ISO 27005:2018 Risk Manager, préparation et certification

Cours Pratique de 5 jours
Réf : RMC - Prix 2022 : 3 990€ HT
Le prix pour les dates de sessions 2023 pourra être révisé

Cette formation, basée en partie sur la norme ISO/CEI 27005:2018, permet aux participants d'acquérir les bases théoriques et pratiques de la gestion des risques liés à la sécurité de l'information. Elle prépare efficacement les candidats à la certification ISO 27005 Risk Manager à partir d'études de cas. Vous verrez également comment mettre en place la méthode EBIOS afin de pouvoir apprécier et traiter les risques relatifs à la sécurité des SI.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre le concept de risque lié à la sécurité de l'information

Utiliser ISO 27005:2018 pour l'analyse de risque

Connaître d'autres méthodes (EBIOS, MEHARI)

Faire un choix rationnel de méthode d'analyse de risque

CERTIFICATION

L'examen de certification est dirigé en partenariat avec l'organisme de certification LSTI (accrédité COFRAC). Il se déroule pendant la dernière demi-journée. Ce diplôme international officiel ISO vous apportera la plus grande crédibilité dans la conduite de vos projets d'analyse de risques.

LE PROGRAMME

dernière mise à jour : 06/2020

1) Introduction

- Terminologie ISO 27000 et ISO Guide 73.
- Définitions de la Menace. Vulnérabilité. Risques.
- Principe général de la sécurité ISO 13335.
- La classification CAID.
- Rappel des contraintes réglementaires et normatives (SOX, COBIT, ISO 27001...).
- Le rôle du RSSI versus le Risk Manager.
- La future norme 31000, de l'intérêt de la norme "chapeau".

2) Le concept "risque"

- Identification et classification des risques.
- Risques opérationnels, physiques et logiques.
- Les conséquences du risque (financier, juridique, humain...).
- La gestion du risque (prévention, protection, évitement de risque, transfert).
- Assurabilité d'un risque, calcul financier du transfert à l'assurance.
- Les rôles complémentaires du RSSI et du Risk Manager/DAF.

3) L'analyse de risques selon l'ISO

- La méthode de la norme 27001:2013.
- L'intégration au processus PDCA.
- La création en phase Plan de la section 4.
- La norme 27005:2018 : Information Security Risk Management.
- La mise en œuvre d'un processus PDCA de management des risques.
- Les étapes de l'analyse de risques.

PARTICIPANTS

RSSI ou correspondants Sécurité, architectes de sécurité, directeurs ou responsables informatiques, ingénieurs, chefs de projets (MOE, MOA) devant intégrer des exigences de sécurité.

PRÉREQUIS

Connaissances de base dans le domaine de la sécurité informatique.

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.

- La préparation de la déclaration d'applicabilité (SoA).

4) Les méthodes d'analyse de risques

- Les méthodes françaises. EBIOS RM.
- Etude du contexte, des scénarios de menaces, des événements redoutés, des risques, des mesures de sécurité.
- EBIOS dans une démarche ISO PDCA de type SMSI 27001.
- MEHARI. L'approche proposée par le CLUSIF.
- Elaboration d'un plan d'actions basé les services de sécurité. Alignement MEHARI 27005 et référentiel ISO 27002.
- CRAMM, OCTAVE... Historique, développement, présence dans le monde. Comparaisons techniques.

5) Choix d'une méthode et conclusion

- Comment choisir la meilleure méthode ?
- Les bases de connaissances (menaces, risques...).
- La convergence vers l'ISO, la nécessaire mise à jour.
- Etre ou ne pas être "ISO spirit" : les contraintes du modèle PDCA.
- Une méthode globale ou une méthode par projet.
- Le vrai coût d'une analyse de risques.

6) La méthode EBIOS RM

- Introduction.
- Réaliser une étude du contexte.
- Réaliser une étude des événements redoutés.
- Réaliser une étude des scénarios de menaces.
- Réaliser une étude des risques.
- Réaliser une étude des mesures de sécurité.

Travaux pratiques : Définir quel est le sujet de l'étude. Identification des événements craints. Définir les scénarios possibles. Définir ceux qui sont les plus vraisemblables.Cartographie des risques. Traiter les différents risques.Identification des mesures à appliquer. Définir l'acceptabilité des risques résiduels.

7) Préparation de la certification

- Mise en situation, tests de connaissance de type QCM, études de cas.
- Inventaire d'actifs, évaluation des menaces et vulnérabilités.
- Elaboration de plans de traitement des risques, etc.

Travaux pratiques : Echanges sur pourquoi et comment gérer les risques. Définir quel est le sujet de l'étude.

8) Corrections collectives

- Restitution des résultats des exercices et des TP sous forme de corrections collectives.
- Explications des erreurs éventuelles.

9) Révision finale et durée de l'examen

- Pour clore la préparation, une révision finale est réalisée.
- Les astuces pour éviter les pièges.
- L'examen écrit dure environ 2h30.
- Pour assurer l'anonymat lors de la correction des examens, les copies sont numérotées.
- Seul le formateur connaît la correspondance entre le numéro de copie et l'identité du candidat.

10) Epreuves, points et résultats

- L'examen comporte au minimum un questionnaire relatif à la norme ISO/IEC 27005:2018.
- Un exercice sur le modèle PDCA et une étude de cas sur la gestion des risques.
- L'évaluation du formateur sur l'attitude générale et sur la capacité à s'exprimer oralement.

- Evaluation de l'attitude générale (participation, ambiance de travail, etc.) et de la capacité à travailler en équipe.
- Evaluation de la capacité à s'exprimer oralement : respect du temps imparti, esprit de synthèse et clarté.
- L'évaluation du formateur est sur 3 points, elle s'ajoute à la notation de l'examen écrit pour un total de 100 points.
- Le candidat doit obtenir un minimum de 70 points (examen écrit et évaluation du formateur) pour être certifié.
- Les résultats de l'examen vous parviendront par courrier environ 6 semaines plus tard.

LES DATES

BREST
2023 : 20 mars, 12 juin, 21 août, 20 nov.

CLERMONT-FERRAND
2023 : 20 févr., 24 avr., 17 juil., 06 nov.

AIX-EN-PROVENCE
2023 : 16 janv., 24 avr., 31 juil., 23 oct.

ANGERS
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

BORDEAUX
2023 : 27 févr., 12 juin, 25 sept., 11 déc.

DIJON
2023 : 20 févr., 24 avr., 17 juil., 06 nov.

GRENOBLE
2023 : 20 févr., 24 avr., 17 juil., 06 nov.

LILLE
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

LYON
2023 : 20 févr., 24 avr., 19 juin, 17 juil., 11 sept., 06 nov.

MONTPELLIER
2023 : 16 janv., 24 avr., 31 juil., 23 oct.

NANCY
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

NANTES
2023 : 20 mars, 12 juin, 21 août, 20 nov.

NIORT
2023 : 27 févr., 12 juin, 25 sept., 11 déc.

ORLÉANS
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

PARIS LA DÉFENSE
2023 : 13 févr., 03 avr., 22 mai, 19 juin, 04 sept., 23 oct., 13 nov., 04 déc.

REIMS
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

RENNES
2023 : 20 mars, 12 juin, 21 août, 20 nov.

ROUEN
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

SOPHIA-ANTIPOLIS
2023 : 16 janv., 24 avr., 31 juil., 23 oct.

STRASBOURG
2023 : 20 mars, 12 juin, 21 août, 20 nov.

TOULON
2023 : 16 janv., 24 avr., 31 juil., 23 oct.

TOULOUSE
2023 : 27 févr., 12 juin, 25 sept., 11 déc.

TOURS
2023 : 13 févr., 03 avr., 04 sept., 23 oct.

CLASSE A DISTANCE
2022 : 24 oct., 05 déc.

2023 : 13 févr., 03 avr., 22 mai, 19 juin, 04 sept., 23 oct., 13 nov., 04 déc.