Association des Utilisateurs des Systèmes d'Information au Maroc

RENDEZ-VOUS DE L'AUSIM

« ISO 27001 : LE RETOUR D'EXPERIENCE DES CERTIFIES »

15 janvier 2016

Récit de la présentation par Abla EL HOSNI, Chargée de mission à l'AUSIM

Dans le cadre des « **Rendez-vous de l'AUSIM** », l'association a reçu le vendredi 15 janvier 2016 quatre intervenants pour une présentation autour du thème « **ISO 27 001 : Le retour d'expérience des certifiés** ».

Constituant une plateforme d'échange et de partage pour ses membres et la communauté, et dans un souci permanent de mettre à la disposition du DSI des outils de travail et de prise de décision à forte valeur ajoutée, l'AUSIM a souhaité à travers cette thématique mettre en avant le retour d'expérience d'entreprises ayant relevé le challenge de la **certification ISO 27001**.

La sécurité des systèmes d'information est un **véritable défi**, à la fois **technologique** et **économique**. Elle représente aujourd'hui un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de l'informaticien. Sa finalité sur le long terme est de **maintenir la confiance des utilisateurs** et des clients. La finalité sur le moyen terme est la **cohérence de l'ensemble du système d'information**. Sur le court terme, l'objectif est que chacun ait **accès aux informations** dont il a besoin. La norme traitant des **Système de Management de la Sécurité de l'Information** (**SMSI**) est l'**ISO 27001**.

> *La norme ISO 27001 s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…). Elle décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) qui recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels. L'objectif est de protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion. Cela apportera la confiance des parties prenantes.*
>
> *La norme précise que les exigences en matières de mesures de sécurité doivent être adéquates et proportionnées pour ne pas être ni trop laxistes ni trop sévères.* *Source Wikipédia*

Ainsi, les interventions ont porté sur :

- La méthodologie de management de projet de mise en place d'un SMSI et de la certification ISO 27 001 ;
- L'apport des prestataires de service accompagnateurs ;
- Le pré-requis à la certification ;
- Les difficultés rencontrées lors de la mise en place du projet ;
- Les facteurs clés de succès ;
- Les couts estimatifs du projet ;
- La Certification ISO 27 001, so what Next !

Lifting Global Trade.
APM TERMINALS

Bien au-delà de l'aspect conformité, l'expérience de l'implémentation et du maintien de la norme ISO 27001 est un 'eye-opener' permettant une meilleure gouvernance et gestion des risques. Telle est la vision du géant du trafic portuaire, présentée par son DSI de son siège marocain M. Wissam EL ASSAL.

M. EL ASSAL a expliqué comment son entreprise, suivant une politique de Total Quality Management a du se mettre en conformité avec plusieurs normes ISO, et notamment la norme 27001. Ainsi, est-il revenu sur le contexte de mise en place du processus de certification :

D'une part, nous trouvons les exigences du secteur en général et de l'activité en particulier en terme de sécurité des personnes et des données, et d'autre part, l'évolution des outils d'exploitation opérationnelle. M. EL ASSAL a ainsi rappelé la démarche que son département a suivie pour la mise en place d'un SMSI performant en préparation à la certification de son entreprise :

1. Compréhension du contexte : En effet, APM Terminals Tangier a connu, en 2014, la refonte de l'outil de gestion portuaire et a été le premier port au monde à migrer vers cet outil. Face à ces nouvelles exigences, la certification paraissait être le meilleur moyen pour gérer cette transition. Par ailleurs, la conjoncture géopolitique instable a fortement contribué à la facilitation de la mise en place de cette démarche.
2. Identification et évaluation des risques avec le concours des différents départements.
3. Création d'un sens d'urgence vis-à-vis du top management, afin de les faire adhérer à l'idée de la certification et de fédérer l'ensemble des départements autour du projet.
4. Evaluation des incidents passés ;
5. Identification des bénéfices futurs en considérant le triangle Confidentialité – Intégrité- Disponibilité.

M. EL ASSAL insiste sur le fait que la certification ISO 27001 permet une gestion plus organisée du risque en entreprise et recommande :

1. Elargissez le périmètre ! Faire de cette démarche, un projet d'entreprise et pas seulement un projet IT.
2. Impliquez toute l'équipe IT ainsi que l'ensemble des départements concernés (un pilote pour chaque processus/départements) : Elément clé pour fédérer les ressources autour du même objectif ;
3. Réduisez le timeline afin de mieux gérer le process et pousser les équipes à s'impliquer d'avantage ;
4. Faites appel à un œil externe ; Faire appel à un cabinet pour bénéficier de solutions innovantes ;

5. Réussir l'audit n'est pas le seul objectif. C'est une notion à intégrer pour assurer une performance continue du SMSI ;
6. Osez !

Lydec est un opérateur de services publics qui gère la distribution d'eau et d'électricité, la collecte des eaux usées et pluviales et l'éclairage public pour 4,2 millions d'habitants de la Région du Grand Casablanca. Son objectif est de fournir en continu un service de qualité à ses clients, tout en anticipant et en accompagnant le développement de l'agglomération. Ceci ne peut se faire sans un système d'information performant et sans faille. L'enjeu pour la Lydec est énorme si le système s'avère défaillant ; s'agissant de l'interruption de l'activité quotidienne des citoyens et des entreprises.

M. Rachid NEFSSI, chef de service Sécurité d'Information à Lydec depuis 2001, présente la configuration des SI à la Lydec. Ainsi, l'entreprise s'est organisée autour de deux grands systèmes d'information gérés au sein de la DSI : Un SI interne appelé « WEBS », gérant le métier de la Lydec et un SI externe « SAP » gérant les fonctions supports.

A cet effet, la mise en place d'un SMSI performant pour la Lydec devrait répondre à un niveau élevé d'exigences, tant les enjeux sont fondamentaux. Le SMSI devrait permettre une disponibilité continue des SI, une mobilité pour le personnel et les clients, une maitrise des risques, une innovation technologique permanente ainsi qu'un un échange sécurisé avec les partenaires. En tant qu'acteur majeur dans son secteur d'activité, le SMSI doit également veiller à la conformité avec les exigences légales, réglementaires et contractuelles exigées par l'Etat, répondre à la directive nationale de la sécurité des systèmes d'information et protéger le SI contre la cybercriminalité et les nouvelles menaces liées à la sécurité de l'information.

Tant d'enjeux auxquels la certification à la norme ISO 27001 apporte une solution efficace, aussi bien au niveau des process internes que vis-à-vis des exigences des consommateurs et des partenaires.

De ce fait, le contexte de certification ISO 27001 de la Lydec se présente comme suit :

- Politique globale de la sécurité SI de la maison mère GDF Suez ;
- Exigences de la DGSSI ;
- Conformité aux lois 09-08 / 53-05 / 24-96 ;
- Vision stratégique de la Lydec : Synergies 2020.

Par conséquent, la démarche de mise en place et de développement du SMSI Lydec est connu plusieurs étapes :

A la fin de son intervention, M. NEFSSI est revenu sur les opportunités et contraintes rencontrées lors des différentes étapes de développement du SMSI Lydec :

Opportunités :

- Engagement de la DG pour la protection du patrimoine immatériel : 27001 ;
- La politique de Gouvernance de la Sécurité du Groupe (ISO 27001) ;
- Exigences Métier (CIA) Lydec ;
- Lydec certifiée ISO9001/18000 = Processus SI et Interfaces (RH, DDP, DAL, etc.) en place ;
- Bonnes pratique ITIL et projet ISO20000 en cours.

Difficultés :

- Changement du comportement des utilisateurs et des administrateurs ;
- Budget (technologie, implémentation) ;
- Effort de mise en place ;
- Maitrise des documents et des enregistrements ;
- Compétences RH en sécurité SI rares ;
- Veille Sécurité ;
- Conflits d'intérêts entre la sécurité SI et l'exploitation SI.

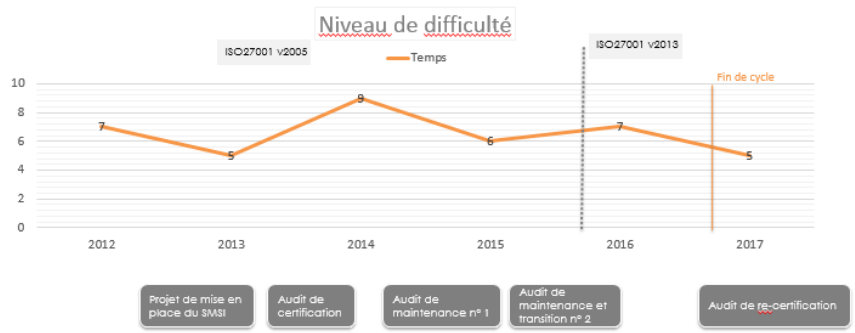
Passage à la nouvelle version 2013 :

- Difficulté à répondre aux nouvelles exigences ;
- Absence d'expérience dans l'implémentation et de l'audit de la nouvelle version ;
- Auditeurs avec un background version 2005,

MAROCLEAR
CSD MOROCCO

Fier d'annoncer que la place boursière marocaine est la seule au monde à avoir son dépositaire central ainsi que sa bourse certifiés ISO 27001, M. Ridouane AZAGROUZE, DSI de MarocClear est revenu dans son intervention sur le contexte de certification de son entreprise. Ainsi, les exigences légales, réglementaires et contractuelles ont fortement contribué à fédérer l'ensemble des départements de l'entreprise autour du projet de certification. L'ambition de développement, la sensibilité des données et des process ainsi que les attaques de plus en plus fréquentes et sophistiquées auxquelles doivent faire face son département constituent également autant de raisons pour la certification.

Ainsi, le projet de certification de MarocClear a connu plusieurs étapes :



Ne souhaitant pas s'attarder sur le volet technique de la préparation de la certification, M. AZAGROUZE a expliqué que malgré le soutien des différentes entités de MarocClear, il y a eu certaines contraintes au niveau du formalisme de la certification. Ainsi, a-t-il recensé un manque d'implication des collaborateurs dans la pratique au quotidien des best practices de l'ISO27001, la restriction de la conformité à l'audit de certification ainsi qu'une résistance au changement et une perception de la sécurité comme une affaire SI.

Afin de remédier à ces problèmes, une campagne de sensibilisation a été lancée au sein de l'entreprise pour fédérer les initiatives autour de la 27001, ainsi que la mise en place d'indices de suivi, de reporting… pour assurer un meilleur suivi du projet. Par ailleurs, un poste de Risk Manager a également été créé. L'appui du top management de l'entreprise a fortement contribué à la réussite de ce projet.

Bourse de Casablanca

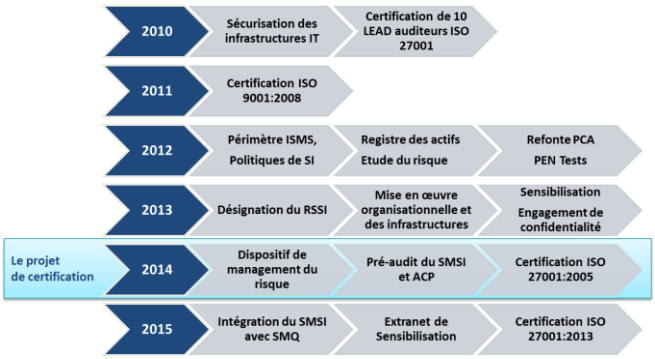
Au même titre que MarocClear, la Bourse de Casablanca doit faire face aux mêmes exigences réglementaires, légales en terme de dispositifs mis en place pour la sécurité des données et des process.

De par son rôle de leader du projet de mise en place du SMSI de la Bourse de Casablanca, M. Yahya ARROUABAT, Responsable Sécurité SI, a fait une présentation portant sur la méthodologie ainsi que les moyens utilisés par l'équipe projet pour l'aboutissement de la certification.

M. ARROUBAT a également présenté les prérequis à un projet de certification, dont voici un extrait :

Exigence de la norme	A formaliser et faire approuver
Support du management	• Les objectifs de sécurité; • Les rôles et responsabilité; • L'engagement de la Direction
Périmètre du SMSI	• Périmètre physique et technologique
Registre des actifs	• Inventaire des actifs, leurs propriétaires; • Classification de l'information
Analyse des écarts	• A effectuer en interne, puis par un prestataires spécialisé
Etude du risque	• La démarche, le planning, le suivi • Le plan de traitement du risque
Déclaration d'Applicabilité (SOA)	• Les contrôles ISO 27001 sélectionnés (ou non) et le justifier; • Les documents d'application…
Documents du SMSI	• Politiques de sécurité et Procédures associées; • Programme de sensibilisation
Revue de direction et Audits	• Planning, Comptes rendus, Fiches d'amélioration

Il est également revenu sur la politique de sécurité SI suivie par la Bourse de Casa.



A la fin de son intervention, M. ARROUBAT est revenu sur les opportunités et contraintes rencontrées lors des différentes étapes de développement du SMSI Lydec.

En effet, le cadre règlementaire favorable ainsi que la préexistence d'un Système de Management de la Qualité ont permis une meilleure cohésion et mobilisation des équipes autour du projet de certification (Soutien du CODIR, Présentation du projet à l'ensemble des collaborateurs, organisation de concours, communication interne…). Par ailleurs, l'intervenant a recensé certaines contraintes dans la mise en œuvre de la certification, à savoir : L'Indisponibilité de l'auditeur externe, le risque de dépriorisation du projet, l'étude du risque, ainsi que la faible intégration SMQ et SMSI.

La matinée s'est terminée par un flot de Questions/Réponses et interventions des participants qui ont trouvé le sujet très riche et captivant, demandant à ce que l'association organise davantage de conférence visant le partage d'expérience entre utilisateurs.