

Maîtriser l'analyse des risques du système d'information

Mise en œuvre de la norme ISO27005

Référence	Niveau	Durée
AT-PI-203	2	2 jours

Avis de l'expert

L'évolution de la réglementation et de la gouvernance des entreprises met aujourd'hui en avant la notion de maîtrise des risques. L'exigence ambitieuse qui nous est donnée est désormais à la fois d'assurer la robustesse de l'entreprise face à l'imprévu, mais aussi d'optimiser l'efficacité économique de son dispositif de maîtrise des risques.

Cette formation approfondit les outils de la gestion des risques liés aux informations, et donne au RSSI ou au risk-manager les clés pour connaître ses risques, élaborer un plan d'action orienté vers les métiers de l'entreprise et piloter sa mise en œuvre.

Bénéfices métier

- Maîtriser les concepts fondamentaux du management des risques
- Connaître les principales normes internationales
- Savoir utiliser une des principales méthodes du marché
- Avoir les clés pour dialoguer efficacement avec les métiers et la direction générale
- Acquérir les réflexes de l'analyse économique du management des risques

Parcours pédagogique

Rappel sur les principes généraux relatif aux systèmes de management de la sécurité

- Présentation générale du modèle PDCA
- Introduction aux normes ISO27000
- Principe de maturité et mise en place progressive des processus

Les concepts généraux de la gestion des risques

- Présentation du Guide 73:2009
- Définition du risque et des typologies de menaces
- Modèle général de gestion des risques

Présentation de la norme ISO 27005

- Objectifs de la norme
- Présentation du contenu de la norme
- Démarche générale de l'analyse des risques
- Démarche d'appréciation et d'analyse des risques
- Présentation des référentiels d'analyse des menaces, des enjeux et des contraintes proposés par la norme
- Présentation des référentiels de vulnérabilité proposés par la norme
- Présentation des métriques d'appréciations des risques proposées par la norme
- La stratégie de traitement des risques et d'acceptation des risques selon la norme
- Les processus de communication et de surveillance des risques

Panorama des principales méthodes d'analyse des risques Françaises

- Présentation de l'historique des normes et méthodes d'analyse des risques
- Présentation de la méthode MEHARI © 2010 du Clusif
- Présentation de la méthode EBIOS © 2010 de l'ANSSI

La définition et la mise en œuvre du Plan de Prévention des Risques (PPR)

- Notions principales et objectifs du PPR
- Le processus d'élaboration du PPR
- La définition des objectifs et des priorités de mise en œuvre.
- Les indicateurs financiers et budgétaires du PPR

Les conseils de mise en œuvre d'une gestion structurée des risques

- La mise en œuvre du système de management de gestion des risques.
- La gouvernance à prévoir, les acteurs, leur rôle et responsabilité.
- Le maintien en condition opérationnelle

Etude de cas

Conclusion

Comment se déroule le stage ?

Les échanges entre participants et l'expérience du formateur facilitent les retours d'expérience. La formation alterne entre présentation de fondamentaux théoriques et études de cas. Tous les outils et démarches proposées ont été utilisés dans des cas réels d'entreprise.

Public concerné

Directeur de systèmes d'information
Responsables sécurité des systèmes d'information
Responsable des risques opérationnels
Risk-manager
Auditeur ou professionnel du contrôle interne