

Note Méthodologique : Communication interne externe

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

Contexte & finalité de la méthodologie

- Pilier de maîtrise des risques SST et sécurité des aliments.
- Aligne communication interne et externe vers parties prenantes.
- Soutient planification, contrôle opérationnel et réponse aux incidents.
- Encadre la diffusion d'informations sensibles (conformité, protection des données).
- Référentiel ISO 22000:2018 §7.4 ; dispositif formalisé revu au moins 1 fois/an.

Point clé : Deux facteurs décisifs : préparation (procédures, modèles, porte-parole, accès aux données) et entraînement (exercices, retours d'expérience).

Objectifs de la mission

- Garantir une circulation fiable des informations, sans interprétation.
- Taux de compréhension ≥ 90 % sur messages critiques.
- Aligner sites, équipes et niveaux hiérarchiques.
- Réduire les délais de réaction (escalade interne N1 : < 60 min).
- Démontrer la conformité documentaire lors des audits.
- Renforcer la confiance des clients et autorités.

Périmètre / livrables attendus

- Cartographie des parties prenantes (interne/externe) et canaux.
- Procédure formalisée de communication (rôles, canaux, délais, escalade).
- Matrice RACI et délégations (dont hors heures ouvrées).
- Référentiel de messages types avec champs obligatoires.
- Gabarits, objets normalisés, arbres de décision et règles d'usage.
- Protocoles d'escalade (3 niveaux) et canaux de secours.
- Tableaux de bord et modalités de revue.
- Traçabilité/archivage des preuves (messages critiques conservés 3 ans).

Démarche méthodologique (étapes)

1) Diagnostic des canaux et parties prenantes

- Interviews, revue documentaire, cartographie des flux, écart-type.
- Échantillon de 30–50 messages vérifiés (validation, sources).

- Livrable : état des lieux et écarts priorisés (cohérence, délais, traçabilité).

2) Cadre de gouvernance et responsabilités

- Définir qui décide/rédige/valide/diffuse + délégations.
- Matrice RACI, procédure et critères d'escalade.
- Repères : voies rapides, binôme opérationnel/juridique, astreinte 24/7 (crise N3).
- Livrable : procédure validée et RACI.

3) Cartographie des messages et criticité

- Classer par familles (sécurité, qualité, réglementaire, commercial, RH) et niveaux (info/incident/crise).
- Référentiel de messages types (faits, risques, actions, contacts).
- Repère : 1ère alerte interne N2 en 15 minutes.
- Livrable : référentiel et seuils/délais associés.

4) Choix des supports et protocoles

- Sélection des supports (réunion flash, affichage, intranet, SMS, courriel restreint).
- Ordre des destinataires, objets normalisés, modèles.
- Limiter à 2 canaux principaux par type + canal de secours ; preuves conservées 3 ans (messages critiques).
- Livrable : kit de diffusion (gabarits, arbres de décision, règles d'usage).

5) Mise en capacité et tests

- Tests à blanc et exercices chronométrés multi-sites.
- Fréquence : ≥ 2 exercices/an/site ; retours structurés sous 72 h ; participation rôles critiques ≥ 95 %.
- Livrable : rapports de test et plan de montée en compétences.

6) Mesure, revue et amélioration continue

- Indicateurs : délais de diffusion, couverture, compréhension, incidents évités.
- Revue trimestrielle dédiée, intégrée à la revue de direction.
- Livrable : tableaux de bord, décisions et plans d'action.

Planning / durée / jalons

Jalon clé	Délai / fréquence	Repère
Première alerte interne (incident niveau 2)	15 minutes	Vue méthodologique / niveaux
Escalade interne (niveau 1)	< 60 minutes	Objectifs & résultats
Point consolidé interne (incident niveau 2)	H+2	Vue méthodologique
Notification aux autorités compétentes	24–72 heures	Autorités sanitaires
Point presse (crise niveau 3)	≤ 48 heures	Canaux externes / porte-parole
Exercices/tests par site	≥ 2 /an	Tests & entraînement

Rôles & responsabilités (client / consultant)

Client

- Définir et valider qui décide/rédige/valide/diffuse ; organiser les délégations.
- Désigner les porte-parole et assurer l'astreinte 24/7 pour les crises de niveau 3.
- Maintenir canaux officiels et listes de diffusion à jour ; garantir la traçabilité/archivage (3 ans pour messages critiques).
- Participer aux interviews et tests ; mobiliser les rôles critiques (objectif ≥ 95 % lors des simulations).
- Respecter les délais légaux de notification (24–72 h) et les protocoles d'escalade.

Consultant

- Conduire le diagnostic (interviews, revue documentaire, échantillon 30–50 messages).
 - Structurer la gouvernance : matrice RACI, procédure et critères d'escalade.
 - Produire le référentiel de messages types, gabarits, objets normalisés et arbres de décision.
 - Planifier et animer tests/exercices ; fournir retours structurés sous 72 h.
 - Mettre en place tableaux de bord et modalités de revue ; proposer plans d'action.
-

Prérequis & données nécessaires (inputs)

- Documents et enregistrements de communication existants ; listes de diffusion à jour.
- Inventaire des canaux en place (réunions, affichage, messageries, intranet, SMS...).
- Cartographie des parties prenantes internes/externes.
- Échantillon de 30–50 messages récents avec validations et sources.
- Références normatives/légales : ISO 22000:2018 §7.4, délais légaux, protection des données.
- Données factuelles pour messages : faits, risques, actions, contacts (+ preuves : analyses, photos, étiquettes, traçabilité).
- Désignation des porte-parole et calendrier d'astreinte.
- Liste des sites et responsables pour coordination multi-sites.

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

- Procédure formalisée revue au minimum 1 fois/an ; intégration à la revue de direction.
- Voies rapides de validation pour messages critiques ; binôme opérationnel/juridique ; astreinte 24/7 (N3).
- Tableau de bord mensuel : délais, couverture des destinataires critiques, compréhension, effets.
- Revue trimestrielle dédiée communication ; décisions et plans d'amélioration.
- Gestion des risques : limiter à 2 canaux principaux/type ; canal de secours ; recadrage des rumeurs ; gestion des canaux informels.
- Traçabilité et conservation des preuves 3 ans pour messages critiques.
- Niveaux d'escalade structurés (information/incident/crise) avec délais associés.

