

## ISO/IEC 27005 Risk Manager («HSR»)

Grâce à cette formation, maîtrisez les principes et les concepts fondamentaux de l'appréciation des risques et de la gestion optimale des risques liés à la sécurité de l'information conformes à la norme ISO/CEI 27005.

**Durée:** 3 jours

**Prix:** 3'550.– excl. 8.1% TVA

**Documents :** Divers manuels

### Contenu

1. <sup>er</sup> jour : Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005
  - Objectifs et structure de la formation
  - Concepts et définitions du risque
  - Cadres normatifs et réglementaires
  - Mise en œuvre d'un programme de gestion des risques
  - Compréhension de l'organisation et de son contexte
2. <sup>ème</sup> jour : Mise en œuvre d'un processus de gestion des risques conforme à la norme ISO/CEI 27005
  - Identification des risques
  - Analyse et évaluation des risques
  - Appréciation du risque avec une méthode quantitative
  - Traitement des risques
  - Acceptation des risques et gestion des risques résiduels
  - Communication et concertation relatives aux risques en sécurité de l'information
  - Surveillance et revue du risque
3. <sup>ème</sup> jour : Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification
  - Méthode OCTAVE
  - Méthode MEHARI
  - Méthode EBIOS
  - Méthodologie harmonisée d'EMR
  - Clôture de la formation

### Objectifs

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant 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
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information

- Cette formation est basée sur la théorie et les meilleures pratiques utilisées dans la gestion des risques liés à la sécurité de l'information
- Les sessions de cours sont illustrées par des exemples basés sur des études de cas
- Les exercices pratiques sont basés sur une étude de cas qui comprend des jeux de rôle et des discussions
- Les tests de pratique sont similaires à l'examen de certification

## Public cible

Responsables de la sécurité d'information. membres d'une équipe de sécurité de l'information. Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation ou mettant en œuvre ISO/CEI 27001, désirant se conformer à la norme ISO/CEI 27001 ou impliqué dans un programme de gestion des risques.

## Prérequis

Il est recommandé de posséder une expérience dans le domaine de la qualité, de l'audit et de la sécurité informatique.

- [ISO/IEC 27001:2022 Lead Auditor \(«HSI»\)](#)
- [CISA – Certified Information Systems Auditor \(«CAM»\)](#)

## Certification

L'examen « PECB Certified ISO/IEC 27005 Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. 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 œuvre 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/IEC 27005
- **Domaine 4** : Autres méthodes d'appréciation des risques de la sécurité de l'information

### Format de l'examen :

- L'examen se déroule à la fin du cours, soit durant le dernier après-midi de la formation.
- Durée : 2h
- Type de questions : questions à choix multiple
- Open book
- Remarques : si vous suivez cette formation à distance, vous passerez votre examen en ligne et en différé du cours selon les créneaux disponibles proposés par PECB au moment de votre enregistrement à la certification sur leur site internet. Quelques jours avant le début du cours, nous vous enverrons un e-mail vous indiquant les démarches à effectuer pour vous inscrire à l'examen. Aussi, nous vous informons que les candidats qui ont terminé la formation, mais qui ont échoué à l'examen peuvent le répéter une fois gratuitement dans les 12 mois à compter de la date de l'examen initial.

## Informations complémentaires

- Les frais de certification sont inclus dans le prix de l'examen

- Un manuel de cours contenant plus de 350 pages d'informations et d'exemples pratiques est fourni
- À l'issue de la formation, un certificat de participation de 21 crédits DPC (Développement professionnel continu) est délivré

## Formations complémentaires

- Certified Information Systems Security Professional (CISSP) («CSP»)
- RGPD/GDPR – Certified Data Protection Officer (DPO) («CDPO»)
- ISO/IEC 27001:2022 Lead Implementer («HSL»)

## Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou [romandie@digicomp.ch](mailto:romandie@digicomp.ch). Retrouvez toutes les informations détaillées concernant les dates sur [www.digicomp.ch/formations-securite/securite-de-linformation-protection-des-donnees-gouvernance/cours-isoiec-27005-risk-manager](http://www.digicomp.ch/formations-securite/securite-de-linformation-protection-des-donnees-gouvernance/cours-isoiec-27005-risk-manager)