Formation ISO 27005 - Risk Manager

Implémenter la norme ISO 27005

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

Avec la généralisation des échanges sur Internet, les risques en matière de sécurité de l'information sont chaque jour plus importants. L'un des éléments clés dans la prévention des fraudes en ligne, vols d'identité ou autres détériorations de sites Web est la gestion et l'évaluation des risques couvertes par la nouvelle norme internationale ISO/CEI 27005. La formation "ISO/CEI 27005 Risk Manager" permet de développer les compétences pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/CEI 27005 comme cadre de référence. Ce programme qui s'inscrit parfaitement dans le processus de mise en oeuvre du cadre SMSI selon la norme ISO/CEI 27001, intègre également une présentation de différentes méthodes d'appréciation des risques (OCTAVE, EBIOS, MEHARI,...). Après la formation, les participants passeront l'examen "ISO/CEI 27005 Risk Manager" qui attestera de leurs capacités à apprécier les risques de la sécurité de l'information et à les gérer.

Référence	MGR209
Durée	3 jours (21h)
Tarif	2 590 €HT
Certification	prix inclus

Objectifs

| Identifier la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
| Identifier les concepts, approches, méthodes et techniques pour mettre en place un processus de gestion des risques conforme
| Interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
| Conseiller efficacement les organisations sur les meilleures pratiques de gestion des risques liés à la sécurité de l'information

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

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

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
- du 15 au 17 juillet 2025
- du 1er au 3 septembre 2025

PARIS
- du 15 au 17 juillet 2025
- du 1er au 3 septembre 2025

AIX-EN-PROVENCE
- du 6 au 8 octobre 2025

BORDEAUX
- du 6 au 8 octobre 2025
- du 8 au 10 décembre 2025

GRENOBLE
- du 6 au 8 octobre 2025
- du 8 au 10 décembre 2025

LILLE
- du 15 au 17 juillet 2025
- du 6 au 8 octobre 2025

LYON
- du 6 au 8 octobre 2025
- du 8 au 10 décembre 2025

NANTES
- du 15 au 17 juillet 2025
- du 8 au 10 décembre 2025

VOIR TOUTES LES DATES

Connaître le cadre normatif et réglementaire
| Norme et méthodologie
| ISO/IEC 31000 et ISO/IEC 31010
| 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, des menaces, des mesures existantes, des vulnérabilités et 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 et 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
| Méthodologies OCTAVE
| OCTAVE Allegro Roadmap

Découvrir la méthode MEHARI
| 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
| Les 5 modules d'EBIOS
| Établissement du contexte
| Étude d'événements redoutés, des scénarios des menaces, des risques et des mesures de sécurité

Passage de l'examen de certification PECB Certified ISO/CEI 27005 Risk Manager (en ligne après la formation)
| Révision des concepts en vue de la certification et examen blanc
| Un voucher permettant le passage du test de certification est adressé à l'issue de la session

Certification

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

PECB Certified ISO/CEI 27005 Risk Manager
| Durée : 2h
| Langue : français
| Score minimum : 70% de bonnes réponses
| En cas d'échec : seconde tentative offerte dans les 12 mois

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.
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 et la norme ISO/IEC 27005
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

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 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.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la

classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

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.