Voici un **modèle d'audit technique** structuré pour l'environnement que tu décris (micro-entreprises, parc hétérogène, cloud déporté, focus sécurité et sauvegarde). Ce modèle peut être utilisé lundi/mardi comme **fiche terrain** à remplir.

Responsable technique & sécurité : délégation à Madame :

Rôles / compétences / cursus

Relations avec les Micro-entreprises :

Modèle d'Audit Technique – Tercium

🔹 I. Informations Générales

Élément	Description à renseigner
Nom de l'entité	Exemple : Agence Web Alpha
Responsable présent	Nom + rôle
Date de l'audit	AAAA-MM-JJ
Auditeur	Nom / rôle
Lieu	Adresse physique / réseau logique
Nombre de postes	Ex : 3 postes utilisateurs + 1 NAS
Connexion Internet	Fibre / ADSL / 4G / Autre (préciser)

🔹 II. Matériel & Configuration Réseau

Poste / Équipement	OS / Version	Adresse IP / DHCP	Rôle fonctionnel	Connexion réseau
PC01	Win 10 Pro	192.168.1.11	Design / Photoshop	Ethernet / Wi-Fi
PC02	Ubuntu 22.04 LTS	DHCP	Développement Web	Ethernet / Wi-Fi
NAS01	Synology DSM 7	192.168.1.254	Stockage / sauvegarde	LAN / VLAN stockage
Routeur	Livebox / pfSense	192.168.1.1	Gateway / DHCP / DNS	Ethernet

➡️ Ajoute autant de lignes que nécessaire. Identifie :

- Système d’exploitation
- Adresse IP fixe ou dynamique
- Usage (bureautique, dev, stockage, etc.)
- Type de connectivité

🔹 III. Comptes, Authentification & Accès

Poste / Équipement	Accès local	Authentification	Accès cloud / externe	Observations
PC01	Compte local	Mot de passe	Aucun	Pas de politique de mots de passe
PC02	Clé SSH + sudoer	Clé + mot de passe	GitHub / Infomaniak	Port 22 ouvert depuis WAN

➡️ Noter présence de :

- Comptes admin / root
- Clés SSH
- Mots de passe faibles / non expirables
- Accès à distance mal sécurisé

🔹 IV. Sauvegardes & PCA

Équipement	Type de sauvegarde	Fréquence	Emplacement	Vérification / Restauration
NAS01	Snapshot Synology	Quotidienne	Disque externe USB	✅ test restauration fait
PC02	Rsync vers NAS	Hebdomadaire	Local	❌ pas testé

➡️ Identifier :

- Fréquence des sauvegardes
- Emplacement physique/logique (local/cloud)
- Procédure de restauration existante ?
- Présence d’un plan de continuité (PRA, PCA)

🔹 V. Sécurité et Mises à Jour

Poste / Service	Antivirus / Firewall	UFW/iptables	Services exposés	Mise à jour auto	Observations
PC01	Windows Defender	❌	Aucun	❌	Version 20H2 obsolète
PC02	ClamAV + UFW	✅ ports 22/80	SSH + Apache	✅	SSH root interdit
NAS01	DSM Sécurité	Port 5000	Admin UI	✅	2FA désactivé

➡️ Inclure :

- Firewall local activé ?
- Services en écoute ? (Apache, SSH…)
- Politique de mises à jour ?
- Antivirus ? Pare-feu externe ?
- Authentification forte (2FA, certificat)

🔹 VI. Intégration cloud

Instance / Service Cloud	Provider	Objectif	IP / Domaine	Sécurité déployée
VM Jitsi (Ubuntu 22.04)	Infomaniak	Visio pro	84.234.28.241	Clé SSH, ports 80/443 only
Sauvegarde S3	Infomaniak	Backup NAS	Bucket tercium-01	Clé API, accès privé

➡️ Documenter :

- Accès via SSH (IP, DNS)
- Ports ouverts
- Firewall provider (security-groups)

- Certificats SSL installés ou non

🔹 VII. Observations / Anomalies / Recommandations

Bloc libre pour compléter à chaud :

- Matériel obsolète
- Services inutiles actifs
- Absence de sauvegarde
- Manque de segmentation réseau
- Pas de PRA / PCA / SLA formalisé