Responsable système de management de sécurité de l'information (ISO 27001-2013) (BV-RSMSI), certification Bureau Veritas

Cours Pratique de 5 jours - 35h
Réf : SYS - Prix 2024 : 3 890CHF HT

La norme ISO 27001-2013 permet la mise en place d'un management de la sécurité de l'information afin de garantir une cohérence sur la protection de l'information de chaque entreprise. Cette certification permet de valider les savoirs pour toute personne en charge de participer à la mis en œuvre d'un SMSI.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Décrire l'objectif et les avantages d'un système de management de la sécurité de l'information

Savoir mettre en œuvre un système de management basé sur la norme ISO 27001

Savoir mener une analyse de risque

Connaitre les principaux concepts de gouvernance et ses principaux enjeux et implication en matière de sécurité de l'information

Utiliser la norme ISO 27001 comme cadre pour l'amélioration continue

CERTIFICATION

Bureau Veritas Certification assure l'examen final de ce programme de formation, délivré par un organisme de formation indépendant. Cet examen permet d'obtenir une certification de personne.
Examen de 3 heures : partie théorique et pratique, l'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets. Il se déroule sur une plateforme à distance.
L'accès au support de cours, aux travaux pratiques est assuré pendant 3 semaines à compter du début de session. Le passage de la certification doit être réalisé en ce laps de temps. En cas d'échec au premier passage, le candidat a la possibilité de réaliser un second passage dans les 15 jours suivants le premier.

PARTENARIAT

La certification est délivrée par Bureau Veritas Certification.
ORSYS et Bureau Veritas Certification se sont associés pour construire une offre de certifications couvrant les principaux domaines de la cybersécurité : architectures sécurisées, sécurité offensive et défensive, sécurité organisationnelle et système de management.

LE PROGRAMME

dernière mise à jour : 02/2022

1) Les principes fondamentaux de la sécurité de l'information et de la protection des données

- Les normes ISO.
- Vocabulaire.
- Le CID.

PARTICIPANTS

DSI, RSSI, Risk manager, chef de projet sécurité, auditeur sécurité, consultant sécurité.

PRÉREQUIS

Connaissance du fonctionnement managérial et organisationnel d'une organisation et connaissance de base en sécurité de l'information.

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.

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 stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage 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 stagiaire 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Le risque.
- Définition du SMSI.
- Structure des normes et le PDCA.
- Les exigences de l'ISO 27701. Le contenu de l'annexe A de l'ISO 27001.
- Les livrables attendus.

Travaux pratiques : Etude de la norme.

2) Préparation et planification du projet SMSI

- Le lancement du projet SMSI.
- Compréhension de l'organisme.
- Cartographies.
- Analyse des écarts.
- Définition du domaine d'application.
- Matrice des compétences.

Travaux pratiques : Etude de cas.

3) Leadership et management

- Business Case.
- Politique de sécurité de l'information.
- Domaine d'application.
- Rôles et responsabilités.
- Principaux éléments attendus.
- Politiques connexes. Comitologie.
- Communication.
- Ressources.

Travaux pratiques : Etude de cas.

4) L'analyse de risque

- Le processus de management du risque.
- Le risque résiduel et l'acceptation du risque.
- Plan de traitement des risques.
- Les méthodologies d'analyse de risque.

Travaux pratiques : Exercices d'identification des risques pour le SI.

5) Déclaration d'applicabilité

- Présentation des exigences.
- Justifications.

Travaux pratiques : Etude de cas : DDA.

6) Mise en place du SMSI

- Gestion documentaire.
- Plan de formation et de sensibilisation.
- Plan de communication.
- Gestion des incidents.
- Autres mesures à mettre en œuvre.

Travaux pratiques : Exercices et étude de cas.

7) Suivi et amélioration

- Le suivi et la mesure des performances.
- L'audit interne.
- Revue de direction.
- Le traitement des non-conformités.
- L'amélioration continue.

Travaux pratiques : Exercices et étude de cas.

8) Examen

- Révisions.

- Passage de l'examen.

LES DATES

CLASSE À DISTANCE
2024 : 11 mars, 27 mai, 16 sept.,
18 nov.