Mis à jour le 22/08/2025

S'inscrire

Formation ISO/IEC 27035 - Information Security Incident Management - Foundation

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

Notre formation « ISO/IEC 27035 - Information Security Incident Management - Foundation » vous permettra de comprendre les fondamentaux de la gestion des incidents de sécurité et d'acquérir les compétences pratiques nécessaires pour appliquer la norme dans un contexte organisationnel. Dès le départ, vous découvrirez la structure et les objectifs de la norme, ainsi que son articulation avec d'autres référentiels clés (ISO/IEC 27001, 27002, 27005, RGPD, NIS2).

Grâce à une approche centrée sur les processus, vous apprendrez à définir les rôles et responsabilités, à mettre en place une chaîne d'escalade adaptée, à détecter et analyser efficacement les incidents, à orchestrer les actions de réponse, et à documenter un retour d'expérience.

Tout au long de la formation, des mises en situation progressives vous permettront de construire pas à pas un plan de gestion des incidents de sécurité complet, directement transposable dans votre organisation.

À l'issue de la formation, vous serez capable de mettre en œuvre un plan de gestion des incidents de sécurité de l'information, conformément à la dernière version de la norme ISO/IEC 27035, et préparé à l'examen de certification Foundation.

Objectifs

- 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.

Public visé

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

PRÉ-REQUIS

- Cette formation ISO 27035 Foundation ne nécessite aucun prérequis particulier.

Programme de notre formation certification ISO/IEC 27035 - Information Security Incident Management - Foundation

[Jour 1 - Matin]

Introduction et Compréhension de la norme ISO/IEC 27035

- Contexte et enjeux de la gestion des incidents de sécurité de l'information
- Structure et objectifs de la norme ISO/IEC 27035
- Les trois parties : principes, processus et lignes directrices
- Terminologie : événements, incidents, vulnérabilités, faiblesses

[Jour 1 - Après-midi]

Organisation et rôles dans la gestion des incidents

- Acteurs internes et externes (RSSI, DSI, CERT, CSIRT, prestataires)
- Responsabilités, processus d'escalade et coordination
- Sensibilisation et formation des collaborateurs
- Communication interne et externe lors d'un incident
- Atelier pratique : Définir une chaîne d'escalade adaptée à une PME.

Lien avec les autres normes et cadres réglementaires

- Articulation avec ISO/IEC 27001 et ISO/IEC 27002
- Apport d'ISO/IEC 27005 (gestion des risques) et ISO/IEC 22301 (continuité d'activité)
- Intégration avec RGPD et NIS2 (obligations de notification et responsabilités légales)
- Gouvernance sécurité et intégration dans un SMSI
- Atelier pratique : Relier un plan de gestion d'incidents aux exigences RGPD et NIS2.

[Jour 2 - Matin]

Cycle de vie d'un incident selon ISO/IEC 27035

- Détection et enregistrement des incidents
- Analyse et évaluation de l'incident
- Réponse, éradication et rétablissement
- Clôture et capitalisation (retour d'expérience, amélioration continue)
- Atelier pratique : Simulation d'un incident et journalisation des actions.

[Jour 2 - Après-midi]

Mise en œuvre d'un processus de gestion des incidents

- Élaboration de politiques et procédures
- Définition d'indicateurs (KPI/KRI) et suivi de performance
- Intégration avec les outils SOC, SIEM et ticketing
- Planification des exercices et tests réguliers
- Atelier pratique : Construire un mini-plan de gestion d'incidents pour une organisation fictive.

Préparation à l'examen

- Résumé des concepts clés à maîtriser pour l'examen
- Conseils pour l'approche des questions types
- Exercices et quiz de révision
- Plan de progrès pour implémenter ISO 27035 dans son organisation
- Atelier pratique : Passage d'un examen blanc et correction.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format

numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.