Fiche Technique:Audit Cybersécurité au Niger

Objectifs de la formation

- Détecter vulnérabilités techniques, organisationnelles et humaines.
- Vérifier conformité aux normes ISO 27001 et réglementations nigériennes.
- Analyser dispositifs de protection et politiques de sécurité.
- Fournir recommandations hiérarchisées selon criticité.
- Accompagner la mise en place d’un plan d’action sécurisé.

Population cible

- Entreprises et organisations basées au Niger, tous secteurs.
- Directions des systèmes d’information et responsables sécurité.
- Équipes informatiques, managers de proximité, dirigeants.
- PME, grandes entreprises, institutions publiques.
- Secteurs financiers, miniers, logistiques et télécommunications.

Durée de la formation

Durée	Format
2 à 6 semaines selon taille et complexité	Sur site, télétravail partiel ou totalement à distance

Programme de la formation

> **Note importante :** Chaque phase vise à garantir un diagnostic rigoureux et un accompagnement sur-mesure.

Étape 1 : Diagnostic initial

- Analyse structurelle et entretiens IT.
- Identification périmètres critiques.

Étape 2 : Analyse documentaire et réglementaire

- Revue des politiques, normes, conformité locale et internationale.

Étape 3 : Identification des vulnérabilités techniques

- Tests de vulnérabilité, scans réseaux, audits applicatifs.

Étape 4 : Recommandations et plan d’action

- Rapport d’audit avec plan d’action hiérarchisé.

Étape 5 : Suivi et accompagnement

- Accompagnement post-audit et audits périodiques.

Module	Objectif principal	Durée
Diagnostic initial	Cartographier risques et enjeux	2-5 jours
Analyse documentaire	Vérifier conformité réglementaire	3-4 jours
Tests techniques	Identifier vulnérabilités techniques	5-10 jours
Recommandations	Proposer plan d’action sécurisé	2-3 jours
Suivi	Accompagnement et audits réguliers	Continu