Rapport d'Audit du Système d'Information

I. Synthèse Décisionnelle

L'audit réalisé sur l'infrastructure informatique de [Nom de l'entreprise] révèle un système fonctionnel mais hétérogène. Si les outils métiers répondent aux besoins opérationnels, des failles structurelles majeures ont été identifiées, notamment en matière de continuité d'activité et de cloisonnement des réseaux.

L'indice de maturité globale est évalué à **2/5**. Une intervention sur les points critiques (Sauvegarde et Accès) est impérative dans les trente prochains jours pour éviter toute rupture de service ou fuite de données confidentielles.

II. Périmètre et Méthodologie

1. Périmètre de l'étude

- **Infrastructure matérielle :** Serveurs physiques, postes de travail, équipements réseau (switchs, pare-feu).
- **Logiciels et Applications :** ERP, messagerie professionnelle, bases de données clients.
- **Processus humains :** Gestion des mots de passe, procédures d'arrivée et de départ des collaborateurs.

2. Méthodologie employée

L'audit s'est appuyé sur le référentiel **ISO 27001** et les bonnes pratiques du **COBIT**. Les travaux ont inclus :

- Des entretiens avec les responsables de services.
- Une inspection physique de la salle informatique.
- Des tests de vulnérabilité techniques (scans de ports et tests d'intrusion externes).

III. Analyse des Constats et Diagnostic

1. Gouvernance et Sécurité Logique

- **Constat :** La politique de gestion des mots de passe est jugée trop permissive. Aucune double authentification (MFA) n'est activée sur la messagerie.
- **Risque :** Usurpation d'identité et compromission des données stratégiques par ingénierie sociale.

- **Recommandation :** Imposer une complexité minimale (12 caractères, types variés) et déployer le MFA sur tous les accès distants et comptes d'administration.

2. Infrastructure et Réseau

- **Constat :** Le réseau Wi-Fi utilisé par les visiteurs n'est pas isolé du réseau de production contenant les serveurs comptables.
- **Risque :** Un attaquant externe peut accéder aux données internes via une simple connexion Wi-Fi de passage.
- **Recommandation :** Mise en place d'un réseau VLAN dédié pour les invités avec une isolation stricte via le pare-feu.

3. Sauvegarde et Continuité d'Activité (PCA/PRA)

- **Constat :** Les sauvegardes sont quotidiennes mais stockées uniquement sur un NAS situé dans la même pièce que le serveur principal. Aucun test de restauration n'a été effectué depuis six mois.
- **Risque :** En cas d'incendie ou de sinistre physique, l'entreprise perd l'intégralité de ses données sans possibilité de recouvrement.
- **Recommandation :** Appliquer la règle du 3-2-1 (3 copies, 2 supports différents, 1 copie hors site). Automatiser une réplication vers un espace Cloud sécurisé.

4. Maintenance du Parc

- **Constat :** Un tiers des postes de travail utilise encore un système d'exploitation dont le support de sécurité a expiré.
- **Risque :** Exploitation de failles de sécurité connues pour lesquelles aucun correctif ne sera publié.
- **Recommandation :** Planifier le remplacement ou la mise à jour des équipements obsolètes sous 90 jours.

IV. Plan d'Action Priorisé

Les actions suivantes sont classées par ordre d'urgence pour sécuriser le patrimoine informationnel de l'organisation.

Priorité	Action à mener	Responsable	Échéance
Critique	Activation de l'authentification multi-facteurs (MFA)	Responsable IT	Immédiat
Critique	Externalisation des sauvegardes (Cloud ou site distant)	Prestataire IT	1 semaine
Majeure	Segmentation des réseaux Wi-Fi (VLAN)	Administrateur	1 mois
Majeure	Mise à jour de la politique de sécurité (PSSI)	Direction	3 mois

---

V. Conclusion

La modernisation du système d'information de [Nom de l'entreprise] est nécessaire pour accompagner sa croissance. La correction des vulnérabilités liées aux sauvegardes et aux accès doit constituer le socle de la stratégie informatique pour l'année en cours. Une fois ces bases sécurisées, une réflexion sur l'optimisation des performances logicielles pourra être engagée.