FICHE TECHNIQUE DE FORMATION
Gouvernance en Matière de Cybersécurité

Objectifs de la Formation:

Comprendre les principes de gouvernance en cybersécurité.

Développer des compétences pour élaborer et mettre en œuvre des stratégies de gouvernance.

Maîtriser les techniques pour aligner la cybersécurité avec les objectifs stratégiques de l'entreprise.

Public Cible:

Responsables de la sécurité, DSI, consultants en gouvernance, toute personne impliquée dans la gouvernance de la cybersécurité.

Prérequis:

Connaissances de base en gestion des systèmes d'information et en cybersécurité.

Méthodologie Pédagogique:

Exposés théoriques, études de cas, ateliers interactifs, simulations.

Programme de la Formation:

1. Introduction à la Gouvernance en Cybersécurité

Concepts de Base : Comprendre les principes de la gouvernance en cybersécurité.

Rôles et Responsabilités : Définition des rôles et responsabilités en matière de gouvernance.

2. Stratégie de Cybersécurité

Élaboration de la Stratégie : Techniques pour élaborer une stratégie de cybersécurité alignée avec les objectifs de l'entreprise.

Cadres de Référence : Présentation des cadres de référence pour la gouvernance en cybersécurité (NIST, ISO).

3. Politiques et Procédures de Sécurité

Développement des Politiques : Techniques pour développer des politiques de sécurité efficaces.

Mise en Œuvre des Procédures : Stratégies pour mettre en œuvre et maintenir les procédures de sécurité.

4. Gestion des Risques de Cybersécurité

Identification et Évaluation des Risques : Techniques pour identifier et évaluer les risques de cybersécurité.

Plans de Gestion des Risques : Élaboration de plans pour gérer les risques identifiés.

5. Conformité et Régulations

Exigences Réglementaires : Exploration des exigences réglementaires en cybersécurité.

Gestion de la Conformité : Techniques pour assurer la conformité avec les régulations.

6. Surveillance et Reporting

Surveillance de la Cybersécurité : Techniques pour surveiller les activités de cybersécurité.

Reporting de la Sécurité : Stratégies pour rapporter les activités et incidents de cybersécurité.

7. Formation et Sensibilisation

Programmes de Formation : Développement de programmes de formation en cybersécurité.

Campagnes de Sensibilisation : Techniques pour sensibiliser le personnel aux enjeux de la cybersécurité.

8. Applications Pratiques

Ateliers de Développement de Stratégie : Exercices pratiques pour élaborer des stratégies de cybersécurité.

Simulations de Gouvernance : Jeux de rôle pour pratiquer la gouvernance en cybersécurité.

9. Outils de Gouvernance en Cybersécurité

Outils de Gestion des Risques : Introduction aux outils de gestion des risques et de la conformité.

Automatisation de la Gouvernance : Techniques pour automatiser les processus de gouvernance.

10. Évaluation Finale