Formation ISO 27005 - Certified Risk Manager avec EBIOS

Évaluer les risques et mettre en place les réponses ad'hoc

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	MGR828
Durée	5 jours (35h)
Tarif	3 675 €HT
Certification	prix inclus

SESSIONS PROGRAMMÉES

PARIS

du 22 au 26 juillet 2024
du 30 sept. au 4 octobre 2024
du 25 au 29 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| 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

Public

| 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 gesti

Prérequis

| Connaitre le guide d'hygiène sécurité de l'ANSSI

Programme de la formation

1ère partie : ISO 27005 - Risk Manager
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

Connaître le cadre normatif et réglementaire
| Norme et méthodologie
| ISO/IEC 31000 et ISO/IEC 310010
| Normes de la famille ISO/IEC 27000

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

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

Identifier les risques
| Techniques de collecte d'information
| Identification des actifs
| Identification des menaces
| Identification des mesures existantes
| Identification des vulnérabilités
| Identification des impacts

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

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

Traiter les risques
| Processus de traitement des risques
| Option de traitement des risques
| Plan de traitement des risques

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

Communiquer sur les risques
| Objectifs de communication sur la gestion des risques
| Communication et perception des risques
| Plan de communication

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

Découvrir la méthode OCTAVE
| Présentation générale
| Méthodologies OCTAVE
| OCTAVE Allegro Roadmap

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

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

2ème partie : EBIOS Risk Manager certifiant
| 16.1)

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

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

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

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

Apprécier les événements redoutés
| Analyse d'événements redoutés
| Évaluation de chaque événement redouté

Apprécier les scénarios de menaces
| Analyse de tous les scenarios de menaces
| Évaluation de chaque scenario de menace

Apprécier les risques
| Analyse des risques
| Évaluation de chaque risque

Identifier les objectifs de sécurité
| Choix des options de traitement des risques
| Analyse des risques résiduels

Formaliser les mesures de sécurité à mettre en oeuvre
| Détermination des mesures de sécurité
| Analyse des risques résiduels
| Établissement d'une déclaration d'applicabilité

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

Préparation de l'examen à travers une étude de cas
| Passage en revue de tous les thèmes abordés

3ème partie : Passage des examens de certification ISO/IEC 27005 Risk Manager et EBIOS Risk Manager
| 28.1)

Examen de certification ISO/IEC 27005 Risk Manager
| Révision des concepts en vue de la certification
| Examen blanc
| Passage de l'examen écrit de certification en français qui consiste à répondre à 12 questions 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 non seulement les supports de cours mais aussi la norme ISO/IEC 27005
| 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

Examen de certification EBIOS Risk Manager

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

EBIOS Risk Manager
Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification.
À l'issue du cours y préparant, un certificat de participation de 21 crédits DPC (Développement professionnel continu) est délivré.

| Durée : 2h30
| Format : 12 questions
| Score minimum : 70%

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

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.