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

Mis à jour le 22/08/2025

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 – Information Security Incident Management Incident Manager » vous apporte les compétences indispensables pour bâtir et piloter un dispositif complet de gestion des incidents de sécurité. Centrée sur la norme ISO/IEC 27035, elle vous permettra de maîtriser les principes, techniques et méthodologies clés du cycle de vie des incidents, depuis la préparation et la détection jusqu'au retour d'expérience et à l'amélioration continue. Vous apprendrez à définir une politique d'incidents, à structurer et animer un CSIRT performant, et à conduire des analyses post-mortem pour renforcer durablement la résilience de votre organisation.

La formation mettra en lumière la relation étroite entre ISO/IEC 27035 et les autres normes et cadres réglementaires tels qu'ISO/IEC 27001, 27002, 27005, 22301, le RGPD et la directive NIS2. Cette approche intégrée vous permettra de comprendre comment inscrire la gestion des incidents dans un SMSI global, tout en garantissant la conformité aux exigences légales et sectorielles.

Un accent particulier sera porté sur les dimensions organisationnelles et managériales : gestion et pilotage d'une équipe de réponse aux incidents, répartition des rôles et responsabilités, coordination avec le SOC, la DSI et les métiers, ainsi que communication en situation de crise. À travers des ateliers pratiques et des mises en situation réalistes, vous développerez les compétences nécessaires pour organiser efficacement la réponse à des incidents critiques et superviser la performance opérationnelle à l'aide d'indicateurs pertinents.

À l'issue de cette formation, vous serez en mesure de mettre en œuvre un processus de gestion des incidents conforme aux standards internationaux, capable de résister aux crises, de s'améliorer en continu et d'être audité avec succès. Vous serez ainsi prêt à accompagner votre organisation dans la mise en place et le pilotage d'un plan de gestion des incidents de sécurité de l'information aligné sur la norme ISO/IEC 27035.

Comme toutes nos formations, celle-ci est fondée sur la dernière version de la norme et

s’appuie sur des exercices pratiques, des études de cas et des simulations, afin de garantir une montée en compétence concrète et immédiatement opérationnelle. Elle inclut également une préparation complète à l’examen de certification, avec révision des points clés, mise en condition via un examen blanc et corrections, afin de consolider les acquis et maximiser vos chances de réussite.

Objectifs

- Connaître l'ensemble des principes, techniques et méthodologie de la gestion des incidents de la sécurité de l'information
- Connaître la relation entre la norme ISO/IEC 27035 et les autres normes et cadres réglementaires
- Gérer une équipe adéquate pour le suivi et la gestion des incidents
- Mettre en place et piloter un processus de gestion des incidents
- Analyser les incidents et améliorer les processus

Public visé

- Responsables sécurité / RSSI / Consultants ou auditeurs en cybersécurité
- Chefs de projet SSI ou gestion de crise
- Toute personne impliquée dans la gestion des incidents de sécurité informatique

Pré-requis

- Avoir une bonne connaissance des processus de gestion des incidents, des principes de sécurité de l'information et de la famille des normes ISO/IEC 27000

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

[Jour 1 - Matin]

Principes fondamentaux de la gestion des incidents

- Pourquoi chaque incident est une opportunité d’apprentissage ?
- Définition : incident vs événement, alerte, faille
- Objectifs et enjeux de la gestion des incidents selon ISO/IEC 27035
- Périmètre couvert par la norme
- Rôles, acteurs et gouvernance associée
- Impacts métiers et risques cyber

[Jour 1 - Après-midi]

Architecture et compréhension de la norme ISO/IEC 27035

- Vue globale des 3 parties : 27035-1, -2, -3
- Logique du cycle de vie des incidents
- Préparation vs opérations vs retour d’expérience
- Positionnement dans un SMSI global
- Atelier pratique : Cartographier les étapes d’un cycle de gestion d’incidents.

Diagnostic initial & audit de maturité

- Pourquoi mesurer la maturité du dispositif actuel
- Grille d’autoévaluation ISO/IEC 27035
- Analyse des écarts : organisation, procédures, outils
- Préparer un plan de montée en capacité

[Jour 2 - Matin]

Lien avec les autres normes et cadres réglementaires

- Articulation avec ISO/IEC 27001, 27002, 27005 et 22301
- Alignement RGPD et NIS2 : obligations de notification, responsabilités
- Exigences sectorielles (santé, finance, OSE/SE)
- Référentiels complémentaires (NIST, ENISA/ANSSI)
- Atelier pratique : Relier un plan d’incidents aux exigences RGPD/NIS2.

[Jour 2 - Après-midi]

Élaborer une politique de gestion des incidents

- Structure et contenu d’une politique ISO/IEC 27035
- Liens avec les politiques sécurité globales et la conformité RGPD
- Processus de validation, communication et mise à jour
- Gouvernance et sponsoring de la direction

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 pratique : Définir la structure opérationnelle d’un CSIRT.

[Jour 3 - Matin]

Management et gestion d’équipe de réponse aux incidents

- Leadership et pilotage d’une équipe CSIRT
- Gestion du stress, de la charge et des priorités en crise
- Communication managériale interne/externe
- Développement des compétences et gestion des conflits

[Jour 3 - Après-midi]

Triage, classification et priorisation des incidents

- Étapes de qualification d’un événement en incident
- Niveaux de criticité (impact, vraisemblance, urgence)
- Catégories d’incidents : malware, compromission, fuite de données…
- Registre des incidents : structure et éléments clés
- Introduction au référentiel MITRE ATT&CK pour la classification et l’analyse des modes opératoires
- Apport des Threat Intelligence Feeds pour enrichir la qualification et le suivi des incidents
- Atelier pratique : Simuler un triage multi-sources.

Réponse : confinement, éradication, récupération

- Techniques de confinement selon le type d’incident
- Éradication : suppression de la cause, neutralisation du vecteur
- Restauration : sauvegardes, revalidation, bascule
- Documentation continue et rôle du CSIRT
- Atelier pratique : Reconstituer un plan de réponse complet.

[Jour 4 - Matin]

Communication de crise et coordination externe

- Plan de communication interne et externe
- Interface avec la direction, le juridique, la conformité
- Obligations de notification (CNIL, clients, autorités…)
- Collaboration avec CERT/ANSSI et partenaires
- Atelier pratique : Élaborer un plan de communication de crise.

[Jour 4 - Après-midi]

Reprise d’activité et retour à la normale

- Vérifications 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
- Rapport d’incident complet et analyse causale
- Plans d’action correctifs et suivi
- Capitalisation et amélioration continue
- Atelier pratique : Produire un rapport d’incident + plan d’amélioration.

[Jour 5 - Matin]

Pilotage, supervision et maintien en condition opérationnelle

- Choisir des KPI/KRI (MTTD, MTTR, taux de détection…)
- Tableaux de bord pour le pilotage du PGI et revues périodiques
- S'appuyer sur outils de supervision (Grafana, Kibana, etc.)
- Panorama des solutions modernes : SIEM, SOAR, XDR, Threat Intelligence, IA/ML appliqués à la détection et à la corrélation d’événements
- Exercices de simulation, tests réguliers, formation continue
- Mise à jour des scénarios de détection/traitement

[Jour 5 - Après-midi]

Auditabilité et conformité

- Exigences ISO/IEC 27001 & 27035 en matière de preuves
- Registre des incidents et traçabilité des réponses
- Alignement RGPD/NIS2 et exigences sectorielles
- Préparation à un audit (interne, externe)
- Documentation attendue lors d’un audit ISO

Préparation à l’examen

- Récapitulatif des points clés du programme
- Conseils méthodologiques (format, questions, pièges)
- Exemples de sujets d’épreuve et corrections guidées
- Orientation post-certification
- 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.