Note Méthodologique : Analyse Post-Crise en Plan d Urgence

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

Contexte & finalité de la méthodologie

Après un incident significatif, l'analyse post-crise éclaire les faits, structure les apprentissages et oriente des corrections durables.

- Combine collecte de preuves, contradiction des points de vue, traçabilité et mise à jour de la gouvernance.
- Fenêtre d'analyse resserrée : ouverture sous 72 h, jalon J+7, clôture visée sous 30 jours.
- Renforce résilience et conformité (repères ISO 22301, ISO 45001) et protège la mémoire organisationnelle.
- Fournit critères de gravité, seuils de performance et preuves utiles aux audits/comités.

> **Point clé :** Mieux vaut 6 preuves robustes vérifiables que 30 éléments hétérogènes difficiles à auditer.

Objectifs de la mission

- Réduire la récurrence, améliorer la maîtrise opérationnelle, démontrer la conformité.
- Valider la chronologie et l'adéquation des déclenchements.
- Clarifier les causes et qualifier la gravité (3 niveaux approuvés).
- Établir des actions correctives datées, responsables nommés, preuves attendues.
- Actualiser plans, check-lists, consignes avec contrôle de version formel.
- Programmer une vérification d'efficacité sous 60 jours et une communication adaptée.

Périmètre / livrables attendus

- Périmètre: sinistres techniques, incidents HSE, ruptures d'activité, incidents cyber, crises fournisseurs.
- Dossier de preuves: journaux horodatés, relevés/photographies, check-lists signées, témoignages (conservation ≥24 mois).
- Frise chronologique consolidée et évaluation des déclenchements/notifications/décisions.
- Rapport d'analyse causale et qualification des écarts.
- Plan d'actions priorisé avec indicateurs de succès.
- Mise à jour du Plan d'Urgence et supports (organigrammes, fiches réflexes, procédures) avec contrôle de version et diffusion tracée.
- Note de clôture et vérification d'efficacité (test/exercice, revue d'indicateurs).

- Fiche REX synthétique et communication aux équipes (message initial ≤72 h, clôture à J+30).

Démarche méthodologique (étapes)

1) Cadrage initial et sécurisation des preuves

- Geler journaux SI/GMAO, sceller équipements si besoin, collecter photos/relevés/témoignages (priorité J+1).
- Cartographier les sources et fixer un protocole de collecte; décision de gel documentaire par la direction.
- Livrables: périmètre cadré, plan de collecte, dépôt sécurisé des preuves.

2) Reconstitution de la chronologie et analyse des déclenchements

- Croiser badges, appels, alarmes, capteurs, tickets et consignations.
- Produire une frise minute par minute; vérifier seuils/notifications/décisions.
- Acter une tolérance d'horodatage et/ou une synchronisation NTP.

3) Analyse causale et qualification des écarts

- Appliquer 5M, 5 Pourquoi, arbre des causes; ateliers contradictoires neutres.
- Distinguer causes immédiates/contributives/systémiques; qualifier les écarts vs exigences.

4) Décision et priorisation des actions correctives

- Comité ad hoc: arbitrages coût/risque; fixer responsables, délais, indicateurs (ex. −20% temps de réaction).
- Livrable: plan d'actions priorisé, mesurable et traçable.

5) Mise à jour du Plan d'Urgence et des supports

- Réviser plans, organigrammes d'astreinte, fiches réflexes, check-lists, consignes; aligner avec la gouvernance.
- Publier avec n° de version, date d'effet, approbation direction; diffusion et preuves de prise de connaissance.

6) Vérification d'efficacité et clôture formelle

- Planifier un test ciblé/mini-exercice et une revue d'indicateurs.
- Rédiger la note de clôture; décision à J+30 (poursuite/ajustement/clôture).

Planning / durée / jalons

Jalon	Délai repère	Objectif / Commentaire
Ouverture officielle du dossier	≤ 72 h	Nommer le pilote, cadrer et lancer l'analyse.
Sécurisation des preuves (gel)	J+1	Figer journaux/systèmes, collecter les traces prioritaires.
Revue intermédiaire	J+7	Sécuriser les données critiques, valider

		hypothèses initiales.
Mise à jour documentaire	≤ 15 j (mineures) / ≤ 30 j (structurelles)	Contrôle de version, approbation direction, diffusion tracée.
Clôture de l’analyse	≤ 30 jours	Décisions tracées, plan d’actions et MAJ publiées.
Vérification d’efficacité / actions	≤ 60 jours	Test ciblé; viser ≥80% à 90% d’actions critiques soldées.

Rôles & responsabilités (client / consultant)

Client (Entreprise)

- Nommer le pilote, décider du gel documentaire et ouvrir le dossier.
- Donner accès aux sources (SI, capteurs, GMAO), mobiliser référents métiers.
- Valider chronologie et causes; participer aux ateliers factuels.
- Tenir le comité de décision, allouer ressources, approuver MAJ et diffusion.
- Programmer test d’efficacité et archiver les preuves (≥24 mois).

Consultant

- Cadrer le périmètre, cartographier sources, formaliser protocole de collecte.
- Structurer la frise chronologique; animer analyses causales de façon neutre.
- Appuyer arbitrages coût/risque; formaliser plan d’actions et indicateurs.
- Sécuriser la gestion documentaire (contrôle de version) et la note de clôture.
- Outiller (gabarits, indicateurs stables) et préparer aux audits/suivis.

Prérequis & données nécessaires (inputs)

- Fenêtre d’analyse fixée: ouverture ≤72 h, collecte prioritaire J+1, revue J+7.
- Sources probantes: journaux horodatés (SIEM/alertes), relevés techniques, check-lists signées, photos/témoignages.
- Seuils d’escalade et niveaux de gravité (3 niveaux) validés par la direction.
- Synchronisation/ tolérance d’horodatage (NTP) et intégrité des preuves garantie.
- Accès aux systèmes (GMAO, badges, tickets, consignations) et aux documents applicables.
- Gabarits de frise, d’analyse causale et de plan d’actions; plan de classement documentaire.
- Cartographie des risques et engagements de gouvernance (ISO 22301 / 45001).
- Responsabilités et comités identifiés; 5 à 7 indicateurs stables et auditables.

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

- Gouvernance jalonnée: revue J+7, clôture J+30; alignement ISO 19011/22301.
- Comité ad hoc: valide plan d’actions (responsable, délai, indicateurs, preuves attendues).

- Contrôle de version documentaire; approbation direction; diffusion et preuve de lecture (cible 95% sur populations critiques).
- Suivi bihebdomadaire possible des actions; test d’efficacité planifié; décision documentée.
- Neutralité et traçabilité: séparer faits/opinions; éviter la recherche de coupables.
- Risques qualité: contamination/perte de preuves, écarts d’horodatage, formats hétérogènes; mesures préventives explicites.
- Archivage des preuves ≥24 mois; indexage permettant une recherche < 2 minutes.
- Indicateurs resserrés (5–7): délais d’alerte/mobilisation, MTTR, taux d’actions critiques soldées, taux de lecture.