Norme ISO/IEC 27001 : 2005. Mise en place et certification : faire encore et encore

Nurudeen Odeshina, CISA, CISM, CRISC, ISO 27001 LI, ITSM, est consultant et formateur chez Digital Jewels Limited. Il a travaillé avec l'entreprise pour attribuer la certification ISO/IEC 27001:2005 à quatre sociétés au Nigeria en 2012. Il a contribué à la formation des équipes et à l'adaptation des méthodologies de bonnes pratiques, des normes et des référentiels en réponse aux demandes des clients. Avant de rejoindre Digital Jewels, Nurudeen Odeshina a travaillé au sein du groupe de conformité et de contrôle interne, ainsi que du groupe de sécurité des systèmes d'informations et de contrôle de l'une des banques nouvelle génération de premier plan au Nigeria. Il peut être contacté à l'adresse suivante : nurudeen@digitaljewels.net

Les organisations sont susceptibles d'appliquer une méthodologie et/ou une approche du processus similaires à celles spécifiées dans la norme ISO/IEC 27001:2005, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*, lors de la mise en œuvre d'un système de management de la sécurité de l'information (SMSI). Toutefois, les défis et les opportunités liés à l'élaboration et à l'exploitation du système de management sont toujours différents, même lorsque les organisations sont en apparence similaires. Il n'y pas deux organisations identiques.

Pour chaque organisation, l'essentiel de l'élaboration, de la mise en œuvre, de l'exploitation, de la surveillance, de la maintenance et de l'amélioration d'un SMSI dépend de la nature et des caractéristiques de l'activité propre à l'organisation, de son emplacement géographique, de ses actifs et de la technologie utilisée. Dans la mesure où la nature et les caractéristiques de deux entités/entreprises, ainsi que leurs actifs et technologies, ne sont pas en tous points similaires, le processus d'implémentation et de certification de la norme ISO/IEC 27001:2005 ne peut être que différent.

Le périple commence généralement par la définition du périmètre d'action et l'évaluation ou l'analyse des lacunes existantes. L'évaluation de diagnostic, qui désigne la comparaison entre les politiques, procédures et pratiques (PPP) de l'organisation et les exigences de la norme ISO/IEC 27001:2005, permet de déterminer les lacunes du SMSI existant ou inexistant au sein de cette organisation. L'objectif n'est pas seulement de déterminer ces lacunes, mais aussi de les combler et d'assurer la conformité avec les exigences de la norme ISO/IEC 27001:2005. Sans cette phase, l'implémentation serait un projet onéreux. Cette phase implique également de définir des politiques (politique du SMSI et autres politiques inhérentes) et de réaliser une évaluation complète des risques de l'ensemble des actifs informationnels de l'organisation (c.-à-d., se trouvant dans le périmètre d'action du SMSI). Cette phase aboutit à l'élaboration de politiques, à l'énoncé des résultats de l'évaluation du risque (plan de traitement du risque) et à la mise en place de contrôles afin de réduire ce dernier en fonction du niveau de tolérance et du seuil d'acceptation de l'organisation. Une déclaration d'applicabilité (DdA) est également déterminée, qui identifie les contrôles applicables et non applicables parmi les 133 présentés dans l'annexe A de la norme ISO/IEC 27001:2005. Cette DdA doit inclure la justification de la non-exclusion des contrôles non applicables, ainsi qu'une raison expliquant le choix des contrôles applicables.

L'évaluation de diagnostic indique la conduite à suivre lors de la phase de conception. Cette dernière consiste à élaborer une feuille de route et/ou un plan directeur d'implémentation visant à guider l'organisation dans ses efforts pour mettre en place les contrôles choisis et le plan de traitement du risque. Il est extrêmement important d'avoir cette vision de synthèse globale afin de connaître le coût de cet effort en termes de ressources (budget, temps, personnel, technologie).

La phase d'implémentation consiste à combler les lacunes observées lors de la phase de diagnostic conformément à la feuille de route établie lors de la phase de conception. Il s'agit essentiellement d'implémenter, puis d'exploiter et de gérer le SMSI. Le traitement du risque identifié lors de la mise en place des politiques et des contrôles choisis s'effectue lors de cette étape. Il est recommandé de mettre en œuvre les éléments pouvant fournir des résultats rapides avec un minimum d'efforts en premier lieu, car ils peuvent servir de tremplin pour atteindre des objectifs plus déterminants et permettre de surmonter les obstacles lors de l'implémentation. Des contrôles sont intégrés afin de répondre aux exigences des objectifs de contrôle spécifiés dans l'annexe A de la norme ISO/IEC 27001:2005. Des conseils sur la mise en place de ces contrôles sont disponibles dans la norme ISO 27002, *Code de pratique pour la gestion de la sécurité de l'information*, et/ou plusieurs autres référentiels ou normes. Il est également important de spécifier les critères de mesure de l'efficacité de ces contrôles. Les contrôles peuvent être considérés comme les PPP nécessaires pour réduire le risque identifié.

Avant toute demande de certification, il est impératif que le SMSI de l'organisation passe par

au moins un cycle de gestion de la qualité, dite PDCA (*Plan-Do-Check-Act*) (**figure 1**). Cette phase de gestion de la qualité permet de garantir que les contrôles instaurés sont évalués et améliorés, que leurs performances sont mesurées et qu'ils sont améliorés, si nécessaire. En résumé, cette phase, qui est essentiellement une phase de certification préalable, consiste à faire évaluer les contrôles instaurés par un auditeur interne ou externe (en l'absence d'un auditeur interne). Un rapport d'audit doit être adressé à la direction pour être analysé, mais également à l'équipe chargée de l'implémentation afin qu'elle prenne des mesures correctives et préventives en réponse à l'éventuelle inefficacité de ces contrôles. Comme dans tout autre système de gestion, il est important d'améliorer continuellement le SMSI de l'organisation. Les incidents, les événements et les failles de sécurité doivent aussi être surveillés en temps réel et documentés afin de garantir une détection et une correction rapides, ainsi que la prise de mesures préventives pour anticiper toute résurgence. Si l'ensemble de ces mesures est effectué systématiquement, la certification n'est plus qu'une formalité.

Figure 1—Approche du processus de gestion de la qualité de l'implémentation de la norme ISO 27001

Planifier (créer le SMSI)	Définir la politique du SMSI, les objectifs, processus et procédures pertinents pour la gestion du risque et l'amélioration de la sécurité de l'information, afin de fournir des résultats cohérents avec l'ensemble des politiques et objectifs de l'organisation.
Déployer (implémenter et exploiter le SMSI)	Implémenter et exploiter la politique, les contrôles, les processus et les procédures du SMSI.
Contrôler (surveiller et analyser le SMSI)	Évaluer et, le cas échéant, mesurer les performances du processus en les comparant à la politique, aux objectifs et à l'utilisation pratique du SMSI, et consigner dans un rapport les résultats sur la gestion pour les analyser.
Agir (maintenir et améliorer le SMSI)	Prendre des mesures correctives et préventives, en fonction des résultats de l'audit interne du SMSI et de l'analyse de la gestion ou de toutes autres informations pertinentes afin de poursuivre l'amélioration du SMSI.

L'évaluation de la certification est réalisée en deux phases par un organisme de certification. Lors de la première étape, un audit obligatoire est réalisé entre la demande de certification de l'organisation auprès d'un organisme agréé et

l'audit intervenant lors la deuxième étape. Au cours de cette phase, les vérifications visent à garantir que l'organisation est prête pour l'évaluation, qui est alors planifiée. Dans la plupart des cas, il s'agit d'un audit de revue de la documentation, qui consiste à évaluer les documents obligatoires, tels que la déclaration du périmètre d'action, les documents relatifs aux processus, les rapports/documents d'audits internes et de revues de gestion. Cette étape crée une base pour l'audit de la deuxième étape. En effet, elle détermine si l'organisation peut prétendre passer au deuxième audit. Après l'audit de la première étape, le deuxième audit consiste à apporter l'assurance raisonnable que tous les éléments du SMSI de l'organisation inclus dans le périmètre d'action sont conformes aux exigences de contrôle applicables de la norme ISO/IEC 27001:2005 (clauses obligatoires 4 à 8 et objectifs de contrôle de l'annexe A). Au minimum, l'audit évalue (sans ordre d'importance) : le contrôle opérationnel des processus ; la conformité obligatoire et légale, la surveillance et la mesure des performances, la création de rapports et l'analyse de ces résultats ; les responsabilités relatives à la gestion ; et les informations et preuves inhérentes de conformité à la norme.

Idéalement, l'organisation réussit l'audit et reçoit sa certification à la norme internationalement reconnue en management de la sécurité de l'information. Le certificat est signé, authentifié et remis à l'organisation. Mais cela ne s'arrête pas là, car cette procédure est suivie de près par l'audit de surveillance. Il est souvent dit que la sécurité de l'information n'est pas une destination, mais un voyage, et pour l'organisation, cela équivaut à la recherche perpétuelle de l'amélioration.

RÉFÉRENCES

Organisation internationale de normalisation (ISO), ISO/IEC 27001:2005, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*