ISO/CEI 27001 Lead Auditor : audit de systèmes de management de la sécurité de l'information

Date et durée

Code formation : ISO27001LA-RS
Durée : 4,5 jours
Nombre d'heures : 31 heures

Description

L'objectif d'un système de gestion de la sécurité de l'information (SMSI) est d'implémenter des mesures qui permettent une réduction, voire une suppression des différentes menaces dans une organisation afin de **favoriser la continuité de l'activité**, la protection des actifs informationnels et la confiance du client. La norme ISO 27001 version 2022 décrit sous forme d'exigences, un ensemble de bonnes pratiques organisationnelles, techniques et des points de contrôle à mettre en place pour s'assurer de la pertinence du SMSI. L'objectif étant qu'une organisation puisse **maîtriser efficacement les risques** liés à l'information.
L'objectif de cette formation est de vous donner l'expertise nécessaire pour conduire, seul ou en équipe, **un audit de système de management de la sécurité de l'information** (SMSI) selon la norme ISO 27001:2022. Ce cours vous apprendra également le savoir-faire et les qualités personnelles requises pour mener cet audit, telles que définies dans la norme ISO 19011 « Lignes directrices pour l'audit des systèmes de management ».
A l'issue de cette formation, **vous passerez l'examen de certification ISO/CEI 27001 Lead Auditor**. Sa réussite démontrera que vous maîtrisez les techniques d'audit telles que la gestion d'une équipe, la programmation d'un audit, la communication avec les clients, la résolution de conflits, etc.

Skills4All est un organisme certificateur spécialisé dans le développement des compétences numériques et la transformation digitale.

Objectifs

Objectifs pédagogiques :

- Caractériser les menaces et vulnérabilités qui pèsent sur le système d'information de l'organisation,
- Déterminer les risques en analysant la documentation et les processus de l'organisation.
- Composer une équipe d'audit pluridisciplinaire.
- Concevoir un plan d'audit.
- Identifier et apprécier les non conformités en mettant en œuvre le plan d'audit.
- Formaliser ses recommandations dans un rapport final.
- Établir un plan de suivi des actions.

Points forts

Certification internationalement reconnue. Travaux pratiques basés sur des cas réels avec une documentation de 450 pages ; Examens de certification compris dans le prix de la formation.

Certification

Passage de la certification « **Audit de systèmes de management de la sécurité de l'information (ISO/CEI 27001 Lead Auditor)** » inscrite au Répertoire Spécifique n° 6243 (SKILLS4ALL). Examen officiel passé après la formation et vos révisions personnelles.
L'évaluation dure 3h00 et se fait à travers **une mise en situation professionnelle fictive** sous forme d'une étude de cas depuis une plateforme d'apprentissage. Le candidat devra proposer des préconisations et des directives relatives à un **audit du système d'information selon l'ISO 27001 et l'ISO 19011**, d'une organisation fictive dont le contexte spécifique, les particularités, les enjeux et le SI de l'entreprise seront décrits dans la notice d'examen.
Le candidat devra pour cela :

- Répondre à un QCM (questions fermées) de 15 min ;
- Présenter son projet d'implémentation d'un SMSI par écrit et par vidéo (voir explications ci-dessous) en 3 parties :
    - Partie 1 : justification du choix du périmètre ;
    - Partie 2 : description du projet d'implémentation (politique et principales mesures) ;
    - Partie 3 : formalisation de sa démarche d'accompagnement à la mise en place (principaux enjeux humains et actions/positionnement envisagées).

A noter que comme le candidat passe son examen en toute autonomie, il sera également demandé au candidat d'enregistrer 4 capsules vidéo aux fins de présentation et de justification de :

- Vidéo 1 : son identité (le candidat se présente)
- Vidéo 2 : la partie 1 ;
- Vidéo 3 : la partie 2 ;
- Vidéo 4 : la partie 3.

Pour rappel, en suivant cette formation éligible au CPF, vous vous engagez à passer l'examen de certification.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques
Etude de cas

Pré-requis

Suivre cette formation ISO 27001 Lead Auditor nécessite les prérequis suivants :

- avoir une bonne connaissance des systèmes d'information des organisations ;
- avoir une expérience en audit de système est fortement recommandée.

Public

Cette formation s'adresse aux publics suivants :

- les auditeurs internes ;
- les auditeurs souhaitant réaliser et diriger des audits de certification d'un SMSI ;
- les responsables ou consultants souhaitant maîtriser le processus d'audit de Système de Management de la Sécurité de l'Information ;

- les responsables et cadres supérieurs en charge de la gouvernance des TI d’une organisation et de la gestion de ses risques ;
- les membres d’une équipe d'un SMSI ;
- les professionnel des systèmes d'information qui souhaitent acquérir une certification dans ce domaine.

Cette formation s'adresse aux profils suivants

Auditeur interne / externe
Directeur des Systèmes d'Information (DSI)

Programme

Tour de table :

- Introduction individuelle des participants.
- Exploration des attentes et des objectifs de chaque participant.
- Introduction au cadre de la formation.
- Alignement avec les objectifs et enjeux spécifiques de la formation ISO 27001.
- Identification des attentes et des perspectives individuelles des participants.

Partie 1 : introduction au SMSI tel que défini par l’ISO 27001

- Le cadre normatif, réglementaire et juridique relatif à la sécurité de l'information.
- Cadre et objectifs de l'ISO 27001 :
    - introduction aux objectifs et à la structure de la norme ISO 27001, en expliquant comment elle s'intègre dans une approche globale de la sécurité de l'information.
- Éléments clés du SMSI :
    - détail des composants essentiels d'un SMSI efficace, y compris la politique de sécurité, les objectifs, et les processus de mesure de performance.

Partie 2 : principes d’audit et préparation de l’audit

- Fondamentaux de l'audit :
    - exploration des principes d'audit selon ISO 27001, incluant l'objectivité, la confidentialité, l'approche systématique et la compétence professionnelle.
- L’approche de l’audit fondé sur des preuves.
- L'impact des tendances et de la technologie sur l'audit.
- Planification de l'audit :
    - techniques pour la création d'un plan d'audit robuste, choix de l'équipe d'audit, définition du périmètre, et préparation des outils et des méthodes d'audit.

Partie 3 : conduite de l’audit

- L’audit documentaire du SMSI.
- La mise en œuvre des procédures d’audit :
    - conduite de l'audit, y compris les étapes d'observation, d’examen des documents, d’interviews, de techniques d’échantillonnage, la vérification technique, la collaboration et l’évaluation.
- La communication lors de l’audit.
- La gestion des incidents et des non-conformités :
    - stratégies pour identifier, documenter, et rapporter les non-conformités ou autres problèmes rencontrés. Formulations des conclusions de l’audit.

Partie 4 : clôture de l’audit

- La synthèse des résultats et la réunion de clôture :
    - techniques pour analyser les données recueillies, préparer le rapport d'audit final, et conduire la réunion de clôture avec les parties prenantes.
- Les recommandations et le plan de suivi :
    - développement de recommandations constructives et création d'un plan d'actions correctives avec des échéances claires pour le suivi. L’audit de surveillance et le programme de gestion de l’audit interne.

Partie 5 : compétences de l’auditeur

- Le développement professionnel continu :
    - l'amélioration continue des compétences en audit, y compris la formation technique et interpersonnelle.
- L'éthique et la responsabilité professionnelle :
    - discussion sur les normes éthiques et les responsabilités de l'auditeur envers la profession et les parties prenantes.

Partie 6 : Révisions et préparation à la certification (***Dernier jour – Matinée***)

- Réviser les principaux concepts et termes en vue de réaliser un audit d’un SMSI selon la norme ISO 27001.
- Répondre aux questions sur des points qui n’auraient pas été bien compris.
- Fournir des conseils et des stratégies pour réussir l'examen de certification, incluant des pratiques d'examen et des questions types.