Note Méthodologique : Support et ressources ISO 45001

Synthèse structurée de la démarche et des étapes de réalisation de la mission.

Contexte & finalité de la méthodologie

- Structurer compétences, communication et informations documentées pour un SMSST sans rupture.
- Sécuriser les opérations et donner un cadre clair aux managers de terrain.
- Assurer la continuité lors des évolutions (processus, effectifs, nouveaux sites).
- Fédérer la gouvernance autour d'objectifs mesurables et de preuves fiables.
- Concilier simplicité d'usage et rigueur normative pour une amélioration continue.

> **Point clé :** Ne pas confondre quantité et pertinence des moyens : mieux vaut 3 canaux maîtrisés que 10 dispersés.

Objectifs de la mission

- Assurer la disponibilité, la compétence et la cohérence des moyens.
- Atteindre 100 % de couverture des postes critiques sous 12 mois.
- Clore 90 % des actions issues d'audits internes sous 60 jours.
- Cartographier les compétences et déployer un plan de formation aligné sur les risques.
- Structurer des canaux de communication efficaces et maîtriser le cycle de vie documentaire.
- Piloter des indicateurs utiles et arbitrer avec la direction.

Périmètre / livrables attendus

- Diagnostic étayé des écarts et priorisation Top 5 risques.
- Matrice d'efficience des moyens.
- Référentiel de compétences et matrice de couverture des postes critiques.
- Plan de formation type et gabarits d'évaluation.
- Dispositif de communication (rituels, formats, responsabilités).
- Gouvernance documentaire (workflow, droits, preuves, liste maîtresse).
- Plan de déploiement, calendrier, ressources et critères d'acceptation.
- Préparation des audits internes et tableaux de bord (KPI).

Démarche méthodologique (étapes)

Étape 1 — Diagnostic structuré des besoins et des écarts

- Actions : analyse documentaire, entretiens multi-niveaux, échantillonnage terrain, cartographie des processus support.
- Résultats : diagnostic étayé, priorisation Top 5, matrice d'efficience des moyens.
- Repère : formaliser les actions à haute criticité sous 30 jours.

Étape 2 — Conception de l'architecture support

- Actions : définir cible (périmètre, rôles, indicateurs, cadences), élaborer modèles, workflow, droits et preuves.
- Résultats : référentiels (compétences, formation, communication, documentation) et règles de gestion.
- Vigilance : 1 propriétaire et 1 suppléant par actif critique ; charge de tenue à jour cadrée.

Étape 3 — Déploiement pilote et ajustements

- Actions : lancer un pilote (atelier/ligne/site), coordination et coaching, collecte de preuves (indicateurs, feedbacks).
- Résultats : rituels de revue bimensuels (15–30 min), seuil de 95 % de dossiers formation complets pour élargissement.
- Ajustements : simplifier modèles, clarifier rôles, prévenir la dérive des formats.

Étape 4 — Industrialisation et contrôle de maîtrise

- Actions : étendre sur l'ensemble du scope, accompagnement au changement, préparation des audits internes.
- Résultats : plan de déploiement consolidé (calendrier, ressources, critères d'acceptation), contrôles trimestriels (4/an).
- Repères : corriger les écarts majeurs sous 60 jours ; inscrire les pratiques dans revues et tableaux de bord.

Planning / durée / jalons

Jalon	Délai / fréquence	Repères / critères
Actions haute criticité formalisées (post-diagnostic)	≤ 30 jours	Diagnostic étayé et matrice d'efficience disponibles
Pilote (site/atelier/ligne)	Revue bimensuelle (15–30 min)	≥ 95 % dossiers de formation complets avant élargissement
Industrialisation et contrôle	Contrôle trimestriel (4/an)	Écarts majeurs corrigés ≤ 60 jours
Gouvernance documentaire	Revue ≤ 12 mois ; retrait obsolètes ≤ 24 h	Mise à jour sous 48 h en cas de changement critique
Couverture des postes critiques	≤ 12 mois	100 % habilitations valides avant affectation
Pilotage et audits	Comité mensuel ; audits internes 2/an	6–8 KPI suivis ; ciblage périmètres à risque élevé

Rôles & responsabilités (client / consultant)

Organisation (Client)

- Conserve la responsabilité du dispositif et des preuves (y compris prestataires externes).
- Désigne un propriétaire et un suppléant par actif critique ; fixe calendriers d'animation des briefs.
- Tient à jour le référentiel documentaire unique (revue ≤ 12 mois ; retrait obsolètes ≤ 24 h).
- Assure la traçabilité des formations/habilitations et l'intégration au référentiel interne.
- Implique les managers de proximité pour la sensibilisation et les retours terrain.

Consultant (Conseil)

- Conduit le diagnostic (analyse documentaire, entretiens, terrain, cartographie des processus support).
- Conçoit l'architecture cible (référentiels, modèles, workflow, droits, indicateurs, rôles).
- Coordonne le déploiement pilote, coache les équipes et collecte les preuves d'efficacité.
- Consolide le plan de déploiement, le calendrier, les ressources et les critères d'acceptation.
- Prépare les audits internes et transfère les méthodes/outils pour l'autonomie.

Prérequis & données nécessaires (inputs)

- Documentation SMSST existante : politiques, procédures, liste maîtresse, enregistrements.
- Inventaire des postes critiques, habilitations et matrices de compétences.
- Historique des formations : feuilles d'émargement, évaluations, recyclages.
- Indicateurs/KPI en place et actions issues d'audits internes.
- Canaux et rituels de communication existants (fréquences, formats, responsables).
- Retours d'expérience, signalements et quasi-accidents.
- Données des sous-traitants/intervenants externes (formations, habilitations).
- Référentiels RH/IT/HSE pour l'intégration des pratiques.

Modalités de pilotage & qualité (comités, validations, risques)

- Comité mensuel (30–45 min) avec 6–8 KPI resserrés pour décider et arbitrer.
- Revues bimensuelles sur pilotes ; vérifications de proximité mensuelles.
- Contrôles de conformité trimestriels (4/an) et audits internes ciblés 2/an.
- Rôles nominatifs et redevabilité : propriétaire + suppléant par actif critique.
- Seuils de performance : ≥ 95 % dossiers formation complets ; 100 % documents critiques revus ≤ 12 mois.
- Délais clés : 90 % des actions d'audit ≤ 60 jours ; retrait des versions obsolètes ≤ 24 h ; mise à jour ≤ 48 h après changement critique.
- Traçabilité systématique : comptes rendus, registres, accès tracés et archivage.
- Maîtrise des risques digitaux : droits gouvernés, mode dégradé, éviter la surcharge d'outils.