

Note Méthodologique : Digitalisation et qualité 4.0

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

Contexte & finalité de la méthodologie

- Accélérer la transformation qualité par données en temps réel, automatisation et gouvernance des processus.
- Aller au-delà de la dématérialisation : prédictivité opérationnelle, conformité démontrable, apprentissage rapide.
- En SST, relier observations, incidents, actions correctives et décisions pour réduire les délais et fiabiliser les preuves.
- Exiger une réflexion sur besoins métiers, sécurité de l'information, métriques et conduite du changement.
- Fournir des repères concrets pour cadrer, mettre en œuvre et améliorer la trajectoire de digitalisation.

Objectifs de la mission

- Sécuriser la disponibilité et l'intégrité des preuves, avec une piste d'audit liée aux rôles.
 - Réduire les délais de détection et traitement des écarts (repère 24 h pour un signalement critique).
 - Standardiser pratiques et formulaires pour fiabiliser la donnée source.
 - Accroître la visibilité managériale via des indicateurs contextualisés (revus au minimum 4 fois/an).
 - Renforcer l'apprentissage organisationnel par capitalisation des retours d'expérience.
-

Périmètre / livrables attendus

- Diagnostic et analyse d'écarts, priorités de mise en œuvre et options d'architecture.
- Cartographie des processus (entrées/sorties/rôles/décisions) et exigences associées; métadonnées, statuts et escalades.
- Grille de sélection/cahier des charges intégrant couverture fonctionnelle, interopérabilité et sécurité (ISO 27001).
- Procédures, gabarits et modes opératoires; règles de données, droits d'accès et plan de conduite du changement.
- Plan de déploiement par vagues, rôles d'appui, rituels de suivi de l'adoption et de la complétude.
- Cadre de mesure et tableaux de bord: définitions, sources, fréquences et seuils d'alerte (preuve ISO 19011).
- Noyau fonctionnel: gestion documentaire, gestion des écarts et plans d'actions, avec preuve d'intégrité et d'approbation.

Démarche méthodologique (étapes)

Étape 1 – Diagnostic de maturité et cadrage

- Cartographier flux d'information, responsabilités, outils et contraintes de sécurité.
- Produire analyse d'écart, priorités et options d'architecture.
- Vigilance: gestion du changement et dépendances IT souvent sous-estimées.

Étape 2 – Cartographie des processus et exigences

- Décrire processus (entrées/sorties/rôles/décisions) et relier aux exigences (ISO 9001, ISO 45001).
- Formaliser métadonnées, statuts, règles et mécanismes d'escalade.
- Vigilance: formulaires trop complexes et qualité de donnée source insuffisante.

Étape 3 – Sélection des solutions et architecture

- Évaluer couverture fonctionnelle, interopérabilité, sécurité (ISO 27001), coûts et support.
- Arbitrer standardisation vs spécifiques critiques; cadrer gouvernance des accès/identités.
- Livrable: cahier des charges réaliste limitant les personnalisations coûteuses.

Étape 4 – Conception pilote et gouvernance

- Définir indicateurs, règles de données, droits d'accès et plan de changement.
- Produire procédures, gabarits et modes opératoires; choisir un démonstrateur (site/processus).
- Vigilance: arbitrages clairs sur les demandes d'évolution.

Étape 5 – Déploiement progressif et conduite du changement

- Planifier des vagues; stabiliser processus cibles et rôles d'appui.
- Accompagner de proximité; suivre adoption, complétude et respect des délais.
- Vigilance: cohabitation prolongée des anciens/nouveaux modes et manque d'alignement hiérarchique.

Étape 6 – Mesure de performance et amélioration

- Relier indicateurs à stratégie, risques et exigences d'audit (ISO 19011).
- Préciser définitions, sources, fréquences, seuils d'alerte; tenir des revues régulières.
- Vigilance: piloter par utilité décisionnelle, pas par volume de données.

Planning / durée / jalons

Jalon	Délai / fréquence	Référence / indicateur
Qualification d'un signalement critique	24 heures	ISO 45001 – clause 10.2 (esprit)
Assignment initiale d'une action	48 heures	Automatisation des processus qualité
Vérification de l'efficacité (écarts majeurs)	30 jours	Audit digital – actions correctives

Revue de direction	Trimestrielle (≥ 4/an)	ISO 9001 – clause 9.3
Contrôle/audit interne sécurité	Semestriel (ex.)	ISO 27001 – gouvernance SI
POC/pilote et décision	90 jours	Revue + cible d'adoption 80% à 90 jours

Rôles & responsabilités

Client

- Direction: porte la priorité, arbitre les demandes d'évolution, valide les revues.
- Managers de proximité: animent rituels, relient données aux décisions, veillent à la qualité des saisies.
- Équipes métiers/terrain: expriment besoins, testent cas réels, saisissent les événements à la source.
- Informatique interne: gère habilitations/identités, sécurité, interopérabilité, SLA et escalade.

Consultant

- Réalise le diagnostic, l'analyse d'écarts et le cadrage réaliste.
- Formalise cartographie, exigences, métadonnées et mécanismes d'escalade.
- Pilote la sélection des solutions et le cahier des charges (sécurité, interopérabilité, coûts).
- Conçoit le pilote, les gabarits/procédures et le plan de conduite du changement.
- Met en place le cadre de mesure, tableaux de bord et dispositifs de revue/audit.

Prérequis & données nécessaires (inputs)

- Référentiels: ISO 9001:2015, ISO 45001:2018, ISO 19011:2018, ISO 27001:2022, RGPD (art. 5).
- Cartographie des processus, flux d'information, rôles et responsabilités.
- Politique d'habilitation et gestion des identités (principe du moindre privilège).
- Nomenclature et métadonnées standardisées; gabarits/formulaires homogènes.
- Données sources fiables; définitions stables des indicateurs; règles de traçabilité et d'archivage.
- Inventaire des outils existants; exigences d'interopérabilité et de sécurité.
- Mesures de sécurité opérationnelles: chiffrement, sauvegarde, restauration, journalisation auditable.

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

- Revues de direction trimestrielles minimum; tableaux de bord hiérarchisés et stables dans le temps.
- Comités de pilotage: gouvernance claire des accès, décisions et arbitrage des évolutions; escalades automatiques.
- Audits internes réguliers (ex. semestriels), piste d'audit exhaustive et preuve d'intégrité/approbation.
- Rituels courts de suivi de l'adoption, de la complétude des enregistrements et des délais.
- Seuils et délais standard: 24 h qualification des écarts critiques; 48 h assignation initiale; 30 jours vérification d'efficacité.
- Prévention des risques: limiter la sur-complexité, standardiser avant de personnaliser, conduire le changement.

- Protection des données: sécurité ISO 27001, minimisation RGPD; vigilance sur géolocalisation/anonymisation si nécessaire.

CABINET QUALITE - www.cabinet-qualite.com - info@cabinet-qualite.com