

# ISO 27035: LEAD INCIDENT MANAGER

## Maîtriser la mise en œuvre et la gestion des processus de gestion des incidents de sécurité de l'information basés sur la norme ISO/IEC 27035

Code : ISO27035 LIM

Qu'ils soient délibérés ou accidentels, les incidents de sécurité de l'information sont presque inévitables à l'ère numérique et ont un impact sur les organismes de toutes tailles et de tous secteurs.

Apprendre à naviguer dans les complexités de la détection, de l'évaluation, de la réponse et du rapport des incidents de sécurité de l'information permet aux participants d'aider les organismes à assurer la sécurité de leurs informations et à réduire les conséquences négatives pour l'entreprise.

Cette formation s'aligne sur les normes ISO/IEC 27001, ISO/IEC 27005, et d'autres normes de la série ISO/IEC 27000 et fournit des conseils pratiques sur la sécurité de l'information

## PROGRAMME

**Méthodes mobilisées :** cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition de savoirs du programme (cf. Ressources).

**Modalités d'évaluation :** En amont de la formation, une évaluation des compétences de l'apprenant est effectuée.

Puis, les objectifs sont régulièrement évalués tout au long de la formation et formalisés par le passage de la certification le 5<sup>ème</sup> jour.

### JOUR 1

#### Introduction aux concepts liés à la gestion des incidents de sécurité de l'information et à la norme ISO/IEC 27035

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Concepts fondamentaux de la gestion des incidents
- Gestion des incidents de sécurité de l'information
- Établissement du contexte
- Politiques et procédures

### JOUR 2

#### Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

- Management du risque
- Plan de gestion des incidents
- Équipe de gestion des incidents
- Relations internes et externes
- Assistance technique et autre
- Sensibilisation et formation aux incidents de sécurité de l'information

### JOUR 3

#### Détection et signalement des incidents liés à la sécurité de l'information

- Tests
- Surveillance des systèmes et des réseaux
- Détecter et alerter
- Collecte d'informations sur les incidents
- Signalement des événements liés à la sécurité de l'information
- Appréciation des événements liés à la sécurité de l'information

### JOUR 4

#### Surveillance et amélioration continue du processus de gestion des incidents liés à la sécurité de l'information

- Résolution des incidents liés à la sécurité de l'information
- Confinement, éradication et récupération
- Enseignements tirés
- Surveillance, mesure, analyse et évaluation
- Amélioration continue
- Clôture de la formation

### JOUR 5

#### Préparation et passage de la certification.

### CERTIFICATION

#### Examen

- Les candidats passeront l'examen le vendredi
- Format : examen écrit
  - Durée : 3 heures
  - Langue : français
- L'examen remplit les exigences du programme de certification PECB (ECP - Examination and Certification Program)
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

Pour plus d'informations, vous pouvez consulter le site de PECB.

### RÉSULTATS

Disponibles sous 3 à 8 semaines et directement envoyés par e-mail au candidat.

## PROCHAINES DATES

2 mars 2026  
22 juin 2026  
21 septembre 2026  
7 décembre 2026



## OBJECTIFS

- Expliquer les principes fondamentaux de la gestion des incidents
- Élaborer et mettre en œuvre des plans de réponse aux incidents efficaces et adaptés aux besoins de l'organisme et sélectionner une équipe de réponse aux incidents
- Réaliser des appréciations approfondies des risques afin d'identifier les menaces et les vulnérabilités potentielles au sein d'un organisme
- Appliquer les bonnes pratiques issues de diverses normes internationales afin d'améliorer l'efficacité et l'efficience des efforts de réponse aux incidents
- Effectuer une analyse après l'incident et identifier les leçons tirées de l'expérience



## INFORMATIONS GÉNÉRALES

**Code :** ISO 27035 LIM

**Durée :** 5 jours

**Prix :** 3 790 € HT

**Horaires :** 9h30 - 17h30

**Lieu :** Levallois (92) ou en distanciel

**Examen :** inclus.

**Les + :** petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel



## PUBLIC VISÉ

- Responsables ou consultants souhaitant approfondir leurs connaissances en matière de gestion des incidents liés à la sécurité de l'information
- Professionnels cherchant à mettre en place et à gérer des équipes de réponse aux incidents efficaces
- Professionnels des TI et gestionnaires des risques liés à la sécurité de l'information souhaitant améliorer leurs connaissances en matière de gestion des incidents liés à la sécurité de l'information
- Membres des équipes de réponse aux incidents
- Coordinateurs de la réponse à l'incident ou autres rôles ayant des responsabilités dans le traitement et la réponse à l'incident



## PRÉ-REQUIS

Avoir une compréhension fondamentale de la norme ISO 27035 et des connaissances approfondies sur la sécurité de l'information sont nécessaires.



## RESSOURCES

- Support de cours en français contenant plus de 450 pages d'informations et d'exemples pratiques.
- Cours donnés en français