Fiche Technique:Formation certification et pilotage cybersécurité au Maroc

Objectifs de la formation

> Démarche pragmatique, orientée résultats, adaptée au contexte marocain (gouvernance, conformité, budgets).

- Instaurer une gouvernance claire: rôles, responsabilités, matrice RACI, processus décisionnels.
- Piloter un portefeuille de chantiers sécurité; prioriser par criticité et valeur métier.
- Construire des KPI/KRI pertinents et des tableaux de bord exécutifs pour les comités.
- Relier menaces, contrôles, plans de traitement et objectifs de conformité.
- Préparer audits/évaluations (clients, assureurs, partenaires) avec preuves et plans d’action.
- Assurer traçabilité, alignement budgétaire et amélioration continue.

Population cible

Public managérial et opérationnel impliqué dans la gouvernance et le pilotage cybersécurité.

- DG, DAF, DSI, RSSI, Risk Managers, responsables conformité.
- PMO, chefs de projet IT/digital, consultants internes.
- Équipes risques et audit interne (contrôles, traçabilité des décisions).
- Programmes cloud, data, transformation numérique nécessitant sécurité et conformité.
- Organisations souhaitant passer d’initiatives dispersées à un pilotage par la valeur.

Durée de la formation

Parcours	Durée	Format	Modalités / Focus
Executive Focus	2 jours	Présentiel / distanciel	Cas d’usage, tableaux de bord exécutifs
Management Track	5 jours	Mixte	Ateliers, RACI, KPI/KRI, roadmap 12–24 mois
Bootcamp Pilotage	8 jours	Intensif	Simulations comités, incident/crise, reporting
Coaching appliqué	8–12 semaines	Accompagnement	1:1, ateliers équipes, OKR sécurité, quick wins

Programme de la formation

Module 1 — Gouvernance stratégique et alignement

- Cadre de gouvernance: charte, comité cyber, rôle du RSSI, relation DG.
- Priorisation des investissements et feuille de route 12–24 mois.

Module 2 — Risques, conformité et normes

- Référentiel de risques, exposition, appétence, exigences sectorielles.
- Lien menaces–contrôles–conformité; axes ISO 27001 et CEH.

Module 3 — Opérations de sécurité et performance

- SOC interne/partagé, contrôles de base (correctifs, durcissement, identités).
- Tableaux de bord, backlog, SLA/SLO, seuils d’alerte.

Module 4 — Tableaux de bord exécutifs

- Indicateurs pour COMEX/Conseil: lisibilité et soutien aux arbitrages.
- Canevas prêts à adapter; cohérence stratégique-opérationnel.

Module 5 — Réponse à incident et continuité

- Préparation, détection, réponse, communication de crise.
- Alignement PCA/PRA; exercices et post-mortem pour améliorer.

Module 6 — Cloud, tiers et supply chain

- Évaluation fournisseurs, due diligence, clauses, scoring.
- CNAPP, IAM, chiffrement, sauvegardes, segmentation; métriques métiers.

Module 7 — Culture, sensibilisation et conduite du changement

- Messages clés, parcours différenciés, ambassadeurs métiers.
- Mesure de l’adoption et corrélation avec la baisse des incidents.

Module 8 — Conformité locale et contexte marocain

- Particularités réglementaires et attentes des donneurs d’ordre au Maroc.
- Modèles de politiques/procédures compatibles avec les standards internationaux.
