ISO 27001 : Audit

ISO 27001 : Audit

durée : 5 jour(s) code formation : IS1

Description :

Cette formation EGILIA a pour objectif de présenter l`ensemble des normes ISO 27001 traitant de la sécurité du système d`information et de son management. Grâce à l`alternance systématique de phases pratiques et théoriques, il permet d`acquérir la maîtrise de l`implémentation des normes 27000 pour les adapter à votre contexte dans un périmètre allant d`un projet informatique sensible à l`ensemble de la Sécurité du Système d`information.

Pré-requis :

Posséder une formation initiale au minimum de second cycle ou justifier d?une expérience professionnelle d?au moins cinq ans dans le domaine de la sécurité informatique ou des normes ISO

Programme :

Présentation des normes ISO 2700X

- Historique des normes ISO.
- Les normes actuelles (ISO 27001, 27002, 27003, 27004 et 27005)
- Rappels. Terminologie ISO 27000.
- D?finitions : menace, vuln?rabilit?, protection.
- La classification CAID (Confidentialit?, Auditabilit?, Int?grit?, Disponibilit?).
- Description de la notion d'ISMS (Syst?me de Management de la s?curit? de l'information)
- Pr?sentation du mod?le PDCA (Plan, Do, Check, Act)
- Analyse de la sinistralit?. Tendances. Enjeux.
- La gestion du risque (pr?vention, protection, report de risque, externalisation).
- L'apport de l'ISO pour les cadres r?glementaires.
- Liens avec COBIT, ITIL et CMMI dans le cadre de la gouvernance SI

Le référentiel d'audit ISO 27001

- Description des points de contr?les et des ?l?ments Techniques de l'Annexe A de ISO 27001
- Pr?sentation des lignes directrices de l'audit d?finies dans l'ISO 19011
- Processus continu et complet. Etapes, priorit?s.
- Les cat?gories d'audits, organisationnel, technique...
- L'audit interne, externe, tierce partie, comment choisir son auditeur ?
- Le d?roulement type ISO de l'audit, les ?tapes cl?s.
- Les objectifs d'audit, la qualit? d'un audit.
- La d?marche d'am?lioration (type PDCA) pour l'audit.
- Les qualit?s des auditeurs, leur ?valuation.

- L'audit organisationnel : d?marche, m?thodes.

- Apports compar?s, les implications humaines.
?

Contenus du référentiel documentaire SMSI conformément à l?ISO 27001

- Indicateurs et surveillance du SMSI : les contr?les et l'audit interne

- Expos? des principes de l'ISO 27003

- Guide d'impl?mentation d'un SMSI et de l'ISO 27004

- Indicateurs de mesures

- Mesures physiques: authentification, biom?trie, politique de nettoyage des bureaux

- Mesures techniques : authentification num?rique et gestion des acc?s, Firewall, PKI, VPN, Backup

- Mesures organisationnelles : Elaboration et gestion du plan de continuit? des activit?s (PCA), PRA, gestion du changement

- Points cl?s d'un audit de certification

Présentation du projet d?implémentation

- De la d?finition, ? l'organisation et ? la mise en oeuvre

- Naissance du SMSI

- Analyse et gestion des risques

- Pr?sentation de la d?marche ISO 27005

- Mise en oeuvre op?rationnelle

- Politiques et processus supports au syst?me de Management de la S?curit? de l'Information :

- Politiques et usages SMSI,

- Comit?s

- Gestion des incidents,

- Gestion documentaire

- Les bonnes pratiques juridiques

- Application d'une loi, d'une r?gle de droit, d'une d?cision de justice.

- La propri?t? intellectuelle des logiciels, la responsabilit? civile d?lictuelle et contractuelle.

- Responsabilit? : p?nale, des dirigeants, d?l?gation de pouvoir, sanctions, loi LCEN.

- Entre conformit? ISO et conformit? juridique.

Préparation à l?examen

L'examen "Lead Implementer" certifie que vous disposez des connaissances et comp?tences pour mettre en oeuvre un SMSI suivant la norme ISO/IEC 27001: 2005 " Technologies de l'information – Techniques de s?curit? – Syst?mes de management de la s?curit? de l'information – Exigences".

Ce certificat ISO conf?re une tr?s haute cr?dibilit? dans la conduite des projets d'impl?mentation de SMSI de type ISO 27001.

L'examen ?crit dure 3 heures 30. Il comporte un questionnaire ? choix multiples relatif ? la norme ISO/IEC 27001, des exercices pratiques et une ?tude de cas.

Afin de vous mettre toutes les chances de votre cot?, EGILIA vous propose des exercices ?crits et oraux de mise en situations, des tests de connaissances de type QCM, des cas pratiques de mise en oeuvre d'une d?marche PDCA et de d?claration d'applicabilit? ? partir d'une analyse de risques de type ISO 27001 et vous indiquera des trucs, astuces et pi?ges ? ?viter !
?