Date de publication : 21/03/2025

Formation : Certified ISO/IEC 27005 Risk Manager, certification PECB

Formation pratique - 3j - 21h00 - Réf. RMP
Prix : 2460 € H.T.

Cette formation vous permettra d'acquérir les connaissances et les compétences nécessaires pour identifier, évaluer, analyser, traiter et communiquer les risques liés à la sécurité de l'information selon la norme ISO/IEC 27005.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Expliquer les concepts et principes de gestion des risques tels que définies par les normes ISO/IEC 27005 et ISO 31000
- Établir, maintenir et améliorer un cadre de gestion des risques liés à la sécurité de l'information
- Appliquer des processus de gestion des risques liés à la sécurité de l'information
- Planifier et mettre en place des activités de communication et de consultation sur les risques

Public concerné

Responsables de la sécurité de l'information, personnes responsables du maintien de la conformité aux exigences de sécurité de l'information, gestionnaire de projet, conseillers experts...

Prérequis

Connaître un guide de bonnes pratiques (hygiène ANSSI, ISO 27002 ou équivalent), avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

PARTICIPANTS

Responsables de la sécurité de l'information, personnes responsables du maintien de la conformité aux exigences de sécurité de l'information, gestionnaire de projet, conseillers experts...

PRÉREQUIS

Connaître un guide de bonnes pratiques (hygiène ANSSI, ISO 27002 ou équivalent), avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Introduction à la norme ISO/IEC 27005 et à la gestion des risques

- Objectifs et structure de la formation.
- Cadres normatifs et réglementaires.
- Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information.
- Programme de gestion des risques.
- Établissement du contexte.

2 Appréciation des risques, traitement des risques, communication des risques et concertation selon ISO/IEC 27005

- Identification des risques.
- Analyse du risque.
- Évaluation du risque.
- Traitement du risque.
- Évaluation des risques liés à la sécurité de l'information.
- Communication et concertation relatives aux risques liés à la sécurité de l'information.

3 Risk recording and reporting, monitoring and review, and risk assessment methods

- Surveillance et revue des risques de sécurité de l'information.
- Méthodologies OCTAVE et MÉHARI.
- Méthode EBIOS.
- Cadre NIST.
- Méthodes CRAMM et EMR.

4 Domaines de compétences couverts par l'examen :

- Domaine 1 : principes et concepts fondamentaux d'un système de gestion des risques liés à la sécurité de l'information.
- Domaine 2 : mise en œuvre d'un programme de gestion des risques liés à la sécurité de l'information.
- Domaine 3 : cadre de gestion des risques liés à la sécurité de l'information et processus de la norme ISO/IEC 27005.
- Domaine 4 : autres méthodes d'appréciation des risques liés à la sécurité de l'information

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

Dates et lieux

CLASSE À DISTANCE
2026 : 24 juin, 28 sep., 30 nov.

PARIS LA DÉFENSE
2026 : 17 juin, 21 sep., 23 nov.