Expert

BEST PRACTICES

Points clés d'une démarche d'implémentation d'un Système de Management de la Sécurité de l'Information selon la norme ISO/IEC 27001

Nicolas Mayer
Ingénieur R&D
et doctorant au
CRP Henri Tudor
www.tudor.lu

La norme ISO/IEC 27001 s'impose de plus en plus comme la référence principale en matière de confiance vis-à-vis de la sécurité des systèmes d'information. Cependant, un tel projet reste complexe et se trouve confronté à l'actuel manque d'expérience sur le marché. Conseils pratiques du spécialiste Nicolas Mayer.

Démarrer un projet d'implémentation ISO/IEC 27001 par une analyse d'écart –

Cette analyse d'écart va se focaliser sur les mesures de l'annexe A de la norme (mesures de sécurité issues de l'ISO/IEC 27002, anciennement ISO/IEC 17799), déjà mises en œuvre au sein de l'organisation. En effet, bien qu'aucune de celles-ci ne soit obligatoire, la plupart de ces mesures s'imposent de fait, au vu des exigences de la norme. Par exemple les exigences de gestion des actifs, de sécurité liée aux ressources humaines, de gestion des incidents ou de conformité aux exigences légales sont explicitement demandées par la norme. De plus, certaines mesures restent incontournables, comme la définition d'une politique de sécurité, la mise en place de contrôles d'accès, la protection contre les codes malveillants...

Choisir minutieusement le domaine d'application et les limites du SMSI

Le choix du périmètre du SMSI est certainement la première exigence de la norme à traiter lors du lancement d'un projet d'implémentation ISO/IEC 27001. Le choix du périmètre du SMSI est totalement libre et laissé à l'appréciation de l'organisation souhaitant se faire certifier. Afin de garder un projet réaliste et dimensionné par rapport aux besoins en sécurité, des objectifs fixés pour la certification et des moyens pouvant être mis-en-œuvre, le choix d'un domaine d'application adapté (ne comprenant pas nécessairement l'ensemble de l'organisation) est fondamental.

S'assurer du soutien de la direction dès le début du projet

Le soutien de la direction est demandé par la norme principalement au sein de la clause 5.1. On y retrouve l'obligation d'impliquer la direction à différentes étapes clés de la mise en œuvre des exigences de la norme, telles que la validation de la politique du SMSI, la définition de rôles et de responsabilités pour la sécurité de l'information et la fourniture de ressources suffisantes pour le SMSI. Cependant, avant même le lancement officiel du projet, disposer du soutien de la direction est primordial. Sur base d'un estimatif des moyens financiers et humains nécessaires, une validation du projet d'implémentation d'un SMSI doit être réalisée par la direction, dès sa définition.

Savoir dimensionner son appréciation des risques

Si l'analyse des actifs, des menaces, des vulnérabilités et des impacts est requise par la norme, il faut savoir qu' aucune indication sur le niveau de détail ni le nombre de chacun de ces éléments n'est donnée. Il faut garder à l'esprit que l'inventaire des actifs et l'appréciation des risques devront être maintenus et toujours contrôlés dans le temps. Le niveau de granularité de ces éléments et leur nombre devront donc être adaptés et permettre la maîtrise de cette étape, en la gardant à une taille gérable et maintenable. Il est également nécessaire de garder à l'esprit la philosophie générale du SMSI qui ne vise pas à l'atteinte d'un niveau absolu de sécurité, mais à mettre en œuvre au sein de l'organisation un système de management avec amélioration continue de la sécurité.

Communiquer autour du SMSI

Des communications régulières, portant sur les résultats du SMSI et sur l'avancement de son déploiement, doivent être menées sous toutes les formes adéquates et adaptées à la culture de l'entreprise (réunions, mails, journal interne...). La communication est également un outil permettant d'associer la direction de l'entreprise, notamment en l'impliquant dans la présentation et l'animation. Il convient lors des réunions de trouver le juste milieu entre la valorisation du travail accompli et la pression nécessaire à l'avancement et au respect des engagements. Enfin, une communication de fin de projet d'implémentation est aussi indispensable, pour tirer les leçons du déploiement et pour communiquer sur les activités de management du système, qui feront partie des activités permanentes de l'organisation après l'audit de certification.