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 Risk Manager + EBIOS : évaluer et traiter les risques de sécurité de l'information

Date et durée

Code formation : ISO27005SRME-RS
Durée : 5 jours
Nombre d'heures : 35 heures

Description

La maîtrise de la gestion des risques liés aux systèmes d'information est cruciale pour assurer la sécurité et le bon fonctionnement des entreprises. En vous inscrivant à notre **formation combinée ISO/CEI 27005 Security Risk Manager et EBIOS**, vous acquerrez une compréhension approfondie des normes et des meilleures pratiques en gestion des risques informatiques.
Cette formation vous permettra de **maîtriser les processus et les actifs essentiels à la sécurité de l'information**, conformément à la norme ISO/CEI 27005:2022, et d'explorer des méthodes reconnues telles que OCTAVE, MEHARI, et EBIOS. Développée par l'ANSSI, **EBIOS se distingue par son approche collaborative,** utilisant des scénarios de menaces réalistes pour une analyse de risques précise et des stratégies de mitigation efficaces.
Vous développerez des **compétences complémentaires en analyse et gestion des risques**, essentielles pour concevoir et implémenter un système de management de la sécurité de l'information robuste et conforme aux normes internationales. Notre formation renforcera votre expertise professionnelle, vous préparant à naviguer dans le paysage complexe de la sécurité de l'information et à répondre aux défis actuels et futurs.
À travers **des exercices pratiques et des études de cas**, notre programme vous préparera à réussir l'examen de certification ISO/CEI 27005 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 et la méthode EBIOS.

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

Objectifs

Objectifs pédagogiques :

- Identifier les processus métiers sensibles et stratégiques et leur système d'information associé en s'appuyant sur une analyse SWOT.
- Délimiter le domaine d'application (périmètre d'action) sur lequel s'exerce l'analyse de risque.
- Construire et hiérarchiser par criticité des scenarii de dysfonctionnement ou d'agression.
- Elaborer les plans de traitement des risques.

- Accompagner l’entreprise dans la mise en œuvre du plan de traitement.
- Favoriser une culture de la gestion du risque lié au système d’information.
- Assimiler les principes et les fondamentaux de la méthode EBIOS.
- Développer les compétences nécessaires pour mener une étude EBIOS complète, en apprenant à analyser, rapporter, et communiquer les résultats de manière efficace.

Points forts

Certification internationalement reconnue. Travaux pratiques basés sur des cas réels avec une documentation de 350 pages ; Examen 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

Travaux Pratiques
Etude de cas

Pré-requis

Suivre cette formation 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 gestion des risques et à la norme ISO 27005

- Comprendre et définir le risque :
  - définitions fondamentales du risque, distinction entre risque, menace, et vulnérabilité.
- Comprendre la norme ISO/CEI 27005:2022 :
  - exploration des spécificités de la dernière version de la norme, et son rôle dans la gestion des risques de sécurité de l'information.
- Identifier les processus métiers sensibles :
  - techniques pour identifier les processus stratégiques et leur système d'information associé, utilisant une analyse SWOT pour aligner les décisions de traitement des risques avec la stratégie de l'entreprise.
- Mettre en place un programme de gestion des risques : les étapes pour développer un programme de gestion des risques conforme à ISO 27005, incluant la définition des responsabilités et le processus de décision.

Partie 2: mise en œuvre d'un processus de gestion des risques selon la norme ISO 27005

- Délimiter le domaine d'application :
  - méthodes pour synthétiser les informations issues de groupes de travail collaboratifs et de la documentation pour définir clairement le périmètre de l'analyse de risque.

- Construire et hiérarchiser des scénarios de risque :
    - création de scénarios de dysfonctionnement ou d'agression basés sur leur criticité, en collaboration avec des experts pour évaluer leur probabilité et impacts.
- Analyser et évaluer les risques :
    - techniques pour l'analyse qualitative et quantitative des risques.
- Elaboration des plans de traitement des risques : développement de plans de gestion des risques, en intégrant l'analyse des scénarios pour proposer des solutions alignées avec les objectifs stratégiques de l'entreprise.

Partie 3 : suivi et culture de la gestion du risque

- Mise en œuvre du plan de traitement :
    - stratégies pour l'application effective des plans de traitement des risques, incluant l'établissement d'indicateurs de suivi et la collecte de retours d'expérience pour évaluer l'efficacité des actions dans le temps.
- Favoriser une culture de la gestion du risque :
    - techniques pour encourager la remontée et l'analyse des incidents de sécurité de l'information, renforçant ainsi la culture de la gestion des risques au sein de l'organisation.

Partie 4 : analyse des risques avec la méthode EBIOS

- Introduction.
- Présentation de la notion de risques.
- Les 5 étapes de la méthode EBIOS.
- Application pratique de la méthode en petits groupes (2 à 3 personnes) sur un cas prédéfini :
- Les éléments essentiels.

Partie 5 : application de la méthode EBIOS

- L'exploitation des résultats de la méthode vers:
    - SOA (Déclaration d'applicabilité).
    - La politique de sécurité (Exigences ISO 27001).
    - Le plan d'action sécurité (SMSI).
- La conduite d'une analyse des risques.
- Les expressions des besoins.
- Les vulnérabilités.

Partie 6 : conclusion d'une analyse de risques avec EBIOS

- Application pratique de la méthode en petits groupes (2 à 3 personnes) sur un cas prédéfini ;
- L'analyse des risques.
- Les objectifs de sécurité.
- Les couvertures des risques.

Partie 7 : autres méthodologies et préparation à la certification

- Présentation des méthodes d'appréciation des risques : exploration des méthodes OCTAVE, MEHARI et EMR, et discussion sur leur intégration dans la stratégie de gestion des risques de l'entreprise.
- Préparation à l'examen de certification ISO 27005 Security Risk Manager :
    - révision des principaux concepts abordés, pratiques d'examen, et stratégies pour réussir la certification.