Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

ISO/CEI 27005 Security Lead Risk Manager : évaluer et traiter les risques de la sécurité de l'information

Date et durée

Code formation : ISO27005SLRM-RS
Durée : 4,5 jours
Nombre d'heures : 31 heures

Description

Aujourd'hui, **connaître et gérer les risques liés à la sécurité des systèmes d'information** (SI) est essentiel pour le bon fonctionnement d'une entreprise. En effet, le moindre incident peut avoir des conséquences critiques pour une organisation. De ce fait, il est important de se former sur la norme ISO 27005 pour devenir un gestionnaire des risques certifié.
Notre **formation ISO/CEI 27005 Lead Risk Manager** vous donnera toutes les compétences nécessaires pour **maîtriser les actifs et processus liés à la sécurité de l'information,** en conformité avec la norme ISO/CEI 27005:2022**.** Vous aborderez aussi d'autres méthodes de gestion du risque comme OCTAVE, EBIOS, MEHARI ou encore la méthode EMR. Notre formation est également parfaite si vous souhaitez mettre en place un SMSI (Système de Management de la Sécurité de l'Information) conforme à la norme ISO/CEI 27001:2022.
A la fin de cette formation**, vous passerez l'examen ISO/CEI 27005 Security Risk Manager**. La réussite de celui-ci vous permettra d'attester de vos capacités professionnelles à mettre en place une démarche d'analyse de risques du SI d'une organisation en s'appuyant sur la norme ISO 27005.

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

Objectifs

Objectifs pédagogiques :

- Acquérir une compréhension approfondie de la norme ISO/CEI 27005 et son application dans la gestion des risques de sécurité de l'information.
- Identifier les processus métiers sensibles et stratégiques et leur système d'information associé.
- Délimiter le domaine d'application où s'exerce l'analyse de risque.
- Développer des compétences pour identifier, analyser et évaluer les risques de sécurité de l'information.
- Construire et hiérarchiser par criticité des scénarios de dysfonctionnement ou d'agression.
- Élaborer et mettre en œuvre des plans de traitement des risques alignés avec les stratégies d'entreprise.
- Accompagner l'entreprise dans l'application effective des plans de traitement des risques.
- Favoriser une culture proactive de gestion des risques au sein de l'organisation.

- Maîtriser diverses méthodes d'évaluation des risques telles que OCTAVE, MEHARI, EBIOS, NIST, CRAMM et TRA.
- Se préparer à passer l'examen de certification ISO/CEI 27005 Security Lead Risk Manager.

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 « **Évaluer et traiter les risques de sécurité de l'information en s'appuyant sur la norme NF ISO 27005 (ISO/CEI 27005 - Security Risk Manager)** » inscrite au Répertoire Spécifique n° 6399 (SKILLS4ALL). Examen officiel passé après la formation et vos révisions personnelles.
L'évaluation dure 2h00 et se fait en ligne, à travers **une mise en situation professionnelle fictive sous forme d'une étude de cas** depuis une plateforme d'apprentissage. Le candidat devra élaborer une présentation portant sur l'analyse des risques du système d'information, en se référant à la norme ISO 27005, appliquée à une organisation fictive. Cette présentation devra tenir compte du contexte spécifique, des particularités, des enjeux et de l'infrastructure du système d'information de l'entreprise, comme décrits dans la notice d'examen.
Le candidat devra pour cela :

- répondre à un QCM (questions fermées) ;
- présenter les résultats et préconisations de son analyse des risques selon l'ISO 27005 par écrit en 3 parties :
    - partie 1 : établissement de la stratégie d'évaluation et de traitement des risques en faisant références aux exigences de la norme ISO 27005 et aux données fournies dans le cas ;
    - partie 2 : proposition des plans de traitement des risques et de leur analyse comparée au regard des ressources mobilisées ;
    - partie 3 : conception d'un programme de mise en œuvre d'un plan de traitement systématique et pérenne précisant les ressources nécessaires à mobiliser.

A noter que comme le candidat passe son examen en toute autonomie, aussi il lui sera également demandé 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 la formation ISO 27005 Security Lead Risk Manager nécessite le prérequis suivant :

- avoir une bonne connaissance des systèmes d'information des organisations ainsi que des méthodes d'évaluation des risques liées à la sécurité de l'information.

Public

Cette formation s'adresse aux publics suivants :

- les responsables ou consultants impliqués ou responsables de la sécurité de l’information dans un organisme ;
- les personnes responsables de la gestion des risques liés à la sécurité de l’information ;
- les membres des équipes de sécurité de l’information, professionnels de l’informatique et responsables de la protection de la vie privée ;
- les personnes responsables du maintien de la conformité aux exigences de sécurité de l’information de la norme ISO/IEC 27005 au sein d’un organisme ;
- les gestionnaire de projet, consultants ou conseillers experts cherchant à maîtriser la gestion des risques liés à la sécurité de l’information.

Cette formation s'adresse aux profils suivants

Manager
Auditeur interne / externe
Chef de projet / Responsable de projet
Contrôleur de gestion
Administrateur système
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 27005.
- Identification des attentes et des perspectives individuelles des participants.

Partie 1: introduction à la norme ISO/IEC 27005 et à la gestion des risques en sécurité de l'information

- Réviser les cadres normatifs et réglementaires :
  - revue des normes et des cadres réglementaires influençant la sécurité de l'information.
- Comprendre les concepts fondamentaux de la gestion des risques :
  - introduction aux principes de la gestion des risques en sécurité de l'information.
- Mettre en place un programme de gestion des risques :
  - les étapes pour développer un programme efficient, y compris l'établissement du contexte et l'identification des parties prenantes.
- Identification des processus métiers sensibles :
  - l'utilisation de l'analyse SWOT pour aligner les traitements des risques avec les stratégies d'entreprise.

Partie 2 : processus de gestion des risques selon l'ISO/IEC 27005

- Délimiter le domaine d'application :
  - synthèse des informations collectées à partir de groupes de travail collaboratifs et documentation pour définir le périmètre d'action de l'analyse des risques.
- Identifier les risques :
  - les méthodes pour identifier les risques liés à la sécurité de l'information.
- Analyser et évaluer les risques :

    - les techniques d'analyse et d'évaluation, incluant les approches qualitatives et quantitatives.
- Construire et hiérarchiser des scénarios de risque :
    - l'élaboration de scénarios basés sur leur criticité, probabilité et impacts.
- Traiter les risques :
    - le développement de stratégies pour la gestion des risques identifiés.

Partie 3 : mise en œuvre et suivi du plan de traitement

- Élaborer des plans de traitement des risques :
    - la création de plans intégrant l'impact, la probabilité et les risques résiduels pour soutenir les décisions stratégiques.
- Mettre en œuvre un plan de traitement :
    - l'application des plans avec des indicateurs de suivi et collecte des retours d'expérience pour évaluer l'efficacité.
- Favoriser une culture de la gestion du risque :
    - l'encouragement des remontées et des analyses des incidents de sécurité pour renforcer la gestion des risques.
- Communiquer et consulter sur les risques :
    - les techniques pour communiquer et consulter efficacement autour des risques.
- Rédiger un rapport sur les risques :
    - la documentation systématique des risques et des mesures prises.
- Surveiller et réviser les risques :
    - le processus pour une surveillance régulière et une revue des risques.

Partie 4: méthodes d'évaluation des risques et préparation à la certification

- Présentation des méthodologies d'évaluation :
    - détails sur les méthodes OCTAVE, MEHARI, EBIOS, NIST, CRAMM, et TRA.
- Synthèse et clôture de la formation :
    - révision des principaux concepts abordés, pratiques d'examen, et stratégies pour réussir la certification.