+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 Manager

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Notre formation ISO/IEC 27035 – Manager vous permettra de concevoir et piloter un dispositif complet de gestion des incidents à l'échelle de votre organisation. Vous apprendrez à élaborer une politique d'incident, structurer un CSIRT, gérer l'ensemble du cycle de vie d'un incident et conduire des analyses post-mortem conformes aux exigences ISO.

Vous saurez organiser la réponse opérationnelle à des incidents critiques, coordonner les parties prenantes internes et externes, superviser les indicateurs de performance, et garantir la conformité aux exigences ISO 27001, 27002, 27005, RGPD ou NIS2.

À l'issue de cette formation, vous serez en mesure de mettre en œuvre une gestion des incidents alignée sur les standards internationaux, résiliente et audit-ready.

Comme toutes nos formations, celle-ci est basée sur la dernière version de la norme ISO/IEC 27035 et intègre des ateliers pratiques pour une montée en compétence concrète.

Objectifs

- Comprendre l'architecture complète de la norme ISO/IEC 27035
- Structurer une politique de gestion des incidents et un plan opérationnel (PGI)
- Organiser une réponse efficace à tout type d'incident cyber (ex : ransomware, fuite de données)
- Mettre en place et piloter une équipe CSIRT adaptée à votre environnement
- Exploiter les indicateurs clés (KPI, logs, REX) et gérer la phase post-incident
- Se préparer à la certification ISO/IEC 27035 – Information Security Incident Management - Manager

Public visé

- Responsables sécurité / RSSI
- Analystes SOC
- Consultants SSI
- Membres CSIRT
- Responsable IT

PRÉ-REQUIS

- Bonne compréhension des enjeux de la cybersécurité
- Expérience dans un rôle lié à la sécurité opérationnelle, à la conformité ou au pilotage SSI
- La certification ISO/IEC 27035 Foundation est recommandée mais non obligatoire

Programme de notre formation certification ISO/IEC 27035 Manager

Principes fondamentaux de la gestion des incidents

- Définition : incident vs événement, alerte, faille
- Objectifs de la gestion des incidents selon ISO 27035
- Périmètre couvert par la norme
- Rôles, acteurs, et gouvernance associée
- Enjeux métiers et impact cyber

Architecture de la norme ISO/IEC 27035

- Vue globale des 3 parties : 27035-1, -2, -3
- Logique du cycle de vie des incidents
- Différences entre preparation / opération / retour d'expérience
- Alignement avec ISO 27001, 27002 et 27005
- Positionnement dans le système de management de la sécurité

Diagnostic initial & audit de maturité

- Pourquoi mesurer la maturité de son dispositif actuel
- Grille d'autoévaluation ISO 27035
- Analyse des écarts : organisation, procédures, outils
- Préparer un plan de montée en capacité
- Atelier : Cartographier le niveau de préparation incident d'un SI fictif

Élaborer une politique de gestion des incidents

- Structure et contenu de la politique ISO 27035
- Liens avec les politiques sécurité globales et RGPD
- Processus de validation et communication

- Gouvernance et sponsoring de la direction
- Revue et mise à jour régulière de la politique

Organisation opérationnelle et acteurs clés

- Composition d’un CSIRT interne : rôles et responsabilités
- Complémentarité avec SOC, DSI, métiers, conformité
- Compétences clés et ressources humaines nécessaires
- Modèle RACI et coordination inter-services
- Atelier : Définir la structure opérationnelle d’un CSIRT adapté à un contexte donné

Préparer les outils et procédures de détection

- Choix des outils de monitoring et détection (SIEM, EDR, IDS…)
- Écriture de procédures de signalement et d’escalade
- Sensibilisation du personnel et canaux de remontée
- Scénarios de détection préétablis
- Indicateurs de déclenchement

Triage, classification et priorisation des incidents

- Étapes de qualification d’un événement en incident
- Niveaux de criticité (basé sur impact, vraisemblance, urgence)
- Catégories d’incidents : malware, compromission, fuite…
- Registre des incidents : structure, éléments clés
- Atelier : Simuler un processus de triage et d’évaluation d’un incident multi-sources

Réponse : confinement, éradication, récupération

- Techniques de confinement selon le type d’incident
- Eradication : suppression de la cause, neutralisation du vecteur
- Restauration : sauvegardes, revalidation système, bascule
- Documentation continue de la réponse
- Rôle du CSIRT pendant les actions correctives

Communication de crise et coordination externe

- Plan de communication interne et externe
- Interface avec la direction, le juridique, la conformité
- Obligations de notification (ex : CNIL, clients, prestataires)
- Collaboration avec des CERT ou équipes partenaires
- Communication vers les utilisateurs finaux

Reprise d’activité et retour à la normale

- Vérification post-restauration : intégrité, disponibilité
- Autorisation de remise en production
- Mise à jour des contrôles de sécurité
- Suivi court terme post-incident
- Documentation de la clôture d’incident

Retour d’expérience et capitalisation

- Méthodologie d’analyse post-mortem
- Outils d’analyse causale
- Rapport d’incident complet
- Plans d’action correctifs
- Atelier : Élaborer un rapport complet d’incident + plan d’amélioration

Indicateurs de performance et supervision

- Choisir des KPI/KRI pertinents (MTTD, MTTR, taux de détection…)
- Tableaux de bord pour le pilotage du PGI
- Réunion de revue périodique des incidents
- Outils de supervision (Grafana, Kibana, etc.)
- Alignement avec les objectifs de sécurité globaux

Maintien en condition opérationnelle

- Révision régulière du plan de gestion des incidents (PGI)
- Exercices de simulation / tests de réponse
- Formation continue des intervenants
- Mise à jour des scenarii de détection / traitement
- Atelier : Exercice de simulation d’incident avec activation d’un CSIRT fictif

Auditabilité et conformité

- Exigences ISO 27001 / 27035 en termes de preuves
- Tenue d’un registre des incidents et preuves de réponse
- Alignement RGPD et exigences réglementaires sectorielles
- Préparation à un audit (interne, externe)
- Documentation attendue lors d’un audit ISO

Préparation à la certification Manager

- Récapitulatif des points clés du programme
- Conseils méthodologiques pour l’examen (format, questions, pièges)
- Exemples de questions types (QCM)
- Quiz de validation et correction collective
- Orientation post-certification (Lead Implementer, Risk Manager, etc.)

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.