La famille ISO/CEI 27000

Elle est composée de normes relatives à la gestion de la sécurité de l'information, qui sont actuellement au nombre de quatre et complétée par une cinquième norme, qui est un guide.

I. La norme principale, ISO/IEC 27001:2013

Cette norme couvre tous les types d'organismes (par exemple les entreprises commerciales, les organismes gouvernementaux, les organisations à but non lucratif) et spécifie les exigences pour établir, mettre en oeuvre, gérer, surveiller, examiner, maintenir et améliorer un système documenté de management de la sécurité de l'information dans le contexte des risques généraux liés aux activités de l'organisme.

Elle spécifie les exigences pour la mise en oeuvre de contrôles de sécurité adaptés aux besoins d'organismes individuels ou de parties de ces organismes.

ISO/CEI 27001:2013 est conçue pour assurer la sélection de contrôles de sécurité adéquats et proportionnés au risque, qui protègent les biens d'information et donnent confiance aux parties intéressées. Elle convient à différents type d'usages, y compris les suivants :

• utilisation au sein de l'organisme, pour formuler des exigences et objectifs de sécurité ;

• utilisation au sein de l'organisme, en tant que moyen de garantir une gestion économique des risques sur la sécurité ;

• utilisation au sein de l'organisme, pour garantir la conformité à la législation et à la réglementation ;

• utilisation au sein de l'organisme, en tant que cadre de processus pour la mise en oeuvre et la gestion de contrôles pour s'assurer que les objectifs de sécurité spécifiques à un organisme sont atteints ;

• définition de nouveaux processus de management de la sécurité de l'information ;

• identification et clarification des processus existants de management de la sécurité de l'information ;

• utilisation par la direction pour déterminer le statut des activités de management de la sécurité de l'information;

• utilisation par les auditeurs internes et externes pour déterminer le degré de conformité avec les politiques, directives et normes adoptées par un organisme ;

• utilisation par l'organisme pour fournir des informations pertinentes sur les politiques, directives, normes et procédures de sécurité de l'information aux partenaires commerciaux et autres organismes avec lesquels il interagit pour des raisons opérationnelles et commerciales ;

• mise en oeuvre d’une sécurité de l’information constructive pour les activités de l’entreprise;

• utilisation par l’organisme pour fournir aux clients des informations pertinentes sur la sécurité de l’information.

II. La norme ISO/CEI 27013 :2012

Est un Guide qui, propose des recommandations utiles pour la mise en place consécutive ou simultanée des deux systèmes de management ISO/CEI 27001 (sécurité de l’information) & ISO/CEI 20000-1 (gestion des services de l’information – exigences). Cette norme (guide) a en effet pour objet d'expliquer les premières étapes de la démarche aux organisations soucieuses d'efficacité et d'améliorations au niveau des services de l’information, de la sécurité de l'information et de la gestion de ces services.

Les processus et les activités de ces deux systèmes de management sont très similaires et étroitement liés, y compris quant à l'importance du principe de l'amélioration continue. La mise en œuvre intégrée d'un système de management portant sur les services fournis et sur la protection des actifs informationnels, présente un certain nombre d'avantages qui sont les suivants

1. Gage de crédibilité en termes d'efficacité et de sécurité des services pour les clients internes ou externes à l'organisation ;

2. Réduction des coûts avec un programme intégré ;

3. Réduction des coûts avec un programme intégré ;

4. Réduction du temps nécessaire à l'implantation des systèmes du fait de la mise en place intégrée des processus communs aux deux normes ;

5. Élimination des redondances ;

6. Meilleure compréhension entre les responsables de la gestion des services et les responsables de la sécurité ;

7. Processus de certification amélioré.

III. Service et Sécurité - Témoignages

Pour les entreprises, il est essentiel d'établir et de maintenir la confiance des clients.
Des organisations telles que CINDA, l'une des quatre principales sociétés de gestion d'actifs représentant le secteur financier en Chine, ont tiré parti commercialement d'une plus grande confiance des clients, obtenue grâce à l'utilisation conjointe d'un système de management de la sécurité de l'information, fondé sur ISO/CEI 27001 et d'un système de gestion des services informatiques fondé sur ISO/CEI 20000-1.
CINDA a été la première entreprise à obtenir les deux certifications à ces normes auprès d'organismes de certification nationaux et internationaux. CINDA a adapté en permanence son « système intégré – SMIS » au développement des activités et à la culture d'entreprise. Avec la mise en place du SMSI, la société n'a cessé d'améliorer la sécurité de la gestion de ses informations d'entreprise et de gagner ainsi la confiance des clients et des autorités réglementaires.

La large applicabilité d'ISO/CEI 27001 donne maintes occasions de gérer les risques et de renforcer la confiance de la clientèle. FUJITSU Australie, utilise ISO/CEI 27001 pour la gestion de la sécurité interne, en intégrant ISO/CEI 20000 pour fournir des services sécurisés à ces clients sous contrat de gestion. Organisation mondiale, FUJITSU fourni des services à partir de divers points géographiques. Une norme internationalement reconnue comme ISO/CEI 27001 présente l'avantage de donner aux clients l'assurance que la société a mis en place la gestion de la sécurité à un même niveau partout.
Il y a plus, FUJITSU crée des communautés de professionnels de la sécurité à des niveaux de direction et de gestion au sein d'un cadre commun défini par ISO/CEI 27001.
A long terme, FUJITSU Australie continuera d'améliorer la mise en œuvre de la norme ISO/CEI 27001 (et des normes connexes) dans tous ses secteurs d'activité, y compris les services d'information et dans l'informatique en nuage.

IV. Liste des normes

ISO/CEI 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*
ISO/CEI 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*
ISO/CEI 27005:2008, *Technologies de l'information – Techniques de sécurité – Gestion du risque en sécurité de l'information*
ISO/CEI 27006:2007, *Technologies de l'information – Techniques de sécurité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*
ISO/CEI 27013:2012 *Technologies de l'information – Technique de sécurité – Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1*
ISO/CEI 20000-1:2011 *Technologies de l'information -- Gestion des services -- Partie 1: Exigences du système de management des services*

Richard Cox
PME Cert SA
Source : iso.org