

Programme de formation Maîtriser le risque Système d'Information

● Objectifs

Le risque lié au système d'information est un risque opérationnel majeur car dans la plupart des cas il génère un effet systémique ou effet domino qui met en cause le déroulement des processus de l'entreprise. L'analyse de ce risque est le préalable à l'élaboration des PCA et des PRA (obligations réglementaires.) Cette formation Maîtriser le risque Système d'Information vous permettra de : - Appréhender de façon opérationnelle la mission du Risk Manager quel que soit son niveau de responsabilité de manière à développer ses capacités d'intégration dans la « chaîne » de gestion du risque SI. - Inculquer au Risk Manager des concepts et des méthodes référentes en matière de gestion des risques SI (Cobit, ITIL, EBIOS, MEHARI) - Réussir la mise en place d'une cartographie des risques SI

● Pré requis

Aucun

● Durée

2 jours

● Public

DSI, Risk managers,
Auditeurs

● Plan de formation

Gouvernance d'entreprise et gouvernance du SI

Les principes de la gouvernance d'entreprise appliqués aux banques

La gouvernance d'entreprise :

Une définition, le périmètre, les principes

Le management des risques

Les référentiels (AMF, COSO2)

La gouvernance des systèmes d'information

La place des SI dans la gouvernance des organisations

Le SI : un sous système à dimension stratégique

La gouvernance du SI : Principes, Comment démarrer

Exigences d'un cadre de référence : Le Cobit

Le référentiel Cobit : Cadre, objectifs et métriques ; domaines, processus

Étude de processus : PO9 : Évaluer les risques

Le Risk Management

Les principes élémentaires

La démarche de maîtrise des risques :

Identification et évaluation des risques

inhérents

Identification et évaluation du dispositif de contrôle interne

Évaluation des risques résiduels

Le traitement des risques

La gestion des risques SI

Qualification des risques

Les menaces

La cartographie des risques

Objectifs de la cartographie des risques

Approche par processus (construction d'un référentiel).

Identification des événements de risques.

Évaluation et niveau d'exposition : évaluation qualitative, quantitative ou à dire d'experts.

Représentation des cartographies des risques : matrices de références, représentations graphiques et focus destinés au pilotage des risques.

Les méthodes EBIOS (ANSSI) et MEHARI (CLUSIF)



La démarche
Les apports de chaque étape
Les résultats de la méthode intégrés dans une perspective de certification ISO27001.
Étude de cas associée à la présentation

Implication des utilisateurs dans la sécurité du si

La PSSI, La charte utilisateur
Les bonnes pratiques -
Formation/sensibilisation des acteurs.