

Fiche Technique: Audit Cybersécurité au Cameroun

Objectifs de la formation

- Évaluer la posture de sécurité informatique de l'organisation.
- Identifier les failles dans réseau, systèmes et gestion des accès.
- Vérifier conformité aux normes locales et internationales.
- Sensibiliser le personnel aux bonnes pratiques de sécurité.
- Définir un plan d'action pragmatique pour corriger les vulnérabilités.
- Accompagner la maîtrise des risques et l'amélioration continue.

Population cible

- Entreprises, organisations publiques et privées au Cameroun.
- Institutions financières, industrielles et secteurs critiques (énergie, télécom, logistique).
- Directions générales et systèmes d'information.
- Responsables sécurité informatique, QHSE, chefs d'exploitation.
- PME et grandes entreprises souhaitant sécuriser leurs actifs numériques.

Durée de la formation

Type d'audit	Durée estimée	Format
Audit complet	4 à 6 semaines	Sur site & à distance
Audit ciblé (réseaux, applications)	2 à 3 semaines	Sur site ou distant
Audit de conformité	3 à 4 semaines	Mixte

Programme de la formation

Étape 1 : Diagnostic initial

- Collecte du contexte opérationnel et stratégie de sécurité.
- Définition du périmètre et des objectifs spécifiques.

Étape 2 : Analyse documentaire et réglementaire

- Examen de la politique de sécurité, procédures et rapports d'incidents.
- Vérification de conformité aux normes ISO 27001, LPM, RGPD, etc.

Étape 3 : Recommandations et plan d'action

- Élaboration d'un rapport détaillé avec priorisation des recommandations.
- Définition d'un plan opérationnel pour réduire les risques majeurs.

Étape 4 : Suivi et accompagnement

- Accompagnement personnalisé pour la mise en œuvre des recommandations.
- Contrôles réguliers et reporting pour améliorer la posture globale.

L'audit est adapté aux spécificités et contraintes des entreprises au Cameroun, combinant expertise locale et normes internationales.