Fiche Technique Conseil: audit cybersécurité pme

Objectifs de la mission

- Diagnostiquer de manière complète la sécurité du système d'information.
- Identifier les vulnérabilités techniques et organisationnelles.
- Vérifier la conformité (RGPD, ISO 27001, exigences sectorielles).
- Évaluer les dispositifs en place (pare-feu, antivirus, authentification, sauvegardes).
- Analyser les procédures et bonnes pratiques pour améliorer la gouvernance IT.
- Fournir un rapport clair avec plan d'action priorisé pour réduire les risques et assurer la pérennité.

> Livrable principal: rapport d'audit cybersécurité détaillant les constats, les analyses de risques et un plan d'action priorisé.

Entreprises / profils concernés

- PME souhaitant évaluer et renforcer leur posture de sécurité.
- Dirigeants, responsables IT, RSSI/équivalents, chefs de projets IT.
- Responsables risques opérationnels et responsables QHSE.
- Secteurs: commerce, production industrielle, services, santé, finance.
- Entreprises à fort usage technologique et environnements IoT.

Durée et format de la mission

La durée varie selon la taille, la complexité et le périmètre analysé. L'intervention est majoritairement en présentiel, avec préparation et synthèse à distance. Des audits hybrides (site + distant) sont proposés selon le contexte.

Élément	Détails
Durée indicative	2 à 4 semaines (selon taille/complexité/périmètre)
Mode d'intervention	Principalement en présentiel; partie préparatoire et de synthèse à distance; option hybride
Restitution	Rapport détaillé + atelier de restitution (équipes dirigeantes et opérationnelles)
Suivi	Calendrier de suivi défini sur mesure pour la mise en œuvre

Méthodologie / déroulement de la mission

Étape 1 : Diagnostic initial

- Collecte d'informations sur l'architecture du SI, les actifs critiques et la politique de sécurité.
- Entretiens avec responsables IT et utilisateurs clés pour cerner les pratiques terrain.
- Orientation des travaux d'audit à venir.

Étape 2 : Analyse documentaire et réglementaire

- Revue des politiques, procédures, plans de continuité, rapports antérieurs, guides utilisateurs.
- Vérification de la conformité (RGPD, ISO 27001, exigences sectorielles).
- Revue des contrats et SLA fournisseurs.

Étape 3 : Recommandations et plan d’action

- Élaboration de recommandations concrètes et adaptées.
- Plan d’action priorisé avec calendrier et estimation des ressources.
- Alignement sur la réalité économique et technique de la PME.

Étape 4 : Suivi et accompagnement

- Remise du rapport d’audit cybersécurité et restitution.
- Assistance à la mise en œuvre, contrôles périodiques, sensibilisation/formation aux bonnes pratiques.
- Pilotage pour une amélioration continue et une meilleure résilience.

Phase	Objectif	Livrable	Durée
Diagnostic initial	Collecte des données et entretiens	Compte rendu initial	2 à 3 jours
Analyse documentaire	Vérification de la conformité	Rapport d’analyse	3 à 5 jours
Recommandations	Plan d’action priorisé	Rapport d’audit cybersécurité	5 à 7 jours
Suivi	Accompagnement et contrôle	Rapports de suivi	Variable selon besoin