ISO 27001 Lead Implementer

CATEGORIE : B

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse :
- **Totalité des domaines**

Cette certification s'applique à tous les domaines d'activité sans exception dès l'instant que l'organisme fait de la sécurité informatique.

Code(s) NAF : **62.02A**
Code(s) NSF : **326p**
Code(s) ROME : **M1802**, **M1805**
Formacode : **31054**

Date de création de la certification : **20/03/2007**
Mots clés : **sécurité de l'information**, **PROCESSUS**, **SMSI**, **Normes ISO 27001**

Identification

Identifiant : **1817**
Version du : **19/04/2016**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **Attestation d'accréditation de la certification par le COFRAC**

Non formalisé :
- **Norme ISO 27001**

Norme(s) associée(s) :
—

Descriptif

Objectifs de l'habilitation/certification

Devenir responsable de mise en oeuvre d'un Système de Management de la Sécurité de l'Information (SMSI).

La certification «Implementer ISO/CEI 27001» atteste que la personne certifiée :

possède ou a acquis les connaissances et les compétences nécessaires pour mettre en place un système de management de la sécurité de l'information conforme à la norme ISO/CEI 27001 «Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences», en tant que membre d'une équipe de projet ou seul, ou bien, en tant que responsable d'une équipe de projet.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- NON

Descriptif général des compétences constituant la certification

Savoir implémenter un Système de Management de la Sécurité de l'Information (SMSI) et plus précisément :

Mener une revue de direction de système de management selon la norme ISO 27001
Rédiger les documents de politique générale et spécifique de sécurité des systèmes d'information

Public visé par la certification

- salarié
- Demandeur d'emploi
- Profession libérale
- Auto-entrepreneur

Faire une appréciation des risques et rédiger un plan de traitement des risques
Mettre en place et documenter des mesures de sécurité
Être préparé à recevoir des auditeurs en sécurité et de certification
Savoir surveiller et ré-examiner son SMSI notamment grâce aux indicatreurs

Modalités générales

Le passage de la certification nécessite :

- le suivi d'une formation présentielle agréée par LSTI d'une durée de 40 h

- la réussite à l'examen de certification ISO 27001 Lead Implementer.

La formation de 40h se base sur les points suivants :

Cours magistral basé sur les normes ISO 27001, ISO 27002 (anciennement ISO 17799), ISO 27005, ISO 27003 et ISO 27004, illustré de nombreux exemples pratiques basés sur le retour d'expérience d'HSC et de nos clients.
Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur une étude de cas : périmètre, politique, procédures, suivi et réunions, appréciation des risques, indicateurs.
Exercices individuels de révision pour se préparer à l'examen.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification permet de montrer que l'on sait implémenter un SMSI.

La certification est également demandée par les principaux donneurs d'ordres pour les personnes en charge de la mise en oeuvre de la cybersécurité. En conséquence, elle est demandée pour travailler comme implémenteurs sécurité dans les SSII et l'ensemble des entreprises et organismes ayant un département sécurité des systèmes d'information.

Pour l'entité utilisatrice

Savoir implémenter un SMSI.
Mettre en place un SMSI en interne ou faire des prestation d'accompagnement ISO 27001 auprès de leurs clients.
Mieux organiser et mieux maîtriser leur propre sécurité en ayant du personnel certifié ISO 27001 Lead Implementer

Evaluation / certification

Pré-requis

Pour postuler à un examen, le candidat doit :

• posséder une formation initiale au minimum de second cycle (minimum bac +2) ou justifier d'une

expérience professionnelle d'au moins cinq ans dans le domaine des systèmes de management de la

sécurité ou de la qualité,

Centre(s) de passage/certification

- Hervé Schauer Consultants http://www.hsc.fr/
- ORSYS FORMATION http://www.orsys.fr
- SOGETI l'Institut de Formationhttp://www.institut-sogeti.com/

• avoir suivi une formation de 40 heures dispensée par un organisme de formation agréé par LSTI

Compétences évaluées

Les compétences évaluées sont :

- la connaissance de la norme ISO 27001

- les capacités pour conduire un projet de mise en place d'un système de management de la sécurité selon la norme ISO/CEI 27001.

L'examen comporte 9 parties :

un questionnaire relatif à la norme ISO/CEI 27001 et guides associés,
Identification d'activité dans le modèle PDCA
Une étude de cas :
Périmètre de certification
Évaluation des risques
Plan d'action
Implémentation des mesures
Sélection de mesures
Élaboration d'indicateurs
Réexamen du SMSI

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Néant

- FIDENS http://www.fidens.fr/
- ENIGMA Services http://www.enigma-services.fr/
- RESYS Consultants http://www.resys-consultants.com/
- AFNOR Compétences http://www.boutique-formation.afnor.org/
- High Tech Security http://www.hts-expert.com/
- EURL Perrine Diligent http://www.byward.eu/
- The Duquesne Group http://www.duquesnegroup.com/
- Intelligent Security IT http://intelligentsecurity-it.com
- Sarapis http://www.s-arapis.fr/
- FCT Solutions http://www.fctsolutions.com/

La validité est Temporaire

3 ans
Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Certificat cartonné et registre sur le site web de LSTI

Plus d'informations

Statistiques

Environ 100 personnes par an

Autres sources d'information

http://www.lsti-certification.fr/index.php/formations-certifiantes/implementer-lead-implementer-isocei-27001/presentation.html