Implémentation et gestion d'un projet ISO 27001, 27002

(préparation aux certificats ISO Lead Implementer et Lead Auditor)

Durée : 3 jours Référence : ISO27K

Cette formation a pour but de présenter l'ensemble des normes ISO traitant de la sécurité du SI et de sa gestion. Elle développe les thèmes techniques, organisationnels et juridiques liés à l'application d'un référentiel de sécurité aux normes et son application.

Contenu

- Introduction
- Les normes ISO 2700x
- L'analyse de risque, norme 27005
- Les bonnes pratiques, référentiel ISO 27002
- L'application de la sécurité dans un projet (27003, 27004)
- Les audits de sécurité ISO 19011
- Les bonnes pratiques juridiques
- La certification ISO de la sécurité du SI

Participants

RSSI, Chef de projet en sécurité.

Pré-requis

Connaissances de la sécurité informatique.

Programme

Introduction

- Rappels. Terminologie ISO 27000 et ISO Guide 73.
- Définitions : menace, vulnérabilité, protection.
- La notion de risque (potentialité, impact, gravité).
- La classification CAID (Confidentialité, Auditabilité, Intégrité, Disponibilité).
- La gestion du risque (prévention, protection, report de risque, externalisation).

- Analyse de la sinistralité. Tendances. Enjeux.
- Les réglementations SOX, COSO, COBIT, la gouvernance SI, les liens avec ITIL et CMMI.
- L'apport de l'ISO pour les cadres réglementaires.
- L'alignement COBIT, ITIL et ISO 27002.

Les normes ISO 2700x

- Historique des normes de sécurité vues par l'ISO.
- Les standards BS 7799, leurs apports à l'ISO.
- Les normes actuelles (ISO 27001, 27002…).
- Les normes à venir (27004, 27003…).
- Comment anticiper et se préparer efficacement.
- La convergence avec les normes qualité 9001 et environnement 14001.
- L'apport des qualiticiens dans la sécurité.

L'analyse de risque, norme 27005

- Définition d'un Système de Gestion de la Sécurité des Systèmes (ISMS). Objectifs à atteindre par votre ISMS.
- L'approche " amélioration continue ".
- La norme ISO 27001 dans une démarche qualité, le modèle PDCA (roue de Deming).
- Les phases Plan-Do-Check-Act (sections 4 à 8).
- De la spécification du périmètre ISMS au SoA (Statement of applicability).
- Importance de l'analyse, choix d'une méthode.
- Les recommandations pragmatiques de l'ISO 27001 pour l'analyse des risques.
- L'apport des méthodes EBIOS/FEROS, MEHARI dans sa démarche de certification.
- Les audits internes obligatoires.
- Application d'actions correctives et préventives. Mesures et contre-mesures des actions correctives et préventives.
- L'annexe A en lien avec la norme 27002.

Les bonnes pratiques, référentiel ISO 27002

- Objectifs de sécurité.
- Structuration en domaine/chapitres (niveau 1), objectifs de contrôles (niveau 2) et contrôles (niveau 3).
- Analyse complète et détaillée de chaque domaine (Politique de sécurité, Organisation de la sécurité, Classification et contrôle des actifs, Sécurité liée aux ressources humaines, Sécurité physique et environnementale, Exploitation et

réseaux, Contrôle d'accès, Développement et maintenance des systèmes, Gestion des incidents, Continuité de service, Conformité).

- Adaptation des bonnes pratiques à son organisme.
- Les dix bonnes pratiques incontournables.
- Choix des indicateurs clés pour les mesures choisies.

L'application de la sécurité dans un projet (27003, 27004)

- Des spécifications sécurité à la recette sécurité.
- Comment respecter la PSSI et les exigences de sécurité du client/MOA.
- De l'analyse de risques à la construction de la déclaration d'applicabilité.
- Les normes ISO 27003, 15408 comme référentiel.
- La sécurité dans les développements spécifiques.
- Les règles à respecter pour l'externalisation.
- Le suivi du projet pour la mise en œuvre et l'exploitation.
- Les rendez-vous " Sécurité " avant la recette.
- La recette : test d'intrusion et/ou audit technique ? Le choix d'un auditeur/testeur indépendant.
- Intégrer le cycle PDCA dans le cycle de vie du projet.
- Préparer les indicateurs. L'amélioration continue.
- Etablir un tableau de bord. Exemples.
- L'apport de la norme 27004.
- Veille technologique spécifique du projet.

Les audits de sécurité ISO 19011

- Processus continu et complet. Etapes, priorités.
- Les catégories d'audits, organisationnel, technique...
- L'audit interne, externe, tierce partie, choix de l'auditeur.
- Le déroulement type ISO de l'audit, les étapes clés.
- Les objectifs d'audit, la qualité d'un audit.
- La démarche d'amélioration (type PDCA) pour l'audit.
- Les qualités des auditeurs, leur évaluation.
- L'audit organisationnel : démarche, méthodes.
- Apports comparés, les implications humaines.

Les bonnes pratiques juridiques

- Rappel : application d'une loi, d'une règle de droit, d'une décision de justice. Entre jurisprudence et constitution : hiérarchie des règles.
- La propriété intellectuelle des logiciels, la responsabilité civile délictuelle et contractuelle.

- Responsabilité : pénale, des dirigeants, délégation de pouvoir, sanctions, loi LCEN.

- Entre conformité ISO et conformité juridique.

La certification ISO de la sécurité du SI

- La relation auditeur/audité.
- L'intérêt de cette démarche, la recherche du " label ".
- L'ISO pour accompagner sa démarche sécurité.
- L'intégration efficace des normes de sécurité ISO.
- L'ISO : complément indispensable des cadres réglementaires et standard (COBIT, ITIL…).
- Les enjeux économiques escomptés.
- Organismes certificateurs, choix en France, en Europe.
- Démarche d'audit, étapes et charges de travail.
- Norme ISO 27006, obligations pour les certificateurs.
- Coûts récurrents et non récurrents de la certification.