

Fiche Technique: Audit Cybersécurité à Agadir

Objectifs de la formation

- Diagnostiquer précisément le système d'information.
- Détecter failles et évaluer la maturité de la sécurité.
- Identifier risques internes et externes.
- Vérifier la conformité aux normes et réglementations.
- Proposer un plan stratégique d'amélioration.
- Assurer la continuité d'activité et une gouvernance efficace.

Population cible

- Entreprises de toutes tailles opérant à Agadir.
- Directions générales et managers opérationnels.
- Responsables des systèmes d'information (RSSI, DSI).
- Responsables conformité et équipes IT.
- Secteurs industriels, logistiques, agroalimentaires, touristiques.

Durée de la formation

Phase	Durée estimée	Activités clés
Diagnostic initial	1 à 2 semaines	Entretiens, collecte d'informations, audit préliminaire
Analyse documentaire	1 à 1,5 semaines	Revue réglementaire, contrôle des politiques et procédures
Recommandations & plan d'action	1 semaine	Rapport détaillé et priorisation des risques
Suivi et accompagnement	Variable selon besoins	Mise en œuvre, reporting, assistance continue

Programme de la formation

Étape 1 : Diagnostic initial

- Collecte d'informations par entretiens.
- État des lieux des outils et incidents existants.

Étape 2 : Analyse documentaire et réglementaire

- Examen des politiques et procédures de sécurité.
- Vérification conformité (ISO 27001, RGPD, ANSSI).

Étape 3 : Recommandations et plan d'action

- Rapport des vulnérabilités et risques.
- Priorisation et plan d'amélioration stratégique.

Étape 4 : Suivi et accompagnement

- Assistance à la mise en œuvre des recommandations.
- Reporting et ajustements en temps réel.

Note : La durée totale varie de 3 à 6 semaines, selon la taille et la complexité de l'entreprise.