Best

ISO 27005 - Certified Risk Manager avec EBIOS

Évaluer les risques et mettre en place les réponses ad'hoc - Certification incluse

★★★★★ **4,3/5 (13 avis)**

Présentiel ou en classe à distance

5 jours (35 h)

Prix inter : 4.080,00 € HT
Forfait intra : 26.550,00 € HT

Réf.: MG828

Formation Officielle

PECB AUTHORIZED TITANIUM PARTNER

En matière d'appréciation des risques, EBIOS (pour Expression des Besoins et Identification des Objectifs de Sécurité), la méthode proposée par l'Agence National de la Sécurité des Systèmes d'Information (ANSSI) qui a notamment pour mission de proposer des règles à appliquer pour la protection des systèmes d'information de l'Etat français, fait figure de référence. Conforme à la norme ISO 27005 conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche méthodique du risque, EBIOS constitue la boite à outils idéale pour construire son référentiel SSI. Indispensable à tout manager impliqué dans la gestion de la sécurité, cette formation intensive de 5 jours prépare aux certifications EBIOS Risk Manager et ISO 27005 Risk Manager qui seront passées en séance.

A qui s'adresse cette formation ?

- Chefs de projet, consultants, architectes techniques
- Toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation
- Toute personne amenée à mettre en oeuvre ISO/CEI 27001 ou impliquée dans un programme de gestion des risques selon la méthode EBIOS

- Avoir une compréhension fondamentale de la norme ISO/IEC 27005, une connaissance approfondie de l'évaluation des risques et de la sécurité de l'information.
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Pendant

1 - 1ère partie : ISO 27005 - Risk Manager

2 - Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005

- Objectifs et structure de la formation
- Concepts du risque
- Définition scientifique du risque
- Le risque et les statistiques
- Le risque et les opportunités
- La perception du risque
- Le risque lié à la sécurité de l'information

3 - Connaître le cadre normatif et réglementaire

- Norme et méthodologie
- ISO/IEC 31000 et ISO/IEC 310010
- Normes de la famille ISO/IEC 27000

4 - Mettre en oeuvre un programme de management du risque

- Mandat et engagement de la direction
- Responsable de la gestion du risque
- Responsabilités des principales parties prenantes
- Mesures de responsabilisation
- Politique de la gestion du risque
- Processus de la gestion du risque
- Approche et méthodologie d'appréciation du risque
- Planification des activités de gestion du risque et fourniture des ressources

5 - Établir le contexte mission, objectifs, valeurs, stratégies

- Établissement du contexte externe
- Établissement du contexte interne
- Identification et analyse des parties prenantes
- Identification et analyse des exigences
- Détermination des objectifs
- Détermination des critères de base
- Définition du domaine d'application et limites

6 - Identifier les risques

- Techniques de collecte d'information
- Identification des actifs
- Identification des menaces
- Identification des mesures existantes
- Identification des vulnérabilités
- Identification des impacts

7 - Analyser et évaluer les risques

- Appréciation des conséquences
- Appréciation de la vraisemblance de l'incident
- Appréciation des niveaux des risques
- Évaluation des risques
- Exemple d'appréciation des risques

8 - Apprécier les risques avec une méthode quantitative

- Notion de ROSI
- Calcul de la perte annuelle anticipée
- Calcul de la valeur d'une mesure de sécurité
- Politiques spécifiques
- Processus de management de la politique

9 - Traiter les risques

- Processus de traitement des risques
- Option de traitement des risques
- Plan de traitement des risques

10 - Apprécier les risques et gérer les risques résiduels

- Acceptation des risques

- Approbation des risques résiduels
- Gestion des risques résiduels
- Communication sur la gestion des risques

11 - Communiquer sur les risques

- Objectifs de communication sur la gestion des risques
- Communication et perception des risques
- Plan de communication

12 - Surveiller les risques

- Surveillance et revue des facteurs de risque
- Surveillance et revue de la gestion des risques
- Amélioration continue de la gestion des risques
- Mesurer le niveau de maturité de la gestion des risques
- Enregistrement des décisions et des plans de communications

13 - Découvrir la méthode OCTAVE

- Présentation générale
- Méthodologies OCTAVE
- OCTAVE Allegro Roadmap

14 - Découvrir la méthode MEHARI

- Présentation générale
- L'approche MEHARI
- Analyse des enjeux et classification
- Évaluation des services de sécurité
- Analyse des risques
- Développement des plans de sécurité

15 - Découvrir la méthode EBIOS

- Présentation générale
- Les 5 modules d'EBIOS
- Établissement du contexte
- Étude d'événements redoutés
- Étude des scénarios des menaces
- Étude des risques
- Étude des mesures de sécurité

16 - 2ème partie : EBIOS Risk Manager certifiant

17 - Introduction à la méthode EBIOS

- Présentation générale d'EBIOS
- Principales définition
- Les 5 phases d'EBIOS : étude du contexte, des évènements redoutés, des scénarios de menaces, des risques et des mesures de sécurité
- L'ISO 27005 appliquée dans EBIOS
- Les grands principes d'EBIOS : implication sensibilisation, adhésion et responsabilisation

18 - Définir le cadre de la gestion des risques

- Cadrage de l'étude des risques
- Description du contexte général
- Limites du périmètre de l'étude
- Identification des paramètres à prendre en compte
- Identification des sources de menace

19 - Préparer les métriques

- Définition des critères de sécurité
- Élaboration des échelles de besoin
- Élaboration d'une échelle de niveaux de gravité
- Élaboration d'une échelle de niveaux de vraisemblance
- Définition des critères de gestion des risques

20 - Identifier les biens

- Identification des biens essentiels, leurs relations et leurs dépositaires
- Identifier les biens supports, leurs relations et leurs dépositaires

- Détermination des liens entre les biens essentiels et les biens supports
- Identification des mesures de sécurité existantes

21 - Apprécier les événements redoutés

- Analyse d'événements redoutés
- Évaluation de chaque événement redouté

22 - Apprécier les scénarios de menaces

- Analyse de tous les scenarios de menaces
- Évaluation de chaque scenario de menace

23 - Apprécier les risques

- Analyse des risques
- Évaluation de chaque risque

24 - Identifier les objectifs de sécurité

- Choix des options de traitement des risques
- Analyse des risques résiduels

25 - Formaliser les mesures de sécurité à mettre en oeuvre

- Détermination des mesures de sécurité
- Analyse des risques résiduels
- Établissement d'une déclaration d'applicabilité

26 - Mettre en oeuvre les scenarios de sécurité

- Élaboration d'un plan d'actions
- Suivi de la réalisation des mesures de sécurité
- Analyse des risques résiduels
- L'homologation de sécurité

27 - Préparation de l'examen à travers une étude de cas

- Passage en revue de tous les thèmes abordés

28 - Passage de l'examen de certification ISO/IEC 27005 Risk Manager (en ligne après la formation)

- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-pr%C3%A9paration-a-l%E2%80%99examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70% est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- Les candidats sont autorisés à utiliser les supports de cours
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants : Domaine 1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information - Domaine 2 : Mettre en oeuvre un programme de gestion des risques liés à la sécurité de l'information - Domaine 3 : Processus et cadre de gestion des risques liés à la sécurité de l'information conformes à la norme ISO/CEI 27005 - Domaine 4 : Autres méthodes d'appréciation des risques de la sécurité de l'information

29 - Passage de l'examen de certification EBIOS Risk Manager (en ligne après la formation)

- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-pr%C3%A9paration-a-l%E2%80%99examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70% est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants : Domaine 1 : Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information selon la méthode EBIOS - Domaine 2 : Programme de gestion des risques liés à la sécurité de l'information basé sur EBIOS - Domaine 3 : Appréciation des risques liés à la sécurité de l'information basée sur la méthode EBIOS

Les objectifs de la formation

- Connaître les concepts, approches, méthodes et techniques associés à un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
- Être en mesure de conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information
- Connaître les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Maîtriser les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Acquérir les compétences nécessaires afin de mener une étude EBIOS et en analyser et restituer les résultats

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.
Il est fortement recommandé d'être en possession de la norme pour le passage de l'examen.

Les points forts de la formation

- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.
- Les résultats des examens sont disponibles sous 4 à 8 semaines et sont directement envoyés aux candidats par email.
- 86% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.
Il est fortement recommandé d'être en possession de la norme pour le passage de l'examen.

Dates et villes 2027 - Référence MG828

Dernières places disponibles Session garantie

A distance

du 18 janv. au 22 janv.	du 7 juin au 11 juin	du 15 nov. au 19 nov.
du 15 mars au 19 mars	du 6 sept. au 10 sept.	

Paris

du 18 janv. au 22 janv.	du 7 juin au 11 juin	du 15 nov. au 19 nov.
du 15 mars au 19 mars	du 6 sept. au 10 sept.	