+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 17/07/2025

S'inscrire

Formation Certification ISO/IEC 27035 Foundation

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

Notre formation ISO/IEC 27035 Foundation vous permettra de comprendre l'ensemble du cycle de gestion d'un incident, de la préparation initiale jusqu'à l'analyse post-incident.

Vous apprendrez à définir une politique d'incidents, à constituer une équipe CSIRT, à réagir efficacement face à une cyberattaque et à mettre en place des procédures adaptées.

Vous serez ainsi capable de classer un incident, d'en mesurer l'impact, de déclencher les bonnes actions de réponse, et d'élaborer un retour d'expérience documenté. Vous serez également préparé à passer la certification Foundation, valorisant votre capacité à structurer une gestion des incidents conforme aux meilleures pratiques internationales.

À l'issue de cette formation, vous saurez bâtir un dispositif de gestion des incidents de sécurité robuste, auditable, et aligné avec les exigences ISO.

Comme toutes nos formations, celle-ci intègre la dernière version de la norme ISO/IEC 27035 et s'appuie sur des mises en situation concrètes.

Objectifs

- Comprendre les principes, objectifs et vocabulaire de la norme ISO/IEC 27035
- Appliquer les 5 étapes du cycle de vie d'un incident : préparation, détection, réponse, restauration, amélioration
- Élaborer une politique et un plan de gestion des incidents
- Réaliser un triage, évaluer la gravité d'un incident et coordonner les actions de réponse
- Structurer un rapport d'incident et mettre en œuvre un plan d'amélioration post-incident
- Se préparer à l'examen de certification ISO/IEC 27035 – Foundation

Public visé

- Analystes SOC
- RSSI / DSI
- Auditeurs SSI
- Membres CSIRT

PRÉ-REQUIS

- Aucune certification préalable n’est requise
- Une compréhension des enjeux de la sécurité de l’information est conseillée
- Une première expérience dans un rôle lié à la cybersécurité ou à la gestion des risques est un atout

Programme de notre formation certification ISO/IEC 27035 Foundation

Introduction à la norme ISO/IEC 27035

- Pourquoi structurer la gestion des incidents de sécurité
- Objectifs et portée de la norme ISO/IEC 27035
- Vue d’ensemble des trois parties de la norme (27035-1, -2, -3)
- Terminologie essentielle : événement, incident, alerte, CSIRT
- Rôle de 27035 dans un SMSI (et lien avec ISO 27001, 27002, 27005)

Gouvernance et préparation aux incidents

- Élaboration d’une politique de gestion des incidents
- Constitution d’une équipe de réponse (CSIRT, SOC, RSSI, métiers)
- Mise en place de procédures, outils et processus de détection
- Sensibilisation, communication interne et collaboration externe
- Atelier : Diagnostic de maturité et plan de montée en capacité ISO 27035 dans une entreprise fictive

Détection et évaluation des incidents

- Sources de détection : SIEM, logs, signalements, SOC
- Critères de qualification : gravité, impact, périmètre
- Triage et priorisation : urgent ou non ? Incident confirmé ou non ?
- Escalade, enregistrement et documentation initiale
- Atelier : Simulation de triage et d’évaluation d’un incident (ex. ransomware, phishing ou fuite de données)

Réponse et gestion technique de l’incident

- Confinement : isoler les systèmes, bloquer la propagation
- Éradication de la cause : patch, suppression, retrait des accès
- Restauration : reprise des services, tests, retour en production
- Communication de crise : interne, externe, autorités si nécessaire
- Coordination avec partenaires, prestataires, autorités

Rétablissement & amélioration continue

- Vérification du retour à un état normal sécurisé
- Analyse post-incident (retour d’expérience)
- Rapport d’incident : structure, contenu, indicateurs
- Mise à jour des politiques et plans de réponse
- Atelier : Élaboration d’un rapport d’incident et plan d’amélioration suite à une simulation

Préparation à la certification Foundation

- Résumé des concepts clés à maîtriser pour l’examen
- Conseils pour l’approche des questions types
- Exercices de révision et quiz de validation
- Plan de progrès pour implémenter ISO 27035 dans son organisation

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.