COMPTABILITE, GESTION, FINANCE

FICHE PROGRAMMATION

AFGES - LES FONDAMENTAUX DES RISQUES DES SYSTEMES D'INFORMATIONS

Public

Auditeur(trice) interne,Directeur(trice) et responsable d'équipe,Toute personne chargée d'un audit ou de piloter un projet d'amélioration des performances (RH - stock - rentabilité etc)

Prérequis

Aucun prérequis nécessaire pour suivre cette formation

Objectifs pédagogiques

Acquérir une culture informatique au travers du concept de système d'information et de ses différentes composantes.

Comprendre les spécificités du système d'information (SI) bancaire.

Identifier, investiguer et évaluer les risques propres au système d'information.

Acquérir la capacité opérationnelle d'intégrer ces risques dans la réalisation des contrôles.

Contenu

1- RISQUES SPÉCIFIQUES A LA SÉCURITÉ DE L'INFORMATION ET LES DISPOSITIFS ASSOCIES

Les tâches à réaliser pour identifier les risques IT.

Capacité, tolérance et appétit du risque.

Culture du risque et communication.

Les éléments du risques (facteurs, actifs, menaces, vulnérabilités…).

Concepts et principes de la sécurité de l'information :

- Confidentialité, Intégrité et disponibilité.

Méthodes d'identification du risque :

- Exemple d'EBIOS.

Les scénarios du risque :

- Acteur, Type de menace, Evénement, Actif/Ressource, Eléments temporels.

- Approche bottom up et top down.

Les techniques d'évaluation du risque :

- Bow tie analysis, Business Impact Analysis, Analyse.

Analyse des scenarios de risque (organisation, politique, procédure).

- Points importants à considérer pour la 3ème ligne de défense (Audit).

Changement dans l'environnement des risques IT.

Méthodologie d'analyse de risque :

- Analyse quantitative.

- Analyse qualitative.

- Analyse semi-quantitative.

Documenter le risque IT dans un registre.

La politique générale de la sécurité informatique.

Alignement des risques aux objectifs opérationnels.

Les options de réponse aux risques IT (Accepter, Traiter, Transférer, Eviter).

Les techniques d'analyse.

La conception des contrôles IT et son implémentation :

- Démarche et périmètre du contrôle SI de l'entreprise.

- Typologie des points de contrôles : contrôles métiers, contrôles généraux informatiques, contrôles applicatifs.

- Le modèle COSO pour les contrôles informatiques.

Les typologies de risques (inhérent, résiduel, actuels) :

- Exemples de contrôles préventifs, défectifs et correctifs.

Les objectifs de contrôles (Processus, Sécurité IT, management des données, projets, cycle de vie des applications, opérations…).

L'impact des nouvelles technologies:

- Les contrôles et bons réflexes – 1ère ligne de défense (exemple : salarié, responsable opérationnel).

- Les contrôles et bons réflexes – 2ère ligne de défense (exemple : RSSI, Manager).

- Locations financières (normes françaises et IFRS 16).

- Autres.

Le plan de continuité d'activité.

Key Risk Indicator (KRI) – indicateurs clés des risques.

Key Performance Indicator (KPI) – indicateurs clés de performance.

Extraction et collecte des données pour la maitrise des risques IT.

Typologie d'évaluation des contrôles (audit, test de vulnérabilités, test d'intrusion, maitrise des sous-traitants et partenaires).

Analyse des résultats de contrôles.

2- SYNTHÈSE ET CONCLUSION