CHECKLIST OPÉRATIONNELLE · ISO 27001

Les 10 actions avant votre audit ISO 27001

À partager avec votre équipe avant l'échéance de certification

TRANSMUTE CONSULTING

> Un audit ISO 27001 ne teste pas seulement si vos documents existent — il vérifie si votre SMSI (Système de Management de la Sécurité de l'Information) est réellement appliqué, compris et maintenu dans la durée. Utilisez cette checklist dans les semaines précédant votre audit pour ne laisser aucun angle mort.

PHASE 1 — SOLIDIFIER LES FONDATIONS

6 à 8 semaines avant

☐ **01** — **Relire la Déclaration d'Applicabilité (DdA) avec un regard d'auditeur**

Chaque contrôle de l'Annexe A doit être inclus avec justification ou exclu avec explication documentée. Un "non applicable" sans raison est un signal d'alarme immédiat.

☐ **02** — **Vérifier l'alignement entre analyse de risques et contrôles appliqués**

Chaque risque identifié doit se retrouver dans un contrôle actif. Chaque contrôle doit être relié à un risque documenté. Faites cette traçabilité avant que l'auditeur le fasse à votre place.

☐ **03** — **S'assurer que les rôles et responsabilités sont formellement attribués**

"L'équipe IT" ou "la direction" ne suffisent pas. Chaque politique clé doit avoir un propriétaire nommé, joignable, capable d'expliquer son rôle à l'auditeur.

PHASE 2 — TESTER AVANT D'ÊTRE TESTÉ

3 à 5 semaines avant

☐ **04** — **Vérifier l'exécution du programme d'audit interne**

Confirmez que les audits ont été réalisés à la fréquence définie, que les processus critiques ont été couverts, et que les résultats des audits précédents (internes et externes) ont alimenté vos actions correctives.

☐ **05** — **Traiter les non-conformités identifiées et documenter les actions menées**

Un auditeur externe est davantage impressionné par un processus d'amélioration continue bien documenté que par un système présenté comme parfait.

☐ **06** — **Simuler les questions difficiles avec vos équipes**

Les auditeurs interrogeront des collaborateurs non experts. Testez en interne : comment le développeur gère les accès prod, comment le commercial protège les données clients. Les réponses contradictoires créent des non-conformités.

PHASE 3 — CE QUE PERSONNE NE VOUS DIT

1 à 2 semaines avant

TRANSMUTE CYBERSECURITY

Transmute Consulting — SARL au capital de 1 000 euros
SIREN 928705870 · RCS Chambéry · NAF 7022Z · TVA intracommunautaire : FR08928705870

☐ 07

Vérifier la disponibilité et la localisation des documents clés

Politique de sécurité, DdA, analyse de risques, PV de revue de direction, CR d'audit interne, journal des incidents. Vous n'avez pas à tout centraliser — vous devez savoir exactement où chercher.

☐ 08

S'assurer que les preuves sont validées et datées

Logs, tickets, comptes-rendus de formation : vérifiez qu'ils sont approuvés par la bonne personne et datés là où c'est nécessaire. Une preuve non signée ou non datée perd l'essentiel de sa valeur probante.

☐ 09

Dédramatiser l'audit avec votre direction

L'auditeur n'est pas là pour juger les personnes — il audite un système. Une non-conformité est une faiblesse du système, pas la faute d'un collaborateur. Préparez votre direction à aborder cet échange avec sérénité.

☐ 10

Ne pas figer votre système à l'approche de l'audit

Un SMSI vivant — réunions planifiées, revues en cours, actions ouvertes — rassure l'auditeur. Il montre que votre système n'a pas été monté pour l'occasion. Documentez les évolutions en cours plutôt que de les suspendre.

Transmute Consulting — SARL au capital de 1 000 euros
SIREN 928705870 · RCS Chambéry · NAF 7022Z · TVA intracommunautaire : FR08928705870