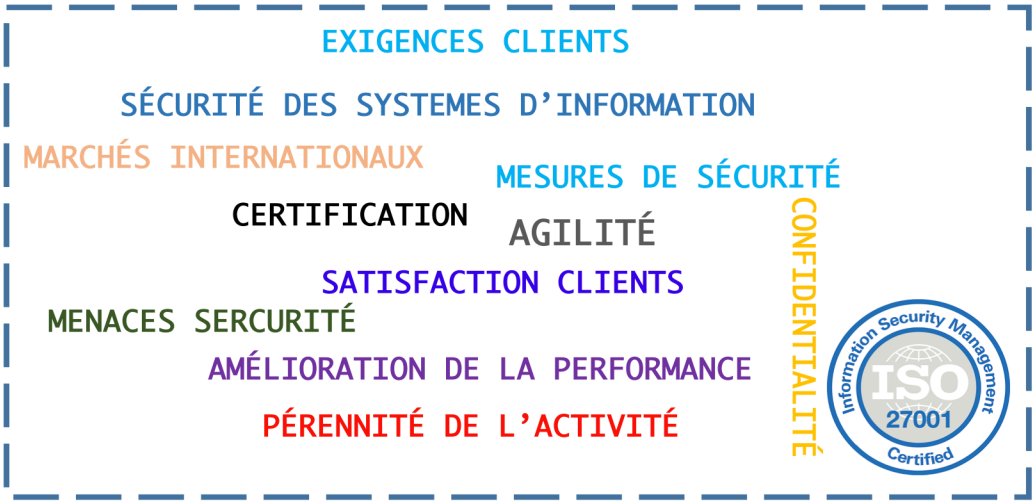
www.utc.fr/master-qualite, puis "Travaux" "Qualité-Management", réf n°403

Du management agile à la certification ISO 27001 version 2013



Mémoire d'Intelligence Méthodologique, Master 2 QPO

NAIT-OUSLIMANE SARA

MASTER 2 QUALITE ET PERFORMANCE DANS LES ORGANISATIONS, Juin 2017

TUTEUR UTC : M. GILBERT FARGES

RESUME

De nos jours, les démarches de progrès sont omniprésentes, elles sont devenues une priorité pour les entreprises qui ont pour vocation de garantir un niveau de qualité et de sécurité irréprochable des services offerts, et une meilleure performance, efficacité, voir efficience dans leurs organisations internes et externes.

L'information étant un actif précieux dans l'entreprise, il est nécessaire d'assurer et de garantir sa protection et son intégrité contre toute perte ou intrusion. De nos jour les menaces sur ces données sensibles sont plus répandues que jamais, ce qui a amplifié le besoin d'assurer l'intégrité, la confidentialité et la disponibilité de l'information. Les entreprises doivent à cet effet garantir la sécurité optimale de leurs systèmes d'information en s'investissant davantage dans des mesures de sécurité et de protection. Cela impose aux organisations de faire que la sécurité soit leur priorité et se lancer de plus en plus dans les démarches « sécurité de l'information » visant ainsi à sécuriser leurs systèmes d'information et gérer tous les aspects liés aux échanges d'information y compris la sécurité du périmètre physique des collaborateurs au sein de l'entreprise. Leur but est d'assurer la pérennité de leurs activités ainsi que renforcer le climat de confiance dans la collaboration avec les différentes parties intéressées.

Afin de faciliter la mise en œuvre d'un SMSI dans un contexte agile ou le maintien de certification ISO 27001, un outil de mesure a été réalisé. Cet outil permettra aux organisations quels que soient leurs types, ou leurs activités d'appréhender les exigences de « l'annexe A » de la norme et le déploiement des mesures de sécurité d'une manière facile et rapide et de mesurer ainsi les écarts et proposer des axes de progrès.

Mots clefs : certification, ISO 27001, système de management de sécurité de l'information, SMSI, DdA, Agilité

Abstract

Nowadays, progress is pervasive and has become a priority for companies who claim to guarantee an irreproachable level of quality and safety of services on the one hand, and better performance, efficiency, efficiency and Their internal and external organizations on the other side.

Since information is a valuable asset in the company, it is necessary to ensure and guarantee its protection and integrity against any loss or intrusion. Today, threats to these sensitive data are more widespread than ever before, amplifying the need to ensure the integrity, confidentiality and availability of information. To this end, companies must ensure the optimal security of their information security systems by investing more in security and protection measures. This requires organizations to make security their priority and to embark more and more on "information security" approaches aimed at securing their information systems and managing all aspects related to the exchange of information therein. Including the security of the physical perimeter of employees within the company. And the aim is to ensure the sustainability of their activities as well as to strengthen the climate of trust in the collaboration with the various interested parties.
In order to facilitate the implementation of a ISMS in an agile context or the maintenance of ISO 27001 certification, a measurement tool has been developed. This tool will enable organizations of all types and activities to understand the requirements of Annex "A" to the standard and to deploy security measures in a quick and easy manner and to measure gaps and Propose areas for progress.

Keywords : certification, ISO 27001, Information Security Management System, ISMS, SoA, Agility

REMERCIEMENTS

Avant d'aller plus avant, je tiens à remercier vivement mon tuteur, pour son accompagnement, son accueil, et sa disponibilité à mon égard.

Je remercie aussi Steeve Leger pour avoir répondu à toutes mes questions tout au long de ma période de stage. Je remercie également les différents acteurs de la société, pour leur bel accueil, leur humour, et leur ambiance agréable et amicale. Ils m'ont appris que l'efficacité est l'alliance parfaite entre l'humain, le respect de l'autre et le travail collectif.

Je tiens à exprimer ma reconnaissance à mes responsables de Master QPO, M. Gilbert Farges et M. Arnaud Derathé de m'avoir accordé la chance et l'opportunité d'intégrer le Master QPO, pour leurs précieux conseils, pour leur disponibilité et leur encadrement.

Enfin, je tiens à remercier ma famille et mes amis, pour leur encouragement et leur confiance.

Merci à tous !

A Massi,

TABLE DES MATIERES

SIGLES

ISO : Organisation internationale de normalisation
TIC : Technologies de l'information et de la communication
SMI : Système de Management Intégré
SMSI : Système de Management de la Sécurité de l'Information
PDCA : Plan, Do, Check, Act
ISO : International Organization for Standardization
SGSI : Système de Gestion de la Sécurité de l'Information
SWOT : Strength, Weakness, Opportunity, Threat
RSSI : Responsable de Sécurité des Systèmes d'Information
QQOQCP : Qui, Quoi, Ou, Quand, Comment, Pourquoi
PDS : Planification Dynamique Stratégique
GED : Gestion Électronique Documentaire
SI : Système d'Information
DdA : Déclaration d'Applicabilité

GLOSSAIRE

- **ISO :** est une organisation internationale non gouvernementale, indépendante, dont les 163 membres sont les organismes nationaux de normalisation. [1]
-
- **Processus :** Ensemble d'activités interactives qui transforment des éléments d'entrée en éléments de sortie. [2]
- **Non-conformité :** Non-satisfaction d'une exigence.

- **Certification :** Procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus ou un service est conforme aux exigences spécifiées. La certification vise à reconnaître que l'organisme postulant fait fonctionner son système de management conformément à une norme internationale. [3]

- **Système d'information :** Un SI est un « ensemble d'éléments (personnel, matériel, logiciel…) permettant d'acquérir, traiter, mémoriser et communiquer des informations. [4]

- **Parties intéressées :** personne ou organisme qui peut soit influer sur une décision ou une activité, soit être influencée où s'estimer influencée par une décision ou une activité [5]

- **Déclaration d'applicabilité (DdA/SoA)** Déclaration documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées et applicables au SMSI d'un organisme. [6]

- **Annexe A :** est composée d'un ensemble de mesures de sécurité, des mesures qui sont détaillées au sein de la norme ISO 27002 (anciennement ISO/CEI 17799) [7]

TABLE DE FIGURES

INTRODUCTION

Grâce à mon parcours scientifique et mes différentes expériences notamment en banque et en production, j'ai pu acquérir des compétences techniques et managériales, ce qui m'a apporté rigueur et autonomie dans le travail. Étant convaincue des bénéfices des démarches qualité et de la place que ces dernières occupent au sein de l'entreprise, en engendrant une réelle valeur ajoutée en terme d'efficacité et de performance, j'ai décidé d'intégrer le Master 2 Qualité et Performance dans les Organisations de l'UTC en 2015. Une formation complète qui m'a permis d'aborder la qualité dans toute sa globalité.

Aujourd'hui dans le cadre de mon projet de fin d'étude, il nous est demandé de réaliser un stage de 22 semaines minimum au sein d'une entreprise afin de mettre à profit nos connaissances théoriques et développer de solides compétences et de la transversalité dans le domaine de la qualité. Étant passionnée par les technologies. J'ai choisi de réaliser mon stage au sein d'une entreprise de nouvelles technologies, qui se lance dans une démarche de progrès, mon rôle est d'aider et de l'accompagner dans la mise en place d'un système de management intégré SMI. J'ai ainsi pu effectuer plusieurs missions énumérées comme suit :

La mise en place d'une base du système de management de la qualité SMQ selon le référentiel ISO 9001 version 2015
Implémentation une base de management relative à l'environnement (ISO 1400 version 2015)
Déploiement d'un système de mangement de gestion de la sécurité de l'information SMSI selon la norme ISO 27001 version 2013 en vue d'une certification en fin 2018 :

- Création et la gestion documentaire (créer les documents réservés à la sécurité : procédures, cartographie des processus…).
- Accroitre l'image de l'entreprise en terme de respect à la réglementation et aux normes.
- Réduire les risques liés à la sécurité.
- Mise en place des mesures de sécurité.
- La conduite du changement (accompagner, sensibiliser, former).
- Mise à disposition des entreprises un outil d'autodiagnostic pour mesurer l'avancement de la démarche.

Ainsi, pour aider les organismes dans la mise en place de la norme ISO 27001 version 2013, le mémoire suivant propose une méthodologie et un outil de mesure à mettre à disposition de toutes les entreprises dites agiles, afin de leur faciliter le déploiement d'un Système de Management de Sécurité de l'Information.

L'outil présenté ici est un outil gratuit et accessible à tout le monde sur internet. Il a été conçu selon les exigences de « l'Annexe A » de la norme ISO 27001 version 2013, avec une méthode d'évaluation et de mesure qui se veut rapide et simple.

Toutefois, ce mémoire ne traite pas les démarches qualité et environnement, il met en exergue les enjeux de la mise en place d'un système de management de la sécurité des systèmes d'information dans un contexte agile.

Chapitre 1 : Contexte, Enjeux et Problématique

I. Qu'est-ce que l'Agilité ?

Le terme "agilité" s'est peu à peu répandu dans les diverses strates de l'écosystème managérial pour aujourd'hui qualifier le besoin de flexibilité, de réactivité et de renouveau de l'entreprise du XXIe siècle. Une entreprise agile, c'est une entreprise capable de prendre des risques pour conquérir de nouveaux marchés en cohérence avec les nouveaux enjeux sociaux et environnementaux. [8]

L'entreprise agile est une entreprise qui apporte des solutions concrètes et personnalisées à ses clients, qui coopère pour améliorer sa compétitivité, qui s'organise pour maîtriser le changement et l'incertitude, et enfin qui se nourrit de la richesse de ses collaborateurs et de son patrimoine informationnel. [9]

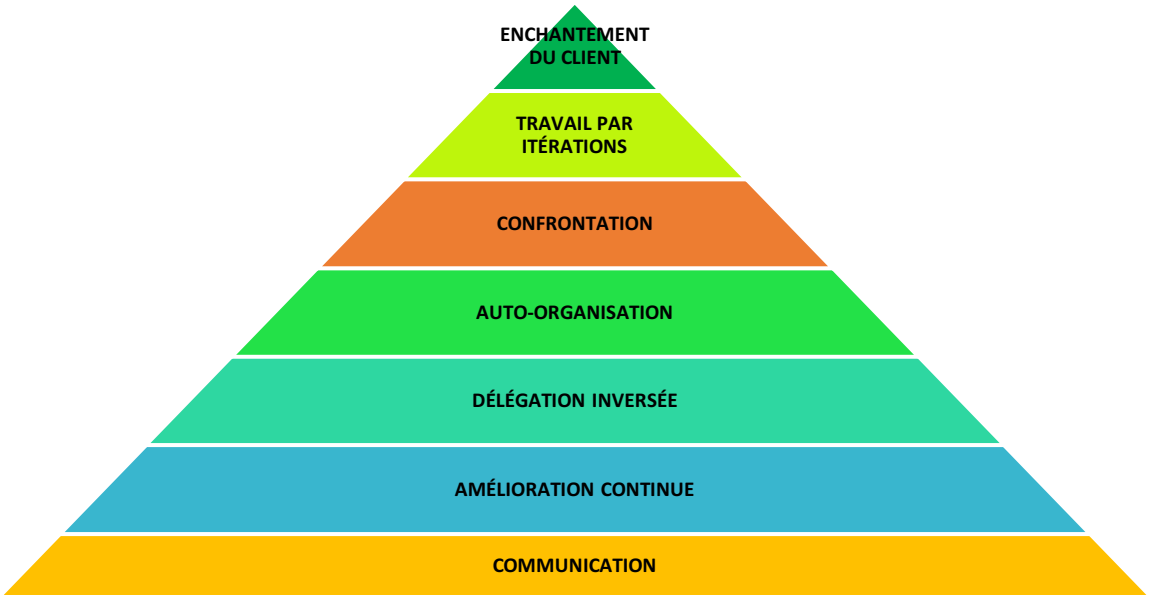


Figure 1: Les 7 principes de l'Agilité [10]

La plus haute priorité des entreprises agiles est l'enchantement du client (Fig.1), par une livraison rapide et continue du service offert. Le client et l'utilisateur final sont le focus ultime du processus tout entier. Les entreprises agiles ont une grande capacité à accommoder d'importants changements du besoin venant du client, de n'importe quel niveau du processus de telle façon à livrer un produit ou service de qualité et dans les temps.

Pour faire face aux perpétuels changements dont les équipes sont confrontées, les entreprises agiles préconisent le travail d'équipe et favorisent le travail ensemble pour casser les silos et le « jeté de besoins par-dessus le mur » des projets.

Le travail en équipe quotidiennement et la communication continue avec le client tout au long du projet est l'une des clés de réussite de ces organisations. L'agilité est donc un modèle stratégique, comportemental et émotionnel. [11]

Une organisation agile est une organisation capable de :

- ⇒ Créer de la valeur tout en s'adaptant à temps aux changements dans son environnement
- ⇒ S'adapter aux imprévus et faire converger les énergies vers le client
- ⇒ Activer l'émergence pour prendre en compte la réalité avec réalité et flexibilité
- ⇒ Réduire les écarts entre "Cycle d'évolution d'un produit/service" et "Processus d'une organisation"

L'agilité ne saurait donc être un état stable et définitif, mais une propension, une aptitude, un cadre général à maintenir et alimenter constamment, Néanmoins, l'agile ne devrait jamais être une excuse pour la mauvaise qualité du produit ou service livré.

« Les personnes qui travaillent vers un but commun parce qu'elles le veulent seront toujours plus efficaces, plus fortes et plus fiables que des équipes travaillant ensemble parce qu'on leur a dit de le faire. » [12]

II. Entreprise d'accueil

Ces dernières années nous sommes rentrés dans une révolution technologique qui est en train de révolutionner et changer radicalement nos habitudes dans tous les domaines de vie. Au moment où les pays développés sont embarqués dans une course à la connectivité 4G, bientôt 5G, les pays émergents ont un accès limité aux TIC et à l'internet notamment aucun accès dans certaines zones d'Afrique et d'Asie, Ceci impacte leur développement et menace leur avenir économique et social. Ces pays ne peuvent donc pas agir dans un monde désormais régi par l'information.

L'entreprise d'accueil qui sera nommée « entreprise BBD » dans ce rapport, est une jeune entreprise qui a su relever le défi en développant une technologie qui offre un service internet partout dans le monde.

L'entreprise est issue de la french-Tech spécialisée dans la télécommunication. Crée en 2011, elle est constituée d'une trentaine de personnes. Elle offre des services internet mobile qui permettent la connectivité partout là où il existe un signal même très faible (sans 3G et 4G). La technologie de l'entreprise se repose sur l'innovation frugale « Faire mieux avec moins ». BBD résume sa mission et sa vision de la manière suivante : « 4 milliards de personnes ne sont toujours pas connectées. Notre technologie apporte la connectivité à tous et partout ». La technologie de BBD utilise un algorithme breveté permettant la compression des data.

II.1 Activités et expertise

BBD est la première entreprise qui offre ce type de solutions de connectivité. En effet, elle conçoit, développe des applications mobiles, met en place et déploie sa technologie au sein de ses clients. Elle assure au travers de ses applications, la connexion à internet dans les quatre coins du monde (Fig.2).

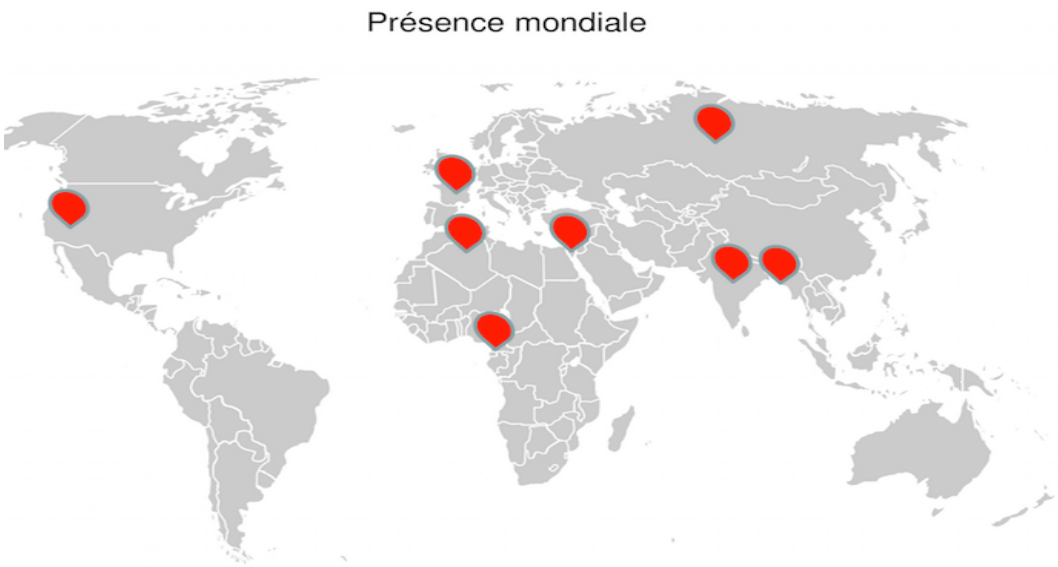


Figure 2: présence mondiale de l'entreprise BBD [Source : Auteur]

II.2 Mode de fonctionnement :

L'entreprise BBD fonctionne en mode management par projet, elle construit des services minimums viables qui sont ensuite mis à la disposition des clients et améliorés pour proposer finalement un produit final qui répond aux mieux aux attentes des clients.

BBD s'appuie sur la méthode agile SCRUM. La méthode est définie comme étant « une méthode de développement agile orientée projet informatique dont les ressources sont régulièrement actualisées. Le principe de base étant d'être toujours prêt à réorienter le projet au

fil de son avancement. C'est une approche dynamique et participative de la conduite du projet »

[13] En effet, les phases de l'activité peuvent changer selon les clients et leurs attentes.

III. Contexte et enjeux du projet

III.1 Contexte du projet

La gestion et la sécurité de l'information sont aujourd'hui plus que jamais un enjeu de management à part entière. Pour une entreprise comme BBD, dont les données personnelles de millions d'usagers sont, la "matière première", une certification de la sécurité de l'information est une nécessité voire une obligation pour répondre aux exigences clients.

Pour faire face aux exigences des donneurs d'ordre internationaux, la direction de BBD s'est lancée dans une démarche de mise en place d'un système de sécurité de l'information en vue d'une certification en fin 2018.

Si la certification ne se révèle pas indispensable en France, elle demeure obligatoire dans certains pays pour pouvoir vendre leur service ; une nouvelle contrainte qui se rajoute aux entreprises telle que BBD, qui recherche à obtenir des contrats et à conquérir des marchés internationaux

L'objectif de la démarche de certification est d'améliorer le niveau de sécurité des systèmes d'information et booster la performance de l'entreprise. Ceci passe d'abord par analyser puis comprendre d'une manière plus exhaustive et précise les attentes des clients. La certification ISO 27001 est une garantie du maintien dans le temps du niveau de sécurité acquis et elle peut être un bras de levier concurrentiel puissant.

Dans sa volonté de déployer une démarche de sécurité des systèmes d'information, la direction de la startup BBD met en œuvre les moyens et les compétences nécessaires, pour réduire les risques liés à la sécurité, maintenir un niveau de confiance vis-à-vis des parties intéressées et enfin accroitre la satisfaction de ses clients.

III.2 Les enjeux de la mise en placent d'un SMSI

III.2.1 Analyse SWOT :

Afin de mieux cerner le contexte général de la mission, une matrice SWOT a été élaborée (Fig.3).

L'intérêt principal de la matrice SWOT (Force, faiblesse, Opportunités, Menaces) est de rassembler et de croiser les analyses internes et externes de l'entreprise, ce qui nous donnera une vision globale et synthétique de l'activité de l'entreprise et de son environnement.

⇒ Forces

La démarche sécurité est portée par la direction générale de BBD, cette dernière est pleinement consciente des enjeux de la mise en place d'un SMSI, parmi les forces de l'entreprise la volonté de réussir malgré les contraintes de temps et de moyens financiers.

⇒ Faiblesses

Le personnel n'étant pas trop sensibilisé à la démarche, ceci peut engendrer la résistance aux changements, d'où l'intérêt d'anticiper le changement et identifier les facteurs de risque en amont de la mise en œuvre de la démarche.

⇒ Opportunités

La volonté de la direction de BBD de se faire certifier d'ici fin 2018, est un projet ambitieux à forte valeur ajoutée pour l'entreprise, cette certification va lui permettre une ouverture sur d'autres projets plus conséquent et faire face à la concurrence accrue (s'élargir à l'international).

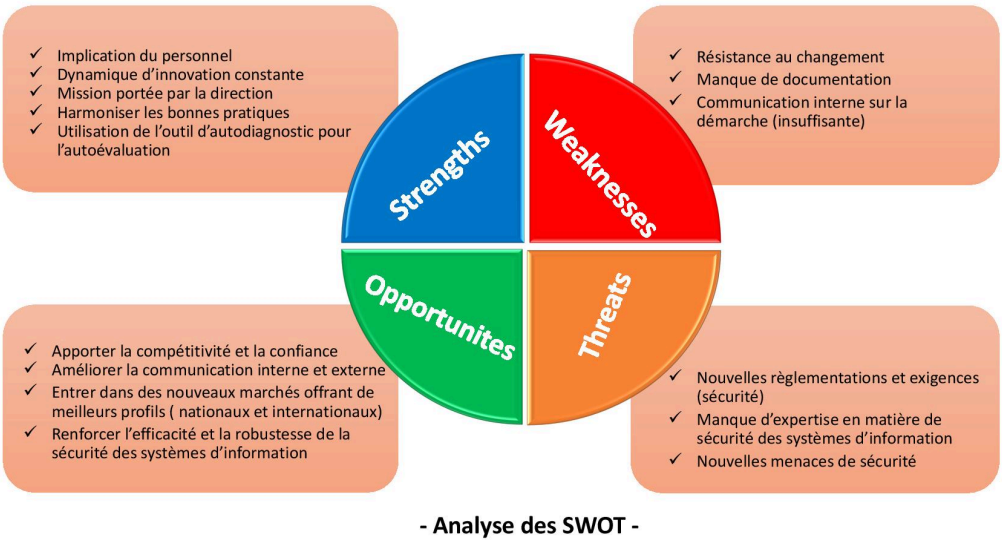


Figure 3: Analyse SWOT de la mise en place d'un SMSI [Source : Auteur]

III.2.2 Problématique et objectifs

Cadrage de la problématique :

Dans le but de cerner et cadrer le projet et les résultats attendus, une analyse QQOQCP a été réalisée (Fig.4) :

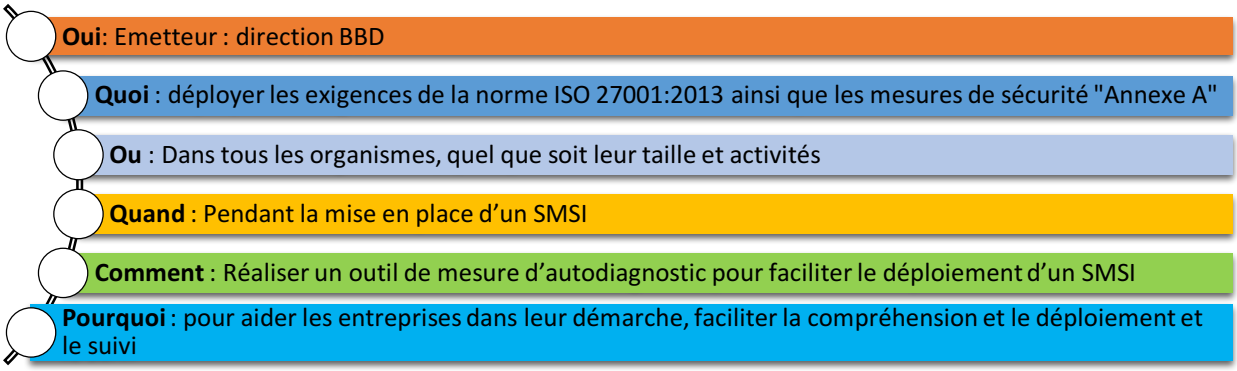


Figure 4: QQOQCP du projet [Source : Auteur]

III.2.3 Planification dynamique stratégique

Afin de bien structurer la planification des actions à mettre en place pour la réussite du projet de déploiement d'un SMSI une planification dynamique stratégique a été réalisée (Fig.5) :

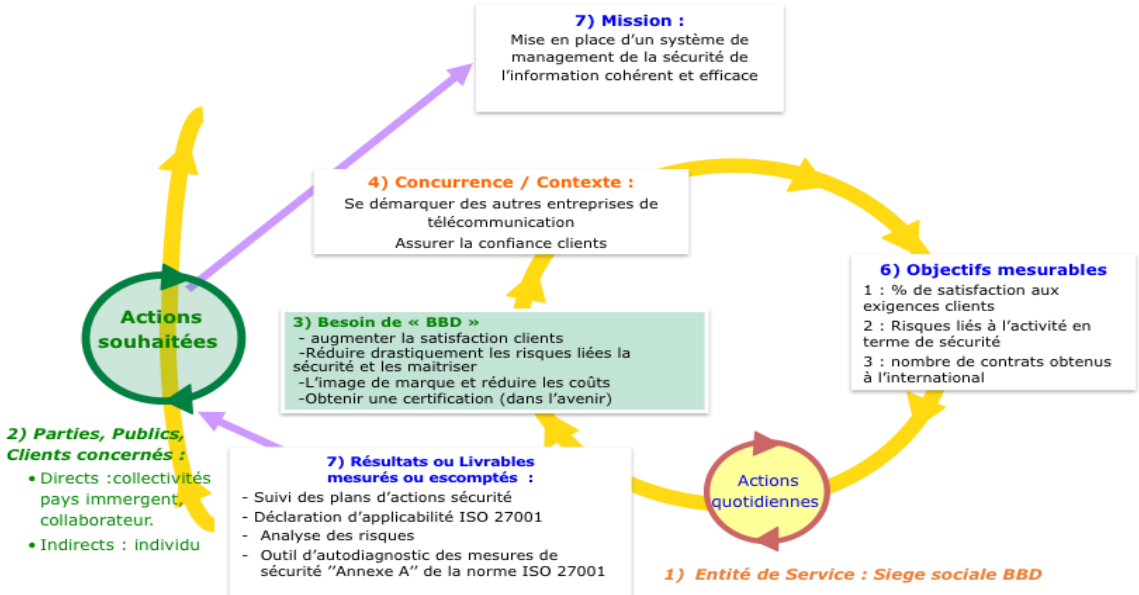


Figure 5: Planification Dynamique Stratégique PDS du projet [Source : Auteur]

Chapitre 2 : Un système de management de la sécurité de l'information, quel enjeu pour les organisations agiles ?

I. Contexte de l'ISO 2700x

La famille de normes du SMSI :

La famille de normes ISO 27000 aide les organisations à assurer la sécurité de leurs informations. Ces normes facilitent le management de la sécurité de l'information, notamment les données financières, les documents soumis à la priorité intellectuelle, les informations relatives au personnel ou les données qui sont confiées par des tiers. [14]

Elle comprend les normes de sécurité de l'information publiées conjointement par l'ISO (Fig.6). [15]

ISO 27001 : décrit les processus permettant le Management de la Sécurité de l'information SMSI
ISO 27002 : Présente un catalogue de bonnes pratiques de sécurité
ISO 27003 : décrit les différentes phases initiales à accomplir afin d'aboutir à un système de Management tel que décrit dans la norme ISO 27001
ISO 27004 : permet de définir les contrôles de fonctionnement du SMSI
ISO 27005 : décrit les processus de la gestion des risques
ISO 27006 : décrit les exigences relatives aux organismes qui auditent et certifient les SMSI

Figure 6: La famille de la norme ISO 27001 [Source : Auteur]

I.1 Historique de la norme ISO 27001

L'ISO 27001 est une norme internationale qui fait partie de la famille de la norme **ISO 27000**. Elle désigne un ensemble de normes relatives au système de management de gestion de la sécurité de l'information. La norme ISO 27001 est une norme britannique qui a vu le jour en Octobre 2005 succédant à la norme BS 7799-2, elle décrit les exigences sur la mise en place d'un Système de Management de la Sécurité de l'information (Fig.7).

Cette norme permet aux entreprises de choisir les mesures de sécurité afin d'assurer la protection des biens sensibles sur un périmètre bien défini en mettant en œuvre une approche systématique et proactive de la gestion des risques de sécurité.

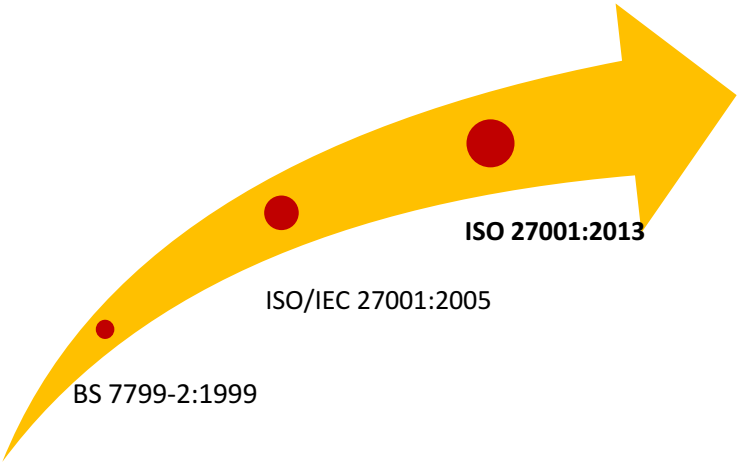


Figure 7: Historique de la norme ISO 27001[Source : Auteur]

La norme ISO 27001 repose sur 10 chapitres avec 114 mesures de contrôle (Annexe A) pour assurer la pertinence des engagements de sécurité, cette norme s'adapte à tout type d'organisme, quel que soit son secteur d'activité, sa structure, sa taille et la complexité de son système d'information.

Système de Management de Sécurité de l'Information SMSI c'est quoi ?

Un SMSI désigne l'approche systémique par laquelle une organisation veille à la sécurité des informations sensibles. Construit selon un processus de management du risque, un SMSI englobe les personnes, les processus et les systèmes de TI. Cette solution peut être utile aux

organisations de tous secteurs et de toutes tailles qui tiennent à la confidentialité de leurs informations. [16]

I.2 Sécurité de l'information :

La norme ISO 27001 fournit un canevas pour la mise en œuvre, le maintien et l'amélioration d'un système de management de la sécurité de l'information (SMSI). Il est important de rappeler qu'un SMSI s'implique avant tout à la direction de l'entreprise et la sécurité de l'information ne se limite pas aux systèmes informatiques (Fig.8), il concerne tous les actifs sensibles de l'entreprise. [17]

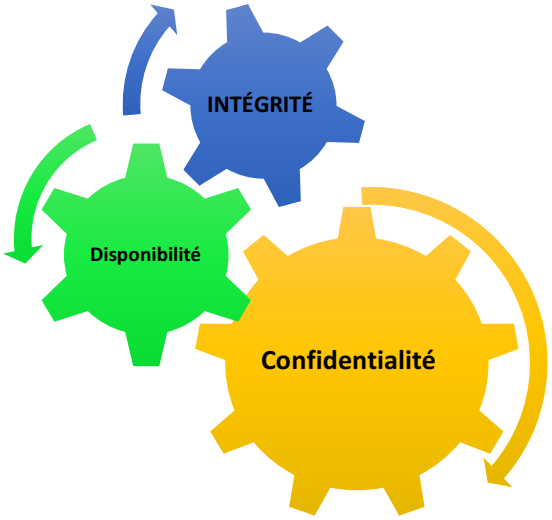


Figure 8: sécurité de l'information [Source : Auteur]

- Intégrité : préserve la fiabilité et l'exhaustivité de l'information et des méthodes de traitement.
- Disponibilité : garantit que les utilisateurs autorisés ont accès à l'information et aux ressources associées lorsque cela est nécessaire
- Confidentialité assure que l'information est accessible aux seules personnes autorisées

I.3 Positionnement de la certification ISO 27001

Standard	Number of certificates in 2015	Number of certificates in 2014	Change	Change in %
ISO 9001**	1033936	1036321	-2385	-0.2%
ISO 14001***	319324	296736	22 588	8%
ISO 50001	11985	6765	5 220	77%
ISO 27001	27536	23005	4 531	20%
ISO 22000	32061	27690	4 371	16%
ISO/TS 16949	62944	57950	4 994	9%
ISO 13485	26255	26280	-25	-0.1%
ISO 22301	3133	1757	1 376	78%
ISO 20000-1	2778		2 778	
TOTAL	**1519952**	**1476504**	**43 448**	**3%**

Figure 9: Évolution de certification ISO 27001 [2014-2015] [18]

Le tableau ci-dessus (Fig.9) montre l'évolution du nombre des certifications ISO accordées dans le monde entre les années 2014 et 2015.
La norme ISO 27001 vient en cinquième position dans le classement des certifications délivrées dans le monde après les fameuses normes : ISO 9001 : Management de la Qualité et ISO 14001 : Management de l'environnement qui sont en tête de classement.

On remarque qu'il y a une grande prise de conscience mondiale de la part des organisations sur le devoir de se protéger des perturbations en temps de crise. Avec plus de 27 536 certificats à travers le monde qui ont été accordés pour l'ISO 2700.
Cependant la France a un retard abyssal par rapport à ses voisins européens avec plus de 227 certifications derrière l'Italie plus de 1013, l'Allemagne plus de 640, l'Espagne plus de 701 certificats. Le Royaume-Uni qui dépasse les 2 790 certifications.

I.4 PDCA et l'approche processus

La norme ISO 27001 est une norme orientée processus et elle recommande le modèle de qualité PDCA (Fig.10) pour établir, mettre en œuvre, surveiller, tenir à jour et améliorer le SMSI.

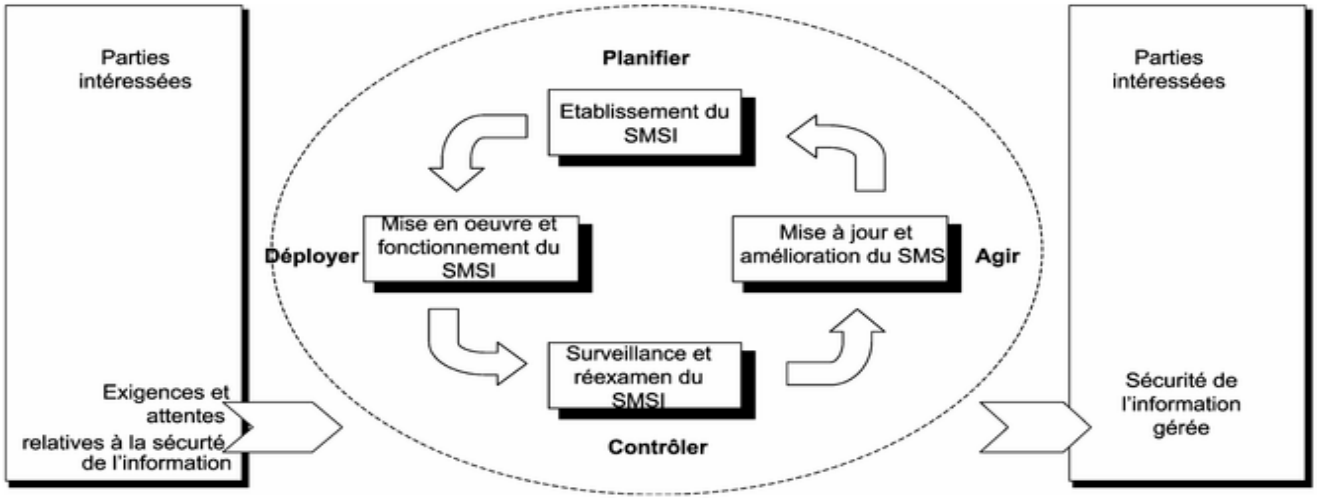


Figure 10: Modèle PDCA appliqué au processus SMSI [19]

⇒ **Planifier le SMSI**

Dans cette phase l'organisme doit établir sa politique sécurité des SI, le périmètre d'intervention ainsi que l'objectif de la démarche, les processus et les procédures du système de management de la qualité relatives à la gestion des risques (analyse et maitrise des risques, identification et évaluation)

⇒ **Déployer la mise en œuvre d'un SMSI**

La mise en œuvre de la politique sécurité et le déploiement des mesures de sécurité qui s'appliquent au contexte de l'organisme choisi de l'Annexe A de la norme, élaboration et application des procédures spécifiques,

Sensibilisation et formation des collaborateurs à la démarche, sélection des indicateurs et réalisation des tableaux de bord de la sécurité.

⇒ **Contrôler, Évaluer**

Le cas échéant, mesurer les performances Il s'agit de la phase CHECK qui s'appuiera sur des procédures de surveillance, sur la fonction d'audit et le dispositif de contrôle interne ainsi que sur des revues managériales en vue de détecter d'éventuels écarts par rapport aux objectifs

⇒ **ACT :** Cette phase permet d'entreprendre et de mener des actions correctives et préventives, sur la base des résultats des audits internes et de la revue de direction pour une amélioration continue du SMSI

I.5 Évolution de la norme ISO 27001 entre la version 2005 et 2013 :

La récente version de la norme ISO 27001 apporte des simplifications et des clarifications sur la mise en place d'un système de management de sécurité de l'information, ci-dessous un tableau (Tab.1) récapitulatif des évolutions :

ISO 27001 version 2005	ISO 27001 version 2013
Chapitre 4 – SMSI Périmètre du SMSI, interface, domaine d'application, maitrise des documents et des enregistrements **Chapitre 5 – Responsabilité de la direction** Implication Direction, management des ressources, formation, sensibilisation **Chapitre 6 – Audits internes du SMSI :** Audits internes **Chapitre 7 –Revue de direction du SMSI** Éléments d'entrée et de sortie **Chapitre 8 – Amélioration du SMSI** Amélioration continue, action préventives et correctives	**Chapitre 4 – contexte de l'organisation** Périmètre du SMSI, interface, domaine d'application **Chapitre 5 – Leadership** Engagement de la Direction Générale et définition des responsabilités vis-à-vis du SMSI **Chapitre 6 – Planification** Management des risques et définition du portefeuille des mesures de sécurité **Chapitre 7 – Ressources** Ressources humaines et compétence, communication (interne & externe), gestion de la documentation (sécurité et SMSI) **Chapitre 8 – Fonctionnement** Contrôle opérationnels, appréciation et traitement des risques **Chapitre 9 – Évaluation des performances** Audit interne, revue de direction, surveillance, mesures **Chapitre 10 – Amélioration** Traitement des non-conformités, actions corrective, amélioration continue

Tableau 1: Évolution de la norme ISO 27001 entre la version 2005 et 2013 [Source : Auteur]

II. Les Enjeux

1- Enjeux de la mise en place d'un SMSI

L'enjeu principal de la mise en place d'un SMSI est de structurer et rationaliser le pilotage de la sécurité de l'information, tout en construisant une vision stratégique à moyen terme. Son but est de garantir la bonne maitrise des risques majeurs et cela grâce au pilotage des risques stratégiques, le SMSI est donc amené à procurer aux dirigeants des organisations, un avantage concurrentiel décisif sur leurs marchés (maintien de la confiance des clients et toutes les parties intéressées). La mise en place d'une démarche **SMSI** à plusieurs vertus, il permet donc de :

- Garantir un haut niveau de sécurité des biens sensibles
- Préserver l'information (confidentialité, l'intégrité, disponibilité)
- Promouvoir les bonnes pratiques de sécurité
- Valoriser et impliquer le personnel
- Apporter la confiance aux clients et aux parties prenantes
- Marketing : un avantage concurrentiel décisif sur le marché (répondre à des appels d'offre à l'international)

2- Enjeux de la certification ISO 27001

La certification répond quant à elle à des enjeux commerciaux, sectoriels, règlementaires ou opérationnels forts. Au-delà des apports de l'alignement, elle constitue un élément différenciant et garantit un pilotage de la sécurité maitrisé aux yeux des clients, partenaires et régulateurs. [20]. Les avantages et les inconvénients de la certification ISO 27001 sont recensés dans le tableau ci-dessous (Tab.2) :

Les avantages	Les inconvénients
✓ Se différencier et créer un avantage compétitif ✓ ✓ Gérer ses risques de manière systématique et inspirer la confiance des parties prenantes ✓ ✓ Répondre à un besoin ou une exigence d'un client ✓ ✓ Réduire les coûts de gestion de la sécurité ✓ ✓ Motiver et rassurer ses collaborateurs	✓ Le champ de certification est clairement défini, il se limite à un métier donné, mais pas à toutes les activités de l'entreprise ✓ L'ensemble des exigences doit être respecté ✓ Difficulté de la démarche : 06 à 12 mois selon le type d'activité, la complexité de la structure ✓ Nécessité d'avoir un RSSI ✓ Le coût de la démarche de certification, elle varie d'une structure à autre

Tableau 2: Avantages et inconvénients de la certification ISO 27001 : 2013

Chapitre 3 Méthodologie de résolution et résultats obtenus

I. La stratégie de déploiement dans un contexte agile : se concentrer sur l'essentiel

Pour réussir la mise en place d'un système de management de la sécurité de l'information, d'une manière **efficace** et rapide dans un contexte **agile** avec une faible culture qualité. Il est **recommandé** de prendre « **l'Annexe A**» de la norme **ISO 27001** comme un point de départ (Fig.11) sans prendre la norme dans sa globalité mais parler le L**angage métier,** un langage qui **intéresse** et **sollicite l'intérêt** chez les collaborateurs. Donc Il s'agit d'utiliser le vocabulaire de l'interlocuteur, d'éviter des vocabulaires abstraits ou conceptuels et aller vers l'essentiel.

Ainsi, les bonnes pratiques de sécurité vont être intégrer dans le quotidien et dans le métier des collaborateurs. A l'issue de cette intégration des mesures de sécurité, Le SMSI va quant à lui atteindre rapidement un maximum de maturité. Ce qui va renforcer la fiabilité de la méthodologie de déploiement MDCA-CS (Fig.12) et permet ainsi d'éviter voire éliminer tous les aspects procéduraux et la rigidité normative, des facteurs critiques qui peuvent provoquer une sorte de résistance et une réticence de la part des collaborateurs.

L'Annexe A de la norme ISO 27001 version 2013, fournit un ensemble de mesures de sécurité (114 mesures) pour aider les organismes dans leur démarche de sécurité de l'information. L'application de tous les mesures de l'Annexe A n'est pas obligatoire, l'organisme choisit les mesures qui s'appliquent à son contexte et en adéquation avec sa stratégie.

En effet, en appliquant l'Annexe A de la norme, le manager assure le déploiement des mesures de sécurité avec **l'implication** et **l'adhésion totale** de tous les niveaux hiérarchiques dans l'entreprise, et il fait en sorte de minimiser voire éliminer toute sorte de résistance ou refus du changement.

Ensuite, un **outil d'autodiagnostic** de l'Annexe A de la norme a été conçu (Fig.16). Il a pour finalité d'aider les organismes agiles à mesurer leur niveau de conformité aux exigences de « l'Annexe A » en terme de sécurité de l'information. L'outil peut servir d'audit interne de sécurité qui donne une vision globale de l'état d'avancement et l'atteinte des objectifs sécurité. Une fois le système atteint entre 98% et 100% de taux de conformité à l'annexe A, à ce stade l'entreprise peut élaborer une **déclaration d'applicabilité Dda** en interne. Puis faire une **Auto-déclaration de conformité** à « l'Annexe A » (voir page 40) selon la norme **NF EN ISO 17050** (Déclaration de conformité du fournisseur) disponible sur l'outil (Fig.19).

Cette méthodologie (Fig.11) va permettre à l'entreprise de sécuriser son système d'information et communiquer avec ses clients sur la démarche, leur niveau de sécurité et de conformité à « l'Annexe A » de la norme sans pour autant perturber les pratiques des collaborateurs en interne.

Le potentiel de cette stratégie ne se limite pas uniquement à la mise en place d'une démarche de sécurité, cette stratégie a pour perspectives de faire **progresser la performance** des systèmes d'information en matière de sécurité sur tous les horizons vers un développement durable et pérenne.

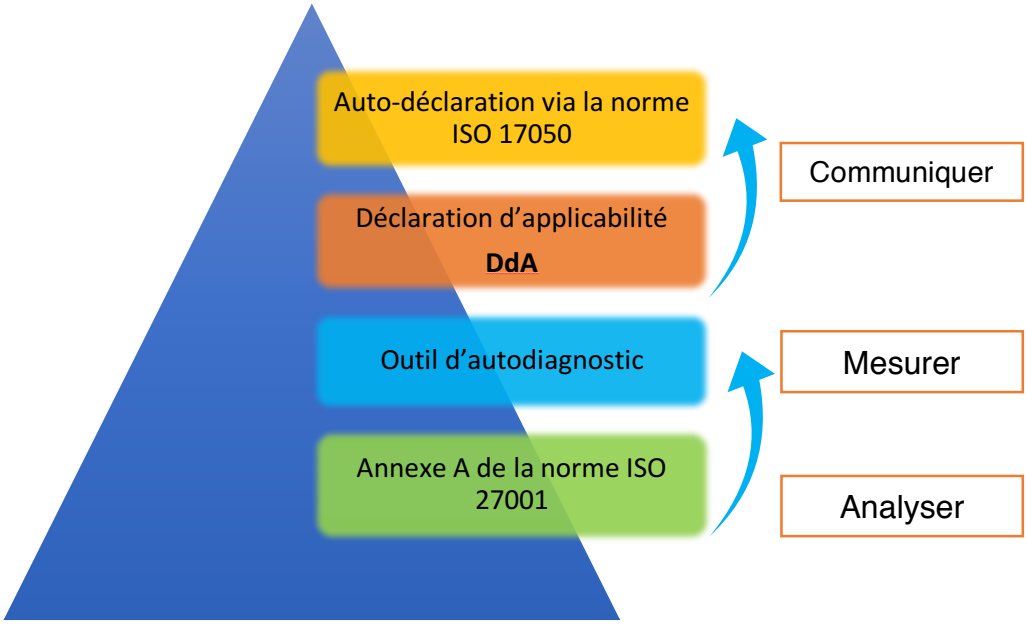


Figure 11 :Stratégie de déploiement [Source : Auteur]

II. Méthode MDCA-CS

Les entreprises avec leurs volontés d'implémenter un SMSI, prennent une décision stratégique, qui nécessite un investissement en temps et en moyens financiers. Pour mieux aider les organismes agiles à être à jour avec les évolutions des marchés, à répondre aux exigences des clients, une démarche **MDCA-CS** constituée de 6 phases a été développée. Celle-ci est représentée par la (Figure 12) :

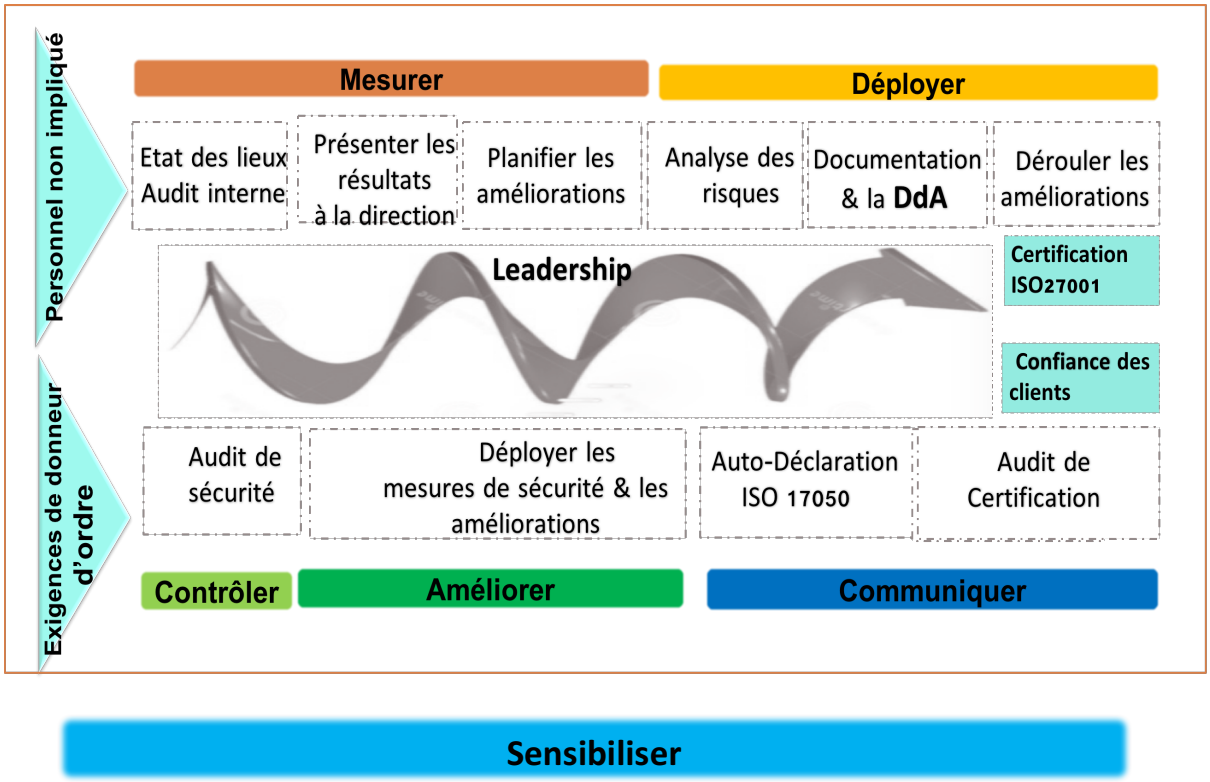


Figure 12 Méthodologie MDCA-CS [Source : Auteur]

La démarche proposée ici est essentiellement basée sur le principe de l'amélioration continue et accompagnée par les bonnes pratiques de la **conduite du changement**, cette méthode vise principalement à faciliter la mise en œuvre de la démarche de sécurité de l'information au sein des entreprises agiles. La méthodologie vient donc pour répondre à la problématique suivante : comment allier **qualité** et **agilité** dans un organisme à **faible culture qualité** tout en gardant **flexibilité** et **agilité** ?

⇒ Mesurer

Dans cette phase le **RSSI** effectue un état des lieux (un audit blanc) du système existant par rapport aux exigences de la norme ISO 27001 :2013 y compris les mesures de sécurité mises en place, pour identifier les écarts existants et élaborer des plans d'action et des axes de progrès, ensuite ces résultats sont structurés et communiqués en interne à la direction, puisque la direction a un rôle moteur dans la démarche, et aux collaborateurs pour les sensibiliser et les faire adhérer à la démarche.

- Mettre en place des procédures de sécurité, pour détecter rapidement les erreurs et identifier ainsi les non conformités aux règles de sécurité et organiser les remontées immédiates des incidents sécurité.
- Identifier les actions à réaliser pour corriger les écarts et les non conformités

⇒ Déployer

Cette phase consiste à mettre en place et à déployer les plans d'action déjà élaborés dans l'étape « Mesurer » pour corriger les écarts détectés.

- Fixer les objectifs du SMSI, définir le périmètre qui peut couvrir toute l'activité de l'organisme ou un périmètre spécifique.

- Définir les documents cadre du système comme la politique sécurité, les procédures sécurité qui visent à garantir un suivi de la sécurité du système d'information.

- Formaliser les processus conformes à la stratégie de gouvernance de l'entreprise.

- **La mise en place de la gestion des risques** : L'analyse des risques est un pilier de la démarche, qui commence par la définition du processus de gestion des risques et l'étude d'appréciation des risques, cette phase consiste à réaliser une analyse détaillée des

risques de sécurité (scénarios de risques). À noter la norme ISO 27005 peut servir de référence aux organismes dans l'évaluation des risques.

- Instaurer les mesures de sécurité qui couvrent la sécurité organisationnelle et la sécurité physique, en passant par la sécurité des systèmes réseaux. Pour garantir la confidentialité, l'intégrité et la disponibilité de l'information.

- **Élaborer la Déclaration d'applicabilité DdA** : un document sous forme de tableau qui énumère les mesures de sécurité appliquées au sein de l'organisme et celles non appliquées avec une explication de l'exclusion.

⇒ Contrôler & Améliorer

À ce stade de la démarche, les mesures de sécurité précédemment identifiées dans la DdA fonctionnent correctement, les collaborateurs de l'organisme sont formés et sensibilisés à la sécurité.
L'organisme planifie des audits régulièrement pour contrôler d'une façon continue l'efficacité de son SMSI, on peut distinguer deux types d'audits :

- ✓ L'audit organisationnel et physique
- ✓ L'audit technique des SI

⇒ Communiquer

A ce stade de la démarche, l'entreprise peut d'ores et déjà communiquer avec ses clients sur l'état d'avancement de la démarche, en se basant sur la DdA qui rassemble toutes les mesures de sécurité appliquées au sein de l'organisme, ou faire une auto-déclaration via la norme ISO 17050 (évaluation de la conformité-Déclaration de conformité du fournisseur), à l'attendant de l'obtention de la certification.

⇒ Sensibiliser

Tout au long de la démarche, le responsable sécurité assure en permanence la sensibilisation des collaborateurs vis-à-vis de la démarche, il les accompagne dans la conduite du changement

pour éviter toutes sortes de résistance au changement, en organisant **des réunions d'information** et de sensibilisation, **communiquer** sur les bénéfices et les valeurs ajoutées de la démarche en terme de performance interne de l'entreprise et en terme d'image et de crédibilité vis-à-vis des clients.

Le responsable de la démarche doit s'assurer que tous les collaborateurs maitrisent les outils et les mesures de sécurité déployées. **Une formation** des collaborateurs peut s'avérer nécessaire, qui peut débuter par un rappel des engagements de leur entreprise en matière de sécurité, la sensibilisation sur l'importance du respect de certaines règles de sécurité.

Leadership

Le leadership est un facteur décisif pour améliorer les chances de réussite des projets et de promouvoir la performance. Il n'y a aucun doute que le bon management de projet est un facteur critique de succès. Par conséquent, la réussite de la démarche dépend principalement de l'appui, de l'engagement de la direction et de sa capacité à impliquer et à motiver ses collaborateurs. Une équipe sensibilisée et performante amène des effets de synergie. La direction a ainsi un rôle moteur dans la réussite de toutes démarches de progrès.

III. Enjeux et risques du projet

Un système de management se caractérise par un engagement de l'ensemble des collaborateurs de l'organisation, quel que soit l'activité de l'organisme et le périmètre du système, il nécessite l'implication de tous les métiers et l'ensemble de la hiérarchie de l'organisme, de la direction jusqu'aux parties intéressées. Le but de la méthode **MDCA-CS** et de l'outil de mesure, c'est d'améliorer la performance des entreprises grâce à une démarche efficace et autonome. L'objectif ici est de franchir la rigidité structurelle de la plupart des entreprises et des startups pour casser ainsi les silos présents, mieux préparer le terrain, faciliter le déploiement et augmenter l'engouement et les marges d'acceptabilité du changement pour les collaborateurs.

Le facteur humain, étant l'élément le plus important dans l'entreprise, les collaborateurs jouent un rôle très important dans l'avancement de la démarche, et la démarche sécurité ne peut réussir sans la contribution des collaborateurs ainsi que l'engagement et le leadership de la direction.

Le comportement de ces derniers peut impacter positivement ou négativement le déroulement de la démarche et l'atteinte des objectifs.

Afin de mener à bien la mission de la mise en place d'un SMSI dans un contexte agile, une analyse des risques a été effectuée en amont (Tab.3) afin de définir des alternatives.

Nature	Risques	Alternatives
Humain	Non adhésion à la démarche (manque de temps)	Communiquer sur la démarche, les objectifs et les valeurs ajoutées (en quoi la démarche peut aider le personnel)
Humain	collaborateurs non sensibilisés à la démarche	Prévoir des réunions d'information de sensibilisation
Humain	Résistance aux changements	communiquer / accompagner les collaborateurs
Organisation	Manque de communication concernant le projet et la démarche	des réunions d'information avec les états d'avancement
Organisation	Mauvaise organisation du projet	prévoir un retro-planning du projet avec les dates et les état d'avancement (un suivi régulier)
Technique	Non existence d'un outil de communication interne	création d'un outil de communication et de partage interne **GED**
organisation	Mauvaise communication	Prévoir un plan de communication interne afin de promouvoir l'outil et les faire adhérer à la démarche
Humain	Turn-over important	sensibiliser les nouveaux arrivants dès le début (dès la période d'intégration)
Organisation	Non-respect des délais projet	réaliser des plannings projet et les faire valider par la direction partager le travail avec une équipe ou personne qualifiée (des jalons)
Organisation	Non engagement de la direction dans la démarche	communiquer sur les bénéfices de la démarche et la certification (les enjeux)
humain	Personnel non qualifié (manque de compétences en qualité)	Réaliser des supports d'information afin de les former (résumé, objectifs des norme..etc)

Tableau 3: risques projet et alternatives

III. 1 Conduite au changement

Le terme de résistance au changement désigne tout comportement ou toute attitude indiquant le refus de soutenir ou d'apporter une modification à un projet de changement [20]. La résistance au changement est donc une réaction naturelle à toutes situations nouvelles, elle peut se révéler particulièrement compliquée à gérer lorsque on travaille dans un contexte agile et avec une organisation verticale. Ce qui peut remettre en cause les repères des équipes et les liens et les rapports avec les supérieurs hiérarchiques. Le changement peut générer des phénomènes d'incompréhension, voire de rejet. Une mauvaise appréhension de ces impacts peut amener les projets à l'échec. Or chaque changement passe par plusieurs étapes voire courbes du changement ci-dessous (Fig.13).

Un élément clé de la réussite de la démarche est d'avoir une communication interne robuste pour que chaque personne dans l'entreprise arrive à comprendre l'objectif global de la démarche et de se l'approprier.

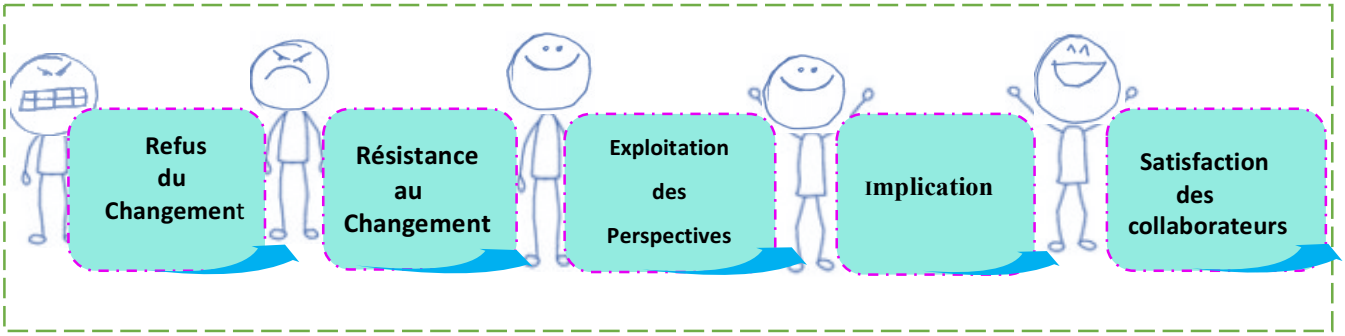


Figure 13 : Courbe du changement [Source : Auteur]

1. Refus du changement

Dans cette phase, le projet du changement est annoncé et les collaborateurs manifestent une sorte de refus, le changement est donc vécu d'une façon brutale accompagner d'un sentiment de colère et de déni.

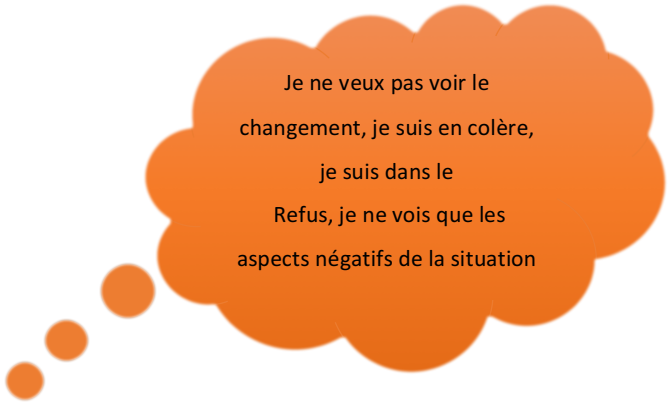


Figure 14 : Refus du changement [Source : Auteur]

2. Résistance au changement

La résistance au changement se manifeste sous forme de peur et d'inconfort, de la nouvelle organisation, du futur. Cette phase est l'étape de transition vers la phase ascendante (exploitation des perspectives d'avenir).

3. Exploitation des perspectives d'avenir

Cette phase se caractérise par un début d'acceptation du changement, les collaborateurs cherchent à comprendre, ils se tournent vers l'avenir et il exploite les perspectives de la nouvelle situation.

4. Implication et appropriation du changement

Le personnel trouve des bénéfices de la nouvelle situation, il est motivé et impliqué, les collaborateurs à leur tour travaillent en collaboration pour l'atteinte de la vision et des objectifs de la démarche. En effet, la collaboration est l'oxygène de tout travail performant.

5. Satisfaction des collaborateurs

Dans ce stade de la démarche, le changement est entièrement intégré par les collaborateurs. Il convient donc, pour les managers de bien préparer les collaborateurs en amont, en communiquant sur la vision de la direction, les bénéfices et les objectifs de la démarche, les sensibiliser aux enjeux de la certification.

III.2 Accompagner au changement afin de conserver une dynamique d'amélioration continue

La dérive la plus fréquemment rencontrée dans ce genre de démarche est la démobilisation des collaborateurs, une fois le projet passé, où l'organisme est certifié, le personnel peut manifester une sorte de lassitude dans le temps voir de rejet, d'où l'intérêt d'avoir un responsable de la démarche qui fait vivre le SMSI d'une manière continue pour garder cette dynamique, par des réunions de comité de pilotage, réunions d'information., Communication sur les axes à améliorer.

Au vu de garder une dynamique en continu et pérenniser les efforts de l'entreprise, le responsable sécurité doit rester à l'écoute des collaborateurs sur tous les aspects sécurité, fonctionnement des processus. Pour favoriser ainsi et instaurer un climat de transversalité qui peut être un moyen efficace d'amélioration de la performance en continu.

III.2 Retour sur la démarche MDCA-CS

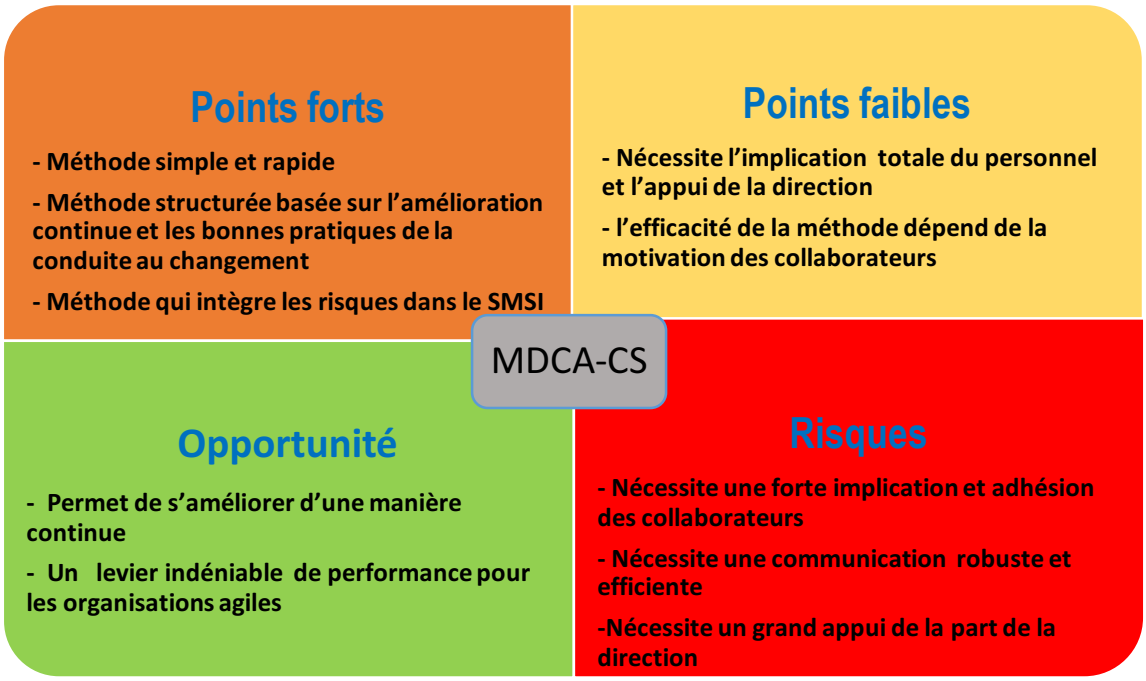


Figure 15 Retour sur la démarche MDCA-CS [Source : Auteur]

La méthodologie MDCA-CS est composée de 6 phases, elle permet de mettre en exergue les leviers de performance de l'implémentation d'un système de sécurité des SI. Elle s'adresse à tout type d'entreprise agile, taille et secteur d'activité confondus.

La démarche MDCA-CS est centrée sur la compréhension du contexte de l'entreprise et orientée vers les besoins de ses parties intéressées. Elle nous a permis non seulement de répondre aux exigences de l'Annexe A de la norme ISO 27001, elle apporte en plus une meilleure gestion des priorités et une meilleure sensibilisation, adhésion des collaborateurs.

Cependant, la méthode MDCA-CS a des points faibles qui peuvent se transformer en risques, ce qui peut impacter la pérennité du SMSI. Comme la nécessite de l'implication totale du personnel et l'appui de la direction.

IV. Stratégie d'élaboration d'outil

L'enjeu du projet et de décrypter la norme ISO 27001 version 2013 et ses exigences ainsi que « l'annexe A » du référentiel pour concevoir un outil de mesure et d'aide pour les organisations.

L'outil de mesure de « l'Annexe A » de l'ISO 27001 a pour but d'évaluer le niveau de respect des mesures de sécurité par les organisations, ainsi que de visualiser les résultats sous forme de graphique, radar et autres, pour finalement proposer des axes d'amélioration et de progrès jusqu'à l'atteinte de 100% de conformité aux exigences de l'Annexe A de la norme, ce qui offre une possibilité de faire une auto-déclaration via la norme ISO 17050.

L'outil de mesure de l'Annexe A de la norme ISO 27001 permet principalement de :

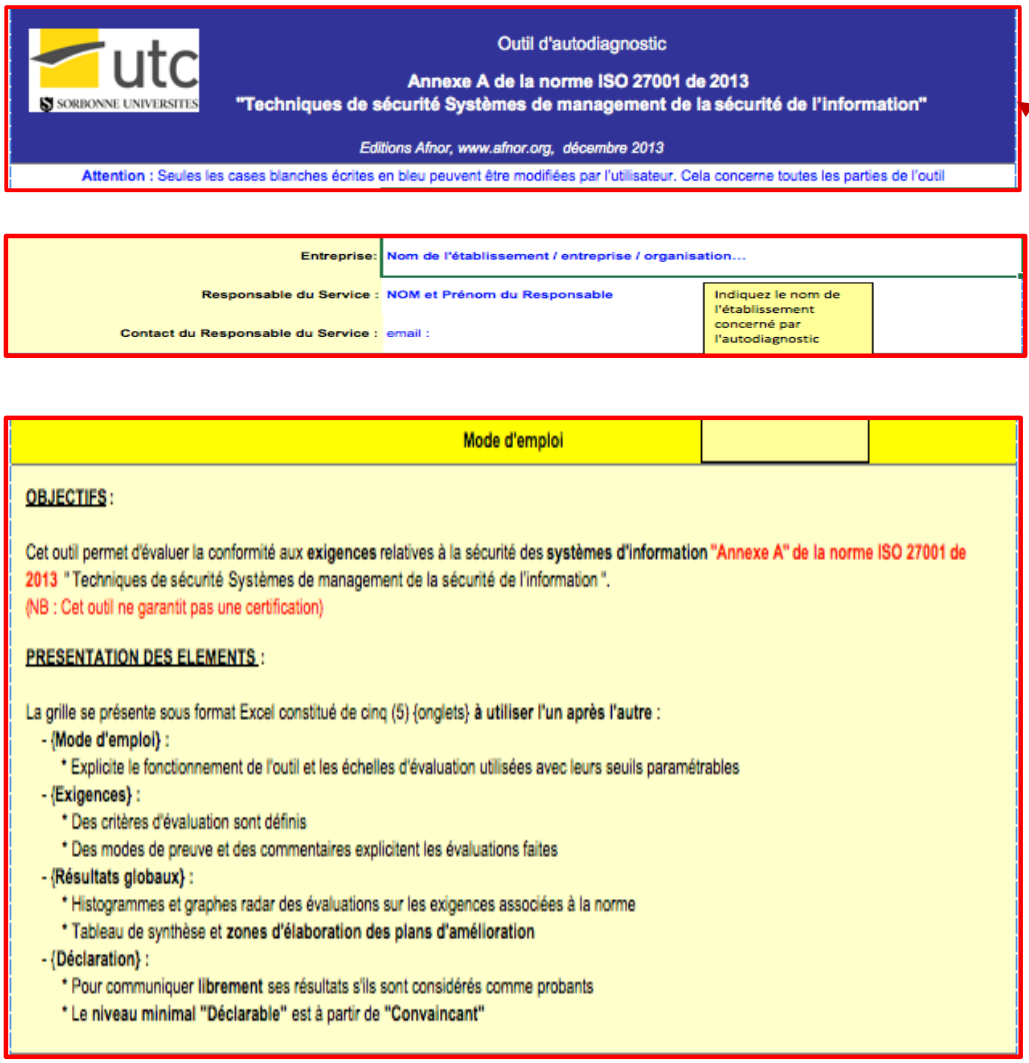
- ✓ Faire un État des lieux du système sécurité existant par rapport aux exigences de la norme
- ✓ Élaborer des plans d'action et des axes de progrès
- ✓ Communiquer les résultats à la direction et aux collaborateurs (en interne)
- ✓ Gérer le suivi et l'état d'avancement de la démarche (Qui, Quoi, fonction, Date de début, date de fin)
- ✓ Outil de communication sur le niveau de sécurité vis-à-vis des clients (pour l'auto-déclaration de la DdA)

La durée de l'autoévaluation est de 2H maximum, l'outil contient :

- ✓ Un mode d'emploi
- ✓ Exigence de l'Annexe A de la norme (114 mesures de sécurité)
- ✓ Une échelle d'évaluation
- ✓ Des résultats globaux puis des résultats pour chaque article et chaque mesure de sécurité
- ✓ Auto-déclaration via la norme ISO 1750 pour l'évaluation de la conformité (Déclaration de conformité du fournisseur)

III.1 Mode d'emploi

Le mode d'emploi (Fig.16) explicite le fonctionnement de l'outil, ainsi que **les échelles d'évaluation** utilisées (Fig.17).



En tête de l'outil : Il permet de renseigner les informations concernant l'entreprise et le responsable sécurité

Le mode d'emploi de l'outil : Décrit l'objectif de l'outil ainsi que son fonctionnement d'une façon détaillée

Figure 16 : Mode d'emploi de l'outil [Source : Auteur]

Echelles d'évaluation						
Niveaux de VÉRACITÉ quant aux MESURES des actions associées aux exigences de la norme			LIBELLÉS des niveaux de CONFORMITÉ des OBJECTIFS et AXES de la norme			
Libellés explicites des niveaux de VÉRACITÉ	Choix de VÉRACITÉ	Taux de VÉRACITÉ	Taux moyen Minimal	Taux moyen Maximal	Niveaux de CONFORMITÉ	Libellés explicites des niveaux de CONFORMITÉ
Niveau 1 : L'action n'est pas réalisée ou alors de manière très aléatoire.	Faux	0%	0%	29%	Insuffisant	Conformité de niveau 1 : Il est nécessaire de formaliser les activités réalisées.
Niveau 2 : L'action est réalisée quelques fois de manière informelle.	Plutôt Faux	45%	30%	59%	Informel	Conformité de niveau 2 : Il est nécessaire de pérenniser la bonne exécution des activités.
Niveau 3 : L'action est formalisée et réalisée.	Plutôt Vrai	75%	60%	89%	Convaincant	Conformité de niveau 3 : Il est nécessaire de tracer et d'améliorer les activités.
Niveau 4 : L'action est formalisée, réalisée, tracée et améliorée.	Vrai	100%	90%	100%	Conforme	Conformité de niveau 4 : BRAVO ! Maintenez et communiquez vos résultats.

Échelle d'évaluation : Il présente les modalités d'évaluation utilisées **-Niveau de conformité -Niveau de Véracité**

Figure 17: Échelle dévaluation de l'outil [Source : Auteur]

III.2 Onglet – Exigences

Il contient les exigences de l'Annexe A de la norme ISO 27001 (les mesures de sécurité) classées en mesure de sécurité et sous-mesures.

La grille d'évaluation est constituée de l'item à évaluer, du niveau de véracité et du taux de conformité correspondant. L'outil permet aux utilisateurs d'intégrer au fur et à mesure de leur évaluation, les commentaires qu'ils jugent nécessaires (Fig.18).

	Taux et niveaux de respect des exigences		39%	Informel
A.5	Politiques de sécurité de l'information		0%	Insuffisant
A.5.1	Orientations de la direction en matière de sécurité de l'information	Insuffisant	0%	Conformité de niveau 1 : Il est nécessaire de formaliser les activités réalisées.
mes 1	Un ensemble de politiques de sécurité de l'information est défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés	Faux	0%	
mes 2	Les politiques de sécurité de l'information sont revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps			
A.6	Organisation de la sécurité de l'information			nformel
A.6.1	Organisation interne			de niveau 3 : Il est nécessaire de tracer et d'améliorer les activités.
mes 3	Toutes les responsabilités en matière de sécurité de l'information sont définies et attribuées			
mes 4	Les tâches et les domaines de responsabilité incompatibles sont cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation	Plutôt Vrai	75%	
mes 5	Des relations appropriées avec les autorités compétentes sont entretenues	Vrai	100%	
mes 6	Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles sont entretenues	Vrai	100%	
mes 7	La sécurité de l'information est considérée dans la gestion de projet, quel que soit le type de projet concerné	Faux	0%	
A.6.2	Appareils mobiles et télétravail	Insuffisant	22%	Conformité de niveau 1 : Il est nécessaire de formaliser les activités réalisées.

Choix de VÉRACITÉ
Faux
Plutôt Faux
Plutôt Vrai
Vrai

Figure 18: Onglet « Exigences » de l'outil d'autodiagnostic [Source : Auteur]

III.3 Onglet – Résultats et Actions :

L'outil permet, à l'issue de l'évaluation, de connaitre les résultats globaux apportés lors de l'évaluation en terme de niveaux de véracité mais aussi de niveaux de conformité par critères.
Les résultats sont représentés sous forme de Radar (Fig.19), il permet donc d'évaluer l'efficacité du SMSI et identifier les axes d'amélioration.
L'utilisateur peut noter des commentaires lors de l'évaluation, d'une façon à avoir un plan d'action qui précise les objectifs et les axes d'amélioration.

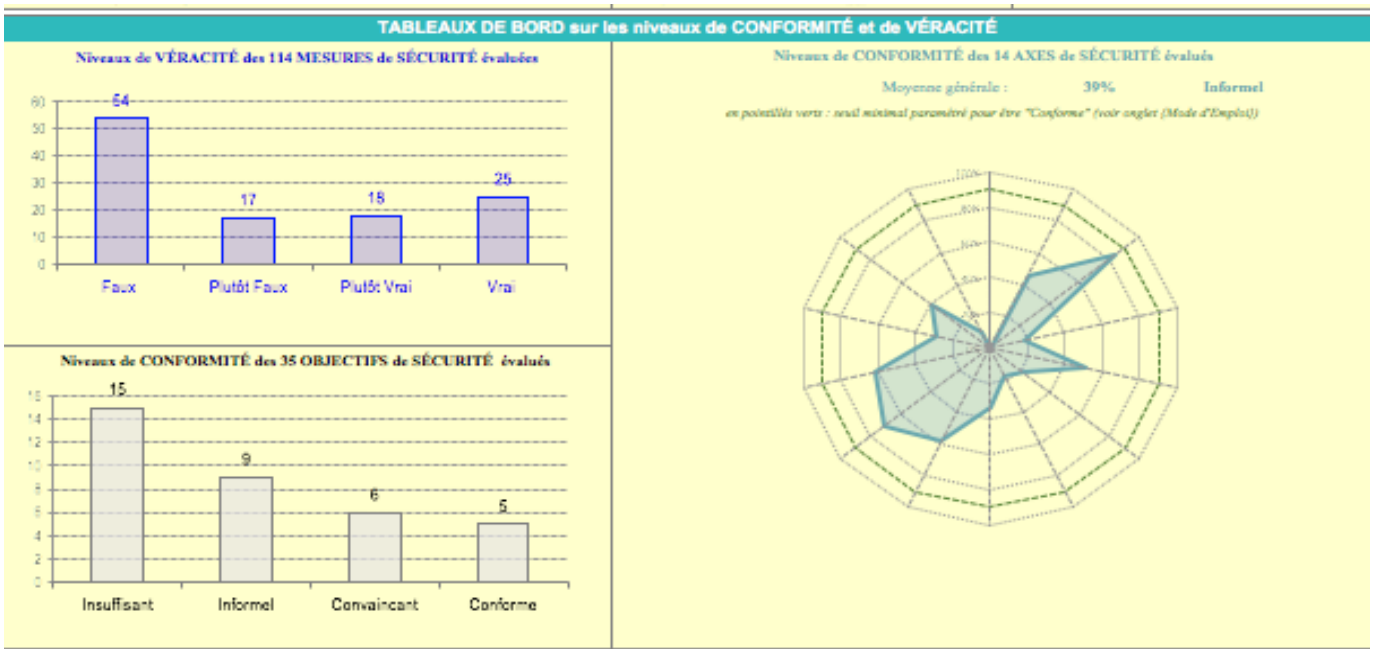


Figure 19: Onglet « Résultats » de l'outil d'autodiagnostic [Source : Auteur]

BILAN GLOBAL, COMMENTAIRES et PLANS D'AMÉLIORATION

Taux et niveaux de respect des exigences	Taux %	Maturité	DÉCISIONS : Plans d'action PRIORITAIRES QUOI (Objectifs mesurables à atteindre (livrables tangibles))	QUI (en Interne ou en Externe)	QUAND (Dates Début)	QUAND (Dates Fin)
	39%	Informel				
A.5 Politiques de sécurité de l'information	0%	Insuffisant	Plan d'amélioration…	Noms, Fonctions	Dates Début	Dates Fin
A.5.1 Orientations de la direction en matière de sécurité de l'information	0%	Insuffisant	rédaction de la politique qualité (liste des engagements de l'organisme) faire valider par la direction	SN, Ingénieur qualité	12/05/2017	03/06/2017
A.6 Organisation de la sécurité de l'information	46%	Informel	Plan d'amélioration…	Noms, Fonctions	Dates Début	Dates Fin
A.6.1 Organisation interne	70%	Convaincant	Revoir la sécurité de l'information dans la gestion de projet sensibiliser les collaborateurs à la sécurité de l'information	AR, RSSI	15/05/2017	07/07/2017
A.6.2 Appareils mobiles et télétravail	22%	Insuffisant	mettre en place un site de Télétravail mettre en place des clés de crypthographie pour les téléphones mobiles (notamment à l'etranger)	RSSI, CTO	01/06/2017	fin juillet
A.7 Sécurité des ressources humaines	84%	Convaincant	Plan d'amélioration…	Noms, Fonctions	Dates Début	Dates Fin
A.7.1 Avant l'mbauche	87%	Insuffisant	à améliorer….voir avec les ressources humaines	SN, Ingénieur qualité	15/05/2017	25/05/2017
A.7.2 Pendant la durée du contrat	65%	Convaincant	sensiliser les nouvels arrivés à la sécurité, les engagements de la direction en terme de sécurité à respecter	MH, XS	à chaque embauche	

Figure 20: Onglet « Bilan Global et plan d'amélioration » de l'outil d'autodiagnostic [Source : Auteur]

III.4 Onglet – Déclaration ISO 17050

À l'issue de l'évaluation, une auto-déclaration de conformité via la norme ISO 17050 est possible « Évaluation de la conformité - Déclaration de conformité du fournisseur » (Fig.21) qui permet à tous les organismes de justifier une déclaration de conformité par tout fournisseur, un système de management, un processus, une personne, un produit ou un service [20].

La déclaration de conformité est l'acte final pour qu'un organisme déclare que le **processus de sécurité de l'information** est conforme aux exigences applicables de l'Annexe A de la norme ISO 27001. Elle peut également être utilisée à des fins "Marketing" en mettant en avant tous les efforts réalisés par l'entreprise pour sécuriser son système d'information.

L'onglet déclaration sert donc de synthèse de l'autodiagnostic, et un outil de communication interne et externe sur le niveau de conformité par rapport aux exigences de la norme. Néanmoins cette déclaration ne peut s'effectuer qu'à partir d'un seuil minimal paramétrable par l'utilisateur de l'outil.

Déclaration de conformité selon la norme NF EN ISO 17050 Partie 1 : Exigences générales

Évaluation de la conformité - Déclaration de conformité du fournisseur (NF EN ISO/CEI 17050-1)

Date limite de validité de la déclaration : **Date de la déclaration + 1 an**

Référence unique de la déclaration ISO 27001 : 2013 **date de la déclaration invalide**

Objet de la déclaration :

Annexe A de la norme ISO 27001 de 2013

"Techniques de sécurité Systèmes de management de la sécurité de l'information"

Editions Afnor, www.afnor.org, décembre 2013

Nom de l'établissement / entreprise / organisation…

lous soussigés, déclarons **sous notre propre responsabilité** que **les niveaux de conformité de nos mesures de sécurité** ont été mesurés 'après les exigences de l'**Annexe A** de la norme NF EN ISO 27001:2013.
lous avons appliqué **la meilleure rigueur d'élaboration et d'analyse** (évaluation par plusieurs personnes compétentes) et nous avons respecté **es règles d'éthique professionnelle** (absence de conflits d'intérêt, respect des opinions, liberté des choix) pour parvenir aux résultats ci-dessous.

Tableau des résultats de CONFORMITÉ de nos activités		*Taux moyen*	*Niveaux de Conformité*
Taux et niveaux de respect des exigences		**39%**	**Non déclarable**
A.5	Politiques de sécurité de l'information	0%	Non déclarable
A.6	Organisation de la sécurité de l'information	46%	Non déclarable
A.7	Sécurité des ressources humaines	84%	Convaincant
A.8	Gestion des actifs	18%	Non déclarable

Figure 21: Onglet « auto-déclaration » de l'outil d'autodiagnostic [Source : Auteur]

CONCLUSION

Dans un monde interconnecté, l'information et les processus de traitement, les systèmes constituent des actifs critiques dans les organisations. S'engager dans une démarche sécurité des systèmes d'information est un vecteur de progrès indéniable et un véritable outil de gouvernance qui permet avant tout, de structurer et rationaliser le pilotage de la sécurité tout en construisant une vision stratégique efficace. Cependant, la réussite et la performance de ces démarches reposent avant tout sur **l'humain**. Le personnel doit se sentir impliqué dans la démarche, d'où l'intérêt d'instaurer un climat et un environnement qui favorisent l'innovation participative visant ainsi à casser les lourdeurs des hiérarchies.

Les clients sont attentifs et exigeants quant à la qualité et la sécurité des services offerts. Au regard de cette situation, il apparait pertinent de commencer par le déploiement des mesures de sécurité fournis dans l'Annexe A de la norme ISO 27001, une approche qui favorise l'écoute interne, pour assurer l'adhésion totale des collaborateurs, et faire ensuite une auto-déclaration de conformité à « l'Annexe A » de la norme via la norme ISO 17050 (déclaration de conformité du fournisseur). Cette stratégie permet entre autres de donner une visibilité sur la performance de l'entreprise (efficacité, efficience et qualité perçu) des pratiques de sécurité appliquées.

Ce stage de 6 mois m'a permis de mettre en pratique les connaissances théoriques acquises au cours de mon Master qualité et performances dans les organisations, il m'a permis de développer le sens de l'analyse et de la réflexion, renforcer mon sens de l'organisation et de la communication.

Cette mission dans une entreprise agile, m'a permis de voir le monde de l'entreprise d'un nouvel angle, ce n'est pas toujours facile ! j'ai compris que le facteur humain est l'élément le plus important dans l'entreprise et que la démarche de progrès ne peut réussir sans la contribution des collaborateurs. Qu'un environnement ouvert, transparent et communiquant est la clé pour la réussite de tous types de projets.

D'autre part, ce projet a affirmé mon choix, et il a renforcé ma volonté de devenir un ingénieur qualité qui accompagne les organismes dans leurs démarches de progrès tout en restant humain et visant l'excellence.

Références Bibliographiques

[1] « À propos de l'ISO ». [En ligne]. Disponible sur: https://www.iso.org/fr/about-us.html. [Consulté le: 20- Avril -2017].

[2]] Michel Invernizzi « MODULE FILIPE « Qualité et gestion de production » [En ligne]. Disponible sur : Filipé http://www.e-filipe.org/modules/qualite/glossaire.pdf

[3] « La méthodologie 7 S pour conduire un projet QSE » [En ligne]. Disponible sur : https://www.boutique.afnor.org/resources/9802ff8c-8635-4d66-8dd4-a3087440ca97.pdf

[4]« Chapitre 1 : Système d'information de l'entreprise ». [En ligne]. Disponible sur: http://profs.vinci-melun.org/profs/adehors/CoursWeb2/Cours/Ch1/Ch1.php. [Consulté le: 28-Mars -2017].

[5] « ISO 14001:2015(fr), Systèmes de management environnemental — Exigences et lignes directrices pour son utilisation ». [En ligne]. Disponible sur: https://www.iso.org/obp/ui/#iso:std:iso:14001:ed-3:v1:fr. [Consulté le: 13-Mai-2017].

[6]« [Certification] Déclaration d'Applicabilité, document né de l'approche ISO27001 : définitions, explications, utilisations - Fidens ». [En ligne]. Disponible sur: https://www.fidens.fr/articles/-certification-declaration-dapplicabilite-document-ne-de-l-approcheiso27001-definitions-explications-utilisations-72.html. [Consulté le: 12-juin-2017].

[7] « [Certification] Déclaration d'Applicabilité, document né de l'approche ISO27001 : définitions, explications, utilisations - Fidens ». [En ligne]. Disponible sur: https://www.fidens.fr/articles/-certification-declaration-dapplicabilite-document-ne-de-l-approcheiso27001-definitions-explications-utilisations-72.html. [Consulté le: 20-Mai-2017].

[8]« Les Echos - Qu'est-ce que l'agilité en entreprise ? - Archives ». [En ligne]. Disponible sur: http://archives.lesechos.fr/archives/cercle/2014/05/19/cercle_98076.htm. [Consulté le: 10 -Mars-2017].

[9] L. Florent, « Qu'est-ce qu'une entreprise agile ? | Unow Mooc », *Unow*. [En ligne]. Disponible sur: https://www.unow.fr/. [Consulté le: 28-juin-2017].

[10]« les-7-principes-de-l'agilité-en-image - Recherche Google ». [En ligne]. Disponible sur: https://www.google.fr/search?q=les-7-principes-de-l%27agilit%C3%A9-en-image&client=firefox-b-ab&tbm=isch&imgil=A_81_8SbDnP96M%253A%253BFqrHr3AoMFuQdM%253Bhttps%25253A%25252F%25252Ffr.pinterest.com%25252Fpin%25252F678565868825452938%25252F&source=iu&pf=m&fir=A_81_8SbDnP96M%253A%252CFqrHr3AoMFuQdM%252C_&

usg=__GfQ3AODQjjy8-PLKupTyz69LIyM%3D&biw=1280&bih=348&ved=0ahUKEwiz-IqXgeHUAhVCDZoKHYLCDokQyjcIRQ&ei=4d9TWfODD8Ka6ASChbvICA#imgrc=A_81_8SbDnP96M: [Consulté le: 15-Mai-2017].

[11]« Définition de l'agilité et d'une organisation Agile », *Agileom*. [En ligne]. Disponible sur: http://agileom.fr/agilite/. [Consulté le: 28-Mai-2017].

[12] « connaissez-vous les 12 principes Agile qui accompagnent les 4 composantes majeures du « Agile Manifesto » ? », *DantotsuPM.com*, 10-janv-2017. .

[13] « Qu'est-ce que Scrum, méthode de développement agile ». [En ligne]. Disponible sur: http://www.piloter.org/projet/methode/scrum.htm. [Consulté le: 18-Mars-2017].

[14] « ISO/IEC 27001 Management de la sécurité de l'information ». [En ligne]. Disponible sur: https://www.iso.org/fr/isoiec-27001-information-security.html. [Consulté le: 19-Mars-2017].

[15] « Qu'est-ce que la famille ISO 27000 ? - Fidens ». [En ligne]. Disponible sur: https://www.fidens.fr/articles/qu-est-ce-que-la-famille-iso-27000-54.html. [Consulté le: 28-juin-2017].

[16] « ISO/IEC 27001 Management de la sécurité de l'information ». [En ligne]. Disponible sur: https://www.iso.org/fr/isoiec-27001-information-security.html. [Consulté le: 28-juin-2017].

[17] « ISO 27001 – Système de management de la Sécurité de l'Information - Business Assurance », *DNV GL*. [En ligne]. Disponible sur: https://www.dnvgl.fr/https://www.dnvgl.fr/services/iso-27001-systeme-de-management-de-la-securite-de-l-information-3327. [Consulté le: 03-Mai-2017].

[18] Organisation International de Normalisation, « The ISO Survey of Management System Standard Certifications 2015 ». [En ligne]. Disponible sur: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/the_iso_survey_of_management_system_standard_certifications_2015.pdf [Consulté le: 03-Mai-2017].

[19] « ISO/IEC 27001:2013 - Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences ». [En ligne]. Disponible sur: https://www.iso.org/fr/standard/54534.html. [Consulté le: 20-Avril-2017].

[20] « Les cinq facteurs de résistance au changement - cadredesante.com ». [En ligne]. Disponible sur: https://www.cadredesante.com/spip/profession/management/article/le-terme-de-resistance-au-changement-designe. [Consulté le: 03-Juin-2017].

[21] « Rendre la norme ISO 27001 opérationnelle : trouver le SMSI gagnant », RiskInsight, 22-juin-2011. [En ligne]. Disponible sur: https://www.riskinsight-wavestone.com/2011/06/rendre-la-norme-iso-27001-operationnelle-trouver-le-smsi-gagnant/. [Consulté le: 11-juin-2017].