

ISO 27032 – Lead Cybersecurity Manager – Avec certification

5 jours (35 heures)

Perfectionnement

à partir de

3 600 € HT par personne (TVA en vigueur)

Contenu mis à jour le 30/09/2026. Document téléchargé le 02/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en oeuvre et gérer un programme de cybersécurité
- Expliquer la corrélation entre ISO/IEC 27032, le cadre de cybersécurité du NIST ainsi que d'autres normes et cadres pertinents
- Décrire le fonctionnement d'un programme de cybersécurité et ses composants
- Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de votre programme de cybersécurité.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Responsables et dirigeants impliqués dans la gestion de la cybersécurité, cadres et dirigeants jouant un rôle crucial dans les processus de prise de décision liés à la cybersécurité, professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité. Professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes et/ou toute personne chargée de la mise en oeuvre pratique des stratégies et des mesures de cybersécurité.

Prérequis

Avoir une compréhension fondamentale des concepts et de la gestion de la cybersécurité. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

L'apprenant s'engage à respecter les prérequis nécessaires ; une déclaration écrite et/ou un CV peut lui être demandé(s). Un QCM réussi de validation des prérequis peut également être nécessaire avant l'entrée en formation.

Programme

1 Pendant votre formation

ISO 27032 – Lead Cybersecurity Manager – Avec certification

Jour 1

Introduction à la cybersécurité et initiation aux programmes d'implémentation cyber

Jour 2

Rôles et responsabilités en matière de cybersécurité, gestion des risques et mécanismes d'attaques

Jour 3

Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité

Jour 4

Management des incidents de cybersécurité, surveillance et amélioration continue

Jour 5

Matin : Préparation à la certification

Après-midi : Passage de la certification

- Le prix et le passage de l'examen sont inclus dans la formation
- L'examen (en anglais) a lieu le dernier jour, à l'issue de la formation (sous réserve de place disponible lors d'un passage en distanciel) et s'effectue en ligne ou sur papier, pour une durée moyenne de 3h00
- En cas d'échec à l'examen, le candidat peut le repasser dans les 12 mois qui suivent sans frais supplémentaires

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap