurisation de l'entreprise. Ces derniers permettent de déterminer la démarche à suivre pour faire face à une menace en fonction du risque.

Il y a 4 réponses possibles imposées par OCTAVE:

• soit on accepte la menace,

• soit on l'accepte mais elle fera l'objet d'une réévaluation,

• soit on prend des mesures contre la menace,

• soit on prend des mesures contre la menace mais elle fera l'objet d'une réévaluation.

OCTAVE intègre aussi une base de connaissances des risques qui permet d'aller plus vite quand on analyse des risques courants.

3.2 La méthode MEHARI [MEHARI, 2007] (*Méthode Harmonisée d'Analyse de Risques*) est une méthode modulaire qui permet de répondre à deux questions :

- Quelle est la finalité de la fonction?
- Comment s'y prendre, avec quels méthodes et outils spécifiques du management de la sécurité ?

Il est assez difficile de répondre à la première question, mais cette méthode apporte la réponse suivante : l'objectif de la sécurité est de minimiser les risques encourus par l'entreprise du fait de son système d'information et de les rendre acceptables.

Mais alors qu'est-ce qu'un risque inacceptable ? MEHARI répond à cette question en donnant le schéma suivant :

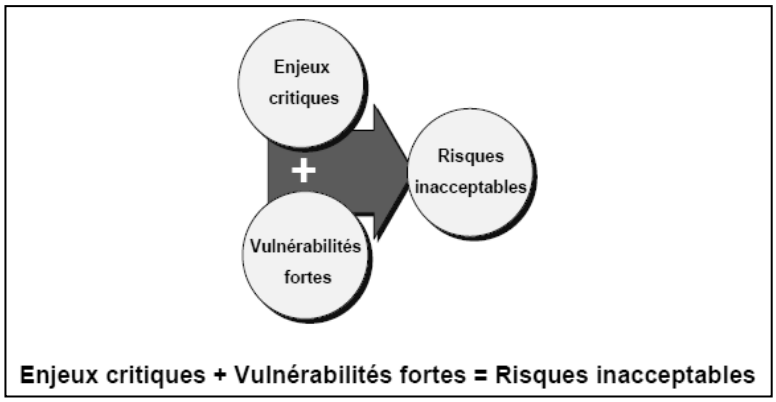


Figure 9 Schéma d'un risque inacceptable [MEHARI, 2007]

Quant à la deuxième question posée précédemment, il existe de nombreuses solutions :

• A partir de l'analyse des enjeux,

• A partir de l'analyse des vulnérabilités,

• A partir de l'analyse des situations de risques, ou une combinaison des 3 analyses et MEHARI, grâce à sa modularité, permet de les concrétiser.

Les différents modules de MEHARI sont :

• L'analyse des enjeux – Classification

• L'analyse des vulnérabilités

• L'analyse de risque

Les différentes solutions/démarches apportées par MEHARI sont montrées dans le schéma suivant :

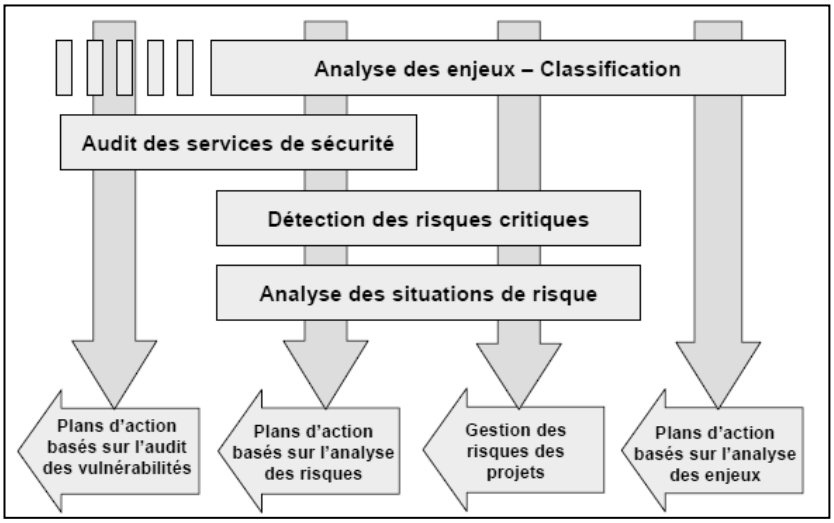


Figure 10 différentes démarches de MEHARI

Le module d'analyse des enjeux – Classification permet de répondre à une question :"*Que peut-on redouter et, si cela devait arriver, serait-ce grave ?*" [MEHARI, 2007].

Il s'agit donc de répertorier les actifs/ressources de l'entreprise, d'identifier les dysfonctionnements redoutés liés à ces ressources, d'évaluer la gravité de ces dysfonctionnements et ensuite de classifier les ressources en vue d'être utilisées pour l'analyse de risque.

Le module d'analyse des vulnérabilités permet de faire un audit de la sécurité déjà présente dans l'entreprise. Pour cela la méthode intègre un questionnaire permettant de réaliser l'audit. Cet audit permettra d'avoir une vision globale de la qualité de la sécurité de l'entreprise et de mettre en évidence ses faiblesses.

Enfin, le module d'analyse de risques permet soit en partant de la base de connaissance des situations de risques de MEHARI, soit en partant de situations de risques mises en place par l'entreprise, soit des deux, de déterminer si oui ou non, un risque est acceptable et ainsi de mettre en place un plan de sécurité pour le risque étudié.

3.3 La méthode EBIOS[EBIOS, 2006] : EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode créée par la DCSSI (Direction Centrale de la Sécurité des Système d'Information), qui est composée d'une multitude de guides méthodologiques. Elle est surtout utilisée dans les administrations françaises.

La méthode EBIOS se décompose en 4 étapes présentées dans la figure 11 ci-après:

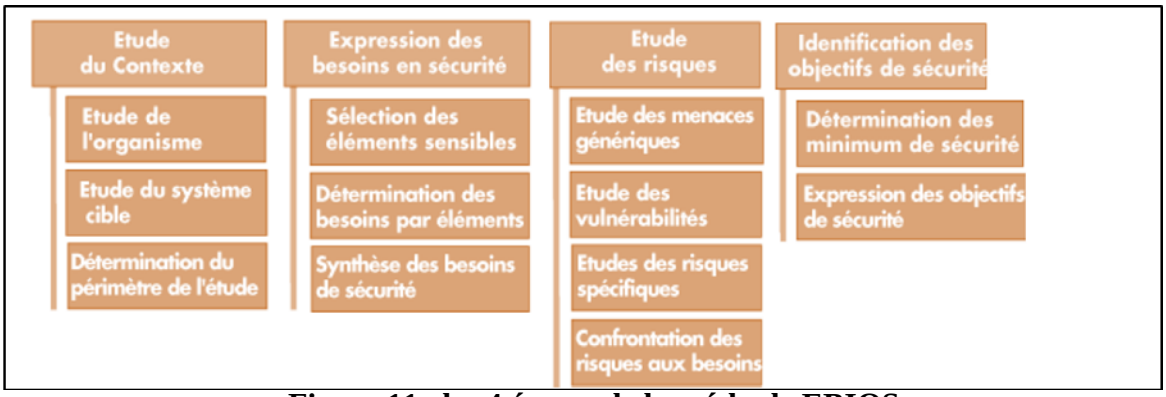


Figure 11 les 4 étapes de la méthode EBIOS

La méthode préconise l'enchainement des étapes suivantes :

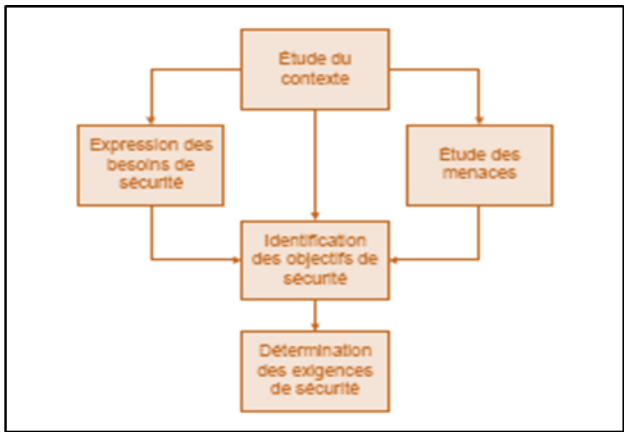


Figure 12 Enchainement des étapes [EBIOS, 2006]

Tout comme MEHARI, EBIOS est une méthode modulaire, c'est-à-dire que l'enchainement des étapes peut être différent d'une entreprise à une autre. Pour l'élaboration d'une sécurité du SI, EBIOS se base sur les critères communs, l'ISO 13335 et l'ISO 17799. EBIOS est très orientée sur l'expression des besoins en termes de sécurité du SI.

3.4 Conclusion sur l'étude des méthodes d'analyse de risques

L'étude de ces différentes méthodes d'analyse de risques qui représentent de plus en plus aujourd'hui le fondement de la sécurité en entreprise, nous permet de voir comment sont traitées les informations d'un SI et de voir comment est gérée la sécurité les concernant. Bien qu'il y ait des différences dans le mode de fonctionnement de chaque méthode, elles se déroulent en grande partie de la même manière :

• Mise en avant des actifs importants pour l'entreprise.

• Mise en avant des vulnérabilités de l'infrastructure du SI.

• Études des scénarios de risques.

• Etablissement de plans de sécurité en conséquence.

Sans détailler chaque méthode, on remarque qu'il y a des similitudes entre elles, puisqu'elles s'appuient principalement sur le classement des scénarii de risques, la différence étant les paramètres de classement utilisés:

- **OCTAVE** classe les scénarii de risques en fonction du score général d'impact. Ce score est obtenu en additionnant chaque score d'impact du scénario sur chaque zone d'impact (image de la société, financier, légal, etc...). Ces scores sont obtenus en classant l'impact en fonction de 3 niveaux (fort, moyen, faible) et en les multipliant en fonction de l'importance de la zone d'impact pour l'entreprise. (De 1 à 5 par exemple).
- **MEHARI** fait un classement des scénarii de risques en fonction de la potentialité du risque et de son impact sur l'entreprise.
- Quant à **EBIOS**, elle ne recourt pas réellement à un classement en fonction de paramètre, mais le classement se fait par les utilisateurs et par les experts en sécurité.

Ces méthodes recourent au classement des informations avec des procédés différents : O**CTAVE** ne classe uniquement les informations importantes sur une permettant d'élaborer des scénarios de risques).

EBIOS fait un classement de l'information en fonction des besoins en termes de confidentialité, intégrité et disponibilité.

MEHARI classe les informations par groupe sur la base des critères de disponibilités, intégrité et confidentialité par rapport aux applications et processus qui les utilisent. D'ailleurs, ce classement de l'information peut être utilisé dans la gestion des habilitations.

EBIOS	• Démarche très logique • Traitement des exigences • Logiciel • Bases de connaissances • Soutenue par la DCSSI • Très reconnue	• Distingue peu l'opérationnel du reste de l'organisation • Difficile d'utilisation pour un novice de la sécurité
MEHARI	• Logiciel • Conçu par le CLUSIF • Reconnue	• Méthode potentiellement lourde
OCTAVE / OCTAVE-S	• Orientée métier • Accessible à tous • Documentation très complète • Catalogue de pratiques • Variante –S pour les PME • Soutenue par le CERT /CC (Computer Emergency Response Team/ Coordination Center	• Ne traite pas les exigences

Tableau 2

Avantages et inconvénients de chaque méthode

La multiplication des méthodes d'analyse des risques ont crée un besoin d'uniformatisation, cette vision partagée par la majorité des intervenants dans la sécurité des systèmes d'information (gouvernement, banques, techniciens,…ect) ont abouti à la rédaction d'une famille de normes IS27k, objet de notre prochain chapitre.

Chapitre 3

La famille de normes ISO27000

Introduction :

Le besoin de directives sur la gestion de sécurité de l'information et de références communes aux entreprises et industries conduisent à des normes de sécurité de l'information et à des guides des meilleures pratiques ; une collection des meilleures pratiques sur la façon pour faire face à la plupart des risques de sécurité ont vu le jour [ISO27002, 2008].

L'information est une des ressources les plus importantes qu'un organisme a à sa disposition. Il est donc primordial que tout système contenant cette information soit protégé contre les dommages, les pertes et le vol. Un système de management de la sécurité de l'information (SMSI) s'avère nécessaire pour assurer la protection de ces données.

La norme ISO 27001 [ISO270001, 2005], publiée en Novembre 2005 par l'organisation internationale de normalisation(ISO), est une norme internationale qui donne des spécifications et des conseils au sujet de l'implantation et du maintien d'un SMSI. Elle a été adoptée par l'Algérie sous l'appellation NA ISO/CEI 27001 en 2008. La norme ISO 27002 [ISO27002, 2008] vient la compléter en reprenant ses objectifs et développe en profondeur les mesures de sécurité et les meilleures pratiques.

Une des notions des plus importantes que nous retrouvons dans la norme ISO27001, est la notion de système de management de la sécurité de l'information SMSI, nous

2. Définition : Système de management de la sécurité de l'information (SMSI) :

Le SMSI est une partie du système de management global, basé sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information.

Il inclut l'organisation, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

2.1. Exigences générales :

L'organisme doit établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI documenté dans le contexte des activités commerciales d'ensemble de l'organisme et des risques auxquels elles sont confrontées, le processus utilisé est basé sur le modèle PDCA (planifier, déployer, contrôler, agir) illustré à la figure ci-après:

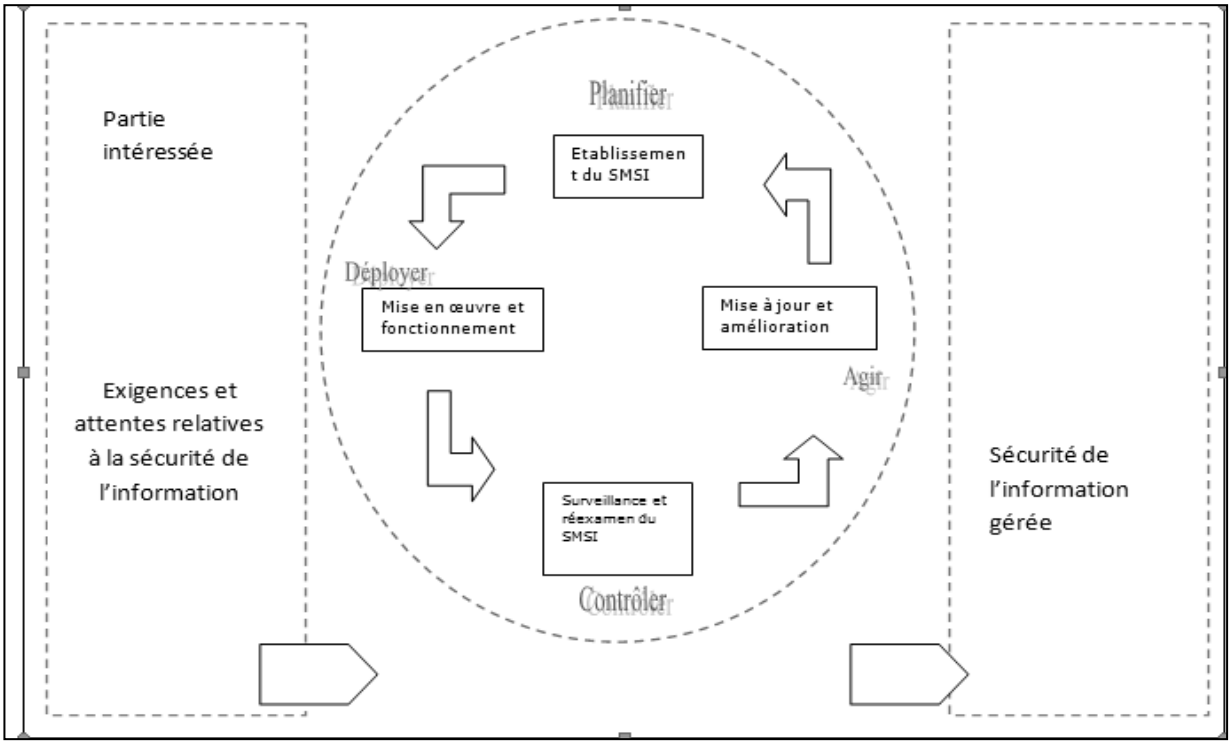


Figure 13 modèle PDCA

Planifier (établissement du SMSI)	Etablir la politique, les objectifs et les procédures du SMSI relatives à la gestion du risque et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformément aux politiques et aux objectifs globaux de l'organisme.
Déployer (Mise en œuvre et fonctionnement du SMSI)	Mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures du SMSI
Contrôler (surveillance et réexamen du SMSI)	Evaluer et le cas échéant, mesurer les performances des processus et les procédures du SMSI
Agir (mise à jour et amélioration du SMSI)	Entreprendre les actions correctives et préventives, sur la base des résultats de l'audit interne du SMSI et de la revue de direction, ou d'autres informations pertinentes pour une amélioration continue dudit système.

2.2. Etablissement et management du SMSI

2.2.1 Etablissement du SMSI

L'organisme doit effectuer les taches suivantes :

a) Définir le domaine d'application et les limites du SMSI en termes de caractéristiques de l'activité de l'organisme, de ses actifs, de l'emplacement de ses actifs, de sa technologie et justifier toutes exclusions du domaine d'application.
b) Définir une politique pour le SMSI en termes de caractéristiques de l'activité, de l'organisme, de l'emplacement de ses actifs et de sa technologie, qui :
    1) Inclut un cadre pour fixer les objectifs et indiquer une orientation générale et des principes d'action concernant la sécurité de l'information.
    2) Tient compte des exigences liées à l'activité et des dispositions légales et réglementaires, ainsi que des obligations contractuelles de sécurité;
    3) S'aligne sur le contexte de management du risque stratégique auquel est exposé l'organisme, dans lequel se dérouleront l'établissement et la mise à jour du SMSI.
    4) Etablit les critères d'évaluation future du risque.
    5) A été approuvée par la direction.
c) Définir l'approche d'application du risque de l'organisme.
    1) Identifier une méthodologie d'appréciation du risque adaptée au SMSI ainsi qu'à la sécurité de l'information identifiée de l'organisme et aux dispositions légales et réglementaire.
    2) Développer des critères d'acceptation des risques et identifier les niveaux de risque acceptables.
    3) La méthodologie d'appréciation du risque choisie doit assurer que les applications du risque produisent des résultats comparables et reproductibles.
d) Identifier les risques :
    1) Identifier les actifs relevant du domaine d'application du SMSI, ainsi que leurs propriétaires ;
    2) Identifier les menaces auxquelles sont confrontés ces actifs ;
    3) Identifier les vulnérabilités qui pourraient être exploitées par les menaces.
    4) Identifier les impacts que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs.

e) Analyser et évaluer les risques :
    1) Evaluer l'impact sur l'activité de l'organisme qui pourrait découler d'une défaillance de la sécurité, en tenant compte des conséquences d'une perte de confidentialité, intégrité ou disponibilité des actifs.
    2) Evaluer la probabilité réaliste d'une défaillance sécurité de cette nature au vu des menaces et des vulnérabilités prépondérantes, des impacts associés à ces actifs et des mesures actuellement mises en œuvre.
    3) Estimer les niveaux de risques.
    4) Déterminer si les risques sont acceptables ou nécessitent un traitement, en utilisant les critères d'acceptations des risques établis. (c.2)
f) Identifier et évaluer les choix de traitement des risques :

    Les actions possibles comprennent :
    1) L'application de mesures appropriées.
    2) L'acceptation des risques en connaissance de cause et avec objectivité au regard des politiques de l'organisme et des critères d'acceptation des risques établis.
    3) L'évitement ou le refus des risques ;
    4) Le transfert des risques liés à l'activité associée à des tiers, par exemple assureurs, fournisseurs ;
g) Sélectionner les objectifs de sécurité et les mesures de sécurité proprement dites pour le traitement des risques.

    Les objectifs de sécurité et les mesures de sécurité proprement dites doivent être sélectionnés et mis en œuvre pour répondre aux exigences identifiées par le processus d'appréciation et de traitement du risque. Cette sélection doit tenir compte des critères d'acceptation des risques ainsi que des dispositions légales, réglementaires et contractuelles.

Note : l'annexe A de la norme ISO27001 contient une liste complète d'objectifs de sécurité et des mesures qui se sont relevés communément appropriés aux organismes. Les utilisateurs de la présente norme internationale doivent se reporter à comme point de départ de sélection de mesure de sécurité afin de s'assurer qu'aucune option importante de sécurité n'est négligée.

h) Obtenir l'approbation par la direction des risques résiduels présentés.
i) Obtenir l'autorisation de la direction pour mettre en œuvre et exploiter le SMSI.
j) Préparer une DdA ;

Une Dda doit être élaborée et inclure les informations suivantes :

1) Les objectifs de sécurité et les mesures de sécurité proprement dites, sélectionnés en **1.g** et les raisons pour lesquelles ils ont été sélectionnés.
2) Les objectifs de sécurité et les mesures de sécurité proprement dites actuellement mis en œuvre.
3) L'exclusion des objectifs de sécurité et des mesures de sécurité non pris en considération.

Note : la Dda fournit un résumé des décisions concernant le traitement du risque. La justification des exclusions prévoit une contre-vérification qui permet d'assurer qu'aucune mesure n'a été omise pas inadvertance.

2.2.2 Mise en œuvre et fonctionnement du SMSI

L'organisme doit effectuer les tâches suivantes :

a) Elaborer un plan de traitement du risque qui identifie les actions à engager, les ressources, les responsabilités et les priorités appropriées pour le management des risques liés à la sécurité de l'information.
b) Mettre en œuvre le plan de traitement du risque pour atteindre les objectifs de sécurité identifiés, ce plan prévoyant le mode de financement et l'affectation des rôles et de responsabilités.
c) Mettre en œuvre les mesures de sécurité sélectionnées en 1g.
d) Définir la méthode d'évaluation de l'efficacité des mesures ou groupes de mesures sélectionnées et spécifier comment ces évaluations doivent être utilisées pour apprécier l'efficacité des mesures.

Note : L'évaluation de l'efficacité des mesures permet aux dirigeants et au personnel de déterminer comment celles-ci permettent pleinement d'atteindre les objectifs de sécurité prévus.

e) Mettre en œuvre des programmes de formation et de sensibilisation.
f) Gérer les opérations du SMSI ;
g) Gérer les ressources consacrées au SMSI
h) Mettre en œuvre les procédures et les autres mesures permettant de détecter rapidement et de répondre tout aussi rapidement aux incidents de sécurité.

2.2.3 Surveillance et réexamen du SMSI

L'organisation doit effectuer les tâches suivantes :

a) Exécuter les procédures de surveillance et de réexamen, ainsi que les autres mesures afin :
    1) De détecter rapidement les erreurs dans les résultats des traitements ;
    2) D'identifier rapidement les failles et les incidents de sécurité ;
    3) De permettre à la direction de déterminer si les activités de sécurité confiées au personnel ou mises en œuvre par les technologies de l'information sont exécutées comme prévu ;
    4) De faciliter la détection des événements de sécurité et par conséquent, de prévenir les incidents de sécurité par l'utilisation d'indicateurs ;
    5) De déterminer si les actions entreprises pour résoudre une faille de sécurité se sont révélées efficaces ;
b) Réaliser des réexamens réguliers de l'efficacité du SMSI (y compris le respect de la politique et des objectifs du SMSI, et le réexamen des mesures de sécurité) en tenant compte des résultats des audits de sécurité, des incidents, des mesures de l'efficacité, des propositions et du retour d'information de toutes les parties intéressées,
c) D'évaluer l'efficacité des mesures afin de vérifier que les exigences de sécurité ont été satisfaites.
d) Réexaminer les appréciations du risque à intervalles planifiés ainsi que le niveau du risque résiduel et le niveau acceptable identifié, compte tenu des changements apportés :
    1) A l'organisme.
    2) A la technologie.
    3) Aux objectifs métiers et aux processus de l'organisme.
    4) Aux menaces identifiées.
    5) Aux événements extérieurs, tels que les modifications apportées à la législation ou à la réglementation, aux obligations contractuelles et au climat social.
e) Mener des audits internes du SMSI à intervalles fixés.

    Remarque : les audits internes, parfois appelés audits première partie, sont menés par ou pour le compte de l'organisme lui-même à des fins internes.
f) Effectuer une revue de direction du SMSI de manière régulière afin de s'assurer du caractère toujours adéquat du domaine d'application du système et de l'identification des améliorations apportées au processus d'application du SMSI.

g) Mettre à jour les plans de sécurité afin de tenir compte des résultats des activités de surveillance et de réexamen.
h) Consigner les actions et les événements qui pourraient avoir un impact sur l'efficacité ou les performances du SMSI.

2.2.4 Mise à jour et amélioration du SMSI

L'organisme doit effectuer les tâches suivantes de manière régulière :

a) Mettre en œuvre les améliorations identifiées du SMSI
b) Entreprendre les actions correctives et préventives appropriées et appliquer les enseignements tirés des expériences de sécurité des autres organismes, ainsi que celles de l'organisme concerné.
c) Informer toutes les parties prenantes des actions d'amélioration avec un niveau de détail approprié aux circonstances et le cas échéant convenir de la méthode à adopter.
d) S'assurer que les améliorations permettent d'atteindre leurs objectifs prévus.

2.3 Exigences relatives à la documentation

2.3.1 Généralités :

La documentation doit inclure les enregistrements des décisions de gestion et assurer que les actions entreprises sont identifiables grâce aux décisions et aux politiques de la direction et que les résultats consignés sont reproductibles.

Il est important de pouvoir démontrer la relation entre les mesures sélectionnées et les résultats du processus d'application du risque et de traitement du risque et par conséquent la politique et les objectifs du SMSI.

La documentation du SMSI doit inclure :

a) Les déclarations documentées de la politique et des objectifs du SMSI
b) Le domaine d'application du SMSI
c) Les procédures et les contrôles pour le SMSI.
d) Une description de la méthodologie d'appréciation du risque
e) Le rapport d'appréciation du risque.
f) Le plan de traitement du risque.

g) Les procédures documentées dont a besoin l'organisme pour s'assurer de la planification du fonctionnement et du contrôle effectif de ses processus de sécurité de l'information et pour spécifier comment évaluer l'efficacité des mesures appliquées.
h) Les enregistrements exigés par la présente norme internationale
i) La Dda

Remarque 1 : le terme « procédure documentée » signifie que la procédure est établie, documentée, appliquée et mise à jour.

Remarque 2 : l'étendue de la documentation du SMSI peut différer d'un organisme à l'autre en raison :

- De la taille de l'organisme et du type de ses activités.
- De la portée et de la complexité des exigences de sécurité, ainsi que du domaine d'application et de la complexité du système effectivement géré.

Remarque 3 : les documents et les enregistrements peuvent se présenter sous toute forme ou tout type de support.

2.3.2 maitrise des documents :

Les documents requis pour le SMSI doivent être protégés et maitrisés. Une procédure documentée doit être établie pour définir les actions nécessaires pour :

a) Approuver l'adéquation des documents avant diffusion.
b) Réexaminer, mettre à jour si nécessaire et approuver de nouveaux documents.
c) Assurer que les modifications et le statut de la version en vigueur des documents sont identifiés.
d) Assurer la disponibilité sur le lieu d'utilisation des versions pertinentes des documents applicables.
e) Assurer que les documents restent lisibles et facilement identifiables.
f) Assurer la mise à disposition des documents aux personnes qui en ont besoin, ainsi que le transfert, le stockage et l'élimination finale desdits documents conformément aux procédures applicables à leur classification.
g) Assurer que les documents d'origine extérieure sont identifiés.
h) Assurer que la diffusion des documents est maitrisée.

i) Empêcher toute utilisation non intentionnelle de documents périmés.

j) Identifier les documents de manière adéquate s'ils sont conservés dans un but quelconque.

2.3.3 Maitrise des enregistrements

Les enregistrements doivent être établis et conservés pour apporter la preuve de la conformité aux exigences et du fonctionnement efficace du SMSI. Ils doivent être protégés et maitrisés. Le SMSI doit tenir compte des dispositions légales et réglementaires et des obligations contractuelles. Les enregistrements doivent être documentés et mis en œuvre.

Les enregistrements des performances du processus ainsi que de toutes les occurrences des incidents de sécurité importants relatifs au SMSI, doivent être conservés.

Exemple : le registre des visiteurs, les rapports d'audit et les formulaires complétés d'autorisation d'accès constituent des exemples d'enregistrement.

2.4 Responsabilité de la direction

2.4.1 Implication de la direction

La direction doit fournir la preuve de son implication dans l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI, par:

a) l'établissement d'une politique relative au SMSI;

b) l'assurance que des objectifs et des plans pour le SMSI sont établis;

c) la définition de rôles et de responsabilités pour la sécurité de l'information;

d) la sensibilisation de l'organisme à l'importance de satisfaire aux exigences relatives à la sécurité de l'information et de respecter la politique établie en la matière, à ses responsabilités au titre de la loi et à la nécessité d'une amélioration continue;

e) la fourniture de ressources suffisantes pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI.

f) la détermination des critères d'acceptation des risques et des niveaux de risque acceptables.

g) l'assurance que des audits internes du SMSI sont menés.

h) la réalisation de revues de direction du SMSI.

2.4.2 Management des ressources

2.4.2.1 Mise à disposition des ressources

L'organisme doit déterminer et fournir les ressources nécessaires pour:

a) Etablir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI.

b) Assurer que les procédures de sécurité de l'information soutiennent les exigences métier.

c) Identifier et exécuter les dispositions légales et réglementaires, ainsi que les obligations de sécurité contractuelles.

d) maintenir une sécurité adéquate par une application correcte de toutes les mesures mises en œuvre.

e) effectuer des réexamens si nécessaire et réagir de manière appropriée à leurs résultats.

f) améliorer, le cas échéant, l'efficacité du SMSI.

2.4.2.2 Formation, sensibilisation et compétence

L'organisme doit s'assurer que le personnel à qui a été affecté les responsabilités définies dans le SMSI, a les compétences nécessaires pour exécuter les tâches requises, en:

a) Déterminant les compétences nécessaires pour le personnel effectuant un travail ayant une incidence sur le SMSI.

b) Fournissant la formation ou en entreprenant d'autres actions (par exemple emploi d'un personnel compétent pour satisfaire ces besoins).

c) Evaluant l'efficacité des actions entreprises.

d) conservant les enregistrements concernant la formation initiale et professionnelle, le savoir-faire, l'expérience et les qualifications.

L'organisme doit également s'assurer que tout le personnel approprié a conscience de la pertinence et de l'importance de ses activités liées à la sécurité de l'information et de la façon dont ces dernières contribuent à l'atteinte des objectifs du SMSI.

2.5 Audits internes du SMSI

L'organisme doit mener des audits internes du SMSI à intervalles planifiés pour déterminer si les objectifs de sécurité, les mesures, les processus et les procédures de son SMSI sont:

a) Conformes aux dispositions de la présente norme internationale et à la législation et aux règlements.

b) Conformes aux exigences de sécurité de l'information identifiées.

c) Mis en œuvre et tenus à jour de manière efficace.

d) Exécutés tels que prévus.

Un programme d'audit doit être planifié en tenant compte de l'état et de l'importance des processus et des domaines à auditer, ainsi que des résultats des audits précédents. Les critères, le champ, la fréquence et les méthodes d'audit doivent être définis.

Le choix des auditeurs et la réalisation des audits doivent assurer l'objectivité et l'impartialité du processus d'audit. Les auditeurs ne doivent pas auditer leur propre travail.

Les responsabilités et les exigences pour planifier, mener les audits, rendre compte des résultats et conserver des enregistrements doivent être définies dans une procédure documentée.

L'encadrement responsable du domaine audité doit assurer que des actions sont entreprises dans le strict respect des délais impartis pour éliminer les non-conformités détectées et leurs causes.

Les activités de suivi doivent inclure la vérification des actions entreprises et le compte-rendu des résultats de cette vérification.

2.6 Revue de direction du SMSI

2.6.1 Généralités

La direction doit, à intervalles planifiés (au moins une fois par an), procéder au réexamen du SMSI de l'organisme pour s'assurer qu'il demeure pertinent, adéquat et efficace.

Ce réexamen doit comprendre l'évaluation des opportunités d'amélioration et du besoin de modifier le SMSI, y compris la politique et les objectifs de sécurité de l'information. Les résultats des réexamens doivent être clairement documentés et les enregistrements doivent être conservés.

2.6.2 Éléments d'entrée du réexamen

Les éléments d'entrée d'une revue de direction doivent comprendre des informations sur:

a) les résultats des audits et des réexamens du SMSI.

b) les retours d'information des parties intéressées.

c) les techniques, produits ou procédures que pourrait utiliser l'organisme pour améliorer les performances et l'efficacité du SMSI.

d) l'état des actions préventives et correctives.

e) les vulnérabilités ou les menaces qui n'ont pas été traitées de manière adéquate dans l'appréciation du risque précédente.

f) les résultats des mesures de l'efficacité.

g) les actions de suivi issues des revues de direction précédentes;

h) les changements pouvant affecter le SMSI;

i) les recommandations d'amélioration.

2.6.3 Éléments de sortie du réexamen

Les éléments de sortie de la revue de direction doivent comporter les décisions et actions relatives aux informations suivantes:

a) l'amélioration de l'efficacité du SMSI;

b) la mise à jour du plan d'appréciation du risque et de traitement du risque;

c) la modification des procédures et mesures qui affectent la sécurité de l'information, si nécessaire, pour répondre aux événements intérieurs ou extérieurs qui peuvent exercer une influence sur le SMSI, y compris les modifications en matière:

1) des exigences métier;

2) des exigences de sécurité;

3) des processus métier affectant les exigences métier existantes;

4) des dispositions légales ou réglementaires;

5) des obligations contractuelles;

6) des niveaux de risque et/ou des critères d'acceptation des risques.

d) des besoins en ressources;

e) d'amélioration de la méthode d'évaluation de l'efficacité des mesures.

2.7 Amélioration du SMSI

2.7.1 Amélioration continue

L'organisme doit améliorer en permanence l'efficacité du SMSI en utilisant la politique en matière de sécurité de l'information, la réalisation des objectifs en termes de sécurité de l'information, les résultats d'audit, l'analyse des événements surveillés, les actions correctives et préventives et la revue de direction.

2.7.2 Action corrective

L'organisme doit mener des actions pour éliminer les causes de non-conformité avec les exigences du SMSI, afin d'éviter qu'elles ne se reproduisent. La procédure documentée pour l'action corrective doit définir les exigences relatives à:

a) l'identification des non-conformités.

b) la détermination des causes des non-conformités.

c) l'évaluation du besoin d'entreprendre des actions pour que les non-conformités ne se reproduisent pas.

d) la détermination et la mise en œuvre de l'action corrective requise.

e) la consignation des résultats de l'action entreprise.

f) le réexamen de l'action corrective entreprise.

2.7.3 Action préventive

L'organisme doit déterminer l'action permettant d'éliminer la cause des non-conformités potentielles avec les exigences du SMSI, afin d'éviter qu'elles ne surviennent. Les actions préventives doivent être adaptées aux effets des problèmes potentiels. La procédure documentée pour l'action préventive doit définir les exigences relatives à:

a) l'identification des non-conformités potentielles et de leurs causes.

b) l'évaluation du besoin d'entreprendre des actions pour éviter l'apparition de non-conformités.

c) la détermination et la mise en œuvre de l'action préventive requise.

d) la consignation des résultats de l'action entreprise.

e) le réexamen de l'action préventive entreprise.

L'organisme doit identifier les risques modifiés et les exigences relatives aux actions préventives, en concentrant son attention sur les risques soumis à une modification importante.

La priorité des actions préventives doit être déterminée sur la base des résultats de l'appréciation du risque.

Remarque **:** L'action visant à prévenir les non-conformités est souvent plus rentable que l'action corrective.

3. **Les organes de normalisation et les normes**

3.1 Les organes

3.1.1 L’organisation internationale de normalisation (ISO)

L'ISO est un **réseau** d'instituts nationaux de normalisation de **162 pays**, selon le principe d'un membre par pays, dont le Secrétariat, situé à Genève (Suisse), qui assure la coordination d'ensemble. L'ISO est une **organisation non gouvernementale** qui jette un pont entre le secteur public et le secteur privé. Bon nombre de ses instituts membres font en effet partie de la structure gouvernementale de leur pays ou sont mandatés par leur gouvernement, d'autres organismes membres sont issus exclusivement du secteur privé et ont été établis par des partenariats d'associations industrielles au niveau national. L'ISO permet ainsi d'établir un **consensus** sur des solutions répondant aux exigences du monde économique et aux **besoins plus généraux de la société.**

3.1.2 L'Institut Algérien de Normalisation (IANOR)

Etablissement public à caractère industriel et commercial (EPIC) sous tutelle du Ministère de l'Industrie et de la promotion des investissements, il a été créé dans le cadre de la restructuration de l'INAPI (Institut Algérien de Normalisation et de Propriété Industriel) par Décret Exécutif n° 98-69 du 21 Février 1998

- Il est chargé de :
  1. l'élaboration, la publication et la diffusion des normes algériennes.
  2. la centralisation et la coordination de l'ensemble des travaux de normalisation entrepris par les structures existantes et celles qui seront créées à cet effet
  3. l'adoption de marques de conformité aux normes algériennes et de labels de qualité ainsi que la délivrance d'autorisation de l'utilisation de ces marques et le contrôle de leur usage dans le cadre de la législation en vigueur.
  4. la certification obligatoire des produits.
  5. la promotion de travaux, recherches, essais en Algérie ou à l'étranger ainsi que l'aménagement d'installations d'essais nécessaires à l'établissement de normes et à la garantie de leur mise en application.
  6. la constitution, la conservation et la mise à la disposition de toute documentation ou information relative à la normalisation.
  7. l'application des conventions et accords internationaux dans les domaines de la normalisation auxquels l'Algérie est partie prenante.
  8. assure le secrétariat du Conseil National de la Normalisation (CNN) et des Comités Techniques Nationaux de Normalisation.

En date du 20 mai 2008, l'IANOR adopte la norme **NA ISO/CEI 27001** comme norme algérienne par le comité technique national N° **01** : «**Normes fondamentales** ».

3.2 Les normes ISO

L'ISO a élaboré plus de 18 500 Normes internationales sur des sujets très variés et quelque 1100 nouvelles normes ISO sont publiées chaque année. Le tableau ci-dessous en donne un bref aperçu.

Norme	Domaine
1 Normes ISO : 1 - 999 /	Langues et caractères
2 Normes ISO : 1000 - 8999 /	Codes et langages
3 Normes ISO : 9000 - 9099 /	Qualité
4 Normes ISO : 9100 - 9999 /	Exigences logiciels, codage, langage (suite)
5 Normes ISO : 10000 - 13999	Divers
6 Normes ISO : 14000 /	Environnement
7 Normes ISO : 14400 - 15999	Divers
8 Normes ISO : 16949	Divers
9 Normes ISO : 19100 /	Information géographique
10 Normes ISO : 19200 - 20000	Divers
11 Normes ISO : 22000 /	Systèmes de management de la sécurité des denrées alimentaires
12 Normes ISO : 26000 - 26999	Divers
13 Normes ISO : 27000 /	Sécurité de l'information

Tableau 3 Les normes ISO

Les normes ISO permettent de:

- Développer, fabriquer et fournir des produits et services plus efficaces, plus sûrs et plus propres
- Faciliter le commerce entre les pays.
- Fournir aux gouvernements une base technique pour la santé, la sécurité et la législation relative à l'environnement, ainsi que l'évaluation de la conformité.
- Assurer le partage des avancées technologiques et des bonnes pratiques de gestion.
- Contribuer à diffuser l'innovation
- Protéger les consommateurs et les utilisateurs en général de produits et service.

La norme ISO 27001 est la norme qui traite de la sécurité de l'information nous développons dans ce qui suit sa structure.

3.2.1 Structure de la norme ISO27001

La norme ISO 27001 est disponible sur le site de l'ISO et sur celui de différents organismes de certification nationaux (AFNOR, BSI, etc.). Cette norme est structurée en huit chapitres dont les trois premiers rappellent des notions de base et ne précisent aucune exigence particulière mais présentent très clairement les objectifs de la norme ainsi que ses apports.

Ce n'est qu'à partir du chapitre 4 que les exigences commencent vraiment à être spécifiées, il constitue le noyau dur de la norme et est articulé autour du modèle Plan, Do, Check, Act. (PDCA)

Quatre chapitres satellites viennent le compléter.

Chapitre 5 : développe tout ce qui possède un rapport avec les responsabilités du management.

Chapitre 6 : précise tout ce qui concerne les actions de l'audit interne.

Chapitre 7 : développe les aspects relatifs aux revues des différents éléments du SMSI.

Chapitre 8 : définit clairement les notions d'action corrective et préventive.

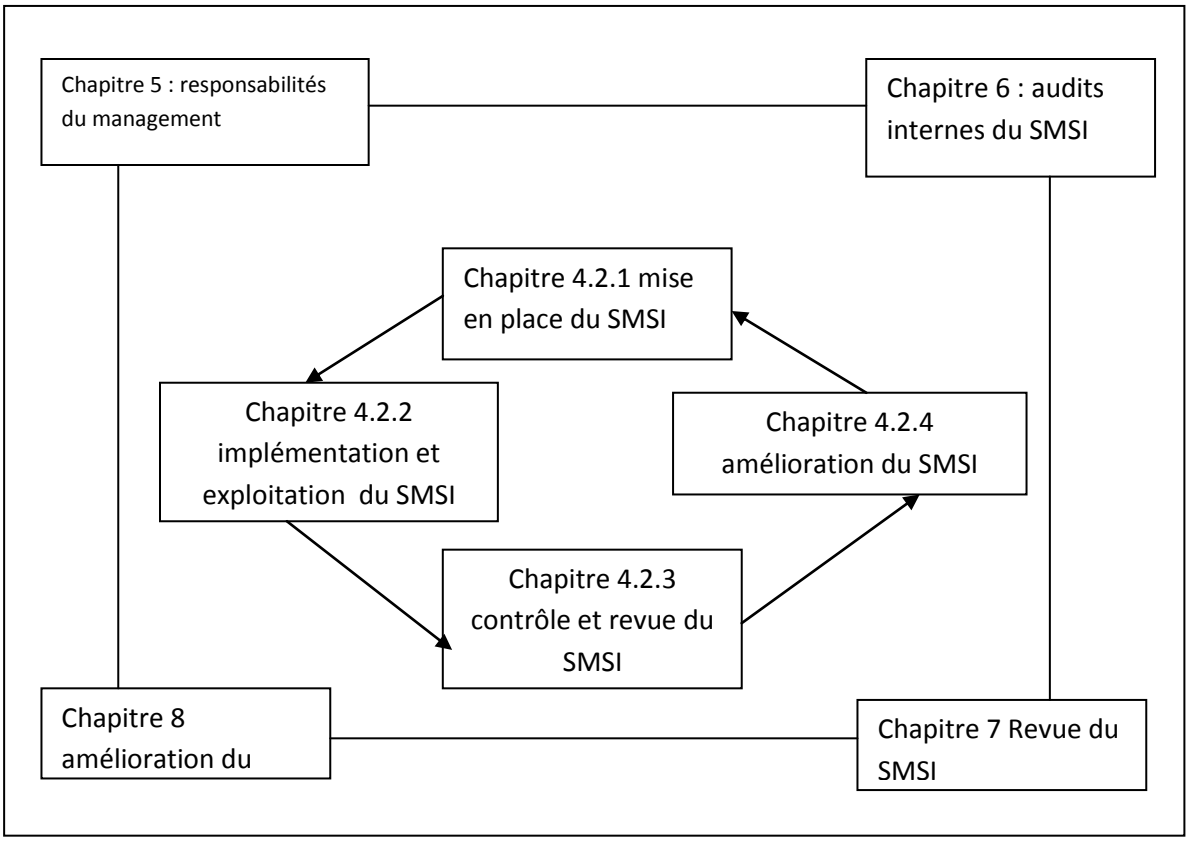


Figure 13 Les chapitres de la norme ISO27001

Trois annexes clôturent le document, dont la première (Annexe A) occupe l'essentiel de la norme en volume. Elle spécifie les domaines d'interventions, les objectifs et 133 mesures de sécurité.

L'ISO 27002 reprend sans exception les 133 mesures dé sécurité, à chaque mesure elle propose une série de préconisations concrètes, abordant des aspects tant techniques qu'organisationnels.

3.2.2 Structure de la norme ISO27002

La norme ISO 27002 est structurée sur 3 niveaux :

- Niveau 1 : les chapitres.
- Niveau 2 : les objectifs de sécurité.
- Niveau 3 : les mesures de sécurité.

Cette norme comporte quinze chapitres, les quatre premiers chapitres décrivent des généralités et rappellent quelques notions de base. Cette norme peut être vue comme un dictionnaire comportant 133 entrées, chacune de ces entrées décrit une mesure de sécurité.

Chaque mesure de sécurité est décrite en quatre parties :

1. Numéro de référence et intitulé de la mesure : ceci permet de référencer la mesure sans la moindre équivoque.
2. Mesure : brève description de la mesure.
3. Préconisation de mise en œuvre : ils sont développées et éventuellement d'exemple pour les illustrer
4. Informations supplémentaires : précisions jugées utiles, mais non abordées dans les préconisations.

Les autres chapitres au nombre de onze, (du 5 au 15) couvrent l'essentiel des domaines relatifs à la sécurité de l'information. La liste ci-dessous présente sommairement chacun de ces chapitres ainsi que les objectifs (sous chapitre) qui les composent.

Chapitre 5 : Politique de sécurité

Toutes les questions concernant l'élaboration de la politique de sécurité sont couvertes dans ce chapitre, il ne comporte que deux mesures de sécurité.

Chapitre 6 : Organisation de la sécurité de l'information

Ce chapitre est divisé en deux « objectifs » bien distincts : tout d'abord les questions relatives à l'organisation interne à l'entreprise, puis celles concernant les tiers.

- Organisation interne : les mesures de sécurité décrites abordent essentiellement la gouvernance de la sécurité, les relations avec les autorités ainsi que la participation aux

groupes spécialisés (forums professionnels permettant de partager l'expérience en matière de sécurité de l'information)

- Relation avec les tiers : le fait de traiter avec les tiers expose l'organisme à un certain nombre de risques que l'entreprise doit identifier et contre lesquels elle doit se protéger. C'est le but des mesures de sécurité présentées dans cette partie (6.2). l'accent est mis sur les accords passés avec les tiers, qui doivent tenir compte des exigences de sécurité.

Chapitre 7 : Gestion des biens

Les mesures de sécurité de ce chapitre sont indispensables à l'application de la clause 4.2.1.d.1 de l'ISO 27001, qui spécifie que l'organisme doit procéder à un inventaire des actifs et désigner, pour chacun d'eux, un responsable.

- Responsabilité relatives aux biens : cette partie (7.1) couvre l'inventaire, la propriété et la définition de l'utilisation correcte des biens.
- Classification des informations : les mesures de la partie 7.2 concernent la classification des actifs, opération qui se révèlera très utile lors de leur valorisation dans le cadre de l'appréciation des risques.

Chapitre 8 : Sécurité liée aux ressources humaines

Ce chapitre aborde toutes les questions relatives au personnel. Il est composé de trois « objectifs » à mettre en place chronologiquement : avant l'embauche, puis pendant la durée du contrat, et enfin au départ de l'employé.

Chapitre 9 : Sécurité physique et environnementale

La sécurité physique s'applique essentiellement aux locaux et aux équipements qui s'y trouvent :

- Sécurité des locaux.
- Sécurité du matériel

Chapitre 10 : Gestion de l'exploitation et des télécommunications

Le chapitre 10 est l'un des plus importants de l'ISO 27002. Il comporte de très nombreuses mesures de sécurité, à la fois techniques et organisationnelles, et couvrantes tous les aspects de l'exploitation du système d'information.

Chapitre 11 : contrôle d'accès

Toutes les mesures se rapportant au contrôle d'accès sont réunies dans ce chapitre hormis le contrôle d'accès physique, déjà traité dans le chapitre 9.

Chapitre 12 : acquisition, développement et maintenance des systèmes d'information

Ce chapitre regroupe toutes les mesures de sécurité relatives au développement et à la maintenance des plates-formes et des applications.

Chapitre 13 : gestion des incidents liés à la sécurité de l'information

La gestion des incidents fait l'objet de deux « objectifs » :

Chapitre 14 : gestion du plan de continuité de l'activité

Ce chapitre, composé de cinq mesures de sécurité, couvre tous les aspects relatifs aux plans de continuité d'activité (PCA), depuis l'analyse d'impact jusqu'aux tests et aux revues du PCA.

Chapitre 15 : conformité

Le dernier chapitre aborde toutes les questions relatives à la conformité avec la réglementation et avec les procédures internes de l'entreprise. Il traite aussi des audits.

Les chapitres de la norme peuvent être représentés sur une pyramide organisationnelle :

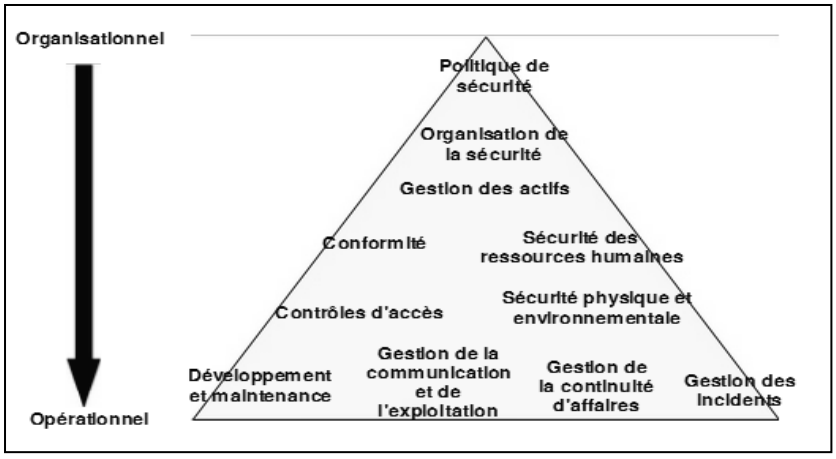


Figure 14 disposition organisationnelle des chapitres

3.3 Comparaison des deux normes :

Les différences entre les deux normes

Les deux référentiels présentent quelques différences, tant sur la forme que sur le fond.

- Sur la forme :

  S'agissant du volume tout d'abord, la norme ISO 27001 ne présente qu'une trentaine de pages. Les exigences ne commencent qu'au chapitre 4 pour se terminer au chapitre 8, c'est-à-dire dix pages plus loin. Le reste du document est constitué d'annexes. De son côté, la norme ISO 27002 comporte plus de 110 pages et la partie utile débute dès le chapitre 5 et mène jusqu'à la fin du document.

- Sur le fond :

Concernant les thèmes abordés, les deux normes présentent également de grandes différences, puisque l'ISO 27001 se focalise exclusivement sur les exigences nécessaires à la mise en place d'un SMSI, alors que l'ISO 27002 couvre un spectre bien plus large, comprenant des domaines aussi variés que la politique, l'organisation, les systèmes et réseaux, la sécurité physique, etc.

L'aspect commun entre les deux normes

Nous relevons un seul point commun l'annexe A de l'ISO 27001 reprend sans exception chacun des 133 titres de mesures de sécurité développées dans l'ISO 27002, ainsi que leur numérotation. L'annexe A constituerait ainsi une sorte de lien entre ces deux normes.

Le tableau ci-après récapitule les principales différences entre les deux référentiels :

ISO 27001	ISO 27002
Traite des systèmes de management	Ne traite pas des systèmes de management Traite en détail des mesures (Best practices)
Modèle PDCA	Pas de modèle PDCA
Usage du verbe SHALL	Usage du verbe SHOULD
Application des clauses 4 à 8 obligatoire	Aucune obligation
Possibilité de certification	Pas de certification possible

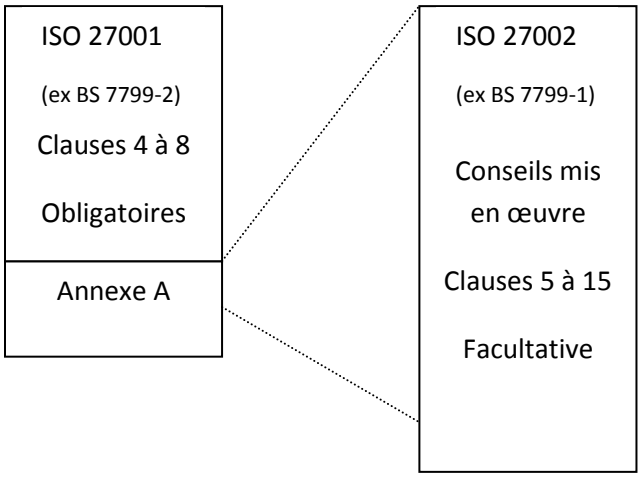


Figure 16 La relation entre la norme ISO27001 et la norme ISO27002

Chapitre IV

Outil d’audit de sécurité

Introduction

L'outil d'audit de sécurité que nous proposons a pour objectif de vérifier la conformité d'une entreprise donnée par rapport à la norme ISO27001. Nous avons donc d'une part les données de l'entreprise que nous lions à un « profil d'entreprise » et d'autre part les règles déduites à partir de la norme. Cet outil comportant deux modules est destiné à l'auditeur et à l'expert dont les rôles sont décrits ci-dessous :

- L'auditeur est celui qui utilise l'outil pour établir un rapport d'audit pour une entreprise donnée.
- L'expert est chargé de constituer la base des règles déduites à partir de la norme. Il peut également modifier une mesure de sécurité.

1 Module Expert

Le module expert comporte plusieurs bases de données :

1 **Une base de données profils auditeurs :** à travers laquelle l'expert gère la base de données des droits d'accès des auditeurs, il peut donc.

- Ajouter un nouveau profil auditeur
- Modifier un profil auditeur
- Supprimer un profil auditeur

2 **Une base de données questionnaire :**

L'étude des règles de la norme permet de dégager un ensemble de questionnaires. Chaque questionnaire est associé à un chapitre de la norme. Chaque chapitre a plusieurs objectifs, chaque objectif a plusieurs thèmes sur lesquels nous devons intervenir ; et enfin chaque thème a des mesures.

Exemple d'une question :

Chapitre 2 : Organisation de la sécurité de l'information (Deuxième chapitre de la norme ISO27001)
Objectif : Il convient d'établir un cadre de gestion pour initialiser, puis contrôler la mise en œuvre de la sécurité de l'information au sein de l'organisme.
Thèmes : Engagement de la direction vis-à-vis de la sécurité de l'information
Question : La direction soutient-t-elle activement la politique de sécurité au sein de l'organisme ?
Réponses proposées : « Oui » ou « Non »

Des associations de type père/fils existent entre les tables, cardinalité maximum à n d'un côté et à cardinalité 1 de l'autre. On indique les attributs clefs de l'entité père (côté (.,n)) et de l'entité fils (côté (.,1))

Exemple :

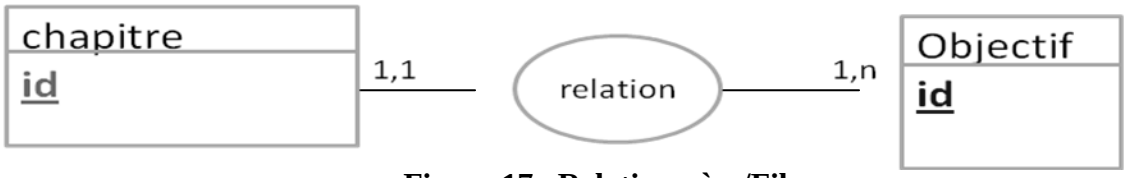


Figure 17 Relation père/Fils

L'ensemble de ces relations définit le modèle relationnel suivant :

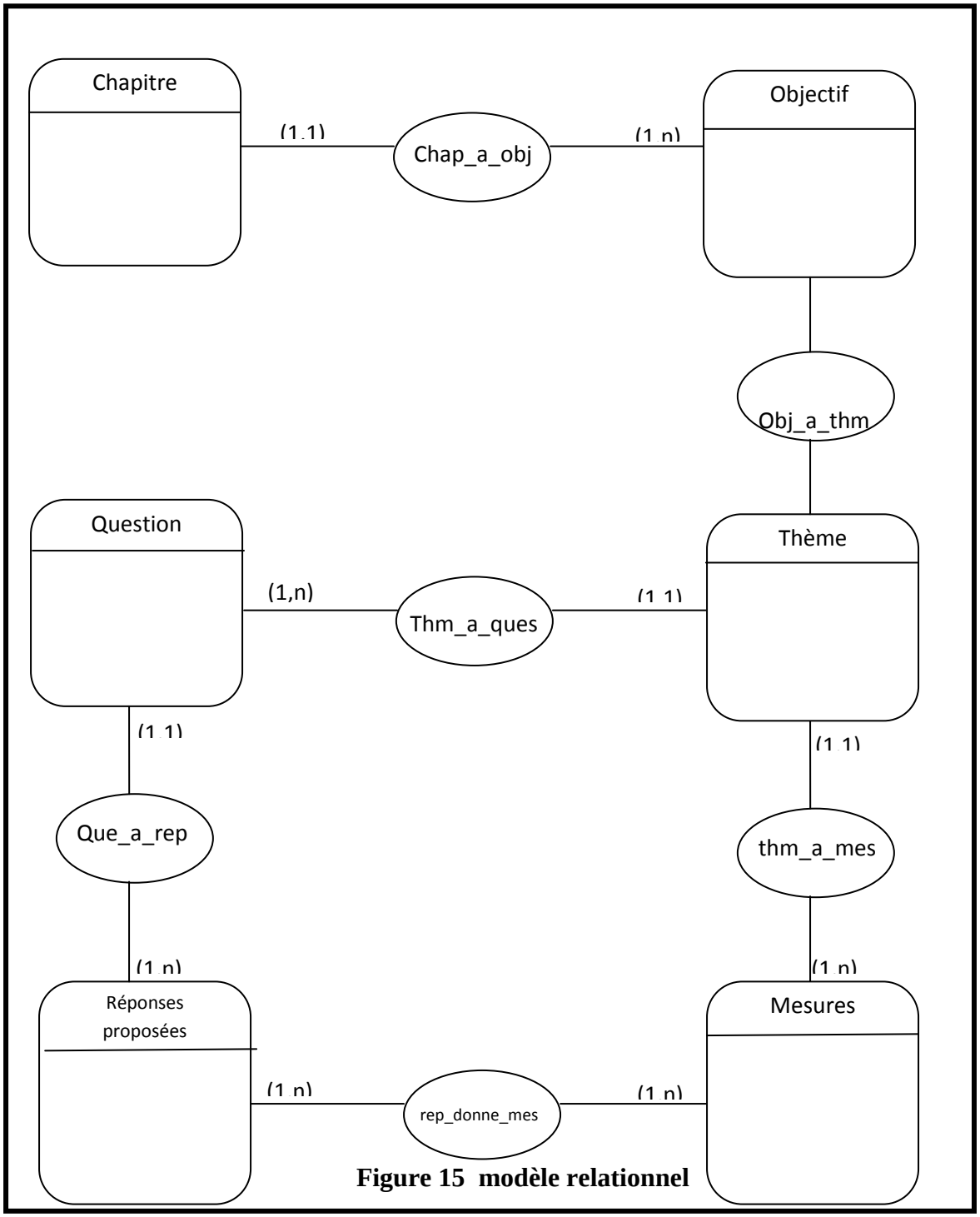


Figure 15 modèle relationnel

L'expert peut donc :

- Ajouter un nouvel objectif, thème, question, et réponse proposée à une question donnée.
- Modifier un objectif, thème, question, et réponse proposée à une question donnée.
- Supprime un objectif, thème, question, et réponse proposée à une question donnée.
- Implémenter également la relation question/réponses proposées.

3 **Une base de données des mesures :** Elle contient l'ensemble des mesures issues de la norme ISO27002. où il peut insérer, modifier ou supprimer des instances.

Chaque mesure contient un intitulé, des préconisations de mise en œuvre ; certaines mesures contiennent un paragraphe 'informations supplémentaires' qui renvoie généralement vers un référentiel.

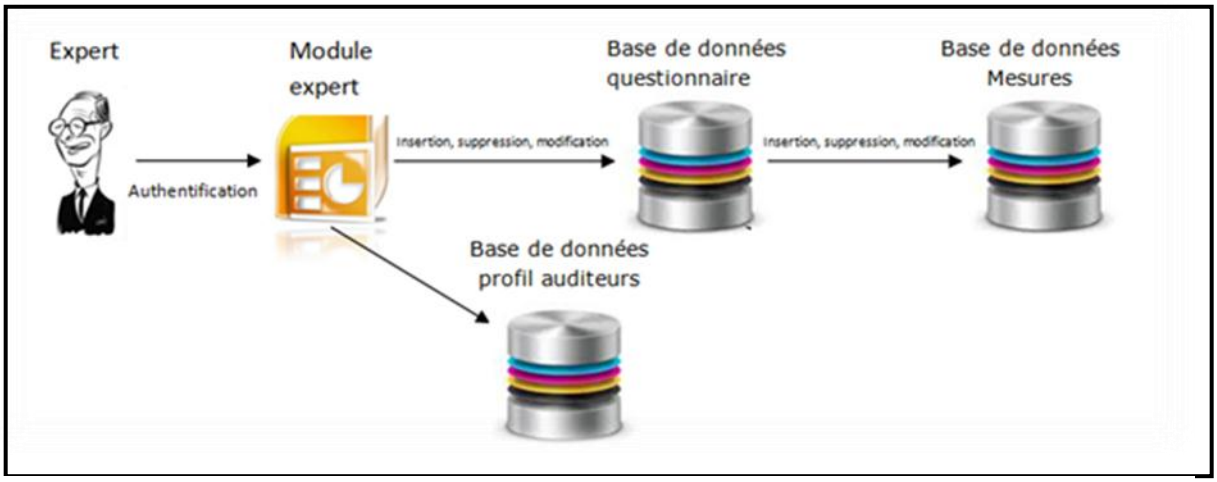


Figure 19 Le module Expert

2.2 Module Auditeur

Le module auditeur gère également plusieurs bases de données:

- **Base de données des entreprises** (à auditer) ; Il gère à travers cette base les profils d'entreprise à auditer ; il peut donc créer un nouveau profil, en modifier un existant ou en supprimer un.
- **Base de données réponses :** dans le déroulement de l'audit, la base de données réponses est implémentée, ces réponses correspondent à un profil d'entreprise donnée; elle peut être revue par la suite par l'auditeur. à travers un accès appelé 'mes audits' dans le programme informatique développé.

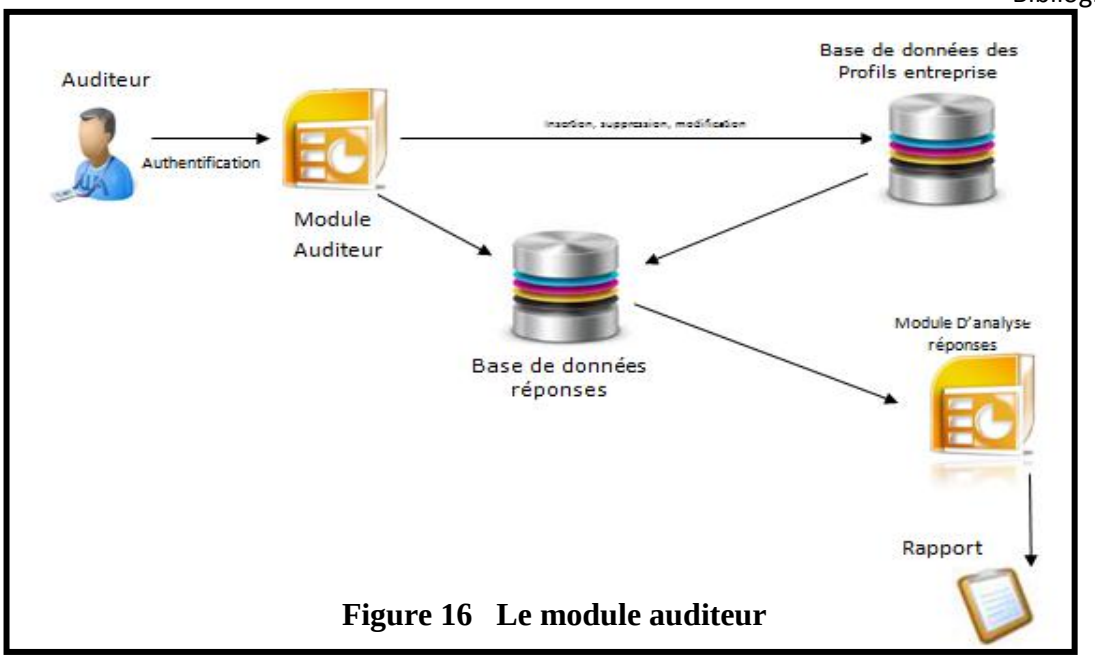


Figure 16 Le module auditeur

Le module d'analyse réponses inclus dans le module auditeur permet de traiter les réponses d'un audit et de générer un rapport, ce rapport pourra par la suite être imprimé ou enregistré sur le disque dur.

Les deux modules expert et auditeur sont reliés entre eux, comme le décrit le schéma ci-dessous.

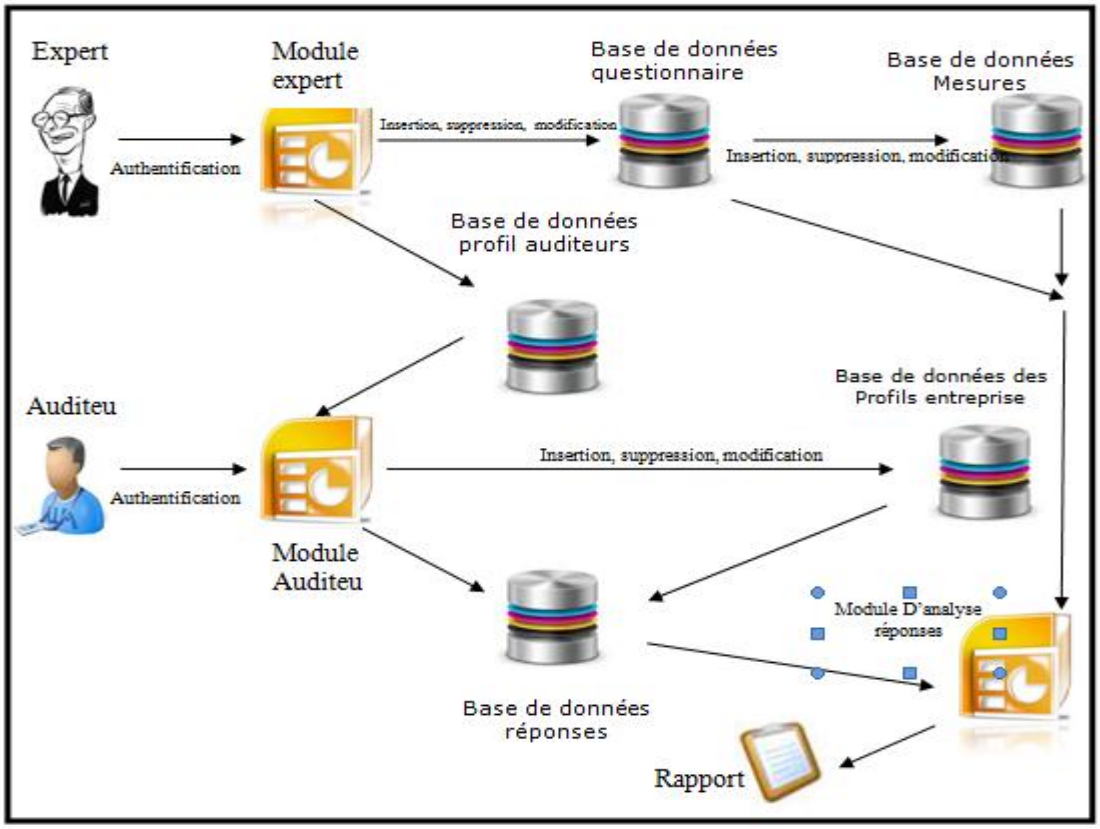


Figure 17 Relation entre le module auditeur et le module

3. l'outil automatique d'audit et son fonctionnement :

Dans ce qui suit, nous présentons l'interface d'accueil de l'outil automatique d'audit développé au cours de notre travail (menu démarrage du programme).

Figure 18 Menu de démarrage

Liste des différents boutons :

1. Connexion auditeur.
2. Nouveau profil (entreprise).
3. Lancer un nouvel audit.
4. Modifier un compte.
5. Gérer les audits.

Module auditeur

6. Comptes auditeurs.
7. Modifier l'audit.
8. Accéder aux comptes.
9. Connexion expert.

Module Expert

10. Menu flash.

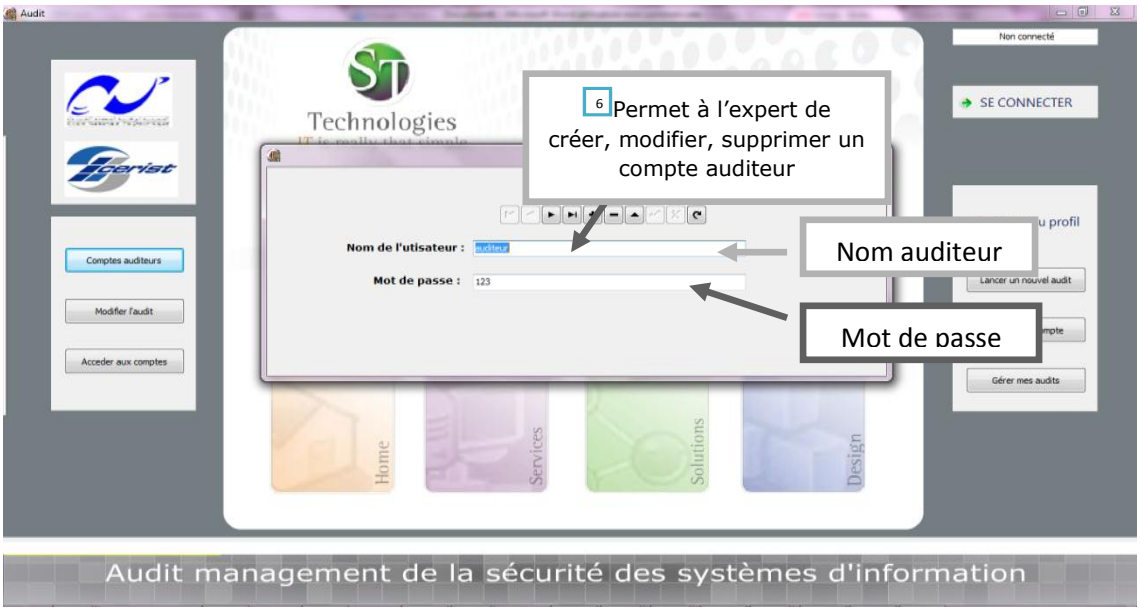


Figure 24 : Connexion auditeur

L'expert doit gérer la base de données et créer si nécessaire de nouvelles questions ; pour cela on clique sur 7 le menu suivant s'affiche.

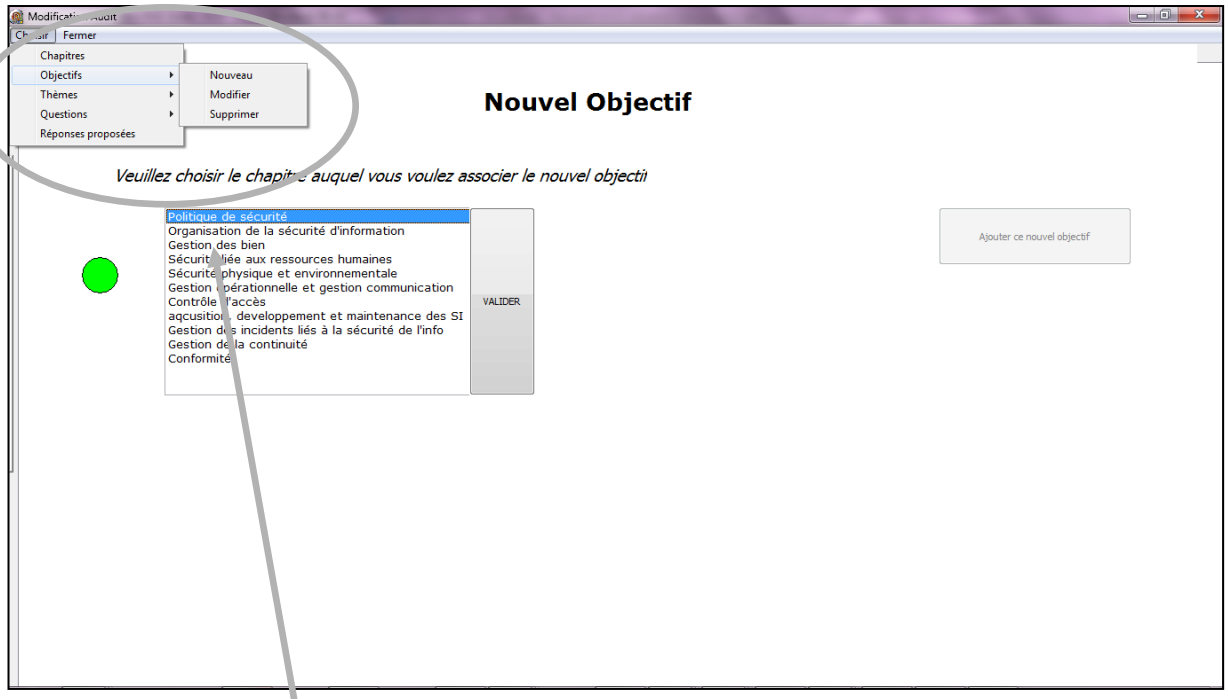


Figure 19 modification audit

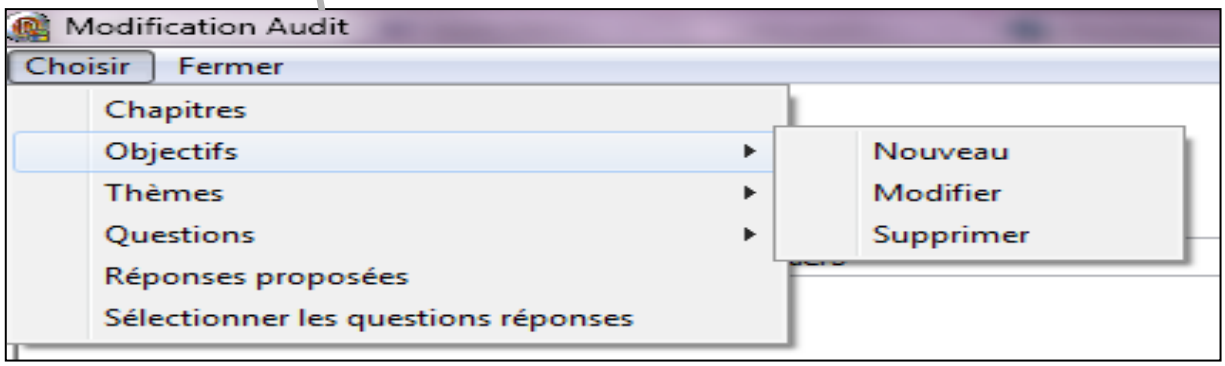


Figure 20 Menu modification audit

En choisissant la création d'un nouvel objectif le menu ci-dessous s'affiche.

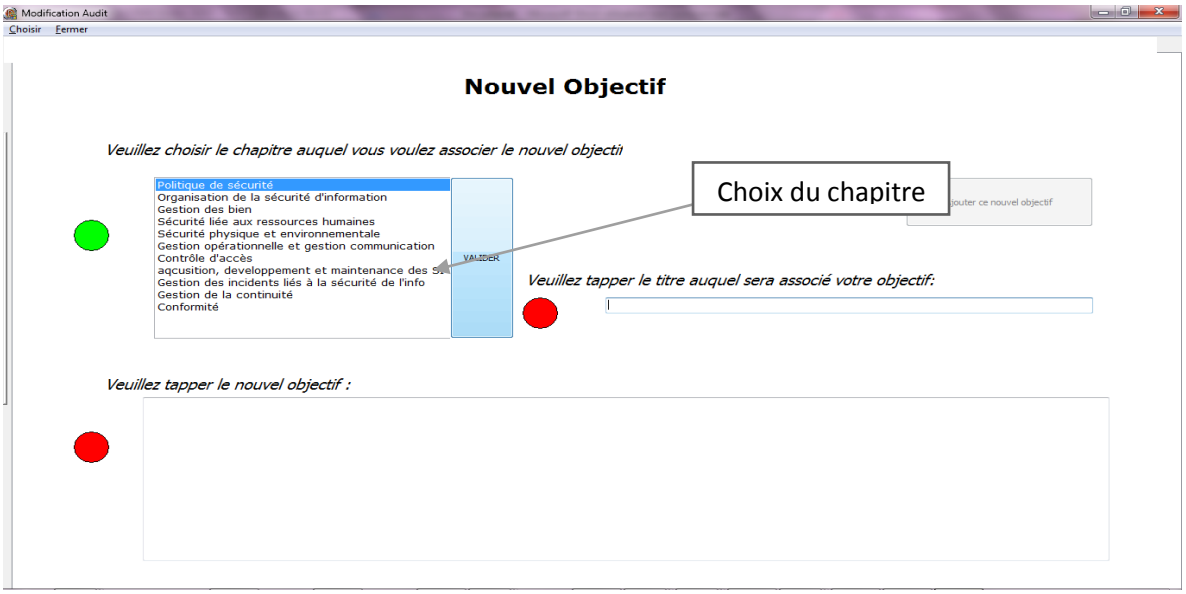


Figure 21 nouvel objectif

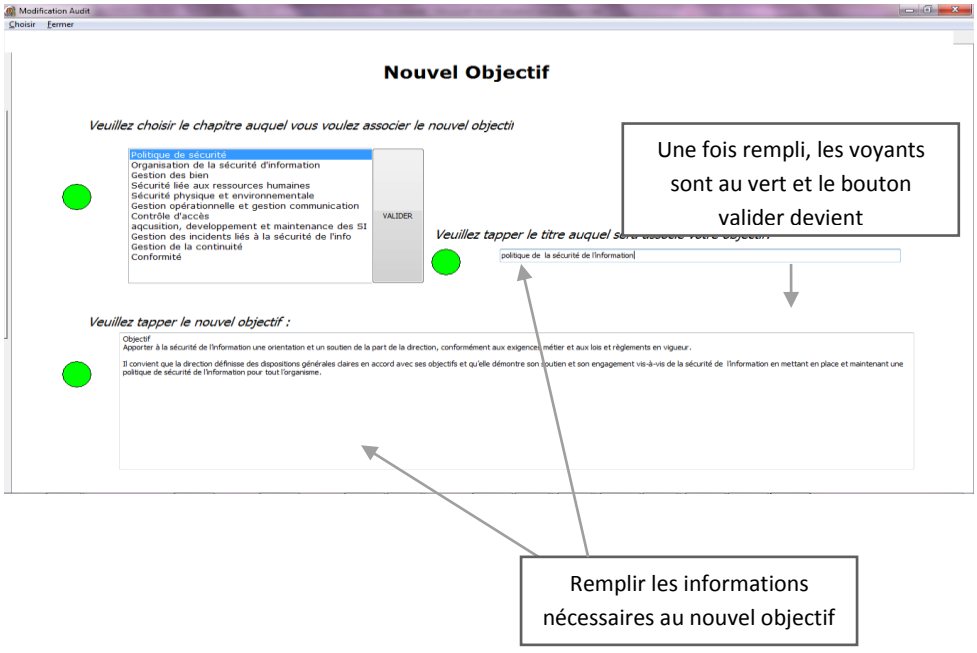


Figure 22 nouvel objectif (2)

Après avoir été créé ; un objectif peut être modifié ou supprimé.

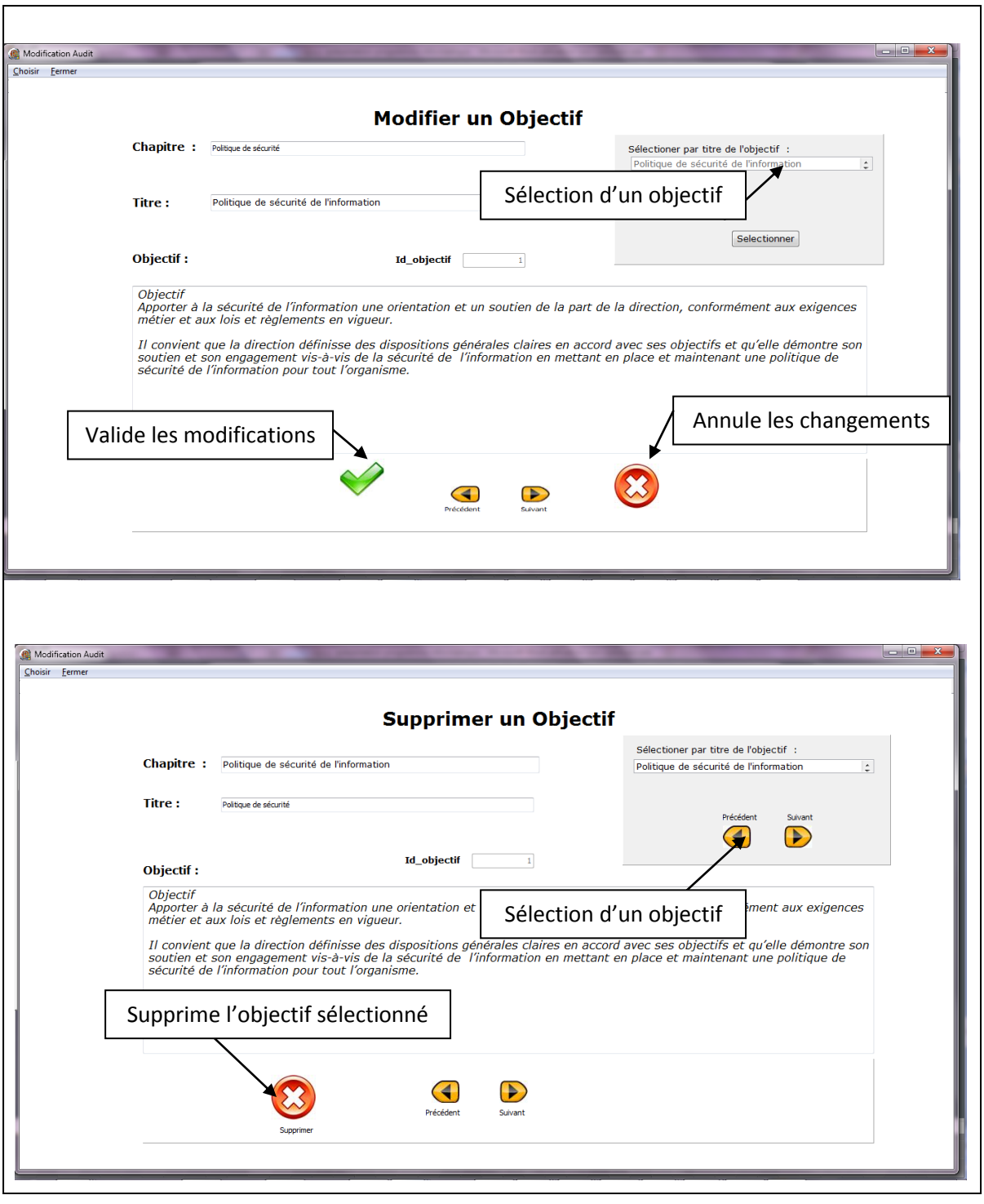


Figure 23 modifier/supprimer objectif

On peut également choisir dans le menu : un nouveau thème ; modifier ou supprimer

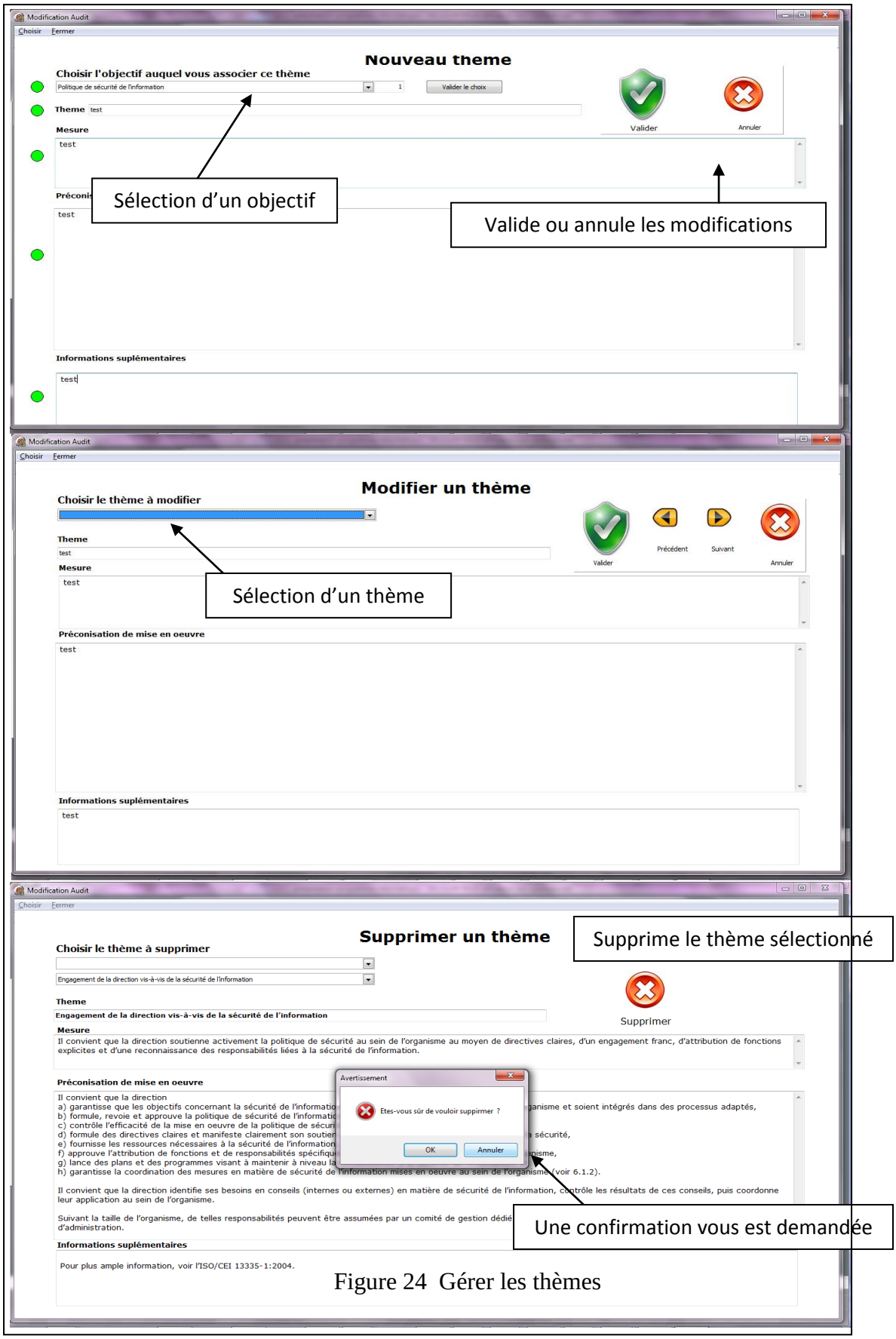


Figure 24 Gérer les thèmes

Le menu question nous donne accès a ce qui suit :

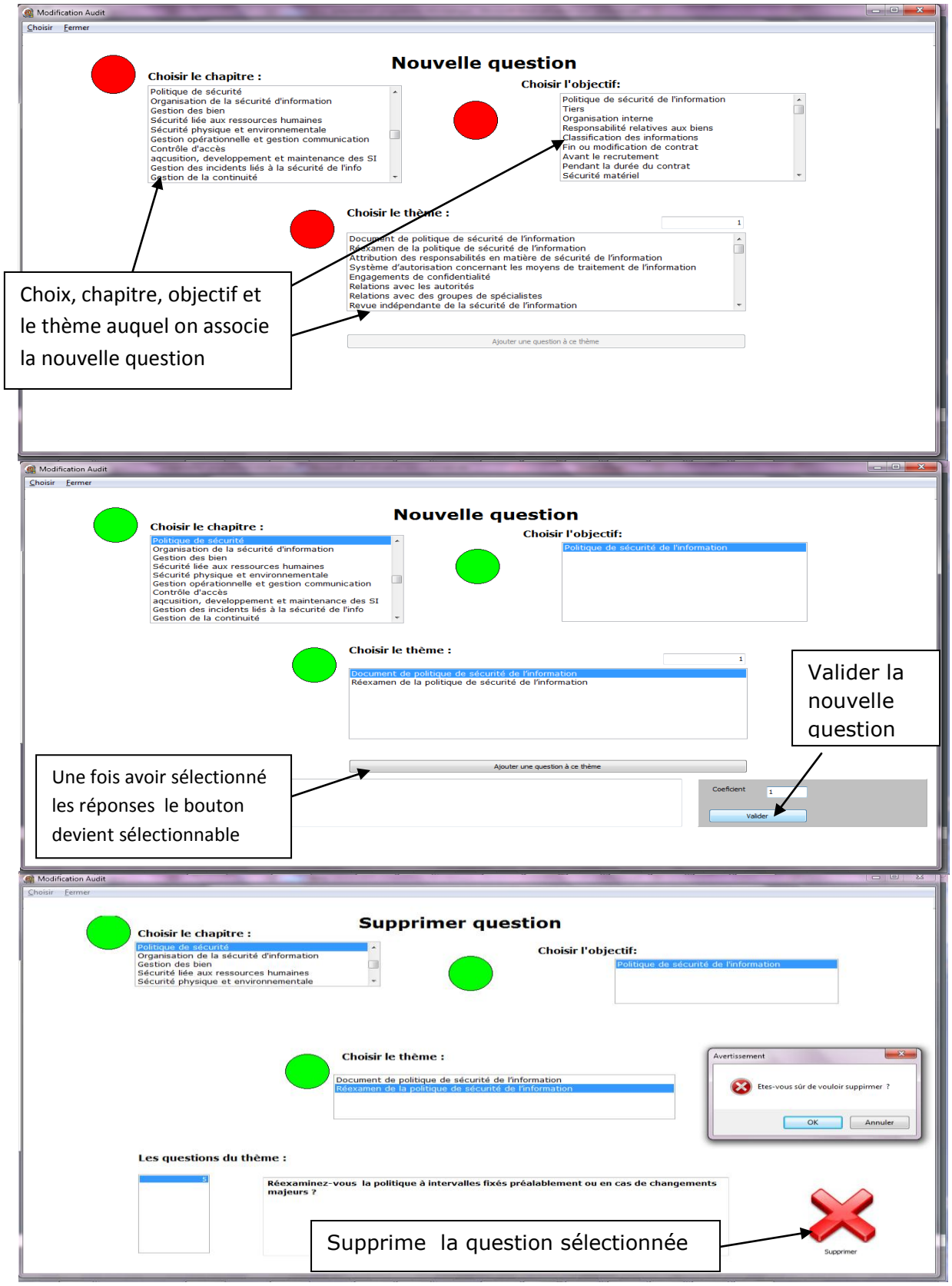


Figure 25 Gérer les Questions

Le menu « sélection questions d'un chapitre » permet de sélectionner les questions que l'auditeur posera lors de son audit, cela veut dire qu'une question même créée peut ne peut figurée lors du questionnement;

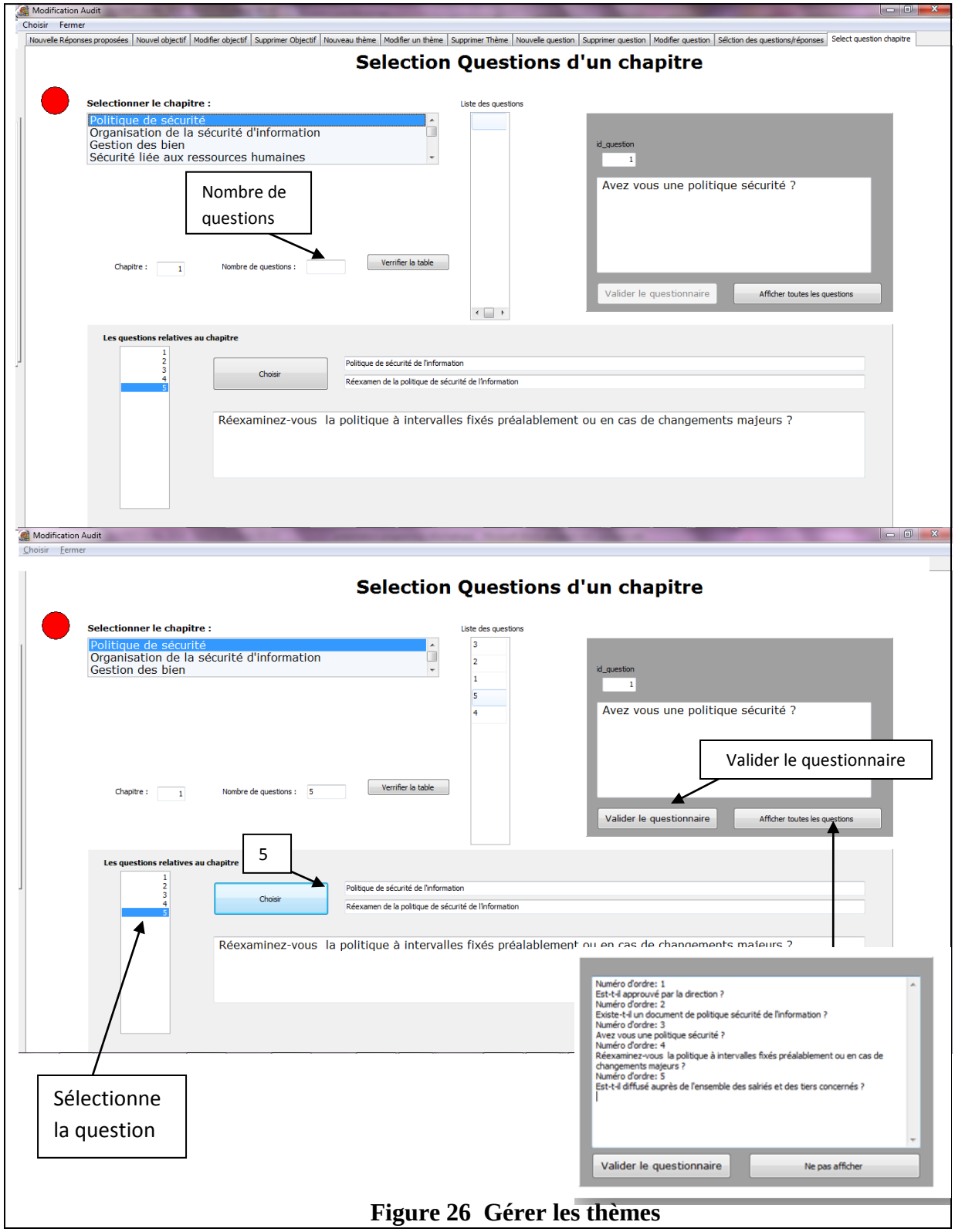


Figure 26 Gérer les thèmes

Ce menu permet de créer des réponses proposées, les modifier et les supprimer

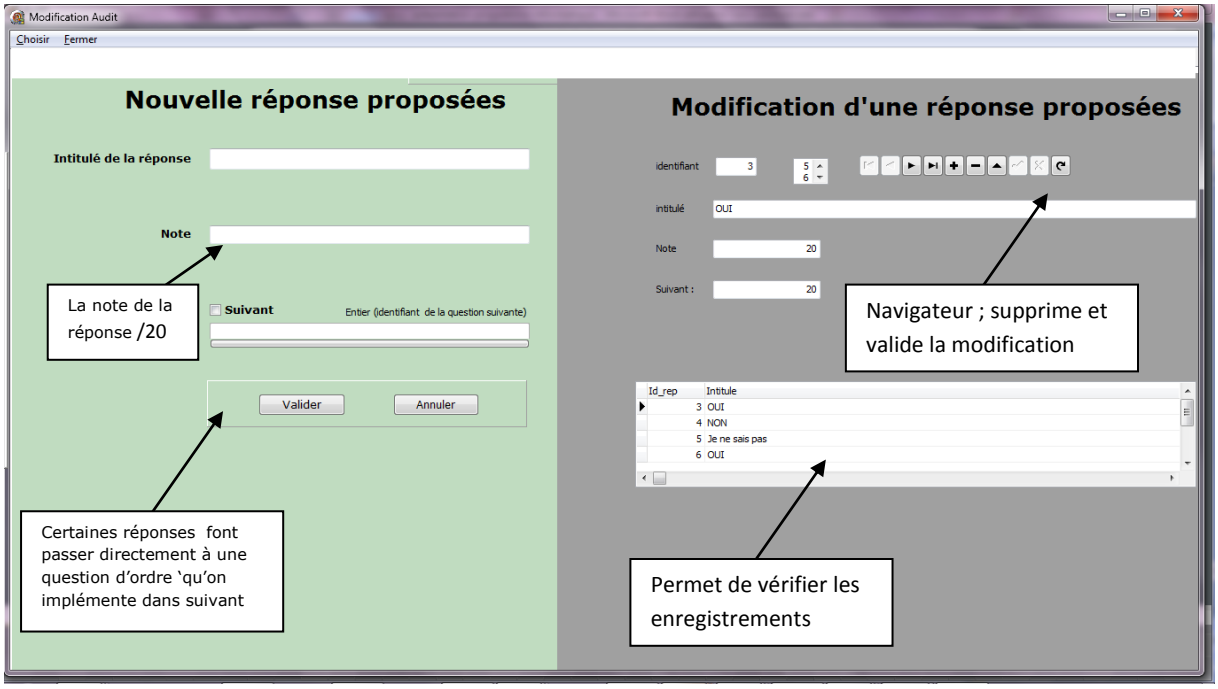


Figure 27 interface réponses proposées

La « sélection question réponse » permet de relier les tables « questions » et « réponse proposées ».

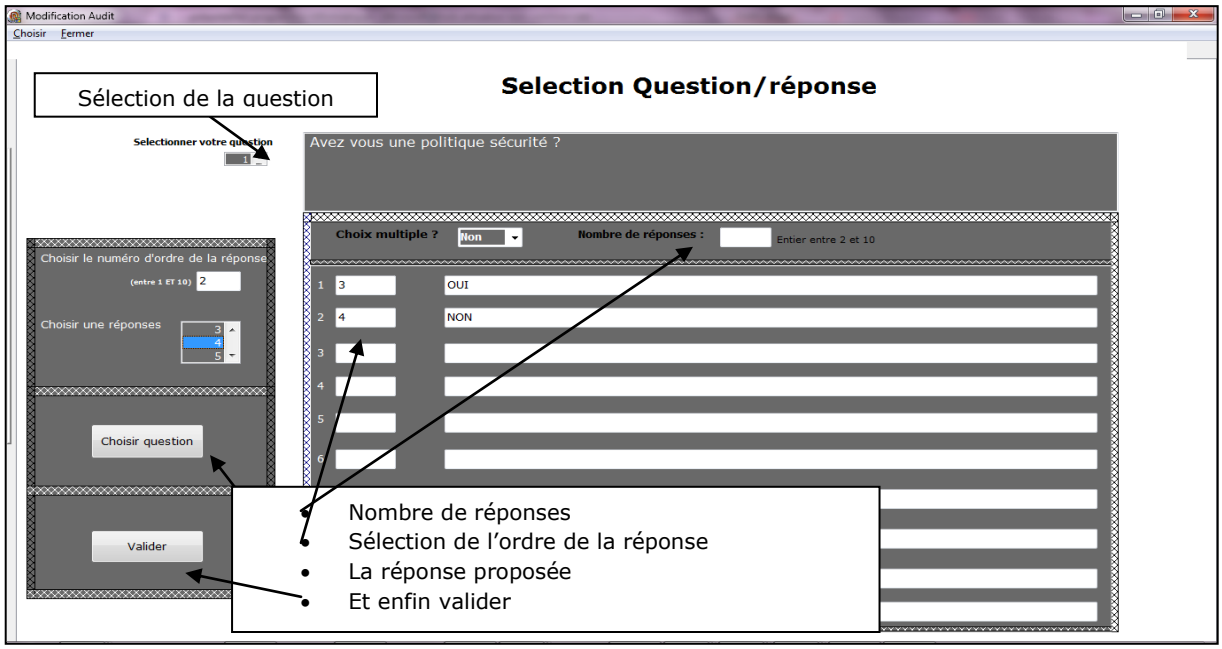


Figure 28 interface sélection Question/réponse

Pour rappel le module auditeur contient les fonctions suivantes.

1. Connexion auditeur.
2. Nouveau profil (entreprise).
3. Lancer un nouvel audit.
4. Modifier un compte.
5. Gérer les audits.

Il commence par l'identification de l'auditeur :

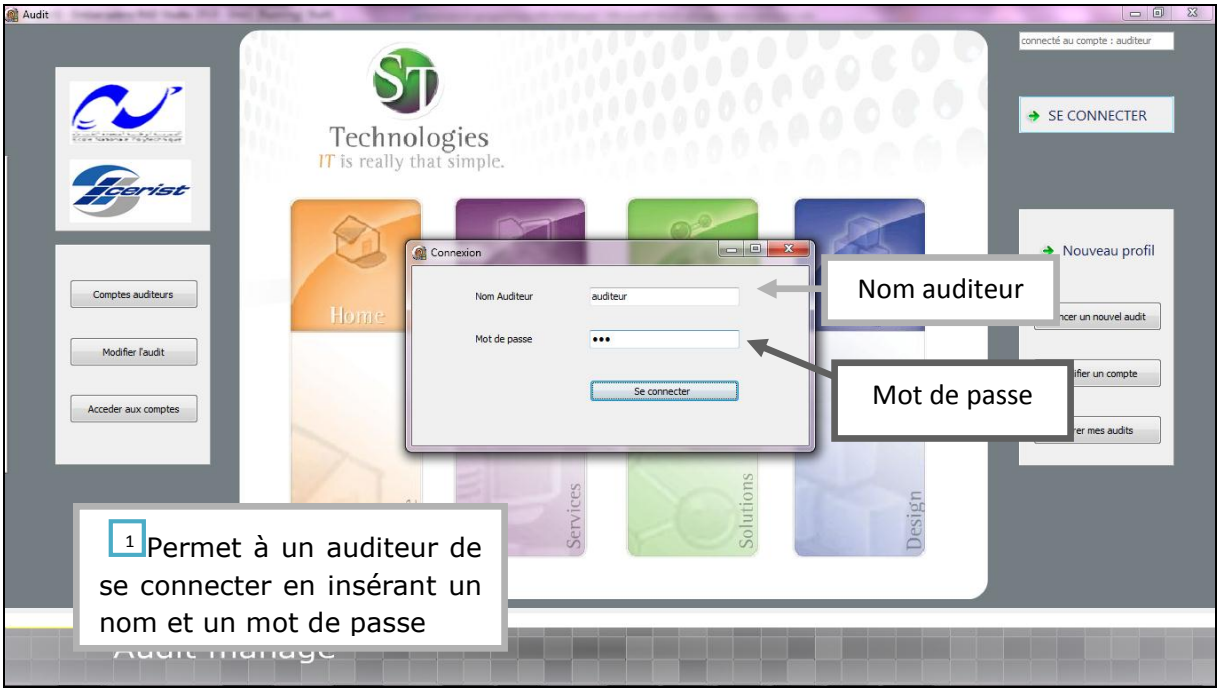


Figure 29 Connexion auditeur

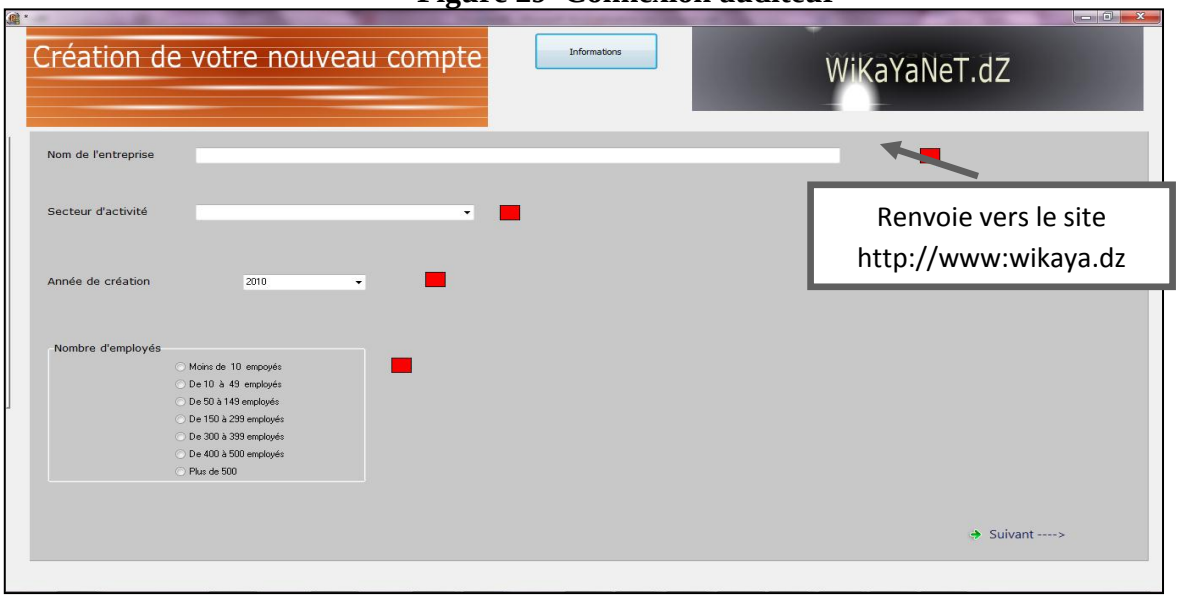


Figure 30 Nouveau profil (entreprise).

Ce menu permet de créer un nouveau profil d'entreprise, pour cela l'auditeur doit insérer les informations suivantes :

Raison social, Secteur d'activité, année de création, nombre d'employés, nombre d'ordinateurs, et nombre de serveurs, le contact, son mail, etc.

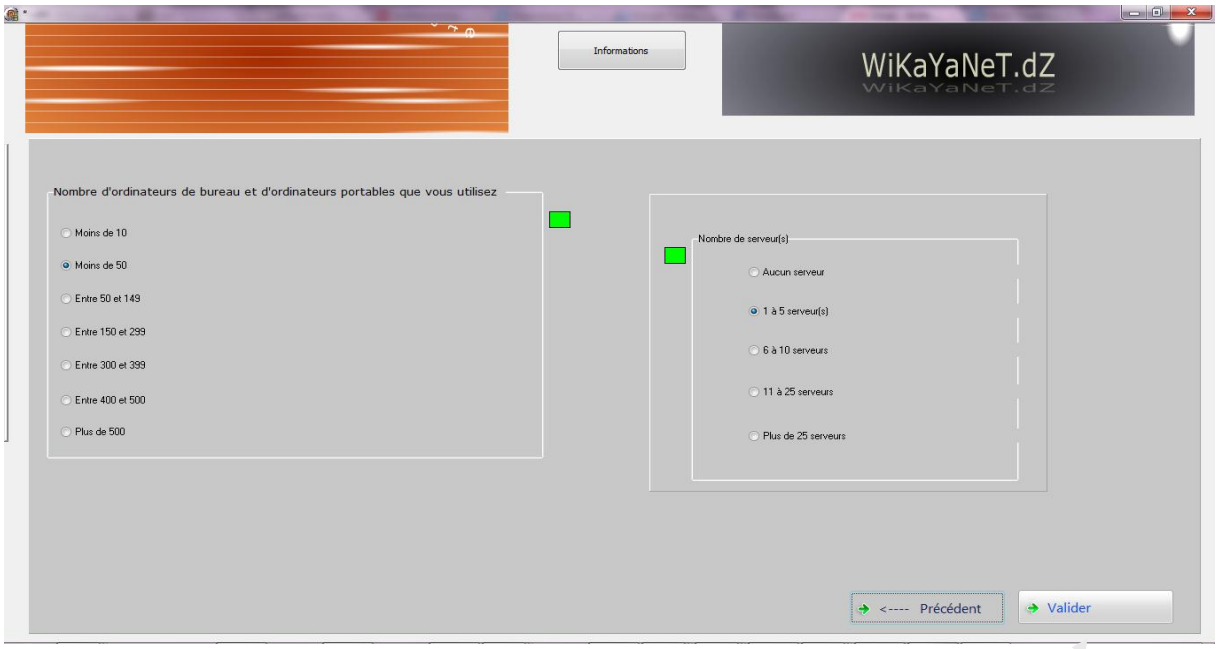


Figure 31 Nouveau profil (2)

Une fois que vous terminez d'insérer toutes les réponses demandées, les voyants sont tous verts et le bouton Valider devient actif. En cliquant dessus vous validez le nouveau profil.

Afin de modifier, ou de supprimer un profil déjà existant, il faut cliquer sur 4 le menu ci-dessous s'affiche ;

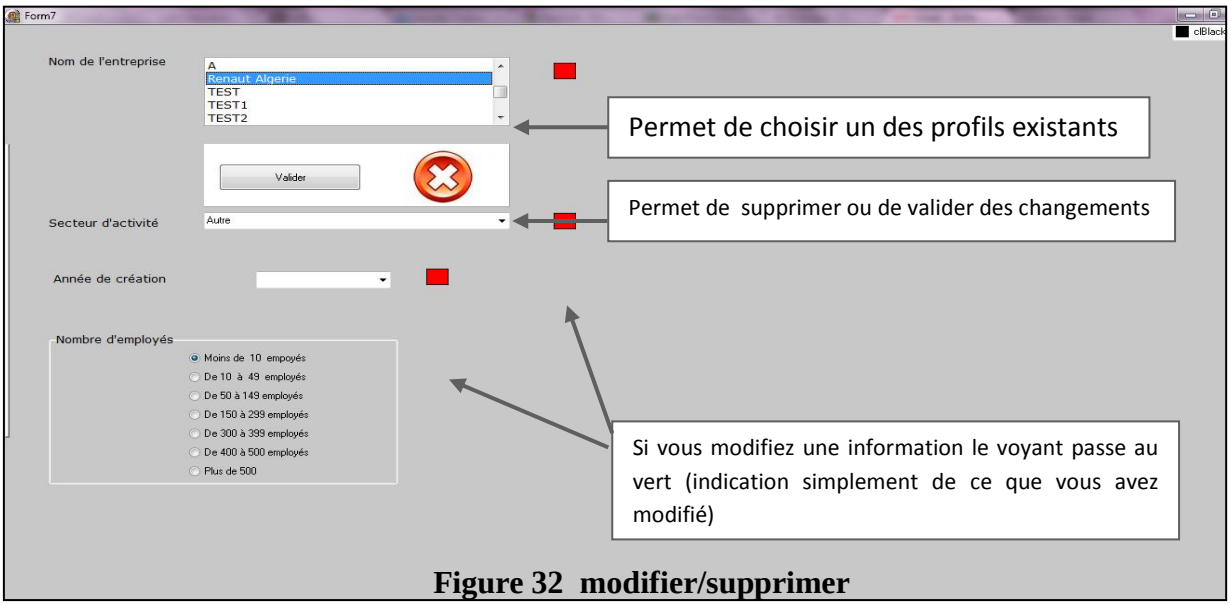


Figure 32 modifier/supprimer

Une fois la base de données implémentée, un audit peut être effectué. En cliquant sur menu principal,

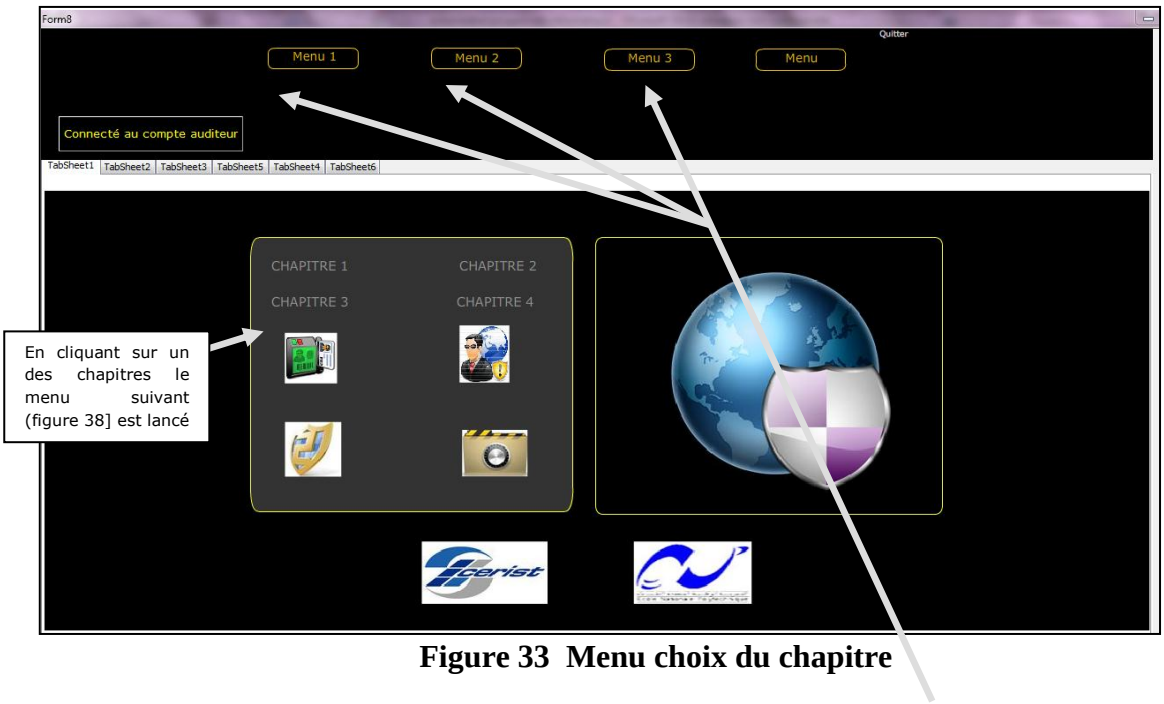


Figure 33 Menu choix du chapitre

La norme se compose de 11 chapitres ils sont répartis sur les menu 1, 2 et 3

- Politique de sécurité
- Organisation de la sécurité de l'information
- Gestion des biens
- Sécurité liée aux ressources humaines
- Sécurité physique et environnementale
- Gestion de l'exploitation et des télécommunications
- Contrôle d'accès
- Acquisition, développement et maintenance des systèmes d'information
- Gestion des incidents liés à la sécurité de l'information
- Gestion du plan de continuité de l'activité
- Conformité

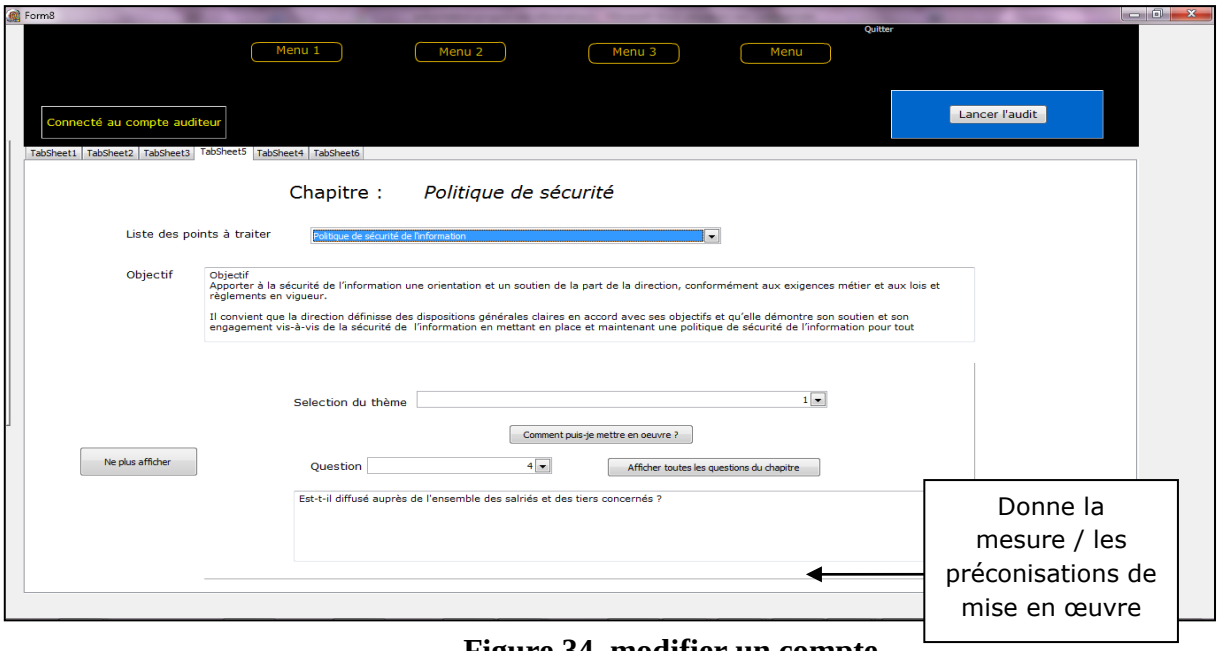


Figure 34 modifier un compte

En cliquant sur le bouton comment puis-je mettre en œuvre ? des indications sur les mesures s'affichent.

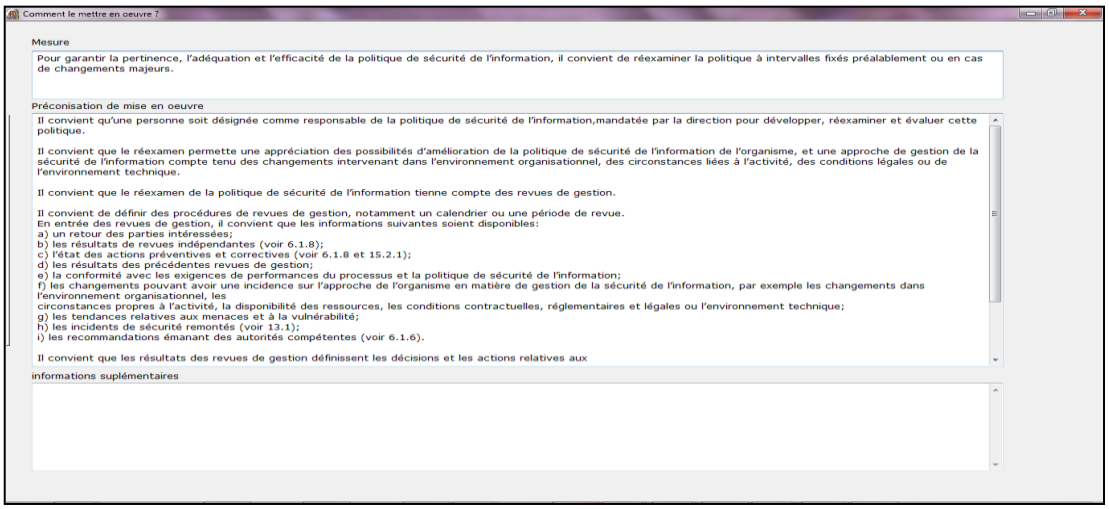


Figure 35 modifier un compte

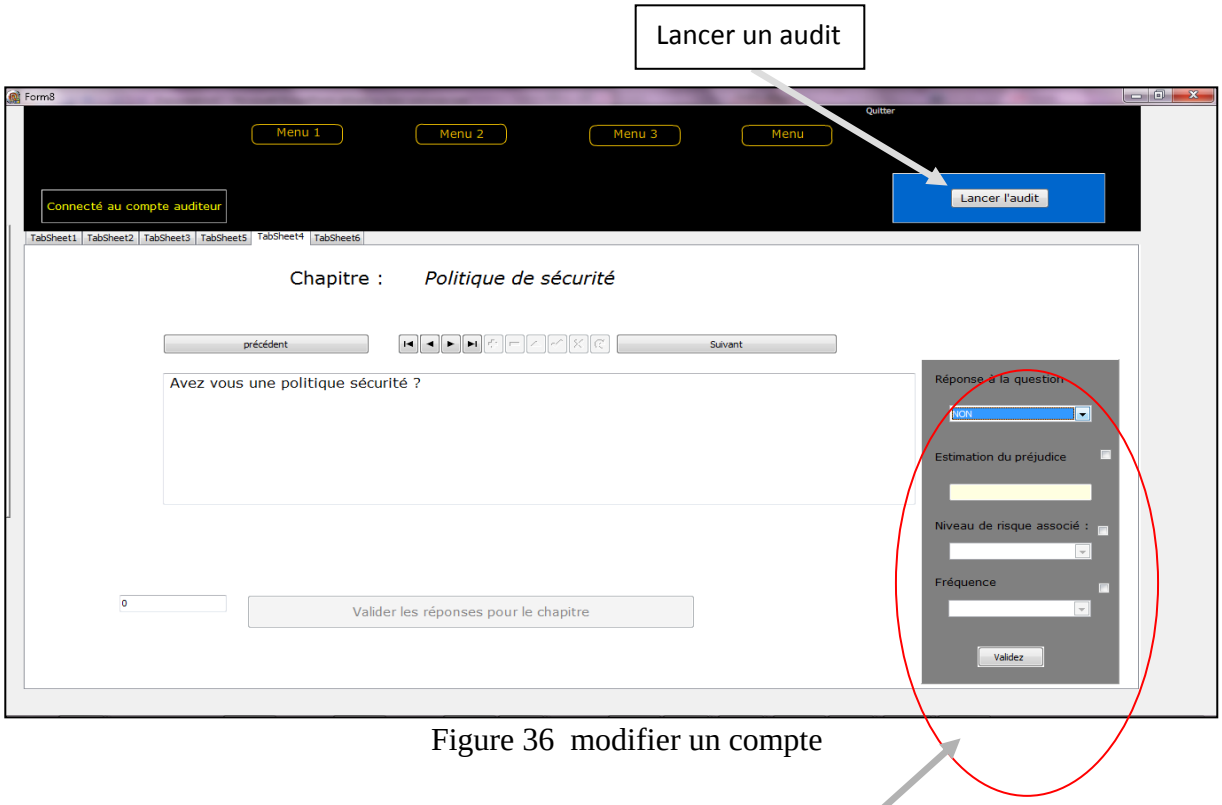


Figure 36 modifier un compte

Ce menu permet de répondre à la question en cours, certaines réponses

Auront un préjudice un niveau de risque et une fréquence à estimer.

En choisissant le chapitre, et le profil de l'entreprise ; les questions défilent, après avoir répondu à toutes les questions vous pourrez valider les réponses d'un chapitre

Nous pouvons visionner les différents audits avec le menu 5

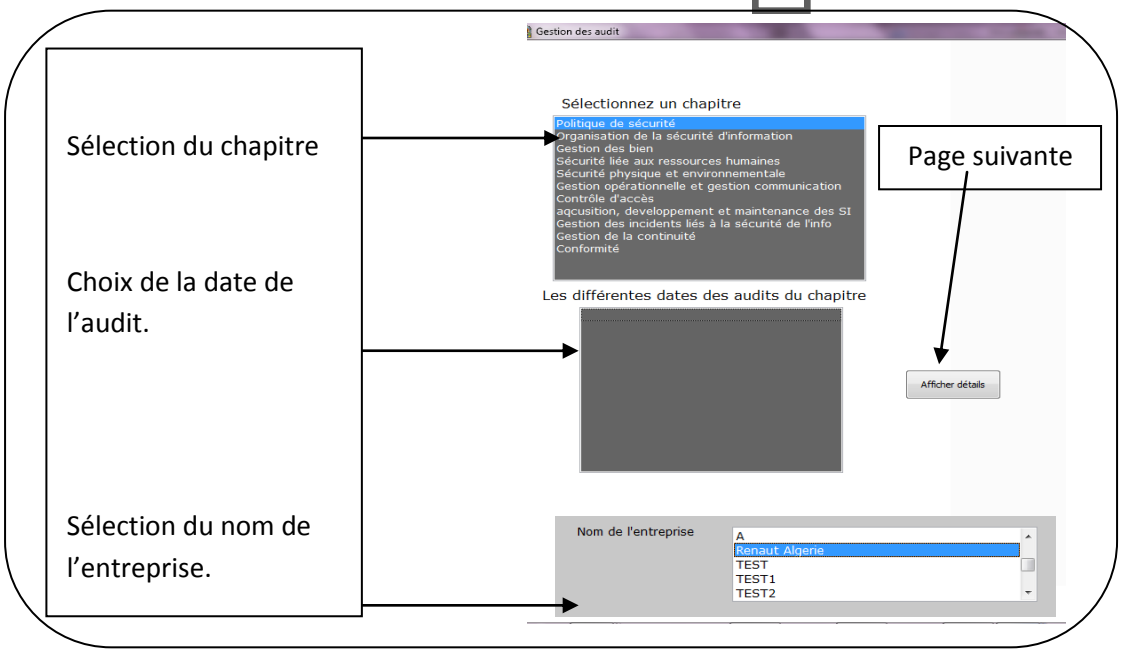


Figure 37 visualiser un audit

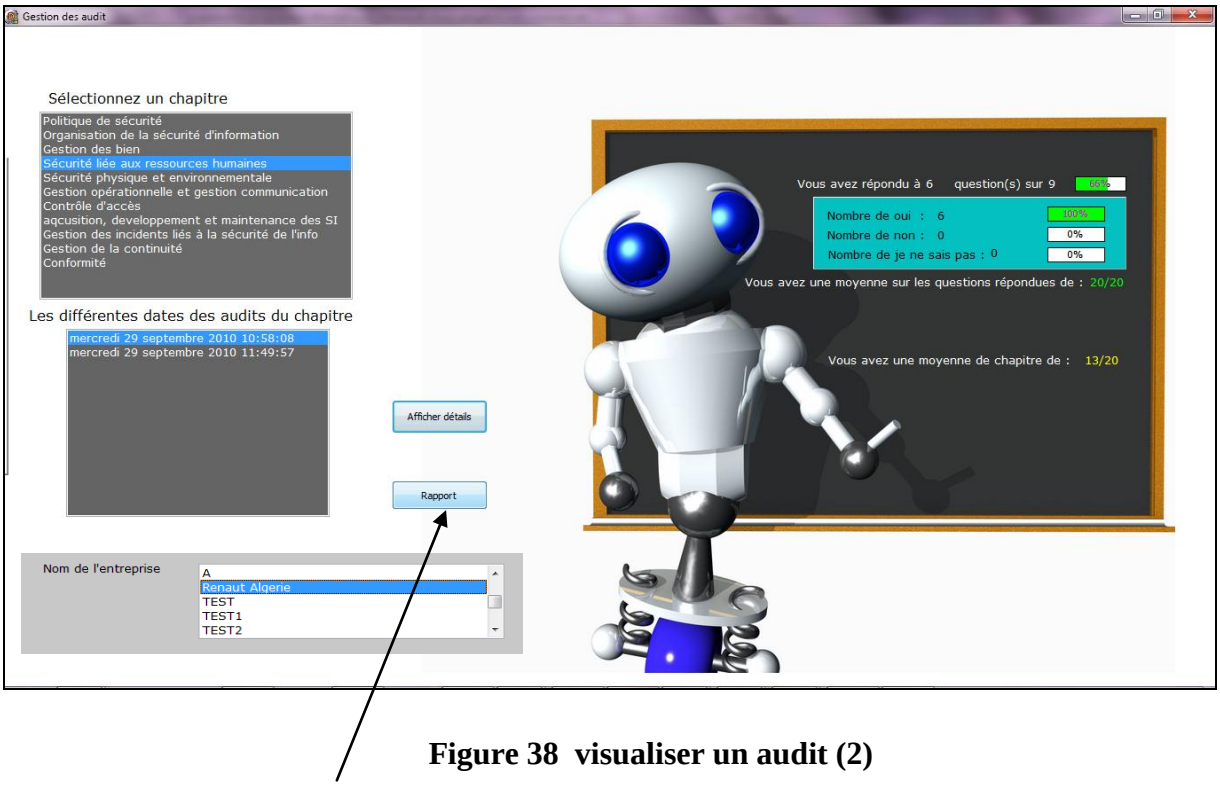


Figure 38 visualiser un audit (2)

En cliquant sur le bouton rapport du menu précédent ; un récapitulatif des questions/réponses, mesures et la mise en œuvre des mesures.

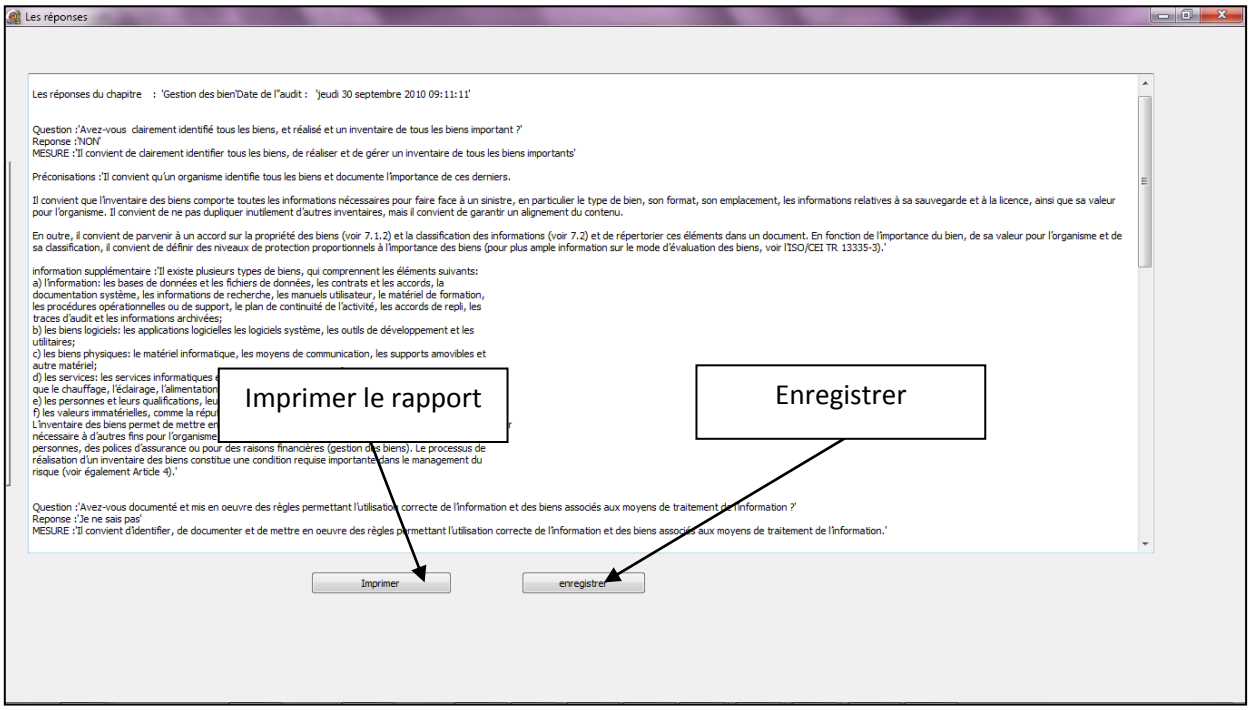


Figure 39 Le rapport

Le rapport comporte : le nom de l'auditeur, le nom de l'entreprise, La date de l'audit, les réponses apportées lors de l'audit ainsi que les mesures à mettre en œuvre.

Conclusion :

Dans ce chapitre, nous avons mis au point un programme d'audit basé sur la norme ISO 27001 destiné à la gestion des audits d'une entreprise. Les travaux menés durant cette phase nous ont permis d'automatiser ce processus et de générer un premier rapport qui peut aider l'entreprise à mettre en place des mesures de sécurité adéquates.

Chapitre V

Une approche de gestion de la sécurité de l'information

Introduction

Rappelons que notre objectif est de proposer un système d'aide à la décision permettant aux décideurs de définir un ensemble optimal de mesures de sécurité pour une entreprise donnée, selon la norme ISO 27001. Il soutient non seulement les décideurs dans la définition des mesures nécessaires à la certification, mais leur fournit également des informations concernant l'efficacité des mesures choisies en fonction de plusieurs objectifs définissables.

Notre approche utilise des données d'entrée d'une ontologie/sémantique de sécurité qui permet l'intégration standardisée de règles qui sont nécessaires pour modéliser les combinaisons de mesures possibles en adéquation avec la norme ISO 27001.

1 Approche proposée

L'approche proposée est de créer un processus qui démarre d'une ontologie de sécurité basée sur la norme ISO27001 qui comprend les connaissances sur la sécurité y compris les relations entre les menaces, les vulnérabilités, les mesures, et les biens de cette ontologie et à travers un outil existant que nous présentons dans ce document, nous passons vers une base de données relationnelle.

L'utilisation des données de la base relationnelle permet de modéliser le domaine de la sécurité IT de manière standardisée et permet l'intégration normalisée des règles qui sont nécessaires pour modéliser les combinaisons de mesures possibles.

Nous développons une modélisation mathématique multi-objective afin de trouver un ensemble de solutions optimales.

Bien que la première étape de création d'ontologie/web sémantiques doit être menée par des experts sécurité de l'information, la base de connaissances finale peut être réutilisée sans le soutien d'experts.

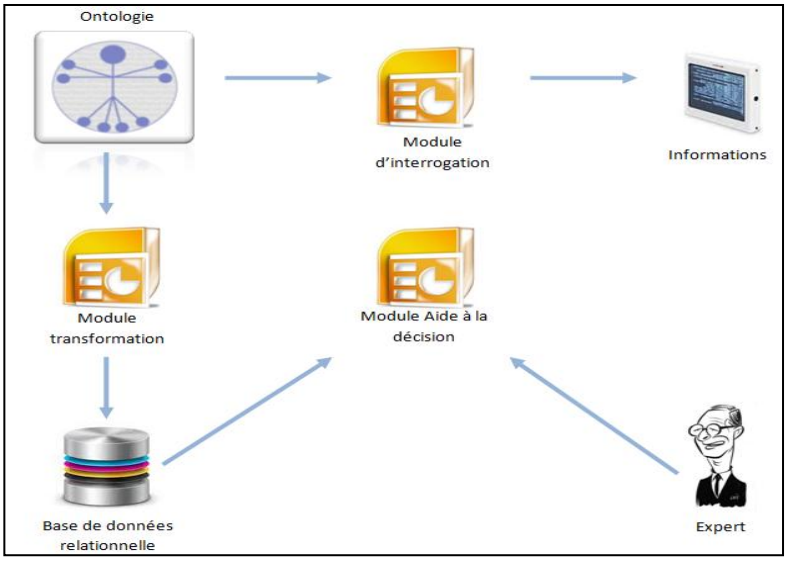


Figure 40

Approche proposée

Avant de décrire notre approche en détail, nous présentons de manière générale l'ontologie.

2 Ontologie : Description générale

Les infrastructures informatiques et Web en particulier dont l'importance ne cesse de croitre répondent à la fois à des besoins de communication et de partage d'information. Concernant le premier besoin, on trouve des applications variées allant de la messagerie à la vision conférence en passant par le chat et la téléphonie. S'agissant du second, on trouve également des applications très diverses, allant des sites web classiques aux bibliothèques numériques de grandes tailles en passant par les weblogs et les sites interactifs de toutes natures offrant des accès à de nombreuses autres applications portées par des ambitions d'ingénierie ; différentes visions du Web ont émergé avec un succès plus ou moins grand. Une d'entre elles est l'ontologie.

Le terme est emprunté à la philosophie, où une ontologie est une description systématique de l'Existence. Lorsque les connaissances d'un domaine sont représentées dans un formalisme déclaratif, l'ensemble des objets qui peuvent être représentés est appelé l'univers du discours. [Goeken et Alter, 2009]

Dans la littérature nous trouvons les définitions suivantes.

La définition de Guarino est : « Une ontologie est une spécification explicite d'une conceptualisation d'un domaine» [Guarino, 1998].

Gruber dit " **Specification of a conceptualization** " [Gruber, 1993] ; **une Ontologie** est une spécification explicite d'une conceptualisation;

Et enfin Schulze-Kremer "Concise and unambiguous description of principle relevant entities with their potential, valid relations to each other [Schulze, 1998]

Les ontologies décrivent généralement des :

- **Classes/ Concepts** : ensembles, collections, ou types d'objets, (menaces, vulnérabilités, mesures, ressources)
- **Attributs** : propriétés, fonctionnalités, caractéristiques ou paramètres que les objets peuvent posséder et partager, (a_pour_fonction, a_pour_produit, a_un_coût)
- **Relations** : les liens que les objets peuvent avoir entre eux, (est un ; une_SousClasse_de, est_ généré_par, est_géré_par)
- **Axiomes :** les vulnérabilités qui causent l'arrêt du service sont de très haute criticité, les objets de la classe toplevelthreat affectent l'attribut **intégrité** de la sécurité

- **Contraintes** (Mesure 1 ou mesure 2 mais pas les deux).
- **Individus/instance** : les objets de base, (incendie, mesure i : Mettre des agents de contrôle).
- **Événements** : changements subis par des attributs ou des relations.
- **Taxonomie de concepts** (ordre de **généralisation** entre concepts).

2.1 Pourquoi l'ontologie ?

Le but d'une ontologie est de définir un vocabulaire pour décrire un domaine de façon formalisée, donc exploitable par un automatisme. Les applications développées autour des ontologies visent à automatiser des traitements sur l'information du domaine : recherches, comparaisons, représentation de connaissances, etc.

Les ontologies permettent deux points importants:

1. La recherche d'information dans un ensemble important. (grande importance avec la taille de plus en plus grande des bases de données).
2. La formalisation de vocabulaires d'une entreprise ou d'un secteur.

Cela donne lieu à:

- Une base de connaissances (objets).
- Un système d'annotation.
- Un système d'indexation documentaire de recherche d'information.

2.3 OWL :

Langage de représentation des connaissances construit sur le modèle de données. Il fournit les moyens pour définir des ontologies web structurées.

Le langage OWL est basé sur la recherche effectuée dans le domaine de la logique de description. Il peut être vu en quelque sorte comme un format de fichier pour certaines logiques de description. Il permet de décrire des ontologies, en définissant des terminologies.

2.4 Les avantages d'OWL :

- Apporte une meilleure intégration, une évolution, un partage et une inférence plus facile des ontologies.
- Ajoute les concepts de classes équivalentes, de propriété équivalente, d'égalité de deux ressources, de leurs différences, du contraire, de symétrie et de cardinalité.

- Grâce à sa sémantique formelle basée sur une fondation logique largement étudiée, elle permet de définir des associations plus complexes des ressources ainsi que les propriétés de leurs classes respectives.
- Adéquat pour le Web sémantique, car il offre une syntaxe définie strictement, et selon le niveau elle peut permettre des raisonnements automatisés sur les inférences et conclusions des connaissances.
- Le partage et l'échange dans ses formats est facile

3 Choix de l'ontologie de sécurité :

Dans leur comparaison de trente ontologies [Blanco et al, 2008] Blanco et ses collègues concluent que la communauté scientifique n'a pas encore atteint l'objectif de l'établissement d'une ontologie générale sécurité de l'information.

Après avoir examiné plusieurs ontologies [Fenz et Ekelhart, 2009] , [Karyda et al, 2006] , [Lee et Gritzalis, 2006] , [Mouraridis et al, 2003], [Raskin et al, 2001], [Tsoumas et Gritzalis, 2006], nous avons décidé d'utiliser celle de [Fenz et Ekelhart, 2009] de part l'accès facile à la base OWL et sa réponse à nos questionnements sur différents aspects notamment les relations existantes entre les entités de la norme étudiée. Cette ontologie est accessible à l'adresse suivante http://securityontology.sba-research.org/securityontology.owl

La figure 41 montre le concept de l'ontologie dont lequel les menaces, les vulnérabilités, les mesures et leur implémentation sont les éléments clés:

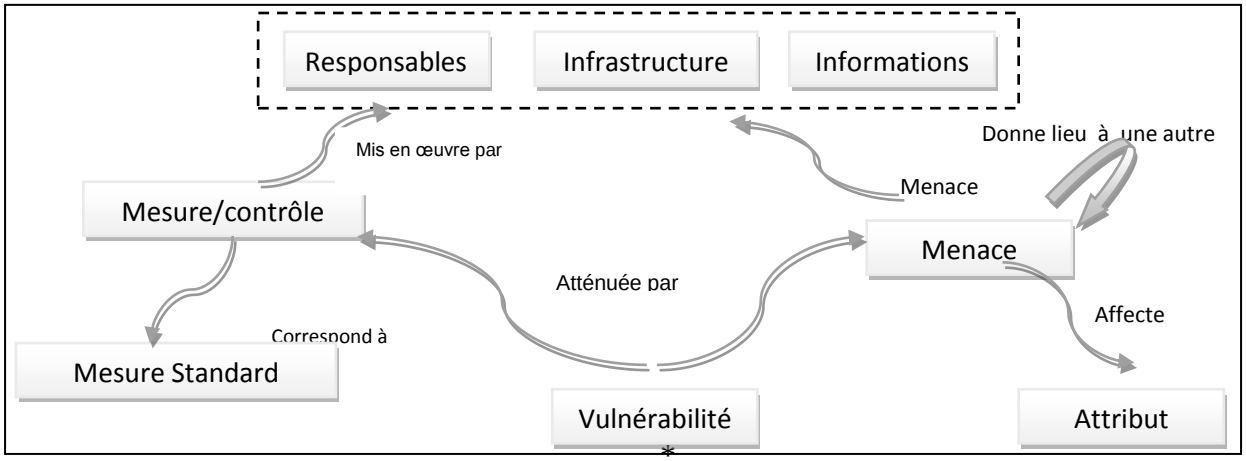


Figure 42 schéma général de l'ontologie

Ce qui nous intéresse, c'est de pouvoir visualiser la norme ISO 27001 et de donner un moyen supplémentaire à l'auditeur afin qu'il se l'approprie, ainsi à travers une visualisation graphique qui peut être réalisé avec des fichiers OWL.

Des outils pour visualiser les ontologies existent, le programme informatique « protégé » développé par l'université de Manchester dans sa 4ème version en 2006, un second est l'ATLAS.ti développé quand à lui par GMBH Berlin ou encore Swoop2.3 développé quant à lui par l'université du Maryland, College Park par le MindsWap research group.

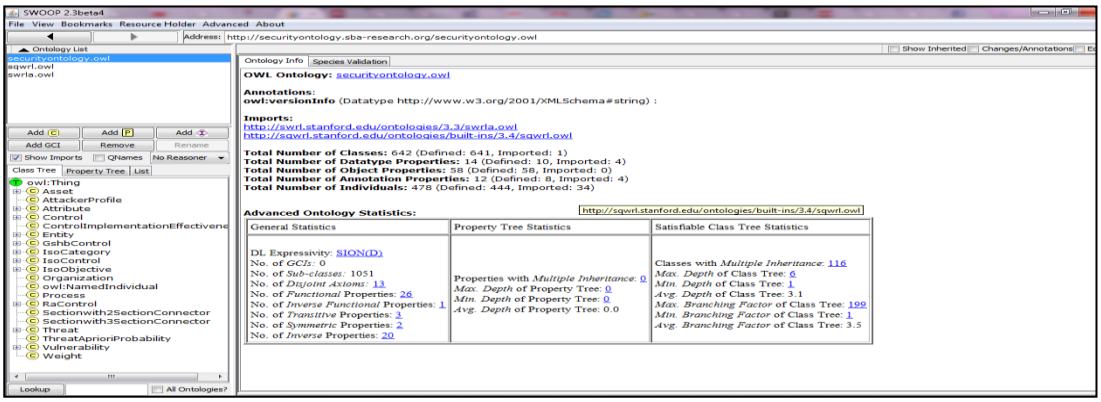


Figure 43 Interface Swoop 2.3

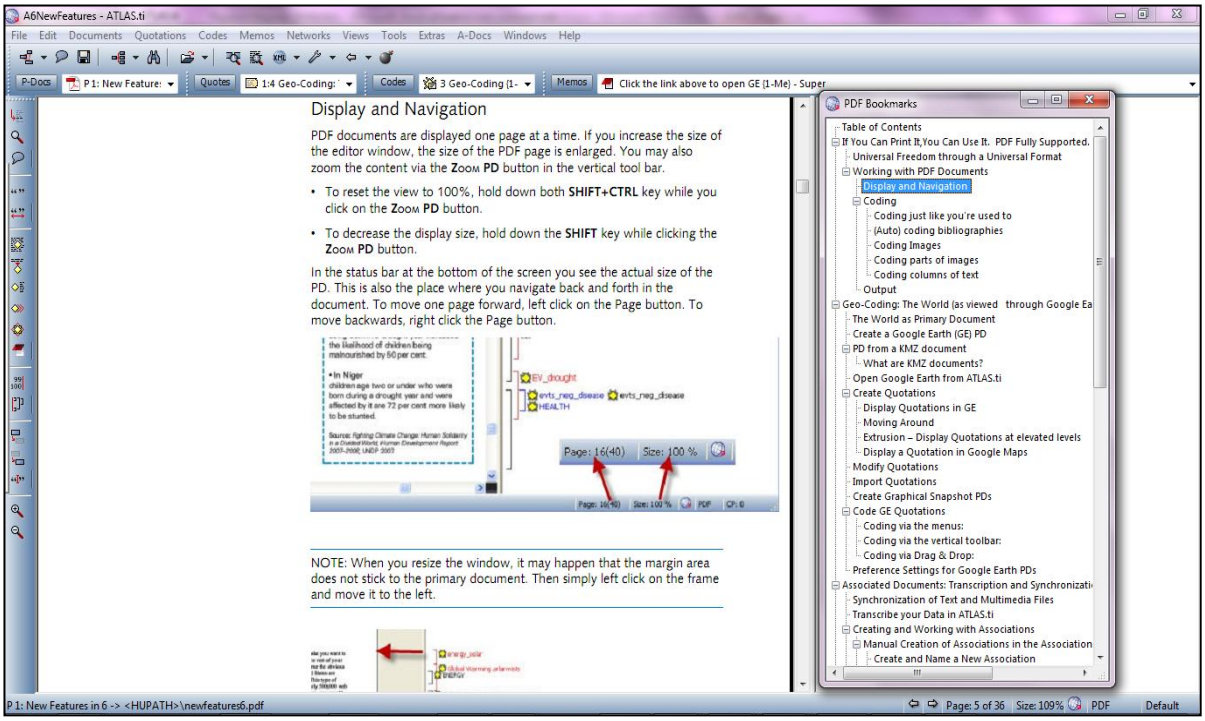


Figure 44 Interface Atlas Ti

Nous préférons le logiciel« Protégé » qui a une prise en main plus rapide et un accès à une base de données plus riche en termes d'ontologie.

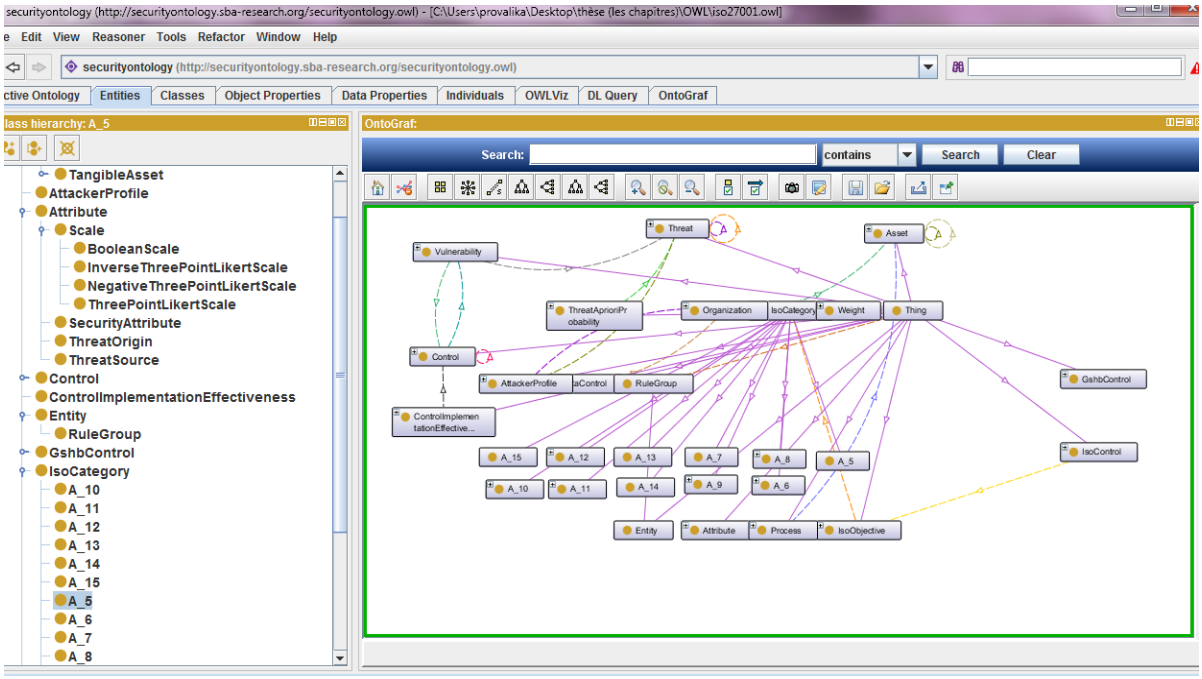


Figure 45 interface protégé avec exemple d'ontologie iso 27001

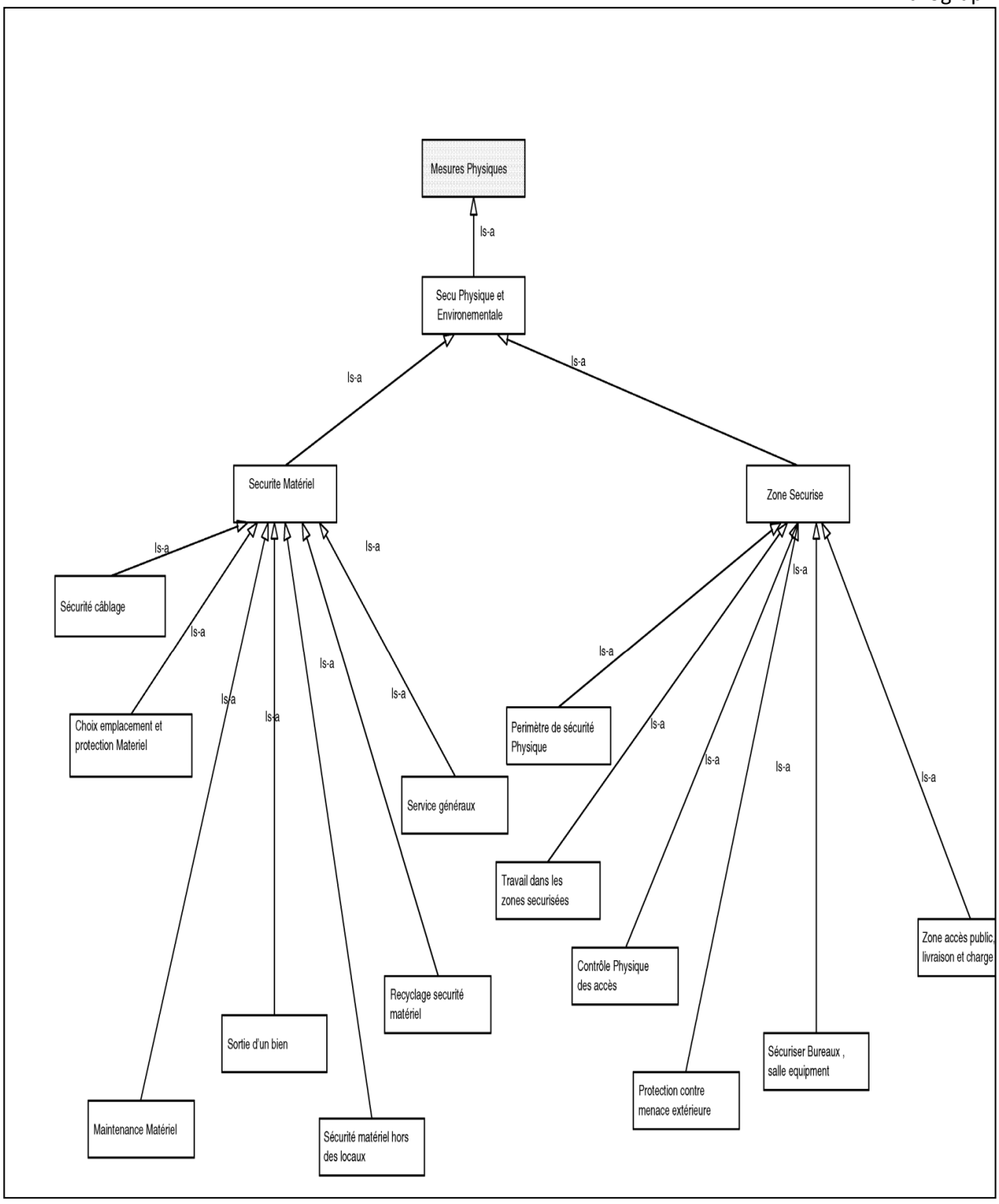


Figure 46 partie de l'ontologie : mesures physiques

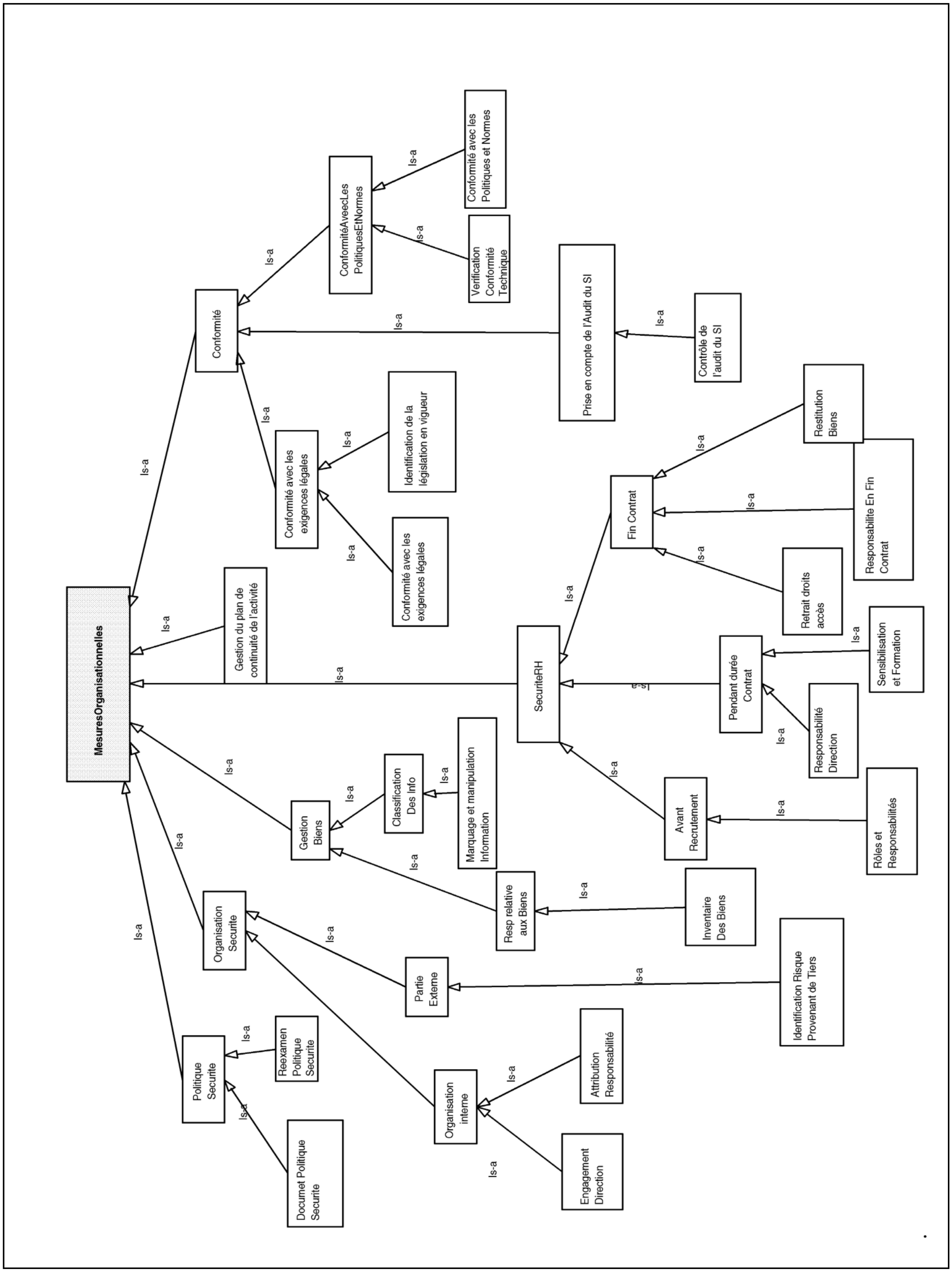


Figure 47 partie de l'ontologie : mesures organisationnelles

4 Module d'interrogation de l'ontologie

Sous Eclipse et avec l'aide du plugin Sparql [SPARQL, 2008] nous avons développé un programme en java qui nous permet d'extraire de l'ontologie de Fenz les différentes occurrences des objets de l'univers de discours.

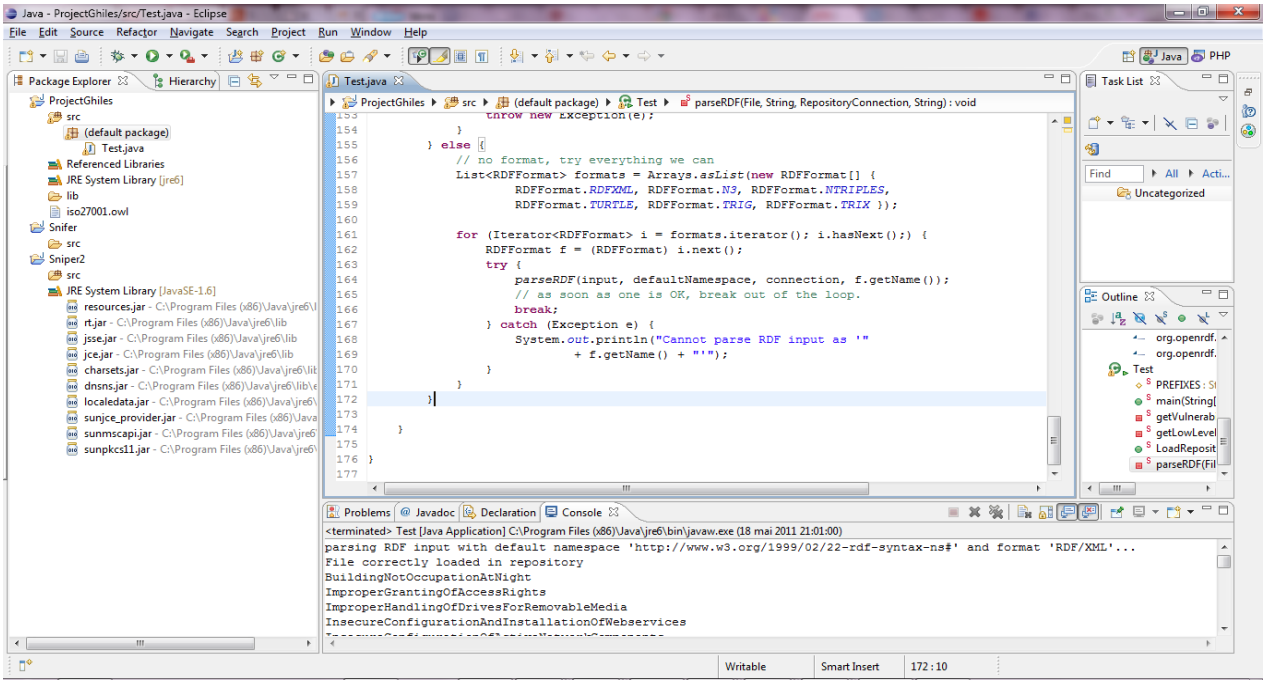


Figure 48 requêtes SPARQL sous eclipse

Exemple de requête SPARQL

```
	private static void getLowLevel(RepositoryConnection con)
	{
		//requete sparql
//recuperer tous les éléments dont le type est Vulnerability, affecter les resultats dans la variable ?a
	String query = "SELECT distinct ?a ?b WHERE { ?a rdf:type secure:vulnerability.}";
		try {
				//Excuter la requete
TupleQueryResult results = con.prepareTupleQuery(QueryLanguage.SPARQL, PREFIXES + " " +  query).evaluate();

while (results.hasNext())
				{
			//pour chaque resultat trouvé néttoyé le text et l'affiché sur l'ecran
					BindingSet bindingSet = results.next();
					String[] s = bindingSet.getValue("a").toString().split("#");
					System.out.println(s[1]);

				}
				results.close();
		} catch (Exception e) {
			e.printStackTrace();
		}

	}
```

Cette requête retourne le résultat suivant, dont les vulnérabilités sont:

BuildingNotOccupationAtNight
ImproperGrantingOfAccessRights
ImproperHandlingOfDrivesForRemovableMedia
InsecureConfigurationAndInstallationOfWebservices
InsecureConfigurationOfActiveNetworkComponents
InsecureDatabaseConfiguration
InsecureDispositionOfMedia
InsecureDomainControllerConfiguration
InsecureFileAndSharingServicesConfiguration
InsecureInstallationAndConfigurationOfSoftware
InsecureLogin
InsecureOperationOfMailServer
InsecurePasswords
InsecureWebserverConfiguration
InsecureWirelessNetwork
InsuffcientReplacementPartsMaintenance
InsufficientApplicationMaintenancePlan
InsufficientCoordinationOfAdministrationStaff
InsufficientMonitoringOfWebserver
InsufficientRestrictionsOnAccessToServers
InsufficientTrainingOfMaintenanceAndAdministration
InsufficientUserAccountManagement
InsufficientWirelessNetworkMaintenancePlan
LackOfITTraining
MultipleServicesPerServer
NoAccessRegulationControl
NoAirConditioningInServerRoom
NoApplicationDataBackup
NoAppropiateStorageOfBackupMedia
NoBackupProcedureDocumentation
NoChangeOfPresetPasswords
NoDeactivationOfUnnecessaryAccountsOrTerminals
NoDeactivationOfUnnecessaryServices
NoDeactivationOfUnnecessaryWalljacks
NoDefaultConfigurationsHardening
NoDocumentationForGrantingRemoteAccessRights
NoDocumentationForGrantingUserRights
NoDocumentationOfAdministratorRights
NoDocumentationOfElectricCircuitPlans
NoDocumentationOfInstallationProcess
NoDocumentationOfNetworkPlans
NoDocumentationOfRoomMaintenance
itchportNoDocumentationOfSwitchportPlans
NoDomainControllerContingencyPlan
NoEncryptionOfConfidentialData
NoLocalStorageOfRelevantData
NoLoggingOfAdministratorActivities
NoOrInsufficientDataBackups
NoOrInsufficientDatabaseBackups
NoOrInsufficientLogging
NoOrInsufficientNetworkLogging
NoOrInsufficientRestrictionsOnAccessToAccountsOrTerminals
NoOrInsufficientRestrictionsOnAccessToBackupMedia
NoPowerBackupProvider
NoPreventionToBootFromRemovableDevices
NoProtectionOfDataConfidentially
NoRegularPatching
NoRegularReviewingOfHardwareAndSoftwareInventory
NoRegularSecurityChecksOfTheNetwork
NoRegularTestingOfPipes
NoRegularlyReviewedRessourceInventory
NoRegulationsOnSoftwareInstallation
NoRenamingOfAdministratorAccounts
NoSecureDoors
NoSecureInternetConnection
NoSecureWindows
NoSecurityAudits
NoSegmentationOfNetworks
NoStandbyGenerators
NoSurveillanceSystem
NoTestingOfFireExtinguishers
NoTestingOfStandbyGenerators
NoTrainingOfITAdministrators
NoUninterruptiblePowerSupply
NoUpToDateServerDocumentationAvailable
NoUseOfEncryptionForExternalNetworkCommunication
NoUseOfEncryptionForInternalNetworkCommunication
NoUseOfKensingtonLocks
NoUseOfProxyServer
NoUseOfSeparateTestAndProductionServers
NoWaterDetector
OpenFireDoors
OpenWindows
UnlockedFuseBox
UseOfUnreleasedSoftware
WaitingRoomsCloseToSensitiveAreas
NoFireSuppression
NoHeatDetector
NoIntrusionAlarmSystem
NoEntranceControl
NoEscortationAndDocumentationOfVisitorsToServerRoom
NoEscrowOfPasswords

Cette partie représente une requête possible :ologie OWL les vulnérabilités existantes en sécurité

5. Module de transformation de l'ontologie à une base de données (le stockage):

Il existe deux techniques de base pour le stockage des ontologies [Harrison et al, 2005]

La première technique consiste à utiliser les systèmes de fichiers pour le stockage d'ontologies dans des fichiers plats. Le principal problème avec cette technique est que les systèmes de fichiers ne fournissent pas d'évolutivité, de possibilités de partage, ou toute plateforme requête.

La deuxième technique consiste à utiliser des systèmes de gestion des ontologies afin de les stocker dans des bases de données.

Le principal problème de cette technique est que les systèmes de gestion de base de données exigent qu'une ontologie doit avoir une structure fixe, qui ne peut être garantie car généralement les ontologies sont construites de façon distribuée/collaborative. Cela signifie, par exemple, qu'un utilisateur peut définir un employé comme ayant un numéro de sécurité sociale, mais ne prévoit pas un statut marital. Cela n'empêchera pas, toutefois, un autre utilisateur de faire valoir qu'un employé donné est marié ajoutant un type de propriété des données (Statut marital) à la Classe Employé.

Il y a plusieurs options pour le stockage des ontologies dans des bases de données, par exemple : relationnelle, objet ou objet-relationnel. Le stockage des ontologies en bases de données relationnelles est moins simple que le stockage des ontologies dans des bases de données type objet ou de bases de données type objet relationnel, parce que les systèmes de gestion de base de données ne permettent pas la fonction héritage.

Cependant, les systèmes de gestion des bases de données relationnelles ont des avantages significatifs sur les systèmes de gestion type objet ou objet-relationnel car ils fournissent: la performance, la robustesse, la fiabilité et la disponibilité.

5.1 Motivations :

Il y a trois raisons principales pour le stockage des ontologies dans des bases de données relationnelles:

- **Accessibilité aux données :** Lorsqu'elles sont stockées dans des bases de données relationnelles, les ontologies peuvent interagir avec une grande quantité de données existantes.

- **Accessibilité aux applications:** Lorsqu'elles sont stockées dans des bases de données relationnelles, les ontologies peuvent être accessibles à partir des applications existantes.

- **Stockage d'Ontologies à large échelle:** La capacité des bases de données relationnelles pour stocker une grande quantité de données prouve que les bases de données relationnelles sont également appropriées pour le stockage des ontologies à grande échelle qui peuvent contenir des millions d'objets. Une condition préalable pour ce stockage est la transformation des ontologies en bases de données relationnelles.

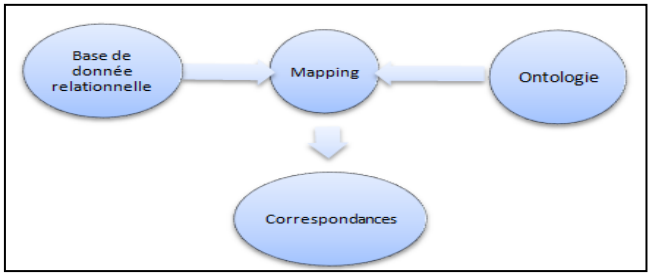
5.2 Problèmes liés à la transformation :

La transformation des ontologies en bases de données relationnelles doit gérer les problèmes suivants:

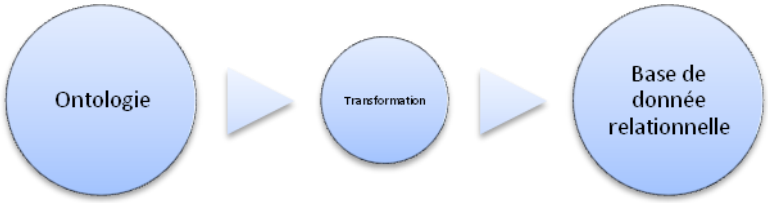
- **Perte de données:** Le résultat de la transformation devrait décrire adéquatement les données d'origine.
- **Perte de la structure:** Dans certains cas, la transformation occasionne une perte dans le sens où la totalité des concepts d'une ontologie donnée ne peut être traduite dans une base de données relationnelle. Par conséquent, la qualité de la transformation doit être analysée.
- **Convergence des structures:** Outre la transformation des structures, des techniques devraient être prévues pour la transformation des données/objets.
- **Convergence sur les données:** Les données doivent être transformées en incorporant les types de données appropriés.
- **Applicabilité:** Dans certains cas, la transformation n'est pas vraiment générale dans le sens où son application est plutôt restreinte. Ce qui rend la transformation non utilisable dans des situations concrètes, dans ce cas elle souffre du problème d'applicabilité.
- **Justesse:** La transformation devrait avoir une exactitude/justesse vérifiable.

5.3 Travaux dans la littérature :

Des travaux ont déjà été effectués par exemple [Une et al, 2005] -[Konstantinou et al, 2006], et [Xu, 2006]. Cependant, certains de ces travaux traitent du mapping qui est très différent de la transformation des bases de données relationnelles d'ontologies, comme le montre la Figure suivante :



(A) Correspondance entre les bases de données relationnelles et l'ontologie.



(B) la transformation des bases de données relationnelles à l'ontologie

Figure 49 Mapping / transformation

La différence est que le Mapping suppose l'existence à la fois d'une base de données relationnelle et une ontologie et produit un ensemble de correspondances entre les deux.

Autrement dit, les entrées au mapping sont à la fois une base de données relationnelle et une ontologie, et en sortie un ensemble de correspondances qui décrit la construction de l'ontologie en base de données relationnelle.

La transformation suppose que seule une ontologie existe, la base de données relationnelle sera alors produite à partir de l'ontologie. En entrée de la transformation, nous avons l'ontologie et en sortie une base de données relationnelle.

Il existe plusieurs approches à la transformation des ontologies aux bases de données relationnelles. Cependant, toutes ces approches souffrent d'un ou plusieurs problèmes:

• Ils ignorent les restrictions de capture supplémentaires sémantique.

• Ils ne sont pas mises en œuvre.

•Ils sont semi-automatique (c'est à dire qu'ils demandent une interaction avec l'utilisateur).

• Ils n'analysent pas la perte causée par la transformation de la structure. Plutôt, ils supposent que toutes les constructions d'une ontologie peuvent être mappées à une base de données relationnelle.

Pour résoudre ces problèmes, une approche de la transformation des ontologies en bases de données relationnelle, a été développé par Irina Astrova, Nahum Korda et Ahto Kalja [Astrova et al, 2007] avec une ontologie écrite en langage standard d'ontologie OWL[OWL,2004] ; et une base de données relationnelle déclinée en SQL [SQL, 2011].

5.4 Module transformation:

Une ontologie est considérée comme une mise en œuvre d'un modèle ontologique. Ce modèle comprend des constructions pour préciser les catégories, les propriétés, les types de données, l'héritage, les restrictions et éventuellement d'autres sémantiques. Cependant, l'ontologie n'a pas besoin d'inclure toutes les constructions du modèle ontologique (c'est à dire qu'elle peut utiliser seulement une partie du modèle ontologique).

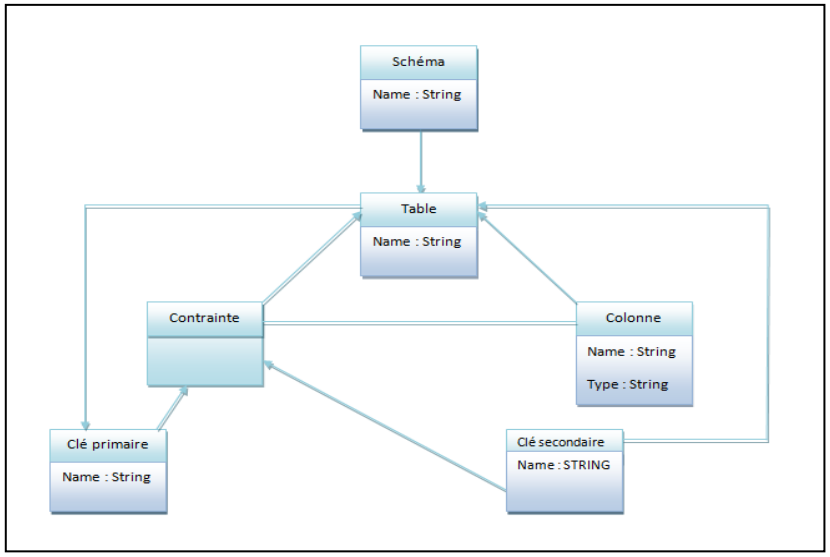


Figure 50 Modèle relationnel

De même, une base de données relationnelle est considérée comme une mise en œuvre d'un modèle relationnel. Ce modèle comprend des constructions pour les tableaux précisant : colonnes, types de données, contraintes et d'autres sémantiques, comme le montre la Figure ci-dessus Cependant, la base de données relationnelle n'a pas besoin d'inclure toutes les constructions du modèle relationnel (c'est à dire qu'elle peut utiliser seulement une partie du modèle relationnel).

La transformation des ontologies en bases de données relationnelles est basée sur un ensemble de règles appelées *règles de correspondance* qui indiquent comment passer du modèle ontologique au modèle relationnel.

Les règles de correspondance sont ensuite appliquées à une ontologie (source) pour produire une base de données relationnelle (cible).Puisque les règles de correspondances sont précisées sur le niveau du modèle, elles sont applicables à toute ontologie qui est conforme au modèle ontologique.

Pour ce qui est des règles de correspondance, le document développé par Irina Astrova, Nahum Korda et Ahto Kalja [Astrova et al, 2007] donne 12 règles de correspondance afin de passer d'une ontologie à une base de données relationnelle.

Ces auteurs ont développé un outil QUALEG qui, en utilisant ces règles, permet de transformer une ontologie en base de données relationnelle.

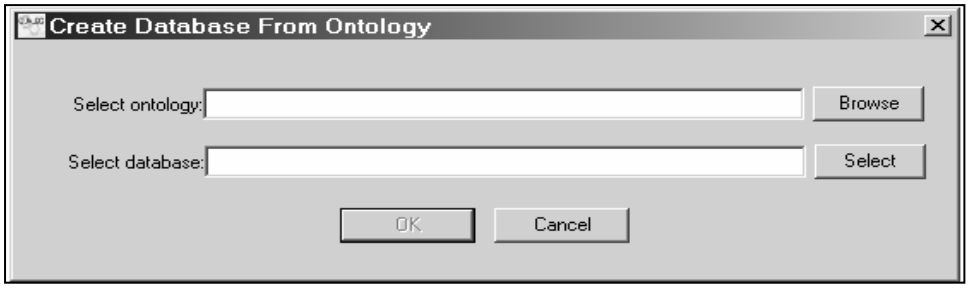


Figure 51 Interface QUALEG pour la transformation

Notre module transformation reprend donc l'interface Qualeg, qui est la solution la plus aboutie que nous ayons trouvé et qui permet de passer d'une ontologie éxistante à une base de données relationnelles, dont le modèle est représenté dans la figure suivante. Ce module comprend quelques améliorations possibles comme par exemple la prise en charge de nom d'objet composé autreement lié que par le caractère '_'.

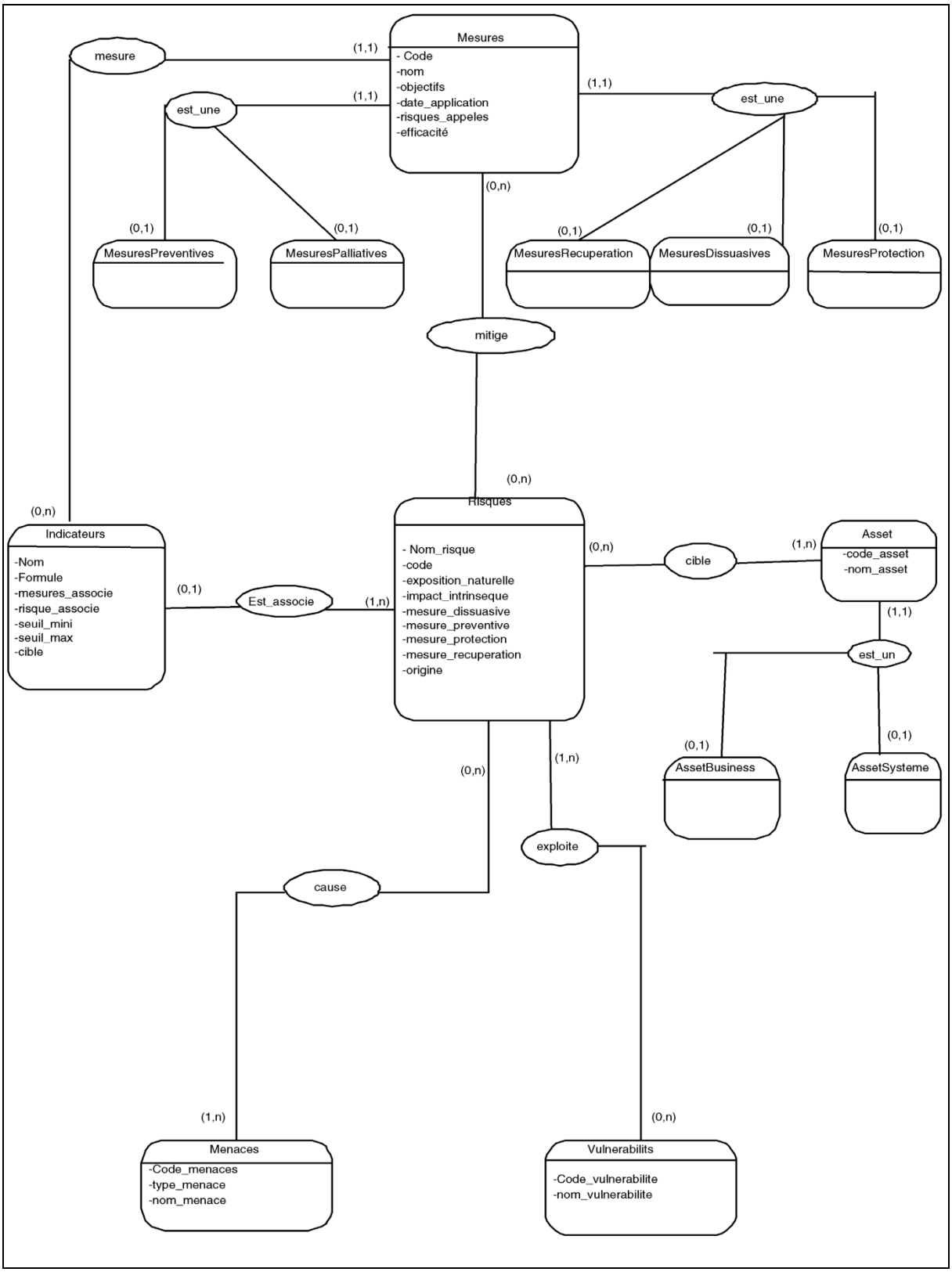


Figure 52 Modèle relationnel issu de Qualeg

6. Module d'aide à la décision :

L'objectif du module d'aide à la décision est d'assister l'expert dans le choix des mesures de contrôle appropriées à mettre en place dans une entreprise. L'étape première nous a conduit à trouver un modèle mathématique représentant cette problématique.

6.1 Modélisation mathématique pour la détermination des solutions efficaces :

La première tâche dans l'approche utilisée réside dans la détermination de la solution efficace possible ; une tâche qui constitue techniquement un problème d'optimisation combinatoire multi objectif(OCMO).

Résoudre ce problème consiste à identifier la combinaison efficace des contrôles pour laquelle les variables binaires $x_i \in \{0,1\}$ indiquent si oui ou non La $i^{ème}$ mesure est sélectionnée ($x_i = 1$ si c'est le cas, et $x_i = 0$ autrement).

Exemple : $x_i \in \{0,1\}$ ou x_i représente un garde au niveau de l'entrée 1

$x_i = 1$ si il y a effectivement un garde d'affecté à l'entrée 1, et $x_i = 0$ autrement

Une solution peut être représentée en tant que vecteur x = (x_1,..,x_n), avec n étant le nombre de mesures proposées. Le problème OCMO consiste dans la maximisation des objectifs K (tel que la fonctionnalité, la facilité d'utilisation ou la capacité d'un fournisseur)

$$\text{Maximiser } u_k(x) \quad pour\ k = 1,..,K \qquad (1)$$

- **Les critères de sélection**

Les critères définis dans cette section peuvent servir comme mesure à l'évaluation des contre mesures candidates. En raison de la nature de notre approche multicritères, un ensemble de critères est nécessaire et doit être en phase avec les objectifs stratégiques de l'entreprise.

Outre l'objectif principal de l'entreprise à réussir à savoir le processus de certification, elle s'intéresse à la mise en œuvre des mesures qui couvrent de façon optimale le besoin de protection et un bon rapport coût-efficacité. Par conséquent, l'ensemble comprend des critères financiers et les objectifs connexes de sécurité prises dans la littérature [Avizienis et ali, 2004].

Les critères peuvent être donc :

• **Les coûts initiaux** $q_{ic}(i)$ représentent le montant d'argent qu'une entreprise doit investir afin d'intégrer une mesure i dans son environnement.

• **Les frais de fonctionnement** $q_{rc}(i)$ dépendent soit des coûts d'entretien soit du nombre de demandes (requêtes).

• **l'efficacité** [BJA, 2011] est définie comme la capacité à atteindre les objectifs fixés, jugée en termes de résultats et impact. Bien que nos implémentations potentielles de contremesures ne soient pas directement liées à une menace spécifique, leur efficacité peut être évaluée en fonction de leur objectif principal. Par exemple, le but principal d'un détecteur d'incendie est de détecter les incendies et le taux de son efficacité repose sur sa capacité à détecter les incendies. Au ce stade de la recherche, nous ne considérons pas les effets secondaires des mesures (par exemple, le but primaire d'un gardien de sécurité est d'empêcher l'accès non autorisé, mais il est également en mesure de détecter un incendie).

• **la Continuité** est une caractéristique de la conception et de l'installation, exprimée en probabilité qu'un objet sera conservé ou remis dans un état spécifié dans un laps de temps donné, lorsque la maintenance est effectuée conformément aux procédures et les ressources prescrites [FED, 2008].

• **La fiabilité** est définie par l'IEEE comme la capacité d'un système ou un composant à effectuer ses fonctions requises dans des conditions déterminées pour une période de temps déterminée (à partir de 0 à t).

Une analyse approfondie doit être menée par un expert sur l'ensemble des critères. Notons que selon que les critères peuvent être mesurés en "unités réelles" (par exemple, les unités monétaires, unités de temps ou de la consommation de ressources mesurables), des échelles différentes seront appliquées. Si une catégorie peut être mesurée en utilisant un nombre discret qui se rapporte à une unité réelle, les candidats sont affectés à leur valeur absolue. Dans le cas contraire (à savoir, dans le cas des actifs incorporels tels que la continuité), une échelle abstraite de points qui varie de 0 à 10 est utilisée.

Les fonctions objectives se référant à des critères qui devraient naturellement être minimisés (par exemple les coûts) peuvent facilement être transformées en **multipliant** simplement la valeur de l'objectif par **(-1)**.

Les fonctions $u_k(x)$ peuvent prendre n'importe quelle forme (linéaire, non linéaire, etc.) tant qu'elles sont définies pour tous x (réalisables) alternatives. Enfin, il convient de reconnaitre que la recherche des fonctions propres pour des critères tels que la disponibilité attendue d'une combinaison donnée de contrôle peut s'avérer délicate ; cependant, cette difficulté est de même degré que pour les autres approches décisionnelles.

Toute procédure appliquée dans cette phase est destinée à identifier ou au moins à fournir une approximation de l'ensemble des solutions efficaces. Bien sûr, toutes les solutions prises en considération doivent être réalisables en ce qui concerne deux ensembles de contraintes.

Le premier ensemble (2) se rapporte aux ressources limitées par exemple, les coûts initiaux ou les coûts en cours d'exécution.

Pour les variables de décision binaire x_i les contraintes peuvent être simplement formulées comme suit :

$$\sum_i r_{iq} x_i \leq R_q \quad \text{pour q = 1,..Q (2)}$$

où r_{iq} représente le montant des ressources de type q requis par la mesure i et R_q représente le montant maximum disponible de ressources.

Le deuxième ensemble (3) assure qu'au plus un maximum (ou au moins un minimum) de nombre de mesures d'un sous-ensemble données est inclus dans des solutions réalisables. Par exemple, une contrainte peut exiger qu'au moins deux mesures définies (en référence aux mesures correspondantes ayant été affecté aux indices 1 à 6) mais pas plus de quatre mesures ne doivent être sélectionnées et, par conséquent, prend la forme

$$2 \leq \sum_{I=1}^{6} x_i \leq 4 \quad (3)$$

En outre, il peut être demandé que par un ensemble donné de dix contremesures (ayant pour indice de 1 à 10) qui répondent à des exigences identiques, un seul est inclus dans le portefeuille final et qui peut conduire à une autre contrainte

$$\sum_{i=1}^{10} x_i \leq 1 \quad (4)$$

En conséquence, les décideurs peuvent veiller à ce que certaines mesures devraient être sélectionnées en combinant les unes avec les autres (par exemple, la norme exige l'utilisation combinée d'un agent de sécurité et un système d'accès) et / ou ils peuvent prendre compte du fait que leur combinaison donne des effets de synergie (par exemple, l'utilisation de deux mesures d'un même fournisseur peut entraîner une réduction des coûts). D'autres contremesures s'excluent mutuellement

(par exemple, des mesures qui offrent exactement la même fonctionnalité) ou causer des **effets cannibalismes**. Par exemple, l'utilisation d'une mesure remplissant une partie seulement de la fonctionnalité nécessaire, pourrait exiger l'utilisation d'une deuxième mesure et donc se traduirait par des coûts plus élevés ou performance réduite voir [Stummeret al, 2003].

6.2 Le modèle mathématique :

Soit $x_i \in \{0,1\}$ variable binaire indiquant si oui ou non La i^{ème} mesure est sélectionnée (x_i = 1 si c'est le cas, et x_i = 0 autrement).

$$\begin{cases} \text{aximiser } u_k(x) \quad pour\ k=1\ ,..,K\ (1) \\ \sum_i r_{iq} x_i \leq R_q \quad pour\ q = 1,..,Q\ (2) \\ 2 \leq \sum_{l=1}^{6} x_i \leq 4 \quad (3) \\ \sum_{i=1}^{10} x_i \leq 1\ (4) \end{cases}$$

6.3 Proposition de résolution :

Dans cette phase, le décideur a besoin d'aide dans le choix de la solution finale qui correspond le mieux à ses attentes parmi les centaines de solutions efficaces de rechange identifiées.

Pour résoudre le problème de choix des mesures, nous proposons l'utilisation d'une méta-heuristique, plus précisément d'un algorithme génétique (AG). [Holland, 1975]. L'approche utilisée est basée sur les modifications des entrées 'valeur de critères' conformément à la préférence du décideur, le système fournit un retour d'information immédiat sur les conséquences de ces choix en termes de solutions restantes.

En effet, les algorithmes génétiques sont l'œuvre de Holland [Holland, 1975]. Il s'est directement inspiré du modèle des lois de la nature de Darwin, modèle basé sur la survie des espèces les plus fortes, il génère une population et par un processus de sélection, il choisit les meilleurs individus de chaque génération jusqu'à ce qu'une des conditions d'arrêt soit vérifiée.

Une des premières applications des AG dans le domaine d'ingénierie fut proposée par Goldberg en 1989 pour l'optimisation et l'apprentissage d'un processus de contrôle de gazoducs. Dés lors et grâce à leur simplicité de calcul et leurs performances, l'apprentissage et l'optimisation par les AG

sont devenus des processus de recherches efficaces qui permettent de s'approcher de la solution optimale. Il semble ainsi que l'AG soit approprié à notre problème.

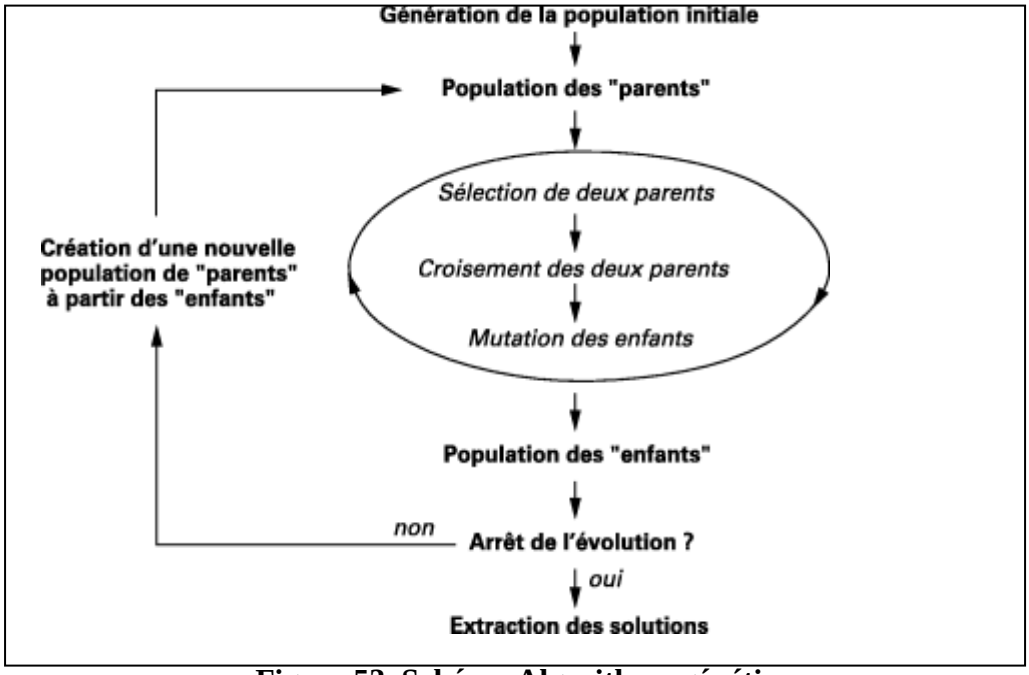


Figure 53 Schéma Algorithme génétique

6.4. Algorithme Génétique

Pour tenir compte de l'aspect multicritère, nous avons retenu ici l'approche proposée par Dietz, [Dietz, 2004], dans laquelle les aspects multicritères sont pris en compte lors de l'étape de sélection et la recherche de solutions de compromis lors de l'étape de croisement. La procédure de sélection étant faite à l'aide de la roulette de Goldberg, on a défini une roulette pour chaque critère à optimiser. Un nombre égal d'individus est sélectionné pour compléter le nombre total des individus qui passeront d'une population à la suivante. La procédure de croisement, chargée de proposer des solutions de compromis n'est pas modifiée.

Les paramètres d'entrée de cet algorithme sont :

- Nombre d'itérations de l'algorithme.
- Nombre d'états minimum.
- Nombre d'états maximum.
- Nombre S' de parents de l'itération t utilisés pour générer les enfants de l'itération t+1
- Probabilité de mutation.

Etape : Initialisation

- Un individu est l'ensemble
- de variable $x_i \in \{0,1\}$ 

  Représentant les mesures sélectionnées.
- Créer une population aléatoirement et vérifier la réalisabilité de chaque individu ; si un individu ne vérifie pas les contraintes, on le supprime. A la fin de cette étape, la population doit être de taille S.
- Aucun individu n'est marqué « parent ».

Un mécanisme de génération de la population initiale doit être établi. Ce mécanisme doit être capable de produire une population d'individus non homogène qui servira de base pour les générations futures.

La stratégie choisie pour la création de la population initiale consiste en une génération aléatoire des individus, en partant du principe que la position de l'optimum dans l'espace de recherche est complètement inconnue. Cette méthode présente l'avantage de proposer une population variée, assurant un bon recouvrement de l'espace de recherche. Elle permet de générer une population acceptable, quand aucune information n'est a priori disponible sur la localisation de l'optimum.

Etape : Sélection

La procédure de sélection étant faite à l'aide de la roulette « wheel selection », on doit définir une roulette pour chaque critère à optimiser.

Pour rappel, le principe de roulette « wheel selection » consiste à associer à chaque individu un segment dont la longueur est proportionnelle à sa valeur de fonction objective.

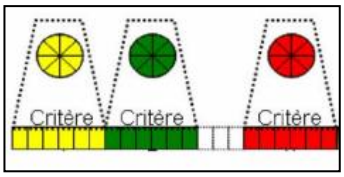


Figure 58

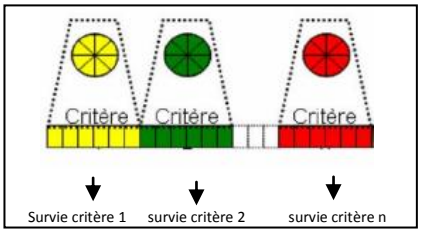
$$FITNESS = \frac{u_k(x_i)}{\sum_{i=1}^{N} u_k(x_i)}$$ Pour chaque critère k

Parmi tous les individus de la population, on sélectionne un certain nombre S'<S, qui seront utilisés comme parents pour régénérer les S - S', ceux-là sont les individus non retenus.

La sélection se réalise suivant les meilleurs scores calculés.

Etape : Croisement

- Pour chaque critère, un nombre égal d'individus est sélectionné pour compléter le nombre total des individus qui passeront d'une population à la suivante.



- Pour chaque individu non marqué « parent », le remplacer par un des fils obtenus après croisement de deux individus « parents » sélectionnés au hasard.
- La sélection d'un des deux fils obtenus après croisement se fait au hasard.

Etape : Mutation & Normalisation

- Sur chaque individu non marqué « parent » on applique l'opérateur de mutation. On lui applique ensuite l'opérateur de normalisation, afin que cet individu soit réalisable.

Etape : Evaluation

- Appliquer sur chaque individu de la population non marqué « parent » une évaluation selon les critères sélectionnés.
- Pour chaque individu marqué « parent » enlever cette marque.

Etape : Vérification des conditions d'arrêt

- Si le nombre d'itérations maximum n'est pas atteint, alors continuer, sinon aller à « terminaison ».

Etape : Recommencer une évolution

- Retourner à l'étape.

Etape : Terminaison

- Renvoyer la meilleure solution contenue dans la population en cours.

Soit F l'espace de solutions réalisable délimité par les contraintes.

On considère qu'un point $x^* \in F$ est Pareto optimal si pour chaque $x \in F$

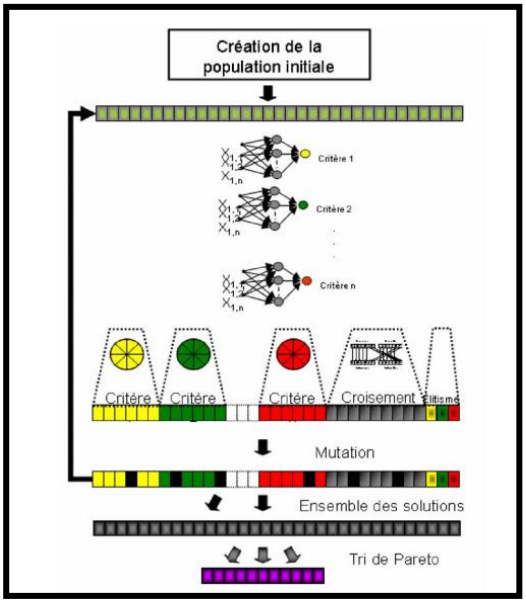
$\forall k \in I \ \left(u_k(x*) = u_k(x)\right) \quad avec \ k = (1,..,n)$

$Ou\ u_k(x*) > u_k(x)$

En d'autres termes, cette définition dit que x est Pareto optimal s'il n'existe aucun vecteur faisable

x qui fasse diminuer un critère sans augmenter dans le même temps au moins un autre critère.

Cependant, dans la plupart des cas, l'optimum de Pareto n'est pas constitué d'une seule solution mais d'un ensemble de solutions appelées solutions non-dominées au sens de Pareto.



7. Conclusions

Dans ce chapitre, nous avons décrit notre approche qui consiste à démarrer d'une ontologie, pour arriver à un programme d'aide à la décision, en passant par une base de données relationnelle.

Ce programme d'aide à la décision est en fait un Programme linéaire qui modélise les attentes d'une entreprise lors de la mise en place d'un SMSI,(norme ISO27001)

Conclusion générale

Le dilemme majeur de la sécurité des systèmes d'information est qu'aucune garantie absolue ne peut être donnée. La seule manière totalement efficace de protéger un système consiste à ne pas y concéder l'accès de quelque manière que ce soit. Toute manière d'accéder au système peut potentiellement devenir une porte d'accès non autorisée.

La plupart des entreprises s'abstiennent de mettre en œuvre des normes de sécurité, entre autres raisons à cause de l'absence de méthodes de mesure du rapport coût /avantages des implémentations

Le but de ce projet est de définir une méthodologie de gestion de la sécurité de l'information en incluant la gestion du risque. Le recours aux normes internationales semble être une réponse aux attentes des entreprises en matière de sécurité.

La conformité par rapport à la norme ISO 27001 permet de garantir aux entreprises d'atteindre un niveau de sécurité appréciable. Néanmoins, ceci nécessite un travail fastidieux vu la consistance de la norme d'une part et les relations de chevauchement qui existent entre les différentes mesures préconisées par la norme d'autre part.

Nous avions deux problématiques auxquelles nous devions répondre:

1 Tester la conformité d'une entreprise donnée par rapport à la norme.

2 Aider l'entreprise à choisir les meilleures mesures de sécurité préconisées par la norme.

Ce travail nous a permis d'offrir à l'auditeur, un outil automatique permettant de collecter les différentes réponses aux interrogations posées par la norme, d'analyser ces réponses et enfin rédiger un rapport d'audit.

Dans un premier temps, notre travail avait pour référentiel la norme ISO27001, notre développement granulaire des mesures de sécurité nous a amené par la suite à utiliser la norme ISO 27002 comme complément et deuxième référentiel.

S'inspirant des normes ISO27OO1 et ISO27002, un questionnaire a été implémenté dans un outil, ce dernier comporte deux modules : expert et auditeur, qui permettent d'implémenter un ensemble de données, de les structurer afin qu'un rapport d'audit puisse être établi en sortie.

Dans la deuxième étape, nous avons proposé une approche de système d'aide à la décision reposant sur une formulation mathématique et une résolution par les algorithmes génétiques pour déterminer des solutions efficaces.

Les solutions proposées peuvent aider considérablement l'auditeur ou tout expert en sécurité afin d'évaluer le niveau de conformité d'une entreprise donnée par rapport à la norme ISO.

Cela donnera aux décideurs un instrument qui leur permettra de donner des mesures tangibles basées sur les descriptions abstraites des contrôles de l'ISO 27001.

L'approche proposée est de créer un processus qui démarre d'une ontologie de sécurité basée sur la norme ISO27001 qui comprend les connaissances sur la sécurité y compris les relations entre les menaces, les vulnérabilités, les mesures, et les biens de cette ontologie et à travers un outil existant que nous avons présenté dans ce document, nous passons vers une base de données relationnelle.

L'utilisation des données de la base relationnelle a permis de modéliser le domaine de la sécurité IT de manière standardisée et l'intégration normalisée des règles qui sont nécessaires pour modéliser les combinaisons de mesures possibles.

Nous avons développé une modélisation mathématique multi-objective afin de trouver un ensemble de solutions optimales.

Nous pouvons suggérer un certain nombre de perspectives, à savoir :

- ✓ implémenter un programme permettant de soutenir la certification ISO 27001 dans l'aspect le plus global.
- ✓ Améliorer le processus proposé.
- ✓ Examiner les dépendances entre les mesures et vulnérabilités afin de garantir que les effets secondaires des mesures potentielles soient considérés.

Bibliographie

[Akio, 1986]	Morita, Akio. *Made in Japan*, New York: Dutton, ISBN 0451151712 1986.
[Arief et Besnard, 2003]	Arief, B., Besnard, D.: Les questions techniques et humaines dans les systèmes de sécurité-ordinateur. Rapport n ° CS-TR 790, 2003.
[Anderson, 1980]	J. P. Anderson, Computer Security Threat – Monitoring and Surveillance, J. P.Anderson CO. Technical report, Fort Washington, Pennsylvania, 1980
[Astrova et al, 2007]	I. Astrova, A. Kalja, et N. Korda, «Storing OWL ontologies in SQL3 object- relational databases », *Conférence européenne IADIS, 2007.*
[Avizienis et al, 2004]	Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing 1(1), 11–33 (2004)
[Barthélémy et Quibel, 2000]	B.Barthélémy, J.Quibel Gestion des risques de l'entreprise, 2000.
[BJA, 2011]	Bureau of Justice Assistance: Center for Program Evaluation - Glossary.Onlinehttp://www.ojp.usdoj.gov/BJA/evaluation/glossary/glossary_c.h Dernier accès septembre 2011.
[Blanco et al, 2008]	Blanco, C., Lasheras, J., de Valence-Garcia, R., Fernandez-Medina, E., Toval, A., Piattini,M.: Un examen systématique et la comparaison des ontologies de sécurité. Dans: Proc. de la troisième Conférence internationale sur la disponibilité, fiabilité et sécurité, p. 813-819 (2008)
[CERIST, 2011]	CERIST, document interne, 'Chaine d'événements enclenchés par un agent de menace', 2011.
[Dacier, 1994]	M. Dacier, Vers une évaluation quantitative de la sécurité, Thèse de doctorat, Rapport LAAS n° 94488, 1994.
[Deswarte, 2003]	Y. Deswarte, "La sécurité des systèmes d'information et de

	communication, in Sécurité des réseaux et des systèmes répartis", Hermès, ISBN : 02-7462-0770-2, 2003
[Dietz, 2004]	Dietz A. Optimisation multicritère pour la conception d'ateliers discontinus multi produits: aspects économique et environnemental, Thèse de doctorat, INP ENSIGC Toulouse, France, 2004.
[EBIOS, 2006]	EBIOSv2-Présentation-Décideurs-2006-11-27 Téléchargeable à l'adresse suivante http://www.ssi.gouv.fr
[FED, 2008]	Federal standard 1037c. URL http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm, dernier accès septembre 2011
[Fenz et Ekelhart, 2009]	Fenz, S., Ekelhart, A.: La formalisation des connaissances sécurité de l'information. Dans: Proc. de la 4e In-Symposium international s l'information, sécurité informatique et des communications, p. 183 194, 2009.
[Goeken et Alter, 2009]	Goeken, M., Alter, S.: Vers la métamodélisation conceptuel de la TI-cadre de gouvernance œuvres. Approche - Utilisation - Avantages. Dans: Proc. annuel Hawaii 42e Conférence sur la Sciences des systèmes, Hawaii 2009
[Gruber, 1993]	Gruber, T.: A translation approach to portable ontology specifications. Knowledge Acquisition 5(2), 199–220 (1993). DOI http://dx.doi.org/10.1006/knac.1993.1008
[Guarino, 1998]	Guarino, N. Some Ontological Principles for Designing Upper Level Lexical Resources. *In:* Proceedings of First International Conference on Language Resources and Evaluation. Granada, Spain, 1998.
[HADOPI, 2009]	La loi Hadopi république française ou loi Création et Internet ou plus formellement « loi n°2009-669 du 12 juin 2009». Cette loi fait suite à la directive européenne 2001/29/CE transposée en droit français par la loi DADVSI qui cherche spécifiquement à protéger les droits d'auteur sur Internet, 2009.
[Holland, 1975]	Holland, J. (1975). Adaptation in Natural and Artifial

	Systems, University of Michigan Press. Ann Arbor, Michigan. 1975
[ISO7493, 1989]	ISO7493, Système de l'information, Modèle de référence de base des applications avancées, 1989.
[ISO7498, 2000]	ISO7498, Systèmes de traitement de l'information -- Interconnexion de systèmes ouverts, Modèle de référence de base, Partie 2: Architecture de sécurité, 2000
[ISO17799, 2005]	International Organization for Standardization and International Electrotechnical Commission: ISO/IEC 17799:2005, information technology – code of practice for information security management, 2005.
[ISO270001, 2005]	International Organization for Standardization and International Electrotechnical Commission: ISO/IEC 27001:2005, information technology – security techniques –information security management system-requirements, 2005.
[ISO27002, 2008]	NA ISO CEI 27002 Techniques de sécurité : Code de bonne pratique pour la gestion de la sécurité de l'information IANOR http://www.ianor.org , 2008.
[Karyda et al, 2006]	Karyda, M., Balopoulos, T., Dritsas, S., Gymnopoulos, L., Kokolakis, S., Lambrinoudakis, C., Gritzalis, S.: Une ontologie pour l'e-gouvernement application de sécurité. Dans: Proc. de la première Int. Conférence sur la disponibilité, de fiabilité et de sécurité de 2006, pp 1033-1037, 2006.
[Lee et al, 2006]	Lee, S.-O., Gandhi, R., Muthurajan, D., Yavagal, D., Ahn, G.-J.: problème de construction ontologie principale des exigences de sécurité dans les documents réglementaires. Dans: Proc. de 2006 Atelier international sur le génie logiciel pour systèmes sécurisés. ACM, Shanghai, 2006.
[MEHARI, 2007]	MEHARI 2007 (Principes et mécanisme) – 2007

[Mouratidis et al, 2003]	Téléchargeable à l'adresse suivante : https://www.clusif.asso.fr/fr/production/mehari/ 2007. Mouratidis, H., Giorgini, P., Manson, G.: Une ontologie pour la modélisation de sécurité: Le Tro- pos approche. Dans: Palade, V., Howlett, RJ, Jain, V (dir.) basée sur la connaissance intelligente Systèmes d'information et d'ingénierie. LNCS (LNAI), p. 1387-1394. Springer, Heidelberg- berg, 2003.
[Nguéna, 2008]	Octave Jokung Nguéna, Management des risques, Edition ellipse, 2008.
[OCTAVE, 2003]	Introduction to the OCTAVE® Approach – Aout 2003 Téléchargeable à l'adresse suivante : www.cert.org/octave/approach_intro.pdf 2003.
[OCTAVE, 2007]	OCTAVE, accéssible à l'adress suivante www.cert.org/octave/ dernier accès, juillet 2010.
[OWL, 2004]	World Wide Web Consortium: OWL - Web Ontology Language http://www.w3.org/TR/owlfeature 2004.
[Raskin et al, 2001]	Raskin, V, Hempelmann, CF, Triezenberg, KE, Nirenburg, S.: Ontologie de l'information la sécurité: un fondement utile théorique et outil méthodologique. Dans: Proc. de 2001 Atelier sur les nouveaux paradigmes de sécurité, 2001.
[SPARQL, 2008]	SPARQL Query Language de RDF , *A. Seaborne, Prud 'hommeaux E. rédacteurs, recommandation du W3C, 15 Janvier 2008, http://www.w3.org/TR/2008/REC-rdf-sparql-query-20080115/ Dernière version disponible à http://www.w3.org/TR/rdf-sparql-query/ 2008.*
[Stummer et Heidenberger, 2003]	Stummer, C., Heidenberger, K.: Interactive R&D portfolio analysis with project interdependencies and time profiles of multiple objectives. IEEE Transactions on Engineering Management 50(2), 175–183, 2003.
[Tsoumas et Gritzalis, 2006]	Tsoumas, B., Gritzalis, D. Vers une ontologie à base de gestion de la sécurité. Dans: Proc. Des Int 20. Conférence sur

[Whitson, 2003]	le Réseau de l'information, 2006. G. Whitson, Computer Security: Theory, Processes and Management, Consortium for Computing Sciences in Colleges, JCSC 18, 2003.