Date de publication : 01/10/2024

Formation : ISO/IEC 27035 Lead Incident Manager, certification PECB

Cours pratique - 5j - 35h00 - Réf. IMC
Prix : 3940 CHF H.T.

Cette formation vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de la mise en œuvre d'un plan de gestion des incidents de sécurité de l'information selon la norme ISO/CEI 27035. Durant cette formation, vous découvrirez l'ensemble du cycle de vie de l'incident, de la planification de l'incident aux activités post-incident.

Objectifs pédagogiques

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

- Expliquer les principes fondamentaux de la gestion des incidents.
- Élaborer et mettre en œuvre des plans de réponse aux incidents, sélectionner une équipe de réponse aux incidents.
- Réaliser des appréciations approfondies des risques afin d'identifier les menaces potentielles au sein d'un organisme.
- Appliquer les bonnes pratiques issues de diverses normes internationales.
- Effectuer une analyse après l'incident et identifier les leçons tirées de l'expérience.

Public concerné

Gestionnaires des incidents de sécurité de l'information, responsables des TIC, administrateurs professionnels des systèmes informatiques, administrateurs professionnels de réseau informatique…

Prérequis

Avoir une connaissance générale des processus de gestion des incidents, des principes de sécurité de l'information et de la famille de normes ISO/IEC 27000.

PARTICIPANTS

Gestionnaires des incidents de sécurité de l'information, responsables des TIC, administrateurs professionnels des systèmes informatiques, administrateurs professionnels de réseau informatique…

PRÉREQUIS

Avoir une connaissance générale des processus de gestion des incidents, des principes de sécurité de l'information et de la famille de normes ISO/IEC 27000.

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.

Certification

L'examen consiste à répondre à 12 questions en 3h00 à livre ouvert. À l'issue du cours, une attestation de suivi de la formation de 31 crédits de FPC (Formation professionnelle continue) sera délivrée. Les candidats ayant suivi la formation mais échoué à l'examen peuvent le repasser gratuitement une seule fois dans un délai de 12 mois à compter de la date initiale de l'examen.

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 aux concepts liés à la gestion des incidents de sécurité de l'information et à la norme ISO/IEC 27035

- Objectifs et structure de la formation.
- Normes et cadres réglementaires.
- Concepts fondamentaux de la gestion des incidents.
- Gestion des incidents de sécurité de l'information.
- Établissement du contexte.
- Politiques et procédures.

2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

- Management du risque.
- Plan de gestion des incidents.
- Équipe de gestion des incidents.
- Relations internes et externes.
- Assistance technique et autre.
- Sensibilisation et formation aux incidents de sécurité de l'information.

3 Détection et signalement des incidents liés à la sécurité de l'information

- Tests.
- Surveillance des systèmes et des réseaux.
- Détecter et alerter.
- Collecte d'informations sur les incidents.
- Signalement des événements liés à la sécurité de l'information.
- Appréciation des événements liés à la sécurité de l'information.

4 Surveillance et amélioration continue du processus de gestion des incidents liés à la sécurité de l'information

- Résolution des incidents liés à la sécurité de l'information.
- Confinement, éradication et récupération.
- Enseignements tirés.
- Surveillance, mesure, analyse et évaluation.
- Amélioration continue.

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.

5 Certification

- Domaines de compétences couverts par l'examen :
- Domaine 1 : Principes et concepts fondamentaux de la gestion des incidents de sécurité de l'information.
- Domaine 2 : Processus de gestion des incidents de sécurité de l'information basé sur la norme ISO/ IEC 27035.
- Domaine 3 : Conception d'un processus organisationnel de gestion des incidents basé sur la norme ISO/IEC 27035.
- Domaine 4 : Préparation et exécution du plan de réponse aux incidents liés à la sécurité de l'information.
- Domaine 5 : Mise en œuvre de processus de gestion des incidents liés à la sécurité de l'information ce en différé.
- Domaine 6 : Amélioration des processus et des activités de gestion des incidents.

Dates et lieux

CLASSE À DISTANCE
2026 : 30 mars, 15 juin, 28 sep., 7 déc.