ISO 27005 – Certified Risk Manager avec EBIOS

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Pilotage de la sécurité organisationnelle

Rubrique : Management de la CyberSecurité : Certifications

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

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.
Cette formation prépare aux certifications ISO/IEC 27005 Risk Manager et EBIOS Risk Manager.

Public visé

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
formation.fr/guide_hygiene_informatique_anssi.pdf)

Pré-requis

Connaitre le guide d'hygiène sécurité de l'ANSSI
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

PROGRAMME

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

Code de formation : MG828

€ Tarifs

Prix public : 3570 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 35 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

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

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

29 - 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

30 - Examen de certification EBIOS Risk Manager
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
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

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Les plus 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.