

# ISO27001 - ISO27005 Fondamentaux de la gestion des risques pesant sur le Système d'Information

2 jours - 14 heures

Code formation : ADHDEV0259



## Objectifs

Découvrir les normes ISO 27001/27002 et ISO 27005. Comprendre les enjeux de sécurité et intervenir concrètement sur des problématiques liées au management de la sécurité de l'information et de la gestion et l'analyse des risques sur le système d'information dans l'entreprise. Découvrir les bonnes pratiques de management de la sécurité de l'information et son articulation avec la gestion des risques.

## Participants

Toute personne devant réaliser une appréciation portant en particulier sur les risques en termes de sécurité informatique. Cette formation peut s'inscrire dans le cadre d'un processus d'implémentation de la norme ISO 2700. Cette formation convient aux RSSI et aux consultants en SSI.

## Prérequis

Une connaissance des fondamentaux de l'informatique est nécessaire afin de suivre cette formation.

## Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

## Remarques

Cette formation à la maîtrise et à la gestion des risques s'inscrit parfaitement dans le cadre d'un processus d'implémentation d'un système de management de la sécurité de l'information dans le respect de la norme ISO 27001, en s'appuyant sur une analyse de risques selon la norme ISO 27005 et en mettant en œuvre les normes ISO 27002 et 27004.

## Certification

## Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

## Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

## Méthodes d'évaluation des acquis

Un contact téléphonique est systématiquement établi avec le stagiaire ou la personne chargée de son inscription afin de définir le positionnement. Si besoin, un questionnaire est adressé pour valider les prérequis en correspondance et obtenir toute précision nécessaire permettant l'adaptation de l'action. Durant la formation, des exercices individuels et collectifs sont proposés pour évaluer et valider les acquis du stagiaire. La feuille d'émargement signée par demi-journée ainsi que l'évaluation des acquis sont adressées avec la facture.

## Programme

# ISO27001 - ISO27005 Fondamentaux de la gestion des risques pesant sur le Système d'Information



2 jours - 14 heures

Code formation : ADHDEV0259

## Principes fondamentaux de la sécurité des systèmes d'information

La réglementation s'imposant au traitement de l'information  
Les autorités de tutelle

## Les normes «technologies de l'information-techniques de sécurité»

L'articulation de ces normes

## Cadre normatif et réglementaire de la norme ISO 27001

Le Système de Management de la Sécurité de l'Information (SMSI), but du SMSI, pourquoi un SMSI?  
Les grandes étapes dans la mise en place d'un SMSI au sein d'une entreprise/organisme  
établissement et management d'un SMSI  
responsabilité de la direction  
audits internes du SMSI  
revue de direction du SMSI  
amélioration du SMSI  
Découpage des étapes de mise en place et d'exploitation du SMSI  
Phase PLANIFIER (Plan)  
Phase DEPLOYER (Do)  
Phase CONTROLER (Check)  
Phase AGIR (Act)

## L'articulation SMSI et ISO 27005

Cadre normatif et réglementaire de la norme ISO 27005  
Les grandes lignes de la norme ISO 27005  
Etablissement du contexte  
Appréciation des risques en sécurité de l'information de traitement des risques en sécurité de l'information  
Acceptation des risques en sécurité de l'information  
Communication et concertation relatives aux risques en sécurité de l'information  
Surveillance et revue du risque en sécurité de l'information l'articulation de la norme ISO 27005 avec la norme ISO 27001

## L'étude de sécurité

La modélisation d'une étude de sécurité

## Les bonnes pratiques, les outils mettant en œuvre la norme ISO 27005

Présentation de la méthode EBIOS 2010  
La documentation issue de l'étude de sécurité EBIOS