CHECKLIST NIS2
POUR PME

Gouvernance & responsabilités

- ◯ Désigner un Responsable de la cybersécurité (interne ou externe)
- ◯ Mettre à jour l'organigramme avec les responsabilités liées à la sécurité
- ◯ Valider un budget dédié à la cybersécurité annuel
- ◯ Définir une politique de sécurité des systèmes d'information (PSSI) formelle

Cartographie & analyse de risques

- ◯ Cartographier les actifs critiques (infrastructure, données, services essentiels)
- ◯ Identifier les dépendances (prestataires IT, cloud, SaaS...)
- ◯ Réaliser une analyse de risques complète
- ◯ Classer les risques par niveau de criticité

Mesures de prévention techniques

- ◯ Mettre en place un pare-feu, un EDR/MDR et un antivirus à jour
- ◯ Activer l'authentification multifacteur (MFA)
- ◯ Assurer la gestion des accès et des droits utilisateurs
- ◯ Maintenir une politique de mises à jour et de correctifs

Sensibilisation & formation

- ◯ Mettre en place un programme de sensibilisation annuel
- ◯ Organiser des simulations de phishing
- ◯ Suivre les progrès via des évaluations
- ◯ Tenir un registre des actions de formation cybersécurité

Détection & réponse aux incidents

- ◯ Installer des outils de détection automatique d'incidents
- ◯ Définir et documenter une procédure de gestion de crise cyber
- ◯ Mettre en place un journal d'incidents
- ◯ Mettre en place un journal d'incidents

Plan de continuité d'activité (PCA)

- ◯ Créer un plan de continuité (PCA) et un plan de reprise (PRA)
- ◯ Identifier les processus critiques
- ◯ Tester les procédures de reprise sur incidents
- ◯ Sauvegarder les données critiques de manière sécurisée

CHECKLIST NIS2
POUR PME

Documentation & reporting

- ◯ Désigner un Responsable de la cybersécurité (interne ou externe)
- ◯ Mettre à jour l'organigramme avec les responsabilités liées à la sécurité
- ◯ Valider un budget dédié à la cybersécurité annuel
- ◯ Définir une politique de sécurité des systèmes d'information (PSSI) formelle

Gestion des fournisseurs (Supply Chain)

- ◯ Identifier les prestataires critiques
- ◯ Évaluer leur niveau de sécurité
- ◯ Intégrer des clauses cybersécurité dans les contrats
- ◯ Réaliser des audits de sécurité fournisseurs

Audit & amélioration continue

- ◯ Réaliser un audit interne ou externe de cybersécurité
- ◯ Mettre en place un plan d'actions correctives
- ◯ Mettre à jour les politiques en fonction des audits
- ◯ Intégrer les leçons tirées des incidents

Automatisation avec Resilium

- ◯ Générer automatiquement les documents obligatoires
- ◯ Suivre l'avancement via un tableau de bord NIS2
- ◯ Obtenir un cyberscore pour piloter la maturité
- ◯ Réaliser des audits depuis une interface centralisée