

# Formation ISO/IEC 27035, Information Security Incident Management, Foundation + Certification

## Présentation

En partenariat avec PECB, cette formation vous permettra de comprendre les principes fondamentaux de la gestion des incidents de sécurité de l'information selon la norme ISO/IEC 27035.

Vous apprendrez à reconnaître, signaler, évaluer et répondre efficacement aux incidents de sécurité, et à structurer un processus de gestion des incidents au sein de votre organisation.

Cette formation prépare à l'examen PECB Certified ISO/IEC 27035 Foundation, qui valide votre compréhension des bonnes pratiques pour prévenir, détecter et traiter les incidents de sécurité de manière proactive.

Durée : 14,00 heures (2 jours)

Tarif INTRA : [Nous consulter](#)

## Objectifs de la formation

A l'issue de la formation, le stagiaire sera capable de mettre en œuvre un plan de gestion des incidents de sécurité de l'information

- Comprendre les principes fondamentaux de la gestion des incidents de sécurité de l'information.
- Connaître la relation entre la norme ISO/IEC 27035 et les autres normes et cadres réglementaires
- Comprendre l'approche basée sur les processus pour gérer les incidents de sécurité de l'information

## Prérequis

Cette formation ISO 27035 Foundation ne nécessite aucun prérequis particulier

## Public

Toute personne intéressée par l'approche processus de gestion des incidents de la sécurité de l'information

## Programme de la formation

### Jour 1. Fondamentaux et concepts clés



### **Introduction générale**

- Origine et objectifs de la norme ISO/IEC 27035
- Place dans le cadre ISO 27000 et lien avec ISO 27001 et ISO 27002
- Terminologie et définitions clés (incident, événement, vulnérabilité...)

### **Principes de la gestion des incidents**

- Pourquoi gérer les incidents ?
- Conséquences d'un incident mal géré
- Rôle de la gestion proactive et réactive

### **Cycle de vie de la gestion des incidents**

- Identification et enregistrement
- Classification et priorisation
- Analyse, investigation et réponse initiale

### **Rôles et responsabilités**

- Équipe de réponse aux incidents (IRT / CSIRT)
- RACI et coordination interne/externe
- Communication pendant un incident

## **Jour 2. Processus, mise en œuvre et examen**

### **Approches procédurales ISO/IEC 27035**

- Préparation et planification
- Détection et signalement
- Évaluation et prise de décision
- Réponse et récupération
- Clôture et retour d'expérience

### **Lien avec la continuité d'activité (ISO 22301)**

- Scénarios typiques : ransomware, fuite de données, compromission système
- Exercices de simulation

### **Exemples pratiques**

- Étude de cas : incident de phishing
- Analyse d'un incident réel et application de la méthode ISO/IEC 27035
- Rédaction d'un rapport d'incident

### **Examen de certification**

- Préparation à l'audit de certification
- Processus de certification et clôture de la formation

**Cette formation vous prépare à l'examen de certification de PECB (Certification incluse)**

- Durée : 1 heure
- Format : Examen en ligne

L'examen « Certified ISO/IEC 27035 Foundation » remplit les exigences relatives au programme d'examen et de certification de PECB. **L'examen couvre les domaines de compétences suivants :**

**Domaine 1 :** Concepts et principes fondamentaux de la gestion des incidents de sécurité de l'information

**Domaine 2 :** Gestion des incidents de la sécurité de l'information

Pour de plus amples informations concernant l'examen, veuillez consulter le lien vers :

[Règles et politiques relatives à l'examen | PECB](#)

Guide utilisateur: [PECB Exams User Manuals – PECB Help Center](#)

En cas d'échec, les candidats ont l'opportunité de présenter à nouveau l'examen dans un délai de 12 mois après leur première tentative.

## Organisation

### Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

### Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

## **Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

## **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.