Master Qualité et Performance dans les Organisations

SORBONNE UNIVERSITES

Management de la sécurité de l'information

OUTILS D'AIDE AU DEPLOIEMENT DE LA NORME ISO/CEI 27001 VERSION 2013

2017-2018

Lien d'accès au document web : www.utc.fr/master-qualite, puis "Travaux", "Qualité- Management", réf n°423

Réalisé par :

DUMONT Fabien

JEMAI Sofiane

XU Zhaochen

Tuteur :

DERATHE Arnaud

Co-tuteur :

FELAN Pol-Manoël

Table des matières

Remerciements

Nos remerciements sont adressés aux tuteurs de ce projet Monsieur Arnaud DERATHE et notre cotuteur, Monsieur FELAN Pol-Manoël pour le temps accordé et leurs bons conseils tout au long de notre projet.

Nous remercions également Monsieur Gilbert FARGES, qui, à travers les enseignements de QPO11, offre tous les outils pour le bon déroulement du projet et la publication de ce mémoire.

Finalement, nos remerciements s'adressent à tous les membres de l'équipe pour leur implication et travaux et à notre promotion pour leur bonne humeur et sympathie tout au long du semestre.

Glossaire

RSSI	Responsable de la sécurité des systèmes d'information
SMSI	Système de Management de la Sécurité de l'Information
SI	Système d'information
ISO	International Organization for Standardization (Organisation Internationale de Normalisation)
CEI	Commission électrotechnique internationale
IEC	International Electrotechnical Commission
PME	Petites et les moyennes entreprises
BSI	British Standards Institution
BS	British Standards (normes britanniques)
TIC	Technologies de l'information et de la communication
AFNOR	Association Française de Normalisation
PDCA	Cycle "Plan, Do, Check, Act"
PDS	Planification dynamique stratégique
NTIC	Nouvelles technologies de l'information et de la communication
PMBOK	*Project Management Body of Knowledge*
PRINCE	PRojects IN Controlled Environments
CMMI	Capability Maturity Model Integration
ITIL	Information Technology Infrastructure Library
CoBiT	Control Objectives for Information and related Technology
RGPD	Règlement général sur la protection des données

Listes des figures

Liste des tableaux

Résumé

Dans le but d'aider le responsable de la sécurité du système d'information d'un organisme à mieux gérer et établir une bonne politique en matière de sécurité du système d'information, le recours à la norme ISO/CEI 27001 : 2013 est recommandé. En travaillant sur ce projet, notre but est de sensibiliser les entreprises à adopter des stratégies fondées sur la maitrise des risques liés à la sécurité de l'information et sur l'aide à la compréhension sur la famille des normes ISO/CEI 27000 pour mieux gérer leur SMSI.

Ainsi, nous avons décidé de réaliser un outil d'autodiagnostic permettant de se positionner vis-à-vis des exigences de la norme ISO/CEI 27001:2013 et d'identifier les axes d'amélioration du SMSI. Une cartographie des processus a, de même, était réalisée pour garantir une vision claire et une analyse efficace des processus de l'organisation en matière de sécurité de l'information.

Abstract

In order to help an information system manager to maintain a solid control of his system and plan the best information security politic for his company, the use of the ISO/IEC 27001 instruction is so recommended today.

While working in this project, we aim to sensitize companies to adopt some suitable strategies which are based on information security risk management and on the importance of the ISO/IEC 27000 family in piloting and tracking their information security management system.

To assure that, we have worked in an autodiagnostic tool designed to identify the weaknesses and the strengths of this system, also to compare daily practices to the ISO/IEC 27001:2013 requirements.

In addition to that, we have built a process cartography to provide a clear and efficient vision of what does really happen in term of actual security system management.

Introduction

Aujourd'hui, la gestion du système d'information d'un organisme est devenue un élément essentiel pour le fonctionnement de celui-ci. Grâce aux nouvelles technologies, les entreprises produisent et exploitent de plus en plus de données, l'information est de plus en plus rapide mais aussi de plus en plus menacée. Au cours des dernières années, le nombre de cyberattaques n'a cessé d'augmenter, entrainant des pertes financières importantes et un temps remise en sécurité assez long pour les organismes. Selon le sondage Opinionway, effectué en 2015, 81% des entreprises françaises ont été visées par des cyberattaques[i], ce qui représente une menace non négligeable pour celles-ci.(1)

Dans le but de standardiser et de sécuriser le système d'information des organismes, l'organisation internationale de normalisation a mis en place la norme ISO/CEI 27001. Celle-ci a été rédigée afin de sensibiliser les organismes à manager la sécurité de leurs informations et protéger leurs intérêts dans un environnement de plus en plus concurrentiel.

Ce mémoire vise, tout d'abord, à aider les responsables sécurité système d'information ainsi que la direction d'un organisme à comprendre les exigences et le contexte de la norme ISO/CEI 27001 version 2013. Il permettra aussi de comprendre les différences entre les grandes méthodes de gouvernance du SI et les périmètres de certaines certifications du système d'information comme le COBIT, ITIL, la norme ISO/CEI 27001 et le règlement général sur la protection des données (RGPD), qui sera applicable dans l'ensemble des Etats membres de l'Union européenne à compter du 25 mai 2018. Ce mémoire sera accompagné d'outils simples (cartographie des processus et outil d'autodiagnostic) qui seront mis à la disposition des organismes afin de les aider à améliorer la sécurité de leur système d'information, voir à obtenir la certification ISO/CEI 27001 version 2013 ainsi qu'un article et un poster qui permettront de comprendre les enjeux de la certification et nos apports pour l'aide à la certification.

Chapitre 1 : Contexte, enjeux et problématique de la norme ISO/CEI 27001

I. Contexte de l'ISO/CEI 27001

1. Qu'est-ce qu'un SI, SMSI et RSSI(2)

Un **système d'informations** (SI) peut être considéré comme un ensemble cohérent de ressources (personnel, logiciels, processus, données, matériels, équipements informatiques et de télécommunication...) permettant de recueillir, traiter, stocker et diffuser de l'information au sein d'un organisme. Ce système socio-technique possède sa propre interprétation selon chaque secteur d'activité, chaque entreprise, chaque service. L'information est un actif qui, comme tous les autres actifs importants d'un organisme, est essentiel à son fonctionnement et nécessite, par conséquent, d'être protégé de manière adéquate. L'entreprise doit mettre au point un système de management de la sécurité de l'information.

Un **système de management de la sécurité de l'information**, SMSI, est un dispositif qui gère et qui coordonne la manière dont la sécurité de l'information est mise en place. Il est important de bien définir un périmètre sur ce genre de dispositif afin de garantir sa réussite. Il permet de mettre en place des mesures de sécurités garantissant la confidentialité des biens sensibles (données personnelles, administratives, métier...) d'un organisme, l'intégrité de l'information (modification non désirée de l'information) ainsi que la disponibilité de celle-ci aux personnes autorisées à y accéder sur un champ bien défini.

La mise en place d'un SMSI nécessite :

- La sensibilisation des parties prenantes de l'organisme,
- L'attribution des responsabilités liées à la sécurité de l'information,
- La prise en compte de l'engagement de la direction et des intérêts de chaque département opérationnel ou fonctionnel dans l'organisme,
- Un rôle clé pour le RSSI, qui a pour but de de veiller à l'identification et à l'appréciation des risques.

Le **Responsable de la Sécurité des Systèmes d'Information**, RSSI, met en place les mesures de contrôle, assure la maintenance et l'amélioration continue de la politique de sécurité afin d'éviter de ramener le niveau de risque informatique en dessous des seuils d'acceptabilité. Pour organiser tout cela, la RSSI doit déterminer les mesures adéquates pour réaliser les objectifs fixés en termes de sécurité de l'information tout en définissant les principes directeurs, le cadre de référence ainsi que l'organisation permettant d'instaurer un système de sécurité cohérent et performant.

2. Contexte de la famille de l'ISO/CEI 27000(3)

La série des normes ISO/CEI 27000 est une famille de normes apparue à la fin des années 1990 lorsque la BSI publia les exigences pour la mise en place d'un SMSI. Ces documents ont ensuite été regroupés dans une série de normes, l'ISO/CEI 270XX. Cet ensemble est composés de normes d'exigences et de normes outil afin d'obtenir un ensemble d'exigences, de renseignements, de bonnes pratiques pour mieux sécuriser un système d'informations pour tous types d'organismes concernant

la sécurité de l'information, par exemple les données financières, les informations relatives au personnel, les données confiées par un tiers ou soumises à la propriété intellectuelle.

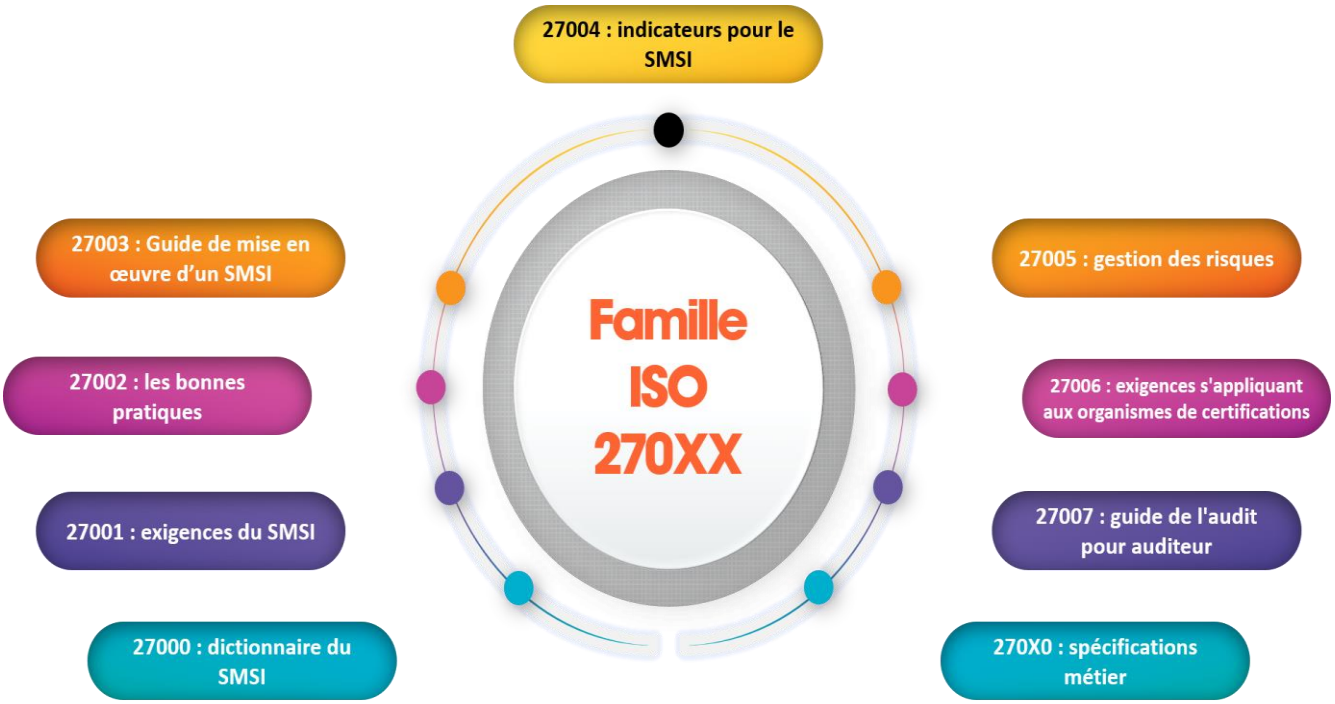


Figure 1: Famille de la norme ISO/CEI 27XX [source: auteurs]

a) *ISO/CEI 27000*

L'ISO/CEI 27000:2016 présente une vue d'ensemble des systèmes de management de la sécurité de l'information. Le document définit les termes qui s'y rapportent.

b) *ISO/CEI 27001*

La norme ISO/CEI 27001:2013 spécifie les exigences pour la mise en place, la mise en œuvre, la mise à jour et l'amélioration continue d'un SMSI. Elle définit également une gestion globale et le cadre de contrôle afin de traiter les risques de sécurité de l'information. Les exigences fixées dans l'ISO/CEI 27001:2013 couvre tous les types d'organisations, quels que soient son type, sa taille et sa nature.

c) *ISO/CEI 27002*

L'ISO/CEI 27002 :2013 donne les lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information. Ce document permet aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'un SMSI selon l'ISO/CEI 27001. A minima, il s'agit de parcourir l'ensemble des contrôles issus de l'annexe 1 de la norme ISO/CEI 27001.

d) *ISO/CEI 27003*

Le document vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001; elle encourage à la mise en place d'une approche processus.

e) *ISO/CEI 27004*

L'ISO/CEI 27004:2016 est un ensemble de lignes directives qui fournit des conseils pour le développement d'un programme de mesures et de contrôles et la formalisation d'indicateurs permettant de mesurer l'efficience d'un système de management de la sécurité de l'information (SMSI).

f) *ISO/CEI 27005*

Ce document vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001; elle est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.

3. Historique, positionnement et répartition de la certification ISO/CEI 27001

La norme ISO/CEI 27001 porte sur le management de la sécurité et de l'information. Elle tire ses origines de la norme britannique BS 7799-2:2002 « Technologie de l'information – Guide pratique pour le management de la sécurité de l'information », dont la première version a été publiée en 1999. En 2005, l'ISO adopte et améliore cette norme pour donner naissance à la norme ISO/CEI 27001. Cette norme vise à la mise en place d'un système de management de la sécurité de l'information efficace. En 2013, celle-ci a été révisée, se rapprochant d'une structure similaire aux autres normes de systèmes de management (ISO 9001, ISO 14001…). La norme est actuellement en cours de révision depuis le 19/05/2017.

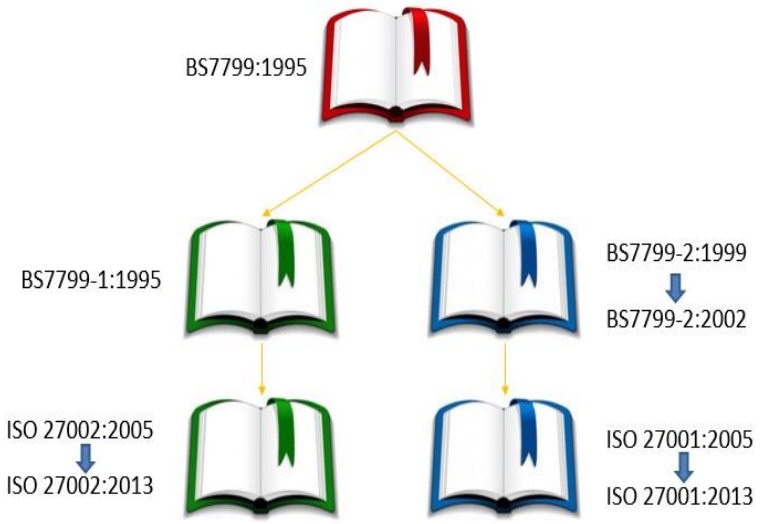


Figure 2 Historique de la norme ISO/CEI 27001 [source: auteurs]

La norme ISO/CEI 27001 est considérée comme la norme la plus célèbre de la famille des ISO/CEI 27000 et une des plus délivrées dans le monde.

A summary of the 2016 results is shown below:

Standard	Number of certificates in 2016	Number of certificates in 2015	Change	Change in %
ISO 9001**	1106356	1034180	72176	+7%
ISO 14001***	346189	319496	26693	+8%
ISO 50001	20216	11985	8231	+69%
ISO 27001	33290	27536	5754	+21%
ISO 22000	32139	32061	78	0
ISO/TS 16949	67358	62944	4414	+7%
ISO 13485	29585	26255	3330	+13%
ISO 22301	3853	3133	720	+23%
ISO 20000-1	4537	2778	1759	+63%
ISO 28000	356			
ISO 39001	478			
TOTAL	1,644,357	1,520,368		+8%

Tableau 1 : Nombre des certificats ISO dans le monde [source: organisation internationale de normalisation]

Sur le tableau ci-dessus, nous pouvons observer l'évolution du nombre de certifications des systèmes de management standard entre l'année 2015 et 2016. Tous ces chiffres sont extraits du lien proposé par le site https://www.iso.org/the-iso-survey.html proposant l'observation de l'évolution d'une norme :

http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

La norme ISO/CEI 27001 trône à la 5ème position des normes les plus délivrées en 2016 avec un total de 33 290 certifications en 2016 et une augmentation de 21%. Ces chiffres montrent bien l'intérêt que porte les organismes face aux problèmes liés à la sécurité de l'information. Cependant cet intérêt semble très disparate.

Rang	Pays	Nombre de Certifications en 2016
1	JAPAN	8945
2	UNITED KINGDOM	3367
3	INDIA	2902
4	CHINA	2618
5	GERMANY	1338
6	ITALY	1220
7	UNITED STATES OF AMERICA	1115
8	TAIPEI, CHINESE	1087
9	SPAIN	752
10	NETHERLANDS	670
11	POLAND	657
12	AUSTRALIA	531
13	ROMANIA	513
14	CZECH REPUBLIC	507

15	TURKEY	500
16	HUNGARY	421
17	ISRAEL	416
18	KOREA, REPUBLIC OF	364
19	BULGARIA	261
20	MALAYSIA	260
21	MEXICO	221
22	THAILAND	218
23	SLOVAKIA	212
24	FRANCE	209
	MONDE	**33310**

Tableau 2 : Classement du nombre de certificats par pays [source: organisation internationale de normalisation]

Ce tableau représente les 24 pays ayant le plus d'organismes certifiée ISO/CEI 27001 de 2006 à 2016. Les pays possédant un nombre important d'entreprises dans les secteurs porteurs de l'information et de la technologie comme le Japon, l'Inde ou encore la Chine représentent une part importante des certifications dans ce classement. Ces pays, ainsi que le Royaume-Uni, représentent à eux quatre plus de 50% du nombre d'organismes certifiés, avec une suprématie accordée au pays du soleil levant.

Les pays Européens ne sont pas en reste avec une 5e et 6e place pour l'Allemagne et l'Italie. En 24ème position, la France reste loin derrière ses collègues avec moins de 300 certifications en 2016. « *Les acteurs français ne semblent pas s'être suffisamment saisis de la question de la sécurité de l'information. Mise en œuvre de la réglementation européenne pour un marché numérique unique, multiplication des cybermenaces, économie de la donnée… les entreprises françaises ne sont pas différentes de leurs voisines européennes et ont tout intérêt à agir. Nous constatons toutefois une émergence d'un écosystème d'organismes qui font de la certification ISO/IEC 27001 un outil de reconnaissance mutuelle pour protéger leurs données et leurs intérêts »,* conclut Benoît Pellan, chef de produit numérique chez AFNOR Certification(4). En effet, les entreprises françaises ne sont pas en reste face à la cybercriminalité, le pays est même le 9ème pays le plus touché par les cyberattaques en 2015.(1) Au niveau des organismes, 81% des entreprises françaises ont été visées par des cyberattaques en 2015. Les conséquences peuvent être graves pour celles-ci avec une facture moyenne de 1,3 millions d'euros pour une entreprise de plus de 5000 salariés ainsi qu'environ 9 semaines pour remettre en place la sécurité de l'information au sein de l'entreprise(1). Les entreprises françaises prennent donc au sérieux ces problématiques liées aux cyber-menaces, reconnaissent l'intérêt de la norme ISO/CEI 27001. Cependant, celle-ci est utilisée comme un recueil de bonnes pratiques plus qu'un désir de certification réel, contrairement au Royaume-Uni où la certification semble indispensable pour la signature de contrat.

4. Comparaison des différentes normes au sein du DSI(5)

Un référentiel est une collection de bonnes pratiques sur un sujet donné. Ceux-ci sont au cœur des processus de la DSI en permettant d'améliorer l'efficacité et le degré de maitrise du SI. Il existe de nombreux référentiels liés aux systèmes d'informations et dans cette partie nous essaierons de déterminer les domaines d'applications de quelques référentiels en essayant de comparer leurs champs d'action avec celui de la norme ISO/CEI 27001.

a) Standards sur la conduite de projet

Il existe de nombreux référentiel pour la conduite de projet comme :

- **PMBOK**: permet à une personne physique d'obtenir une certification en management de projet,
- **PRINCE2**: permet à une personne physique d'obtenir une certification en management de projet,
- **ISO/CEI 10006** : donne des conseils sur l'application du management de la qualité aux projets.

b) Standards sur la gestion des développements de projets

- **CMMI** : est un modèle d'évaluation orienté processus, évaluant la capacité à atteindre les objectifs en matière de réalisation informatique. Fondé sur un référentiel de bonnes pratiques de la profession, il s'inscrit dans une logique d'amélioration continue.

c) Standards sur la gestion des services informatique

- **ISO/CEI 20000 :** Technologies de l'information, gestion des services
- **ITIL** : ensemble d'ouvrages recensant les bonnes pratiques orientées clients afin d'assurer une gestion efficace, risques et qualité, des services informatiques.
- **ISO/CEI 27001** : Sécurité du SI

d) Standards sur l'assurance qualité

- **ISO 9001:2012 :** Management de la qualité,
- **Six Sigma** : méthode visant à l'évaluation de processus dans un cadre d'amélioration de ceux-ci,
- **COBIT** : méthode fournissant des moyens d'évaluation du service informatique.

Dans Tableau 3 compare les quatre standards les plus populaire au niveau des SI :

	ITIL	**CobiT**	**CMMI**	**ISO/CEI 27001**
Domaine d'application	Production informatique	Contrôle et audit des SI	Ingénierie système, acquisition, service	Sécurité des systèmes d'information
Propriétaire du référentiel	OGC	ISACA	SEI	ISO/CEI
Diffusion du référentiel	OGC	En France, AFAJ	SEI	En France, AFNOR
Secteur économique de l'entreprise	Tous secteurs	Tous secteurs	Tous secteurs	Tous secteurs
Objet de la reconnaissance	Personne physique pour son expérience et ses connaissances en fourniture et en support de services	Personne physique pour ses compétences en audit informatique en sécurité des SI	Personne morale pour la mise en œuvre d'un ou plusieurs processus	Personne morale pour le système de management de la sécurité

		ou en gouvernance des SI		
Type de reconnaissance	Certification	Certification	Certification	Certification
Portée	Internationale	Internationale	Internationale	Internationale
Durée de validité	Non spécifiée	3 ans avec confirmation annuelle	3 ans	3 ans avec audits de suivi
Type d'évaluation	Examen en français pour le niveau fondamental, sinon anglais	Examen CISA : en français CISM : en français CGEIT : en anglais	Auto-évaluation Evaluation seconde et tierce partie	Audit tierce partie
Portée du référentiel	L'activité Les personnes	L'activité	L'activité Les personnes Les produits	L'activité Les personnes Les produits
Méthode d'évaluation	QCM d'EXIN et ISEB	QCM de l'ISACA	SCAMPI du SEI	Méthode propriétaire de l'organisation certificateur
Nombre de niveaux	Plusieurs	Un par type d'Examen	Plusieurs	Un

Tableau 3 Tableau comparatif des différentes certifications au cœur du SI [source : auteurs]

L'AFNOR présente sa vision des méthodes à appliquer au sein d'une DSI sous forme d'une maison appelée : La maison des méthodes DSI. La Figure 3 permet de faire le lien entre les différents standards décrits ci-dessus et de remarquer que la norme ISO/CEI 27001 permet d'alimenter et sécuriser les autres pièces de la maison.

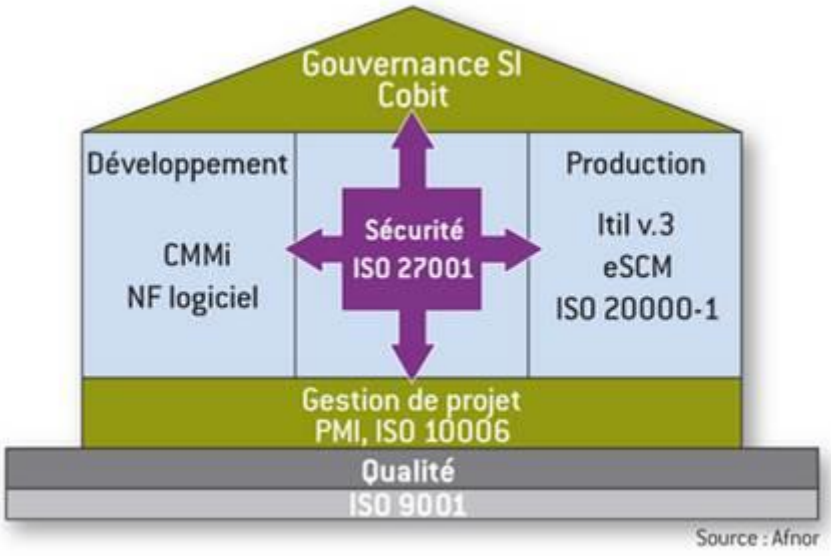


Figure 3 La maison des méthodes DSI. Source: Afnor

e) *Lien entre le RGPD et l'ISO/CEI 27001 :2013(6)*

Le règlement général sur la protection des données (RGPD) est un texte de référence européen en matière de protection des données à caractère personnel. Il a été définitivement adopté le 14 avril 2016 par le parlement européen. Ses dispositions seront directement applicables dans l'ensemble des

28 états membres de l'Union Européenne à compter du 25 mai 2018. Le RGPD remplace la directive sur la protection des données personnelles, adoptée en 1995, devenue obsolète. Ce règlement est l'une des avancées les plus importantes jamais réalisées sur le plan mondial par les gouvernements afin de protéger les données personnelles de leurs citoyens. Selon un sondage réalisé par Bird & Bird Paris sur la période du 15 mai au 15 juin 2017, 97 pourcent des entreprises n'étaient pas prêtes et seulement 44% le seront. Cependant 83% des entreprises le considèrent comme une évolution positive.(7)

Objectif du RGPD	- Renforcer les droits des personnes (création d'un droit à la portabilité des données personnelles et des dispositions propres aux personnes mineures) - Responsabiliser les acteurs (Européens et non-européens) traitant des données en garantissant la sécurité de toutes les données collectées, traitées et stockées. - Crédibiliser la régulation (Coopération renforcée entre les autorités de protection des données et des sanctions renforcées) - Recueillir et prouver le consentement éclairer des individus
Champs d'application	Quoi ? : Toutes les données à caractère personnel traitées automatiquement ou non Qui ?: Toutes les entreprises traitant des données de citoyens européens (responsables du traitement des données et à leurs sous-traitants européens ou non)
Date de mise en application	Être conforme au 25 mai 2018
En cas de risque réel d'atteinte à la vie privée	Notifier la CNIL, sous 72h, en cas de risque réel d'atteinte à la protection
Sanction	Amendes jusqu'à 4% du Chiffre d'Affaire annuel global ou 20 millions d'euros

Tableau 4 Tableau récapitulatif concernant le RGPD [source: auteurs]

Tout en ne remplissant pas tous les critères du RGPD, les exigences de la norme ISO/CEI 27001 semble être une bonne base pour la conformité à la réglementation et à l'amélioration continue du SMSI. Le fait d'être certifié par un organisme tiers accrédité fournit une preuve concrète quant à la sécurité du SI d'un organisme. Les organismes qui ont mis en place un SMSI (ISO/CEI 27001 ou interne) ont déjà un socle solide pour se conformer au RGPD.

6 Evolution de la norme ISO/CEI 27001 entre les versions 2005 et 2013(8)

Le tableau ci-dessous compare la norme ISO/CEI 27001:2005 à la norme ISO/CEI 27001:2013 sur certains points.

Norme ISO/CEI 27001 :2005	Norme ISO/CEI 27001 :2013
Structure	
5 clauses spécifiées qui approchent les SMSI à partir d'une approche managériale 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, actions préventives et correctives	7 clauses spécifiées, qui ne sont pas obligées d'être suivies dans l'ordre listé 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 Contrôles 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 correctives, amélioration continue
Processus de mise en application	
Utilisation explicite du PDCA	Le standard n'impose aucun modèle particulier. Il implique cependant d'utiliser un processus d'amélioration continue.
Contrôles	
L'annexe A contient 133 points de contrôles divisés en 11 catégories. Les contrôles externes sont utilisés pour pallier aux points non traités par l'Annexe des contrôles.	L'annexe A contient 114 points de contrôles divisés en 14 catégories. Les contrôles (de n'importe quelle source) sont identifiés avant de se référencer à l'Annexe A.

Tableau 5: Tableau comparatif entre les versions 2005 et 2013 de la norme ISO/CEI 27001 [source: auteurs]

Ce tableau montre que les deux versions de la norme reposent sur des bases similaires. La nouvelle version de la norme est clairement une étape pour devenir un standard, elle permet aux grands groupes de pouvoir utiliser n'importe quel processus d'amélioration continue, contrairement à la version 2005 qui imposait l'utilisation de l'outil PDCA. De manière générale, la norme est plus flexible et s'intègre dans la norme ISO 31000 "Management du risque".

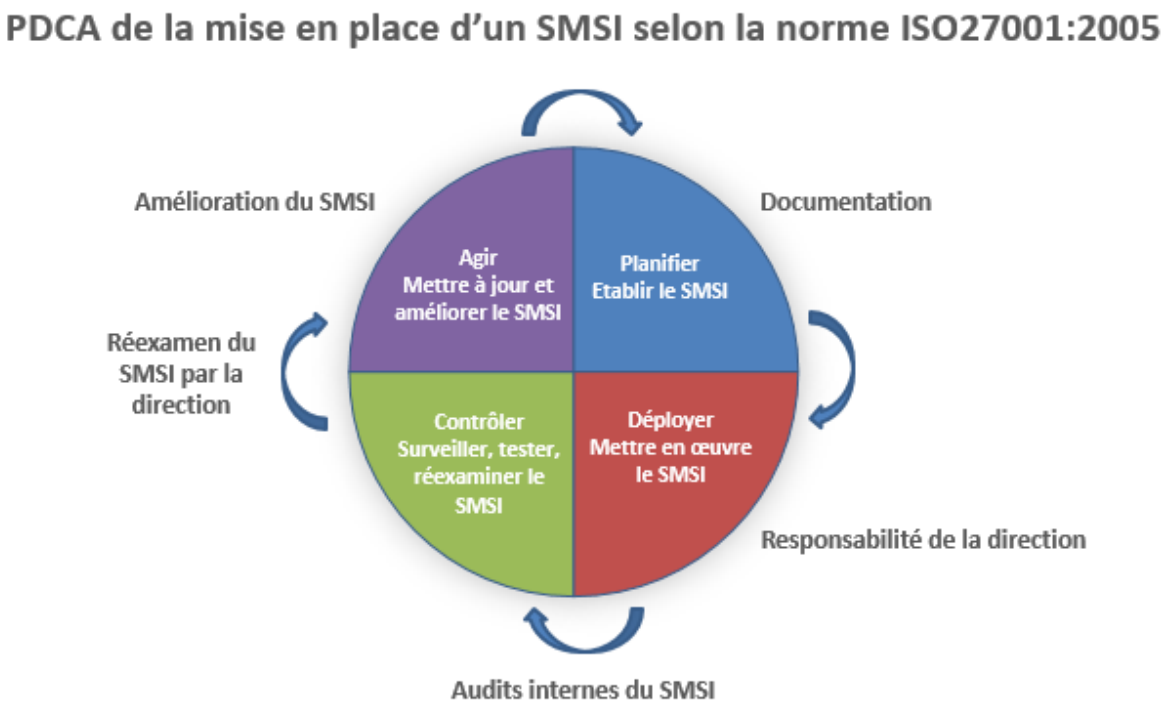


Tableau 6 : PDCA de la mise en place et l'amélioration continue d'un SMSI selon la norme ISO/CEI 27001 [source: auteurs]

II. Enjeux de la norme ISO/CEI 27001 version 2013

1. Les risques et causes liés au Système d'Information(9)

a) Les risques

Avec l'arrivée de l'outil informatique et du Web 2.0 au cœur des organisations, les systèmes d'informations de celles-ci se sont vus complétement bouleversés. La collecte, la mémorisation, le traitement et la diffusion de l'information se fait aujourd'hui énormément avec des systèmes informatisés. Il est désormais possible de conserver beaucoup plus de données dans un espace réduit (support numérique) et de les dupliquer de manière très simple. Les organisations se voient désormais sujet à trois grands types de risques au niveau de leur SI :

- L'intégrité de l'information : modification ou la suppression de l'information,
- La confidentialité de l'information : révélation des informations à un tiers non autorisé,
- La disponibilité de l'information : provoqué par des pannes, erreurs voire malveillances.

Les risques liés à la sécurité du système d'information peuvent causer d'importants dégâts :

- Financiers : détournements d'informations, ransomwares, mauvaises installations d'un progiciel(10), suppressions d'informations importantes. Une entreprise doit mettre environ 9 semaines pour se remettre d'une cyberattaque, avec des dommages moyens de 300 000€ pour les entreprises de moins de 1000 salariés et jusqu'à 1,3millions d'euros pour une entreprise de plus de 5000 salariés.(1)
- Pour le personnel, causant des torts à la vie privée d'une personne en diffusant des informations personnelles sur elle. Le nouveau RGPD obligera les organisations européennes

à notifier auprès des autorités compétentes, sous 72h en cas de risque réelle d'atteinte à la protection de la vie privée. Sinon, l'organisation s'expose à une amende allant jusqu'à 4% du Chiffre d'affaire ou 20 millions d'euros.(6)

- Pour le bon fonctionnement de l'entreprise. Il faut 9 semaines environ à une entreprise pour se remettre d'une cyberattaque.(1)
- D'image, désinformation, diffamation, permettre à une personne de mettre en évidence des failles de sécurité sur un serveur web(11). Nous pouvons citer quelques exemples célèbre comme le piratage de Sony Pictures Entertainment, la cyberattaque mondiale de mai 2017 ou encore la découverte de possibilité de piratage des systèmes de perfusion médicaux(12).

Le risque peut être quantifié, il est évalué en fonction de la valeur attachée aux informations manipulées, de l'importance des vulnérabilités et de la probabilité d'exploitation. La norme ISO/CEI 27001 aide l'organisation à évaluer ces risques. Les risques liés au SI peuvent-être réduits en limitant la sensibilité des informations qu'il manipule, en réduisant la vulnérabilité de chaque entité du système et en multipliant les éléments de défense convenablement architecturés pour compliquer la tâche des attaquants potentiels. Un SMSI permet alors de gérer ces risques liés au SI.

b) *Les causes*

Les menaces liées au système d'information sont généralement générées par 3 causes principales :

- Les causes humaines qui sont généralement divisées en trois catégories. Dans un premier temps, le risque peut être causé par la maladresse humaine. En juillet 2010, un rapport du service de coordination à l'intelligence économique affirmait que dans 80% des cas la perte ou la destruction d'informations sensibles sont causées par des maladresses internes ou l'absence de sauvegarde fiable. La deuxième cause humaine représente l'inconscience du personnel. De nombreux utilisateurs méconnaissent les risques et introduisent des programmes malveillants au cœur du SI. Selon une étude de Cyber Security Study de 2014 mené par Blue Coat (13), 51% des employés utilisent des appareils personnels au travail, 2 personnes sur 5 utilisent les réseaux sociaux pour des réseaux sociaux pour des raisons personnelles au travail, 20% ouvrent des emails provenant des sources inconnues et 6 % regardent du contenu réservé aux adultes. Pourtant 73% des interrogés ont conscience qu'ouvrir une pièce jointe d'une source inconnue est dangereux. La troisième menace humaine est la malveillance.
- Les causes extérieures qui peuvent être un sinistre (vol, incendie, dégâts eaux) ou un problème électrique. La norme ISO/CEI 27001 apporte les bonnes pratiques en termes de management des systèmes, en gérant les risques par exemple en prévenant ces risques.
- Les causes techniques liées à la surchauffe ou l'obsolescence du matériel. Des failles de logiciels ainsi que des programmes malveillants peuvent être identifiés.

Selon une étude indépendante menée pour Robert Half auprès de 100 DSI français, ceux-ci pensent que les principaux risques liés à la sécurité de l'information d'ici 5 ans seront la cybercriminalité à 63%, l'utilisation frauduleuse/compromission de l'intégrité à 52% et le manque de connaissance des salariés en matière de sécurité(14). Selon un sondage OpinionWay pour Symantec, en 2015 81% des entreprises françaises ont été visées par des cyberattaques en 2015. En 2015, le coût des cyberattaques a été estimé à plus de 3,3 milliards d'euros pour les entreprises françaises.

Type de cyberattaques	Pourcentage subit par les entreprises visées
Ransomware	61%
Déni de service	38%
Défiguration page Web	23%
Vol de données personnelles	18%

Tableau 7 Types de cyberattaques subis par les entreprises françaises en 2015. sources: sondage Opinionway, NTT Cam Security, étude Symantec, ANSSI [source: auteurs](1)

2. Enjeux d'un SMSI(2)

La mise en place d'un SMSI permet de sécuriser le système d'informations de tous types d'organismes possédant des données dites "sensibles" en délimitant un périmètre d'action et en développant une vision et une amélioration à moyen terme. Il permet d'offrir une meilleure maîtrise des risques majeurs en pilotant les risques stratégiques. L'utilisation de ce type de systèmes permet donc de satisfaire les exigences de la sécurité des clients et des parties prenantes, en répondant aux objectifs de la sécurité de l'information et en se conformant aux réglementations et à la législation. La mise en point d'un SMSI permet, pour l'organisation, d'améliorer les plans et les activités de celui-ci.

Pour conclure, un SMSI peut apporter plusieurs avantages dans une organisation, comme :

- Garantir la sécurité de l'information et des données sensibles,
- Identifier les risques et mettre des contrôles en place pour les gérer ou les éliminer,
- Permettre la confidentialité, l'intégrité et la disponibilité des informations d'un organisme,
- Valoriser et impliquer le personnel car celui-ci fait partie du SI,
- Rassurer les clients et les parties prenantes,
- Promouvoir les bonnes pratiques de sécurité,
- Éviter les ruptures d'activité en anticipant les risques,
- Réduire la probabilité d'erreur de Technologie de l'information et de la communication,
- Délimiter les champs de la sécurité,
- Protéger l'organisation.

3. Enjeux de la certification

La certification de l'ISO/CEI 27001 permet d'accroître la confiance des clients et de répondre à leurs exigences en matière de sécurité en identifiant les menaces et les dangers pesant sur les systèmes d'information. Cette norme permet de certifier la mise en place d'un SMSI tout en visant son efficacité. Elle permet au RSSI d'instaurer une politique de sécurité en actions, puis de mesurer la performance du SI afin de l'évaluer et de l'améliorer. "*Elle vise à agir sur la sécurité physique (accès aux locaux, protection des postes de travail et des serveurs…) et sur la sécurité logique (conception des logiciels, utilisation d'internet…). […] L'ISO/CEI 27001 couvre tous les supports d'information, de l'ordinateur portable à la sécurité incendie en passant par les comportements individuels*" selon Philippe Bourdalé, chef de produit AFNOR Certification(15).

Avantages	**Inconvénients**
Améliore l'image de l'entreprise	Certification longue à mettre en place, entre 6 et 12 mois selon l'entreprise
Réduit la charge des audits clients	L'ensemble des exigences doit être respecté
Délimite un périmètre optimal pour la SSI	Nécessite d'avoir un RSSI
Consolide la confiance entre une entreprise et ses clients	Le coût de la démarche varie d'une structure à l'autre

Réduit les coûts de la gestion de la sécurité de l'information	En France, certaines entreprises favorisent la formation sans la certification
Peut répondre à un besoin ou une exigence d'un client	Nécessité d'avoir un SI mature pour obtenir la certification
Permet une amélioration continue du SI	
Prépare les petites et moyennes entreprises à intégrer une stratégie de groupe, éventuellement une fusion	
Homogénéise la gestion du SI lorsque le nombre de site est important	
Aide à être conforme aux réglementations	

Tableau 8 Tableau récapitulatif de les avantages et des inconvénients de la norme ISO/CEI 27001:2015 [source : auteurs]

Ce tableau met en lumière les avantages et les inconvénients de la certification. Il faut préciser, cependant, que la certification n'est pas forcément un gage de risque zéro. « *Les mesures liées à une démarche ISO/CEI 27001 rendent le niveau de risque acceptable et gérable, mais ne le suppriment pas.* » met en garde Marcel Schipman, auditeur AFNOR(15). Cependant, l'amélioration continue, une veille technologique permanente ainsi que l'audit régulière et le renouvellement régulier de l'analyse des risques sont des points clefs pour obtenir une bonne sécurité des systèmes d'information.

4. Enjeux du projet

Le recours à la certification ISO/CEI 27001 est une démarche compliquée et un peu floue pour un grand nombre d'organismes. Afin de faciliter son obtention et suivre l'avancement de la certification, l'enjeu de notre projet est de proposer aux organismes notre dossier permettant de mieux appréhender, comprendre et intégrer la norme à travers notre article et des outils d'autodiagnostic simples, interactifs et rapides en optimisant les ressources. Ceux-ci permettront d'aider un responsable SI à piloter la mise en place de la certification en utilisant les outils proposés pour l'aider dans sa mission et dans la prise de décisions.

III. Problématique

1. Définition de la problématique

L'évolution technologique que connaît le monde aujourd'hui et la volonté des entreprises à garantir leurs avantages compétitifs a encouragé celles-ci à développer les systèmes d'information (SI) de plus en plus complexes. Aussi, grâce aux nouvelles technologies de l'information et de la communication (NTIC), les liens entre les entreprises deviennent de plus en plus étroits et les méthodes et les moyens de travail ne cessent d'évoluer.

Aujourd'hui, les entreprises ont besoins d'assurer la fluidité de circulation de leurs informations et de garantir la sécurité des données afin d'éviter les pertes et l'instabilité des processus métiers de l'entreprise. En effet, la norme ISO/CEI 27001 de sa version améliorée de 2013, est devenue au fil des années un outil recommandé dans le milieu des PME et Grandes entreprises en permettant à celles-ci de développer un SMSI efficace.

Dans cet article, nous nous demanderons comment faciliter la démarche de mise en place de cette norme vis à vis d'une entreprise et de son RSSI associé.

2. Définitions des objectifs

En travaillant sur ce projet, nous visons tout d'abord à bien étudier la phase d'avant-projet, d'identifier les axes d'amélioration et de veiller sur l'application des instructions issues des exigences mentionnées dans la norme ISO/CEI 27001:2013. Afin de cadrer les objectifs et leur mise en application, l'outil PDS sera employé pour mieux cerner ce projet.

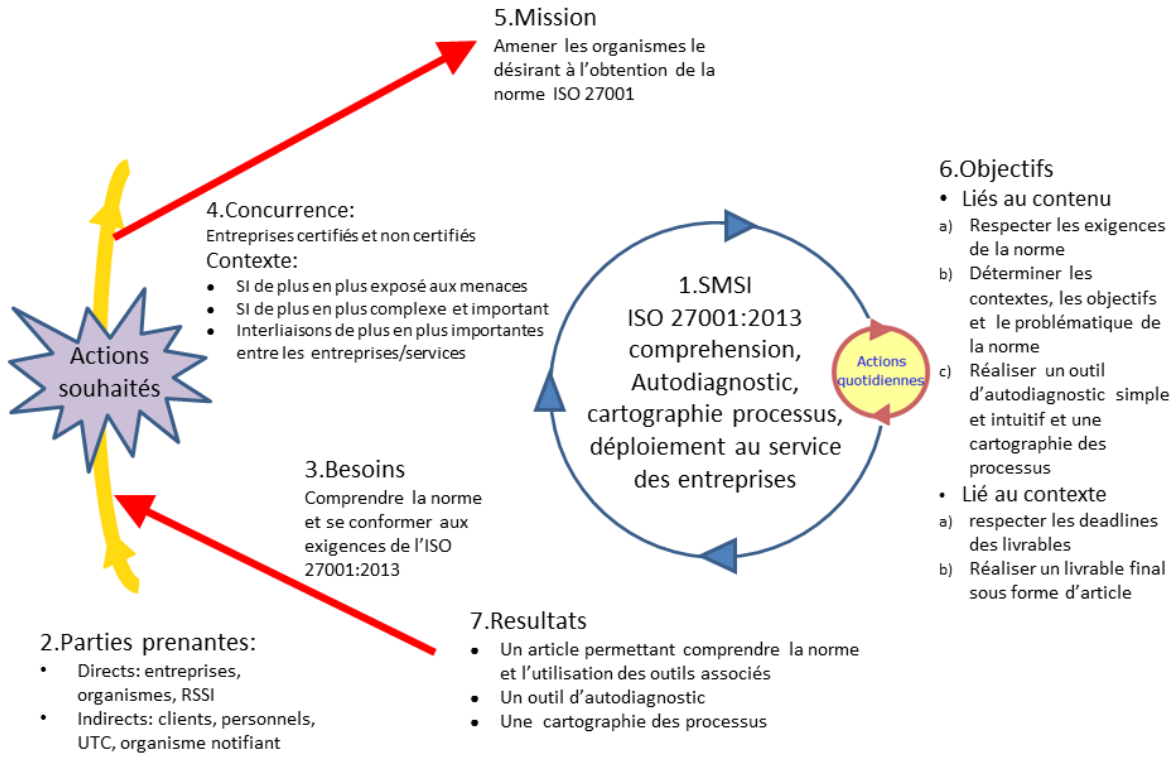


Figure 4 Planification dynamique stratégique de notre projet [source : auteurs]

Chapitre 2 : Méthode de déploiement de l'ISO/CEI 27001

I. Analyse des exigences de la norme

1. Structure de la norme (16)

La norme ISO/CEI 27001:2013 est conforme à une structure qui est appelée l'HLS, High Level Structure. Il s'agit d'une nouvelle structure appliquée dans le cadre commun des normes ISO/CEI. Les normes ISO 9001 et ISO 14001 suivent, par exemple, cette structure. La structure HLS est une approche systématique qui facilite l'identification et le management des normes. Cette nouvelle approche permet de rendre plus efficace l'élaboration des normes ainsi que de simplifier la mise en application de celles-ci.

La nouvelle version de la norme ISO/CEI 27001 comprend 10 chapitres principaux (Domaine d'application, Références normatives, Termes et définitions, Contexte de l'organisme, Responsabilité de la direction, Planification, Support, Activités opérationnelles, Evaluation de la performance et Amélioration). Les 3 premiers chapitres sont généraux et les 7 suivants illustrent les exigences de la norme, pouvant former un modèle de PDCA.

La figure ci-dessous illustre les 7 chapitres illustrant les exigences :

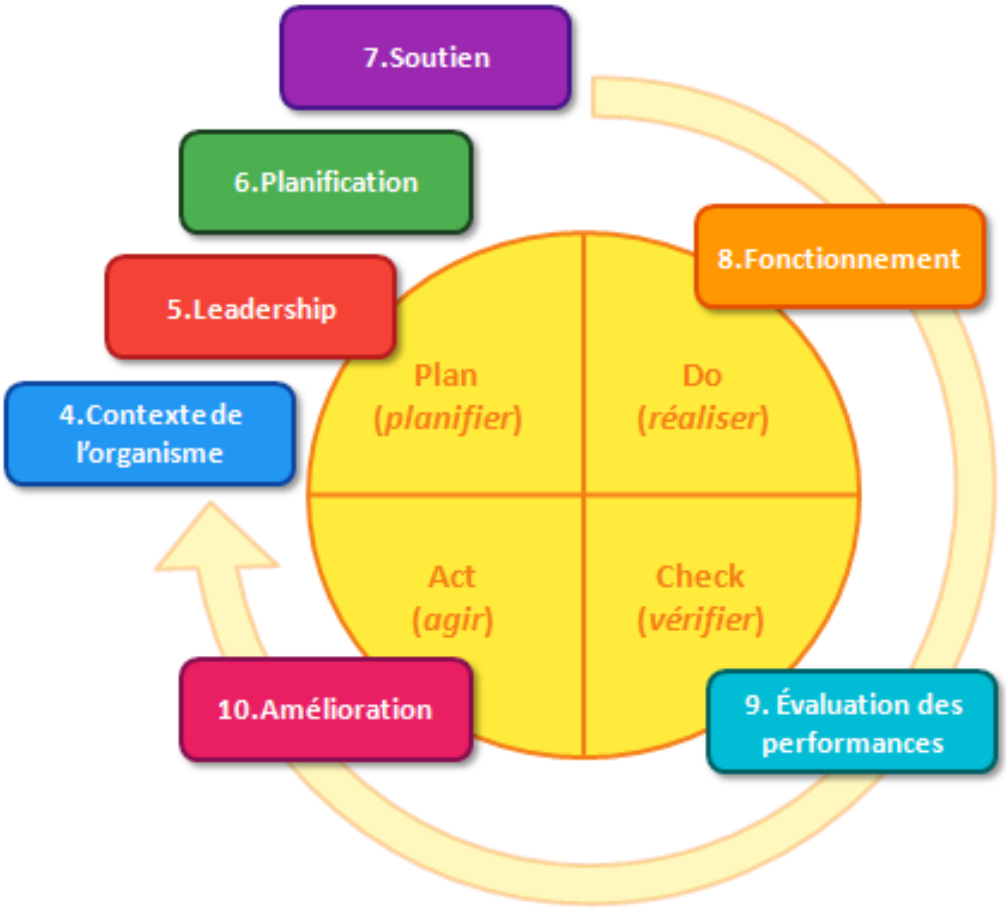


Figure 5 Figure représentant les 7 chapitres illustrant les exigences

2. Principes des chapitres

La norme ISO/CEI 27001 dans sa version 2013 a été l'une des premières normes à intégrer la structure HLS (High Level Structure) proposée dans le cadre commun pour les normes relatives aux systèmes de management.

a) Contexte de l'organisme

Il s'agit d'analyser le contexte de l'organisme afin de définir un périmètre précis pour le SMSI. Dans ce cas, les entreprises sont appelées à prendre en considération les enjeux issus de cette opération et au même temps de penser aux exigences imposées par les parties intéressées.

b) Leadership

La direction doit s'engager dans la démarche de mise en place du SMSI, de fournir les ressources nécessaires pour la réussite de cette opération en prenant en compte l'implication du personnel dans cette mission.

c) Planification

L'organisme doit fixer ses objectifs en planifiant les activités nécessaires et en anticipant les risques potentiels, ce qui va lui permettre de mieux saisir les opportunités. La partie planification comprend la réalisation des exigences de l'Annexe A, découlant des lignes directives des articles 5 à 18 de la norme ISO/CEI 27002.

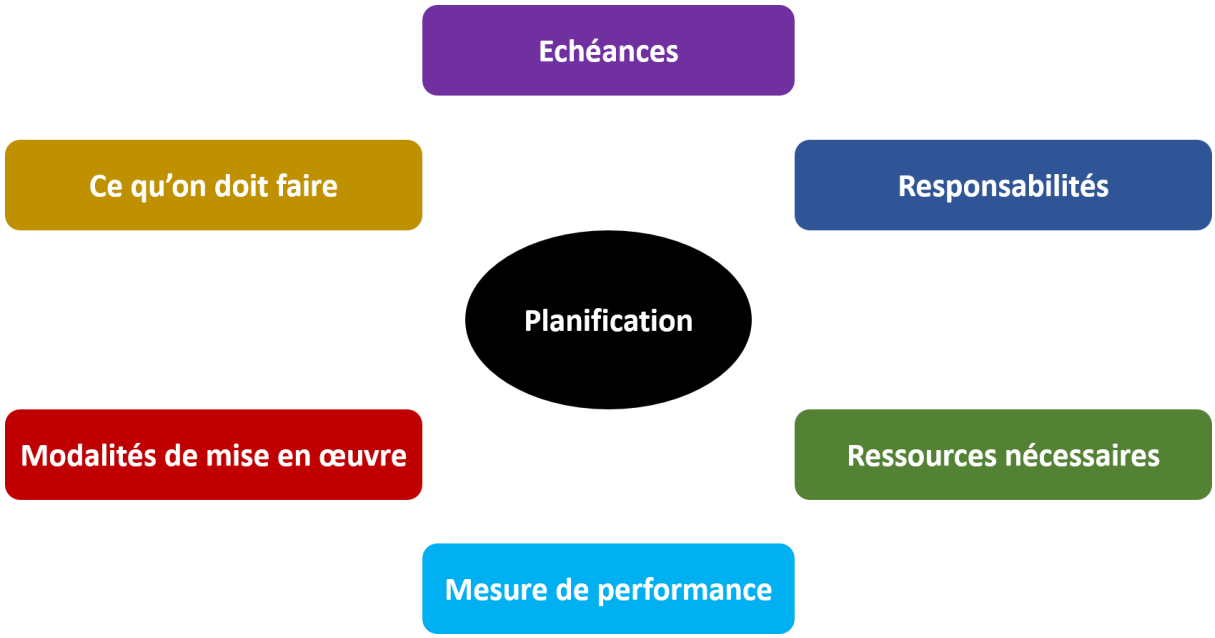


Figure 6 Eléments nécessaires pour la planification [source : auteurs]

d) Soutien

Le soutien concerne trois composantes essentielles ; les ressources, les informations et la communication.

Au vu de la diversité des ressources, l'organisme doit les valoriser et améliorer leur exploitation surtout qu'ils présentent un grand support pour la réalisation des processus de management de la sécurité de l'information.

L'information aussi est très importante pour la réussite de ce projet. Les données doivent être fiables et les informations documentées doivent être conservées.

Et finalement, la communication joue un rôle très important dans le management de la sécurité du SI ; les compétences des collaborateurs doivent être développées afin de les sensibiliser et de les impliquer dans cette démarche.

e) Fonctionnement

L'organisme doit prendre en considération les processus internes et externes selon les critères mis en jeu. Il s'agit de traiter la notion de l'activité en tant qu'ensemble de processus qui permettent de transformer des données d'entrée en éléments de sortie. Ce qui permettra de mieux aborder les différentes activités, leurs managements ainsi que leurs besoins…

f) L'évaluation de la performance

L'organisme, doit définir un ensemble de mesures capable de lui fournir des informations sur les performances des processus et de se positionner par rapport aux objectifs identifiés précédemment.

La revue de direction permet une analyse détaillée sur l'évaluation effectuée pour mieux gérer le système de management du SI. C'est pour cela qu'il est recommandé d'effectuer des audits internes afin d'avoir une bonne vision sur ce système.

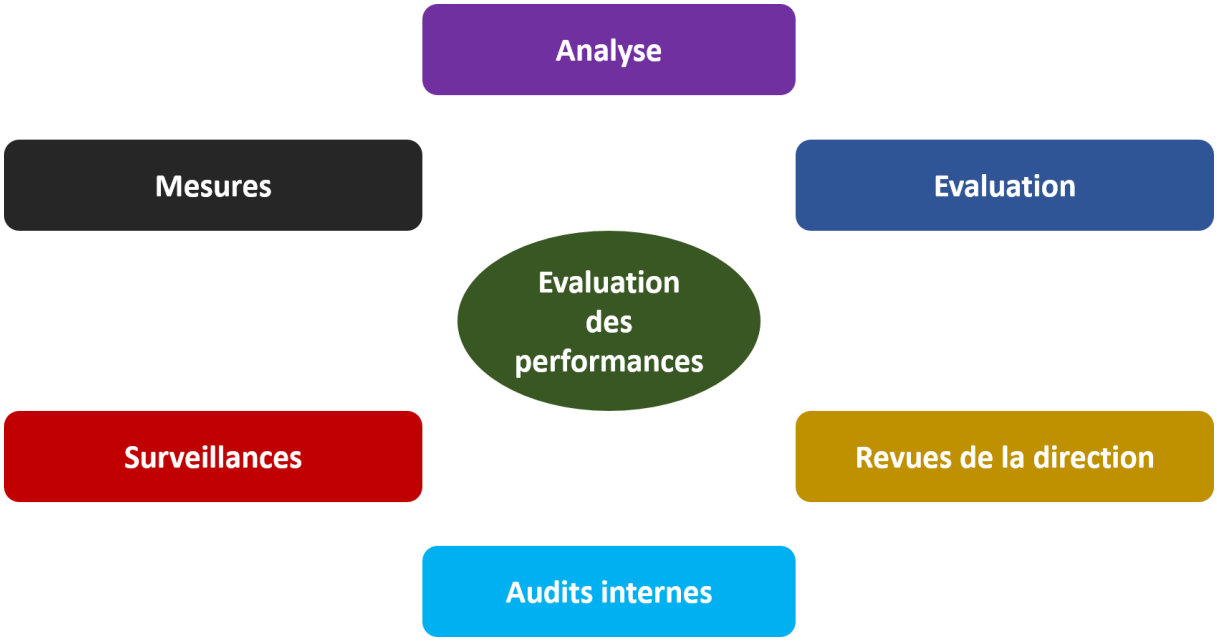


Figure 7 Evaluation des performances [source : auteurs]

g) L'amélioration

L'amélioration continue est l'une des étapes les plus importantes dans notre système. Le SMSI doit être mis à jour régulièrement, adapté aux besoins changeants des entreprises et surtout compatible avec les objectifs des organismes.

3. Annexe et lignes directrices

L'annexe A de la norme ISO/CEI 27001:2013 est bien souvent confondue avec la norme en elle-même. Cette annexe est composée de 114 mesures de sécurité du document ISO/CEI 27002 classées en 14 sections, reprenant les lignes directives de bonne conduite des lignes de l'article 5 à 18 de celui-ci. La norme ISO/CEI 27002:2013 comprends donc des lignes directives nécessaires à l'obtention de la certification ISO/CEI 27001:2013 en termes de mesures pour la sécurité de l'information portant sur les objectifs de contrôle de sécurité de l'information résultant des risques pour la confidentialité,

l'intégrité et la disponibilité des informations. Cette annexe est donc importante pour l'accréditation et donne des exigences concrètes en termes de SMSI.

II. Résultats attendus et anticipation des risques

1. Outil d'autodiagnostic

Il s'agit d'une évaluation complète de l'ensemble des activités de l'entreprise en termes de sécurité de système d'information afin de vérifier la cohérence des résultats de cette évaluation avec les critères exigés par la norme ISO/CEI 27001 :2013.

Les critères d'évaluation sont basés sur :

- Les éléments nécessaires à l'opération de mise en place de la certification ISO/CEI 27001 :2013 comme les facteurs humains et les engagements de la direction.
- Les principes de management de la sécurité de l'information.
- Les exigences issues de la normes ISO/CEI 27001 :2013 qui doivent être respectées et appliquées selon les instructions de la documentation de la norme.
- La stratégie de l'entreprise en ce qui concerne le traitement des documentations et les procédures à prendre en considération pour la maitrise des risques liés à l'information.
- Les objectifs généraux de cet outil.

L'exploitation des résultats générés par cet outil présentera un excellent support pour l'aide à la prise de décision, ce qui permettra de ;

- ✓ Définir la politique de l'entreprise en termes de sécurité de l'information.
- ✓ De mieux cadrer le projet et planifier la démarche de la mise en place de la certification ISO/CEI 27001 :2013.

Donc, notre objectif sera d'exploiter les résultats de notre outil d'autodiagnostic. Ces résultats feront l'objet d'une analyse des besoins et attentes de l'entreprise et des parties intéressées par la démarche de mise en place d'un SMSI. Ce qui va renforcer le dialogue et la communication entre les différents acteurs et la sensibilisation sur les principes de management.

Cet outil sera réalisé à l'aide d'un tableur Excel©, en nous aidant des supports proposés lors des projets QPO « Du management agile à la certification ISO/CEI 27001:2013 »(17) et « Aide au déploiement et outil d'autodiagnostic de la norme ISO 9001:2015 »(18) nous étudions les avantages et les inconvénients de cet outil.

Avantage	Inconvénients
Outil simple à adapter	Fichier lourd
Outil gratuit	Fichier complexe, peut entrainer des erreurs
Possibilité d'insérer des graphiques	Fichier difficile à mettre en place
Outil interactif	Nécessite Microsoft Excel
Résultats directement exploitables	
Outil permettant de se situer facilement par rapport à la norme	
Outil facilement améliorable	

Tableau 9 Avantage et inconvénients de l'outil d'autodiagnostic sur Excel© [source : auteurs]

2. Cartographie des processus

C'est un outil incontournable en ce qui concerne la méthode de travail par approche processus. Il sert à fournir une compréhension efficace de l'ensemble des processus clés pour réussir la mise en place d'un SMSI efficace, permettre d'obtenir une vue claire sur les activités de l'entreprise ainsi que sur les ressources disponibles (support et les facteurs influant sur la prise de décisions du management du SMSI.)

En effet, cette cartographie permet d'analyser les activités de l'entreprise allant du macro-processus, jusqu'à l'ensemble des processus opérationnels.

Cet outil est un parfait complément de l'outil d'autodiagnostic et permet de comprendre les processus, les connections entre ceux-ci et les différents acteurs.

La cartographie est réalisée à l'aide du logiciel ScenariChain qui permet d'obtenir un outil de cartographie fullweb, ergonomique et interactif ne demandant qu'un navigateur internet. Ce logiciel a été développé par l'UTC et est disponible gratuitement sur le web. Les avantage et les inconvénients de cet outil sont les suivants :

Avantages	Inconvénients
Interactif	Exigences ne sont pas détaillées
Gratuit	Nécessite une connexion internet
Cartographie disponible sur le Web	
Libre accès	
Organise les processus de l'entreprise	
Norme et Exigences abrégées	
Visuel clair	

Tableau 10 Avantages et inconvénients de la cartographie des processus sous ScenariChain [source : auteurs]

3. Risques

L'outil d'autodiagnostic est une aide importante pour le déploiement de la norme. Il a pour objectif d'être fiable et efficace lors de son utilisation. Donc, pour assurer que l'outil peut fonctionner correctement, il est nécessaire de réaliser une analyse des risques. On prévoit les problèmes existants possibles et nous essayons de trouver les actions préventives à réaliser, dans le cas où l'utilisateur est confronté à certains risques.

Nous décidons de diviser les risques en deux catégories, les risques techniques et les risques liés au contenu.

	Problème	Conséquences	Actions préventives
Tec	Modification des outils	Génération d'erreurs	Limiter au maximum la modification des outil

h n i q u e	Compatibilité de version	Génération d'erreurs	Recommander des configurations minimales
	Problèmes d'interconnections entre les éléments constitutifs des outils	Génération d'erreurs	Tester l'outil en temps réel plusieurs fois
	Mauvaise diffusion des outils	Pas accessible par les utilisateurs	S'assurer tous les ans que l'outil est disponible sur Internet

Tableau 11 Evaluation des risques techniques de l'outil d'autodiagnostic [source : auteurs]

	Problème	**Conséquences**	**Actions préventives**
C o n t e n u	Manque de compréhension de l'utilisateur	Mauvaise utilisation de l'outil, abandon de l'utilisateur, résultats erronés	Réaliser au sein des outils une notice d'utilisation claire
	Evolution de la norme (non mise à jour des outils)	Outil obsolète	Préciser clairement la version pour laquelle l'outil a été conçu
	La non-couverture totale des outils	Résultats erronés	S'assurer que toutes les exigences sont citées
	Fiabilité des outils	Résultats erronés	S'assurer que toutes les exigences listées sont conformes à la norme
	Manque d'informations sur l'utilisation des outils	Mauvaise utilisation de l'outil, abandon de l'utilisateur, résultats erronés	Réaliser un outil clair et facile d'utilisation
	Fonctions incomplètes	Manque de résultats, outil incomplet	Développer un outil suffisamment complet pour être utilisé lors de l'évaluation complète de la conformité

Tableau 12 Evaluation des risques liés au contenu de l'outil d'autodiagnostic [source : auteurs]

Chapitre 3 : Résultats et perspectives

I. Cartographie des processus

La cartographie de ISO/CEI 27001:2013 a été mise en place grâce au logiciel ScenariChain© et son modèle (process). Elle permet de décrire tous les processus pour déployer cette norme, l'apprentissage est interactif. C'est une façon efficace et claire de comprendre la norme ISO/CEI 27001:2013.

Cette cartographie a été établie en reprenant les différents chapitres de la structure HLS afin de faciliter la compréhension de la cartographie entre la norme et celle-ci. Trois types de processus ont été identifiés : management, opérationnel et support qui transforment des éléments d'entrée en éléments de sortie. Les bonnes pratiques issues de la normes ISO/CEI 27002 sont au centre du processus d'amélioration continue, mis en place au cœur du pilotage opérationnel.

Les pilotages sont définis de la façon suivante :

- Le processus de management : pilote l'organisme pour définir sa stratégie et sa politique et lance une planification des objectifs à réaliser au sein du processus opérationnel,
- Le processus opérationnel : il s'agit du processus réalisant les objectifs fixés par le processus de management et qui forme un cercle d'amélioration autour des bonnes pratiques de la norme ISO 27002,
- Le processus support : processus traitant de la logistique qui soutient le bon fonctionnement du processus opérationnel.

ISO27001 : version 2013

ISO27001 : version 2013

Différents éléments peuvent inciter une entreprise à sécuriser son système d'information autour de trois axes (sécurité de l'information, disponibilité de l'information et intégrité de l'information). Cette décision peut provenir d'une réglementation (Règlement Général sur la Protection des Données), d'un choix interne ou d'une exigence cliente (avec exigence d'audit ou de certification). Le macro-processus réalisé à partir des exigences de l'ISO 27001 permet d'établir, mettre en oeuvre évaluer et améliorer le SMSI d'un organisme pour obtenir la satisfaction des parties prenantes avec un SI sécurisé et performant,et ainsi le préparer à la certification.

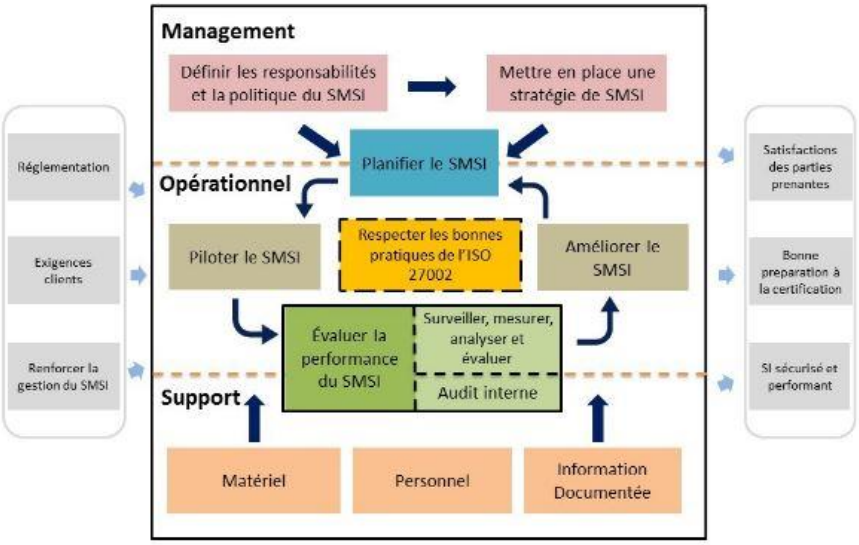


Figure 8 Cartographie des processus de la norme ISO/CEI 27001 sous ScénariChain© [source : auteurs]

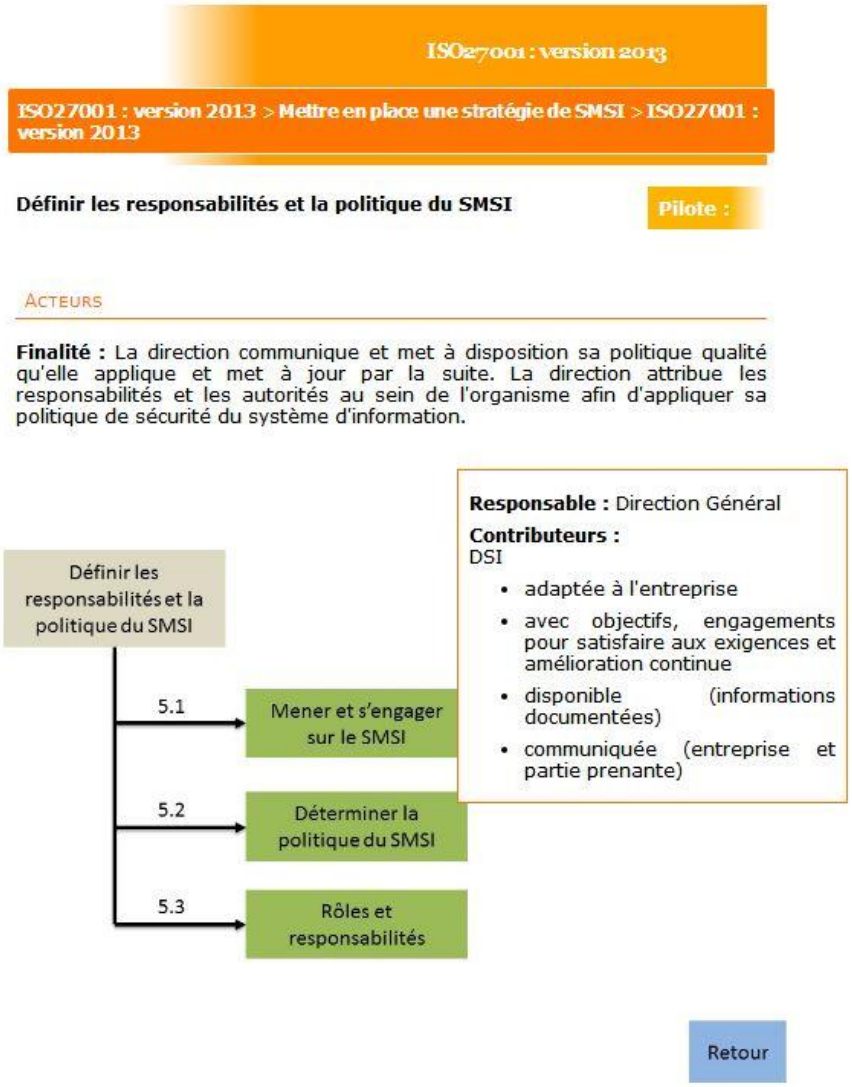


Figure 9 Exemple d'un processus de la cartographie de la norme ISO/CEI 27001 dans ScénariChain©[source: auteurs]

II. Outil d'autodiagnostic

L'outil d'autodiagnostic a donc été mis en place sur le logiciel Microsoft Excel©, il permet d'évaluer le niveau de conformité du SI d'un organisme face à la norme ISO/CEI 27001 :2013 et de visualiser les résultats à travers des graphiques permettant d'identifier les axes de progression et démarrer une démarche d'amélioration continue.

Notre outil permet de :

- Faire un état des lieux du SMSI par rapport à la norme,
- Observer les résultats de l'état des lieux avec possibilité de communiquer les résultats en interne,
- Mettre en place des plans d'action,
- Gérer et suivre la mise en œuvre des actions définies.

Pour cela, l'outil est structuré en 9 onglets principaux : Mode d'emploi, Exigences, Mesures de l'annexe A, Résultats globaux, Résultats par article, Résultats de l'annexe A, Conseils, Déclaration ISO 17050.

1. Onglet-Mode d'emploi

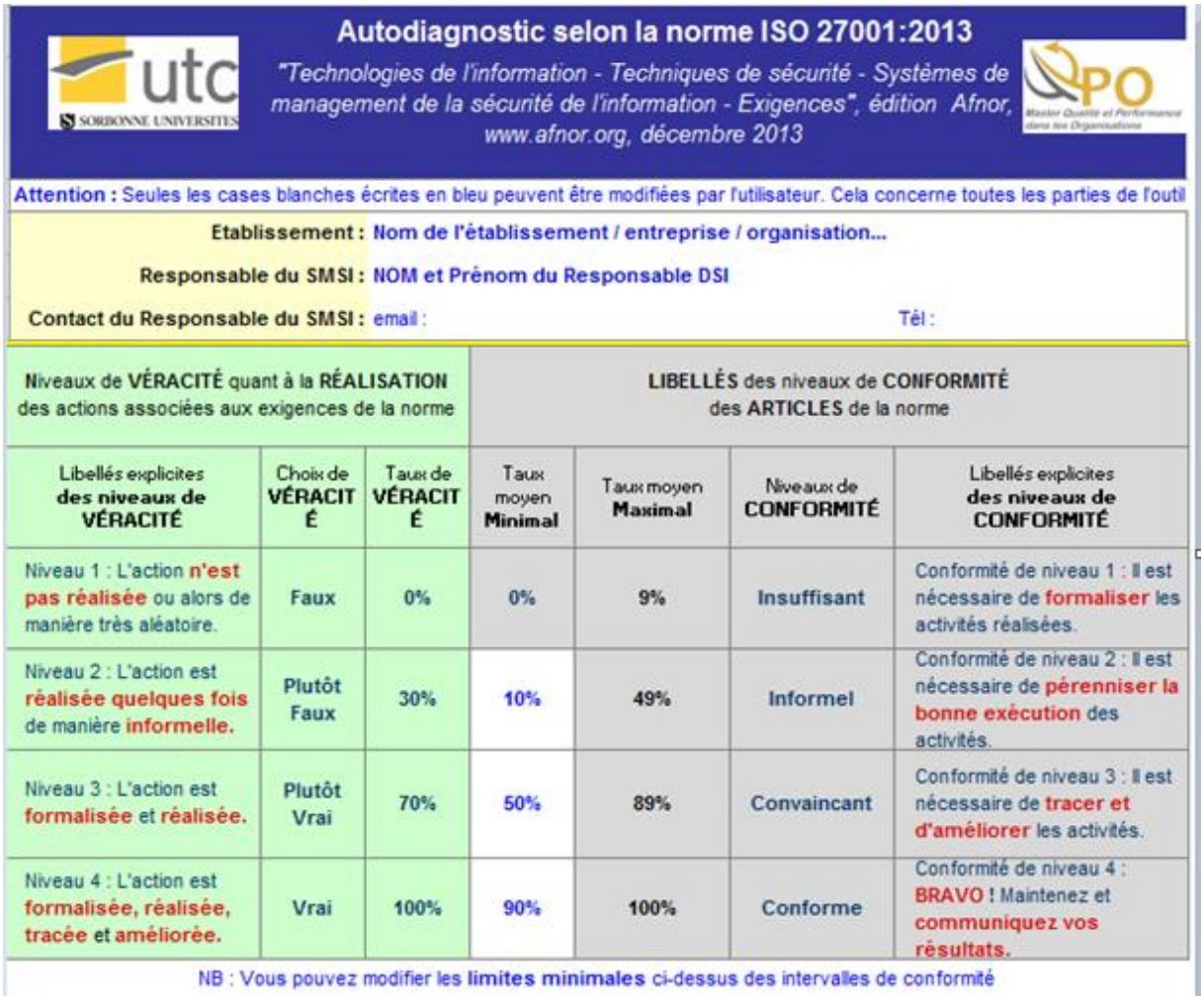
L'onglet « Mode d'emploi » permet d'expliquer à l'utilisateur le fonctionnement de l'outil en le présentant. Il est composé :

- D'un en-tête, qui permet de renseigner les métadonnées (date, nom de l'entreprise, responsable SMSI…)
- D'un manuel d'emploi, qui permet de comprendre les objectifs de l'outil et explique chaque onglet de l'outil.
- D'une échelle d'évaluation, qui présente les modalités d'évaluation utilisées, le niveau de conformité et de véracité. Cette évaluation se fait à travers 4 modalités : ˝Faux˝, ˝Plutôt faux˝, ˝Vrai˝ et ˝Plutôt vrai˝.

Niveaux de véracité	Niveaux de conformité
Faux	Insuffisant
Plutôt faux	Informel
Plutôt vrai	Convaincant
Vrai	Conforme

Tableau 13 Concordance entre les niveaux de véracité et les niveaux de conformité [source: auteurs]

Il est aussi possible d'adapter l'échelle d'évaluation à leurs besoins. Les taux de conformité peuvent être modifiés en changeant les limites minimales des intervalles de conformité selon le niveau d'exigence à satisfaire pour le SMSI.



Autodiagnostic selon la norme ISO 27001:2013

"Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences", édition Afnor, www.afnor.org, décembre 2013

Attention : Seules les cases blanches écrites en bleu peuvent être modifiées par l'utilisateur. Cela concerne toutes les parties de l'outil

Etablissement :	**Nom de l'établissement / entreprise / organisation...**
Responsable du SMSI :	**NOM et Prénom du Responsable DSI**
Contact du Responsable du SMSI :	email : Tél :

Niveaux de **VÉRACITÉ** quant à la **RÉALISATION** des actions associées aux exigences de la norme			**LIBELLÉS** des niveaux de **CONFORMITÉ** des **ARTICLES** 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%	9%	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	30%	10%	49%	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	70%	50%	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.**

NB : Vous pouvez modifier les **limites minimales** ci-dessus des intervalles de conformité

Figure 10 Onglet "Mode d'emploi" de l'outil d'autodiagnostic [source : auteurs]

2. Onglet-Exigences

L'onglet ˝Exigences˝ contient les exigences de la normes reprises point par point, reformulées et classées en article et sous articles.

La grille d'évaluation est constituée de l'item à évaluer, du niveau de véracité et du taux de conformité correspondant. Cet onglet permet à l'utilisateur d'intégrer, au fur et à mesure, les commentaires qu'ils jugent nécessaires.

Document d'appui à la déclaration première partie de conformité à la norme ISO 27001:2013 sur pages A4 100% en format horizontal

Autodiagnostic sur les exigences de l'ISO 27001:2013

Etablissement :	**Nom de l'établissement / entreprise / organisation...**	
Date de l'autodiagnostic :		Signature du responsable de l'autodiagnostic :
Responsable de l'autodiagnostic :	**NOM et Prénom** Tél : @ :	
L'équipe d'autodiagnostic :	Noms et Prénoms des participants	

Réf.	Critères d'exigence des articles de la norme	Evaluations	Taux %	Libellés des évaluations	Modes de preuve et commentaires
Art. 4	Contexte de l'organisme	Convaincant	87%	Conformité de niveau 3 : Il est nécessaire de tracer et d'améliorer les activités.	
4.1	Compréhension de l'organisme et de son contexte	Convaincant	67%	Conformité de niveau 3 : Il est nécessaire de tracer et d'améliorer les activités.	
cr 1	Les enjeux internes et externes sont **déterminés** relativement à la **finalité** et l'orientation stratégique de l'organisme	Choix de VÉRACITÉ		Libellé du critère quand il sera choisi	

Figure 11 Onglet "Exigences" de l'outil d'autodiagnostic [source : auteurs]

3. Onglet-Mesures de l'annexe A

L'onglet ˝Mesures de l'annexe A˝ contient les mesures de l'annexe A de la norme ISO/CEI 27001 reprises point par point et classées en article et sous articles.

La grille d'évaluation est constituée de l'item à évaluer, du niveau de véracité et du taux de conformité correspondant. Cet onglet permet à l'utilisateur d'intégrer, au fur et à mesure, les commentaires qu'ils jugent nécessaires.

Les bonnes pratiques issues des lignes directives issues du document ISO/CEI 27002 sont reprises pour chaque mesure et propose au DSI des mesures à mettre en place pour réaliser chacune des mesures.

100%	Conforme	Conformité de niveau 4 : BRAVO ! Maintenez et communiquez vos résultats.	Guides des bonnes pratiques selon ISO 27002
100%	Conformité de niveau 4 : BRAVO ! Maintenez et communiquez vos résultats.		
100%	Niveau 4 : L'action est formalisée, réalisée, tracée et améliorée.		**Mesure 1** **Il convient que** l'organisme définisse la stratégie, les règlementations, les législations et les contrats & l'environnement convenable pour l'identification des menaces SSI La politique de la sécurité du SI comporte ; Une définition claire de la sécurité du SI ainsi que les objectifs principaux pour mieux gérer les activités SSI. L'attribution des responsabilités Les processus de traitement des dérogations et des exceptions **Mesure 2** **Il convient que** chaque politique soit affectée à un responsable qui accepte de développer, évaluer et revoir cette politique.
100%	Niveau 4 : L'action est formalisée, réalisée, tracée et améliorée.		

Figure 12 Onglet "Mesures de l'annexe A" de l'outil d'autodiagnostic [source : auteurs]

4. Onglet-Résultats globaux

Cet onglet permet de traiter les résultats de la partie ˝Exigences˝ en les synthétisant à travers des représentations graphiques. Il permet d'évaluer l'efficacité du SMSI et d'identifier les axes d'amélioration. L'utilisateur peut noter ses remarques et plans d'action en précisant les objectifs à atteindre, les personnes responsables ainsi que le périmètre d'application et les échéances.

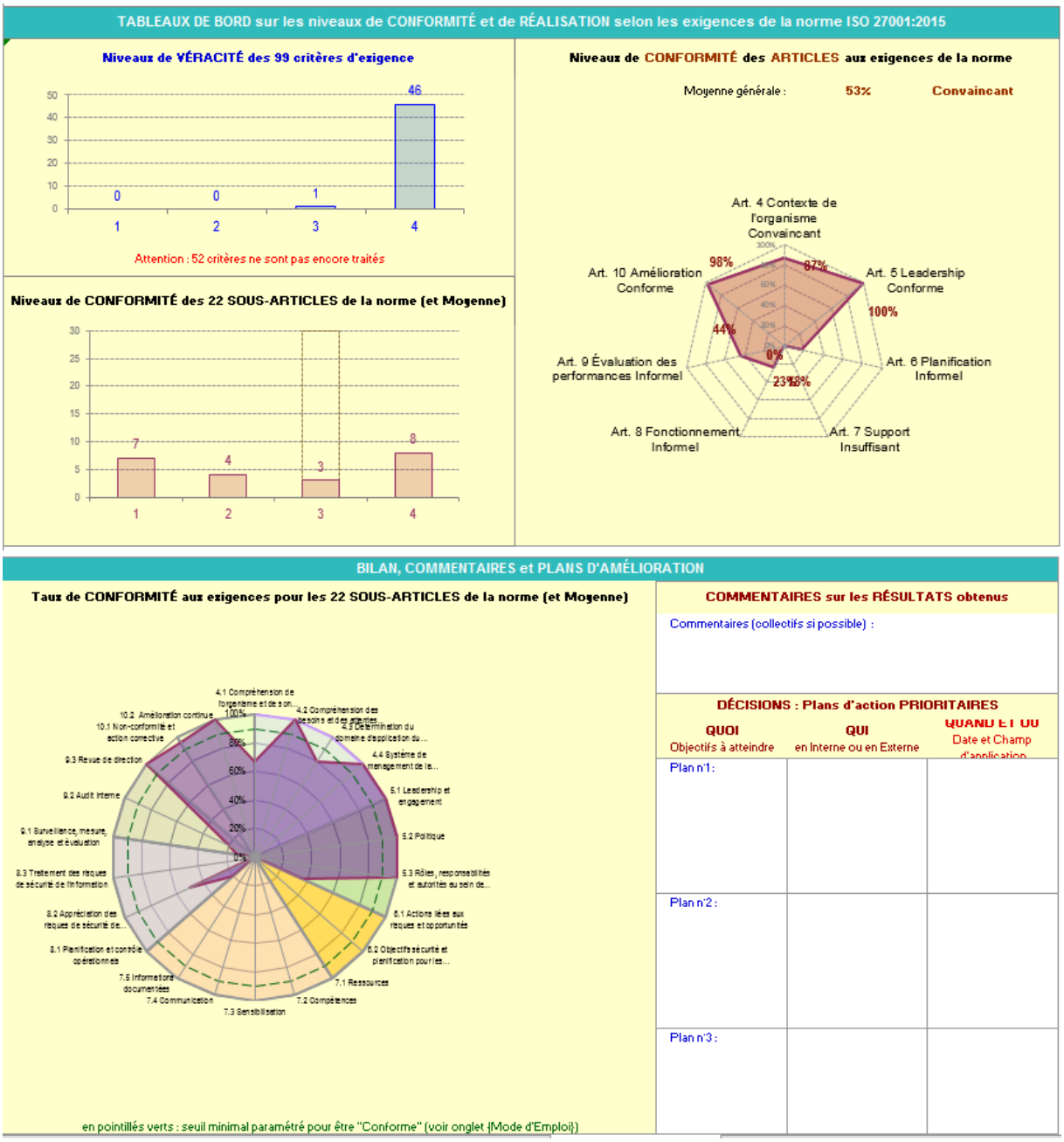


Figure 13 Onglet " Résultats globaux " de l'outil d'autodiagnostic [source : auteurs]

5. Onglet-Résultats par article

Après une vue globale des résultats, cet onglet permet de visualiser les résultats de chaque article séparément. Cet onglet donne une meilleure visibilité des point sensibles du SMSI.

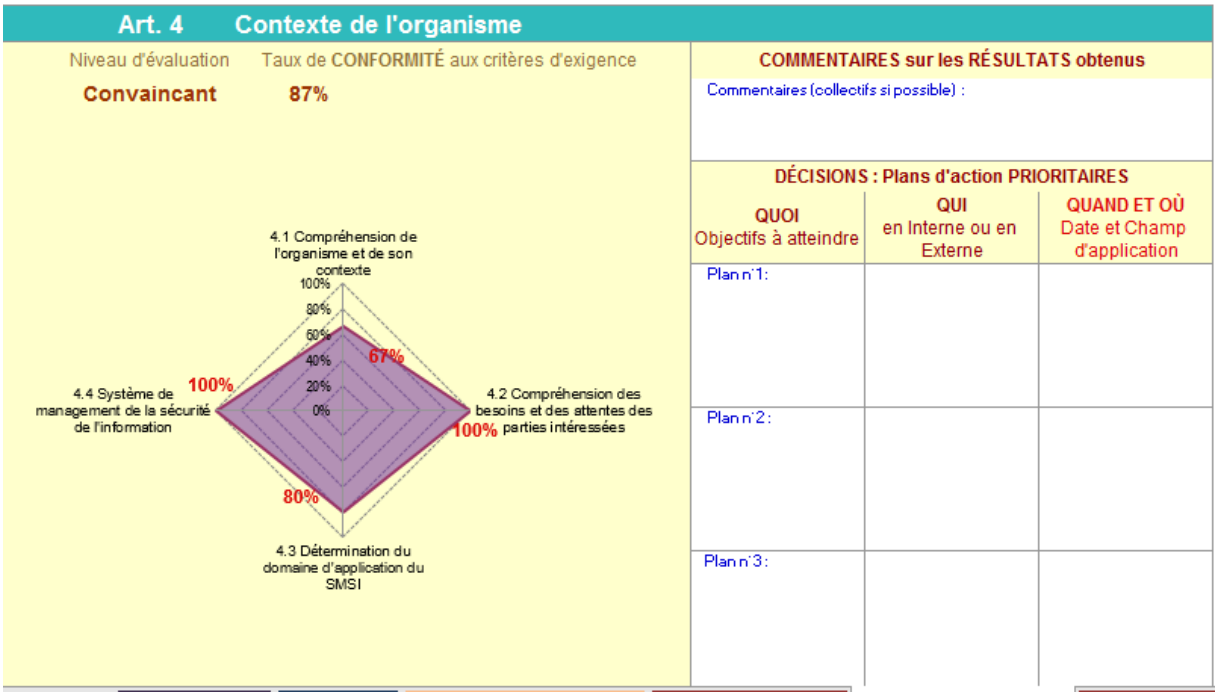


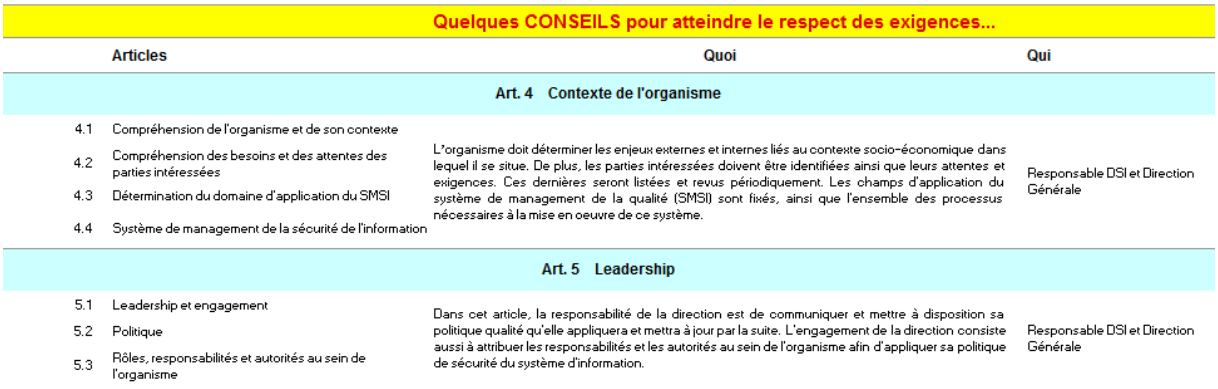
Figure 14 Onglet "Résultats par Article" de l'outil d'autodiagnostic [source: auteurs]

6. Onglet-Résultats de l'annexe A

Cet onglet permet de traiter les résultats de la partie ˝Mesures de l'annexe A˝ en les synthétisant à travers des représentations graphiques. Il permet d'évaluer la conformité des bonnes pratiques proposées dans le document ISO/CEI 27002 et d'identifier les axes d'amélioration. L'utilisateur peut noter ses remarques et plans d'action en précisant les objectifs à atteindre, les personnes responsables ainsi que le périmètre d'application et les échéances.

7. Onglet-Conseils

Cette partie comprend des conseils et des suggestions adaptés à chaque article de la norme. Les éléments de cette rubrique guident les utilisateurs en résumant le contenu de chaque article.



Quelques CONSEILS pour atteindre le respect des exigences...			
	Articles	Quoi	Qui
	Art. 4 Contexte de l'organisme		
4.1	Compréhension de l'organisme et de son contexte	L'organisme doit déterminer les enjeux externes et internes liés au contexte socio-économique dans lequel il se situe. De plus, les parties intéressées doivent être identifiées ainsi que leurs attentes et exigences. Ces dernières seront listées et revus périodiquement. Les champs d'application du système de management de la qualité (SMSI) sont fixés, ainsi que l'ensemble des processus nécessaires à la mise en oeuvre de ce système.	Responsable DSI et Direction Générale
4.2	Compréhension des besoins et des attentes des parties intéressées		
4.3	Détermination du domaine d'application du SMSI		
4.4	Système de management de la sécurité de l'information		
	Art. 5 Leadership		
5.1	Leadership et engagement	Dans cet article, la responsabilité de la direction est de communiquer et mettre à disposition sa politique qualité qu'elle appliquera et mettra à jour par la suite. L'engagement de la direction consiste aussi à attribuer les responsabilités et les autorités au sein de l'organisme afin d'appliquer sa politique de sécurité du système d'information.	Responsable DSI et Direction Générale
5.2	Politique		
5.3	Rôles, responsabilités et autorités au sein de l'organisme		

Figure 15 Onglet "Conseils" de l'outil d'autodiagnostic [source: auteurs]

8. Onglet-Plans d'action détaillés

Cet onglet permet à l'utilisateur de planifier et détailler ses plans d'action en précisant les moyens à mobiliser, les mesures de succès et les objectifs à atteindre.

Désignation du Problème	N°	Action	Pilote	Moyens	Gain Estimé	Gain Réalisé	Debut (semaine)	Durée (semaine)	25%	50%	75%	100%
ZONE / Processus....												
	1								1	1	1	1
	2								1			

Figure 16 Onglet "Plans d'action détaillés" de l'outil d'autodiagnostic [source: auteurs]

9. Onglet-Déclaration ISO 17050

À l'issu du processus d'évaluation, une auto-déclaration de conformité est possible selon l'ISO 17050 « Évaluation de la conformité - Déclaration de conformité du fournisseur ». Cette norme permet de justifier une déclaration de conformité par tout fournisseur sur un organisme, un système de management, un processus, une personne, un produit ou un service. Dans cette optique, une fiche d'auto-déclaration de conformité est intégrée à l'outil. Elle sert comme une synthèse de l'autodiagnostic et peut être utilisée comme un support de communication interne sur le niveau de conformité atteint du système de management de la qualité. Cette déclaration ne peut s'effectuer qu'à partir d'un seuil minimal paramétrable par l'utilisateur.

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 17050 : **date de la déclaration invalide**

Objet de la déclaration : **Niveau de CONFORMITÉ aux EXIGENCES de la norme NF EN ISO 27001:2013**

Nom de l'établissement / entreprise / organisation...

Nous soussigés, déclarons **sous notre propre responsabilité** que **les niveaux de conformité de nos pratiques professionnelles** ont été mesurés d'après les exigences de la norme NF EN ISO 27001:2013. Nous avons appliqué **la meilleure rigueur d'élaboration et d'analyse** (évaluation par plusieurs personnes compétentes) et nous avons respecté **les 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 selon les critères d'exigence tirés de la norme NF EN ISO 27001:2013		*Taux moyen*	*Niveaux de Conformité*
Niveau moyen sur l'ensemble des articles de la norme ISO 27001:2013 :		**53%**	**Non déclarable**
Art. 4	Contexte de l'organisme	**87%**	**Non déclarable**
Art. 5	Leadership	**100%**	**Conforme**
Art. 6	Planification	**18%**	**Non déclarable**
Art. 7	Support	**0%**	**Non déclarable**
Art. 8	Fonctionnement	**23%**	**Non déclarable**

Figure 17 Onglet "Plans d'action détaillés" de l'outil d'autodiagnostic [source: auteurs]

III. Retours sur les livrables

Notre projet peut être considéré comme réussi que si les livrables sont clairs et utilisables.

Nos livrables ;

La cartographie des processus : elle permet de schématiser les éléments d'entrée et de sortie traduisant les objectifs et les engagements de l'organisme en matière de sécurité d'information. Ce

qui nous aide à travailler sur l'ensemble des processus « Management – Métier – Support » nécessaire afin de garantir l'atteinte des objectifs et le respect des engagements.
Cette cartographie a été faite à l'aide du logiciel SenariChain ; et avec un simple clic sur l'un de ses éléments principaux, il est possible de naviguer vers d'autres écran permettant d'avoir plus de détails et d'informations.
L'outil d'autodiagnostic : il s'agit d'un outil d'aide à la prise de décision qui a pour rôle l'évaluation des pratiques quotidiennes en matière de sécurité de l'information en comparant ces pratiques par rapport aux exigences intégrées dans l'outil et qui sont issues de la norme ISO/CEI 27001:2013. Il est constitué par plusieurs feuilles xls ;

- Un guide d'utilisation
- Les exigences selon ISO/CEI 27001 :2013
- Les résultats de l'évaluation
- L'auto déclaration
- Guide des bonnes pratiques selon ISO/CEI 27002

Le mémoire d'intelligence méthodologique : c'est là où l'on peut trouver tous les détails du projet allant de la définition du périmètre et étude de faisabilité jusqu'à la présentation finale de nos outils et les perspectives de notre projet. Composé de trois grandes parties réparties selon trois jalons fixés afin d'informer nos tuteurs sur les états d'avancement de nos travaux.
Un poster récapitulatif : destiné aux lecteurs, ce poster renseigne sur le contenu de notre projet en figurant les différentes étapes de réalisation et les facteurs clés influant sur un SMSI. Il sera affiché lors de la journée AGORA qualité organisée par l'UTC, le 18 janvier 2018.
Présentation Powerpoint : ce livrable permet de présenter notre projet et convaincre les personnes intéressées d'essayer nos outils et de présenter notre travail aux enseignants et tuteurs.

IV. Perspectives d'amélioration

Dans une perspective d'évolution continue, une amélioration intéressante serait de rendre fonctionnel notre outil d'autodiagnostic à partir d'une interface VBA avec un ensemble de boutons et de données d'entrées analysables. Par conséquent, l'utilisateur pourrait jouir d'un ensemble d'interfaces plus interactives intégrant des écrans d'analyse et une visualisation chiffrée d'une situation donnée ce qui rendra la prise de décision plus efficace et rapide.

Aussi, il serait intéressant de permettre aux utilisateurs d'avoir des rapports générés par cet outil afin de communiquer les résultats à la direction et les parties intéressées.

Conclusion

Ce travail entre dans le cadre de la réalisation de notre projet « Aide à la mise en place de la certification ISO/CEI 27001 version 2013 ».

Assurer la sécurité de l'information est devenu primordial aujourd'hui afin de permettre aux entreprises de persister dans un marché de plus en plus concurrentiel. On rappelle que cette sécurité implique une veille efficace sur les aspects de l'intégrité, la disponibilité et la confidentialité de l'information. De plus, avec la quantité importante de données circulantes, les organismes sont de plus en plus vulnérables à des pertes significatives ou à des problèmes d'efficacité.

La famille des normes ISO/CEI 270XX a été conçue pour sensibiliser les organismes de l'importance de la sécurité de l'information et fournir une opportunité d'adopter une gestion efficace du SI entreprise par la voie de la certification ISO/CEI 27001 qui est devenue de plus en plus certifiée sachant que celle-ci compte parmi les normes les plus certifiées dans le monde.

Notre travail est achevé sous trois parties ;
Dans une première, nous avons essayé de vulgariser et expliquer le principe de notre travail vis-à-vis de la sécurité du SI ainsi que la norme ISO/CEI 27001. Ensuite, nous avons défini les éléments clés du projet son périmètre et ses enjeux ainsi que les apports et le contenu de la famille des normes ISO/CEI 27000.

Puis dans une deuxième partie, nous avons travaillé sur la préparation de nos outils supports que nous avons définis. Pour la cartographie des processus, elle a été conçue pour fournir une vision claire sur l'ensemble des processus de l'entreprise en matière de sécurité de l'information. Quant à l'outil d'autodiagnostic, son rôle était de permettre une évaluation de l'ensemble des pratiques de l'organisme et de comparer ces pratiques aux exigences de la norme ISO/CEI 27001 version 2013, ce qui permet de se positionner vis-à-vis de ces exigences et de se préparer pour une mise en place efficace de la certification.

Enfin, la troisième partie a été consacrée à la présentation finale de nos outils, d'exposer les valeurs ajoutées et les perspectives de notre projet, tout en apportant des suggestions d'amélioration afin de rendre ces outils plus efficaces prochainement.

Références bibliographiques

1. Cybersécurité : la vigilance est de mise ! [Internet]. Groupe AFNOR. 2017 [cité 8 oct 2017]. Disponible sur: http://www.afnor.org/actualites/cybersecurite-vigilance-de-mise/

2. TENEAU Gilles, DUFOUR Nicolas. Normes ISO 2700x : vers la gouvernance de la sécurité des systèmes d'information. Tech Ing Système Manag Risque [Internet]. 10 avr 2013;base documentaire : TIB626(ref. article : g9060). Disponible sur: http://www.techniques-ingenieur.fr/base-documentaire/environnement-securite-th5/systeme-de-management-du-risque-42626210/normes-iso-2700x-vers-la-gouvernance-de-la-securite-des-systemes-d-information-g9060/

3. BUSINESS B. Sécurité : faut-il se certifier ISO 27001 ? [Internet]. BFM BUSINESS. [cité 5 oct 2017]. Disponible sur: http://bfmbusiness.bfmtv.com/01-business-forum/securite-faut-il-se-certifier-iso-27001-384687.html

4. Infographie : le top 5 des certificats ISO les plus délivrés en 2016 [Internet]. Le Mag Certification. 2017 [cité 19 déc 2017]. Disponible sur: https://lemagcertification.afnor.org/blog/infographie-top-5-certificats-iso-plus-delivres-2016/

5. Moisand D, Labareyre FG de. CobiT: Pour une meilleure gouvernance des systèmes d'information. Editions Eyrolles; 2011. 274 p.

6. Calder A. RGPD UE: Guide de poche. IT Governance Ltd; 2017. 98 p.

7. Infographie RGPD : 56 % des marques ne seront pas prêtes au 25 mai 2018 – Magush DataRespect [Internet]. [cité 27 déc 2017]. Disponible sur: https://magush.io/2017/06/28/infographie-rgpd-56-des-marques-ne-seront-pas-pretes-au-25-mai-2018/

8. TENEAU Gilles, DUFOUR Nicolas. ISO 27001 : management de la sécurité des systèmes d'information. Tech Ing Système Manag Risque [Internet]. 10 oct 2013;base documentaire : TIB626(ref. article : g9062). Disponible sur: http://www.techniques-ingenieur.fr/base-documentaire/environnement-securite-th5/systeme-de-management-du-risque-42626210/iso-27001-management-de-la-securite-des-systemes-d-information-g9062/

9. Synthèse sur la sécurité du système d'information (SI) @OpenClassroomsfr [Internet]. OpenClassrooms. [cité 20 nov 2017]. Disponible sur: https://openclassrooms.com/courses/synthese-sur-la-securite-du-systeme-d-information-si

10. L'AP-HP plombée de 80 M€ après installation d'un nouveau logiciel - Le Monde Informatique [Internet]. LeMondeInformatique. [cité 27 déc 2017]. Disponible sur: https://www.lemondeinformatique.fr/actualites/lire-l-ap-hp-plombee-de-80-meteuro-apres-installation-d-un-nouveau-logiciel-66128.html

11. Piratage de Sony Pictures Entertainment. In: Wikipédia [Internet]. 2017 [cité 20 déc 2017]. Disponible sur: https://fr.wikipedia.org/w/index.php?title=Piratage_de_Sony_Pictures_Entertainment&oldid=141207719

12. 01net. Le piratage des systèmes de perfusion médicaux, nouvelle vision d'horreur [Internet]. 01net. [cité 20 déc 2017]. Disponible sur: http://www.01net.com/actualites/le-piratage-des-systemes-de-perfusion-medicaux-nouvelle-vision-d-horreur-657181.html

13. Cyber-sécurité : les comportements à risque des employés [Internet]. [cité 20 déc 2017]. Disponible sur: https://www.directeurinformatique.com/2015/06/cyber-securite-combattre-les-comportements-a-risque-des-employes-infographie/

14. Cybersécurité : ce qu'en disent les DSI français [Internet]. 2016 [cité 20 déc 2017]. Disponible sur: https://www.roberthalf.fr/presse/cybersecurite-ce-quen-disent-les-dsi-francais

15. Certification ISO 27001 : passer à l'offensive pour protéger ses informations [Internet]. Le Mag Certification. 2015 [cité 4 oct 2017]. Disponible sur: https://lemagcertification.afnor.org/blog/certification-iso-27001/

16. CE à propos de l'auteur GPCDMMAS et ITA et formation : marquage, Applicables N. HLS: La structure universelle des normes de management [Internet]. Qualitiso - Le Blog des Dispositifs Médicaux. 2014 [cité 19 nov 2017]. Disponible sur: http://www.qualitiso.com/hls-high-level-structure/

17. NAIT-OUSLIMANE S. Du management agile à la certification ISO 27001 [Internet]. 2017 [cité 26 déc 2017]. Disponible sur: http://www.utc.fr/~mastermq/public/publications/qualite_et_management/MQ_M2/2016-2017/MIM_stages/NAIT_OUSLIMANE_Sara/

18. BARRY Z, BOUKHRIS I, BENSAID Z, HAMRIT S, SOTO L, MNIF F. Aide au déploiement et outil d'auto-diagnostic de la norme ISO 9001 : 2015 [Internet]. 2016 [cité 26 déc 2017]. Disponible sur: http://www.utc.fr/~mastermq/public/publications/qualite_et_management/MQ_M2/2015-2016/MIM_projets/qpo12_2016_gp09_ISO_9001v2015/

Tables des annexes