+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 27005 -Risk Manager

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

3 jours (21 heures)

Présentation

Notre formation « ISO/IEC 27005 - Risk Manager » offre aux participants une compréhension claire des concepts essentiels de la gestion des risques en sécurité de l'information, tels que définis par la norme ISO/IEC 27005.

Elle permet d'apprendre à interpréter les exigences de l'ISO/IEC 27001 et à intégrer efficacement la gestion des risques au sein d'un Système de Management de la Sécurité de l'Information (SMSI).

À travers des cas pratiques et ateliers, les stagiaires développent les compétences nécessaires pour identifier, évaluer et traiter les risques, en construisant des scénarios pertinents et en élaborant des plans de traitement adaptés.

Un accent particulier est mis sur la mise en œuvre opérationnelle : définition des mesures de sécurité, élaboration du plan de traitement des risques (PTRA) et reporting aux instances de décision.

En fin de parcours, les participants sont capables de piloter une démarche de gestion des risques conforme aux normes internationales et de valoriser leurs acquis grâce à la préparation à la certification ISO/IEC 27005 Risk Manager.

Objectifs

- Comprendre les concepts clés de la gestion des risques comme définis par la norme ISO/IEC 27005

- Interpréter les exigences de la gestion des risques au sein d'une SMSI conforme à la norme ISO/IEC 27001
- Identifier, évaluer et traiter les risques liés à la sécurité de l'information

Public visé

- RSSI
- Chefs de projet
- Consultants
- Toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation

Pré-requis

- Avoir une connaissance de base sur la gestion du risque et sur la sécurité des systèmes d'information

Programme de Notre Formation ISO/IEC 27005 - Risk Manager

[Jour 1 - Matin]

Introduction à la gestion des risques en sécurité de l’information

- Définition du risque et enjeux C/I/D (confidentialité, intégrité, disponibilité)
- Panorama des menaces (cyberattaques, malwares, erreurs humaines…) et vulnérabilités courantes
- Présentation de la norme ISO/IEC 27005 et des autres standards clés en gestion du risque
- Présentation des normes et standards clés en gestion du risque
- Rôle du Risk Manager dans le SMSI pour identifier et traiter les risques
- Atelier pratique : Identification de risques connus dans l’entreprise.

[Jour 1 - Après-midi]

Concepts fondamentaux et référentiels en gestion du risque

- Terminologie : actif, menace, vulnérabilité, impact, probabilité
- Importance de la gestion des risques dans un SMSI et lien avec la conformité
- Référentiels et méthodes : ISO/IEC 27005, EBIOS, MEHARI, NIST RMF – articulation
- Comparaison critique des approches (forces/faiblesses) pour positionner ISO/IEC 27005 comme pivot dans le SMSI
- Gouvernance du risque : processus global et intégration à la stratégie d’entreprise
- Atelier pratique : Quiz/validation des définitions & normes associées.

Processus ISO/IEC 27005 (1ère partie) – Contextualisation & identification des risques

- Établissement du contexte : périmètre, actifs critiques, enjeux métiers, critères d'acceptation
- Identification et valorisation des actifs informationnels (données, infrastructures, applications)
- Identification des menaces et vulnérabilités par actif
- Scénarios de risque : combinaison actifs/menaces/vulnérabilités et premières estimations d'impacts
- Lien direct avec les exigences ISO/IEC 27001 (ex. §6.1.2 sur l'identification et le traitement des risques de sécurité de l'information)
- Atelier pratique : Définir le périmètre et réaliser la cartographie initiale des risques.

[Jour 2 - Matin]

Processus ISO/IEC 27005 (2e partie) – Analyse & évaluation des risques

- Analyse : estimation vraisemblance & impact pour chaque scénario
- Méthodes d'estimation : approches quantitatives vs qualitatives
- Évaluation/priorisation : matrice probabilité/impact et identification des risques inacceptables
- Appétence et tolérance au risque : décisions d'acceptabilité
- Mise en perspective avec le rôle du leadership (ISO 27001 §5.1) dans la validation de l'appétence au risque
- Atelier pratique : Estimer impacts & probabilités et positionner sur la matrice.

[Jour 2 - Après-midi]

Intégration de la gestion des risques dans l'ISO/IEC 27001

- Lien ISO/IEC 27005 ? ISO/IEC 27001 : la gestion des risques comme socle du SMSI
- Sélection/justification des mesures via l'Annexe A (ISO 27001:2022)
- Élaboration du plan de traitement des risques (PTRA) : priorisation, responsables, ressources
- Suivi du risque résiduel et validation par la direction
- Communication & reporting (rapports, tableaux de bord) aux parties prenantes
- Amélioration continue dans le cycle PDCA
- Traduction opérationnelle des mesures dans des politiques et procédures SSI adaptées (ex : gestion des accès, sauvegarde, classification des données)
- Retour d'expérience collectif et mise en commun des bonnes pratiques identifiées
- Atelier pratique : Construire un extrait de PTRA ISO 27001 + reporting au COMEX.

[Jour 3 - Matin]

Cas pratique global de gestion des risques

- Application de bout en bout du processus ISO/IEC 27005 sur un scénario complexe

- Cartographie des risques, estimation, analyse et plan de traitement
- Présentation & justification des arbitrages devant un jury fictif
- Atelier pratique : Soutenance en équipe de la cartographie & du plan de traitement.

[Jour 3 - Après-midi]

Bonnes pratiques, facteurs de succès & retours d’expérience

- Implication de la direction, périmètre clair, registre des risques à jour
- Erreurs courantes & pièges à éviter
- Gouvernance : rôles du comité des risques, propriétaire de risque, correspondants SSI
- Outils GRC, ressources ANSSI, bases de connaissances et logiciels spécialisés
- Module complémentaire : veille réglementaire et conformité (RGPD, NIS2, DORA) pour contextualiser la gestion des risques dans l’environnement légal et sectoriel
- Atelier pratique : Partage d’expériences & benchmark animé par le formateur.

Préparation à la certification ISO/IEC 27005 Risk Manager

- Format de l’examen : QCM, durée, score de réussite, langue
- Conseils de réussite : gestion du temps, techniques de lecture
- Révision des points clés (normes, processus, calculs de risque, etc.)
- Session Q/R & astuces de mémorisation
- 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.