

RISQUES OPERATIONNELS ET MAITRISE DES PROCESSUS



23 AVRIL 2026



ESTHER MISHENG MBIDI
PRESIDENTE CLUB
CONGOLAIS DU RISK
MANAGEMENT
EXPERTE EN RISQUES



VERONIQUE LULLIER
RISK SUPERVISOR
SOCIETE GENERALE
PARIS



AGENDA

Risques Opérationnels et
ressources humaines

Maîtrise des Processus et
automatisation

KRI et pilotage du risque

Comprendre, identifier et maîtriser les risques opérationnels

Focus Ressources Humaines

Véronique LULLIER



Objectifs

Alignement sur définition commune

Utilisation des référentiels ISO 31000 et COSO ERM pour clarifier le risque opérationnel et éviter les confusions avec d'autres risques.

Démarche pragmatique d'identification

Identification simple et structurée des risques par activités, ressources et événements perturbateurs pour faciliter l'application opérationnelle.

Rôle des ressources humaines

Les personnes sont à la fois facteurs de performance et sources potentielles de vulnérabilité dans le risque opérationnel.

Leviers d'action concrets

Maîtrise des risques par réduction de l'exposition, prévention des causes et limitation des impacts en cas d'événements.



Définition et portée du risque opérationnel

Définition du risque opérationnel

Le risque opérationnel désigne les pertes liées aux défaillances des processus, personnes, systèmes ou événements externes.

Approche ISO 31000

ISO 31000 définit le risque comme l'effet de l'incertitude sur l'atteinte des objectifs opérationnels.

Perspective COSO ERM

COSO ERM intègre le risque opérationnel dans la performance globale, la continuité et la réputation organisationnelle.

Caractère transversal et quotidien

Le risque opérationnel touche toutes les activités et se manifeste souvent par des erreurs humaines ou des dysfonctionnements.



Objectifs de la maîtrise des risques et logique d'intervention

Maintenir le risque à un niveau compatible avec les performances, la conformité et la résilience de l'organisation **dans des conditions acceptables pour l'organisation, ses clients et ses parties prenantes.**

Approche proportionnée

Adopter une méthode fondée sur la compréhension des enjeux et des choix éclairés

Intervention sur les processus qui composent les activités

Agir en amont pour réduire la probabilité, en modifiant le contexte, l'organisation ou les modes opératoires.

en aval pour limiter les conséquences des événements. et donc leurs impacts **pour l'organisation, ses clients et ses parties prenantes.**

Logique de maîtrise pragmatique pour l'organisation, ses clients et ses parties prenantes.

Combiner mesures de prévention, réduction de vulnérabilité et capacité de réaction pour optimiser les efforts de contrôle.



Vue d'ensemble des leviers : exposition, causes et impacts

Réduction de l'exposition au risque

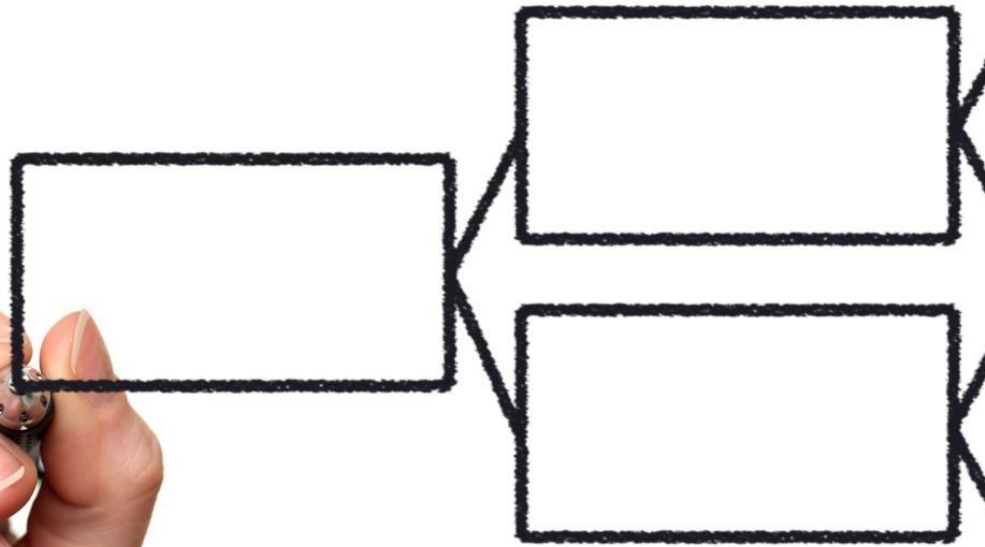
Ce levier vise à diminuer la fréquence et l'intensité des contacts avec les dangers par transformation d'activité ou conception.

Prévention des causes du risque

Ce levier s'appuie sur la formation, organisation, et gestion des compétences pour éviter la survenance des événements risqués.

Réduction des impacts

Cela concerne la limitation des conséquences et la maîtrise de la propagation des effets en cas d'événement.



Démarche d'identification basée sur les activités

Recensement des activités

Identifier les activités réelles dans le périmètre, en distinguant celles critiques pour la continuité, conformité ou satisfaction client.

Identification des ressources

Recenser les ressources mobilisées pour chaque activité : ressources humaines, systèmes, données et partenaires externes.

Analyse des perturbations

Examiner les risques pouvant perturber les ressources et l'activité, pour une vision concrète des vulnérabilités opérationnelles.

Appropriation métier et langage commun

Cette démarche facilite l'appropriation par les métiers et crée un langage commun pour discuter des risques spécifiques.

Comprendre les mécanismes de perturbation opérationnelle



Chaîne activité-ressource-risque

Cette chaîne représente la relation entre activité, ressources et risques, illustrant comment un risque se manifeste concrètement.

Elle permet de visualiser les mécanismes de causalité et d'éviter une approche trop centrée sur les conséquences finales.

Impact des défaillances des ressources

Une ressource défaillante ou mal utilisée perturbe une activité, générant un risque opérationnel.

Importance des ressources humaines

Les vulnérabilités humaines comme des formations insuffisantes ou une surcharge influencent fortement les risques opérationnels.

Priorisation et maîtrise des risques

Cette approche facilite la priorisation des risques et la justification des actions auprès des instances de gouvernance.



Pourquoi les ressources humaines sont un facteur clé de risque opérationnel

Centralité des ressources humaines

Les ressources humaines sont au cœur des opérations, concentrant compétences, jugement et adaptation essentiels au succès.

Variabilité et risques humains

Les facteurs humains comme stress, fatigue et turnover introduisent une variabilité importante et des risques opérationnels.

Dépendance aux compétences clés

Certaines activités reposent sur des compétences rares, créant une dépendance critique à des personnes clés.

Importance de la maîtrise des risques RH

Reconnaître et gérer les risques RH est essentiel pour prévenir ruptures d'activité et non-conformités.



Principales catégories de dangers affectant les ressources humaines

Disponibilité des ressources

Les risques liés à l'absence imprévue, au sous-effectif et au turnover impactent la continuité des opérations.

Compétences et savoir-faire

La perte ou l'obsolescence des compétences représente un risque majeur pour la performance organisationnelle.

Comportements et facteurs humains

Les erreurs, la fatigue et le stress augmentent les risques opérationnels et affectent la sécurité.

Conformité et éthique

Le non-respect des règles et les conflits d'intérêts peuvent entraîner des risques juridiques et réputationnels.

Agir sur la conception des activités pour réduire l'exposition RH

Automatisation des tâches répétitives

Automatiser les tâches sensibles réduit les erreurs humaines et diminue l'exposition aux risques opérationnels.

Simplification et réorganisation des processus

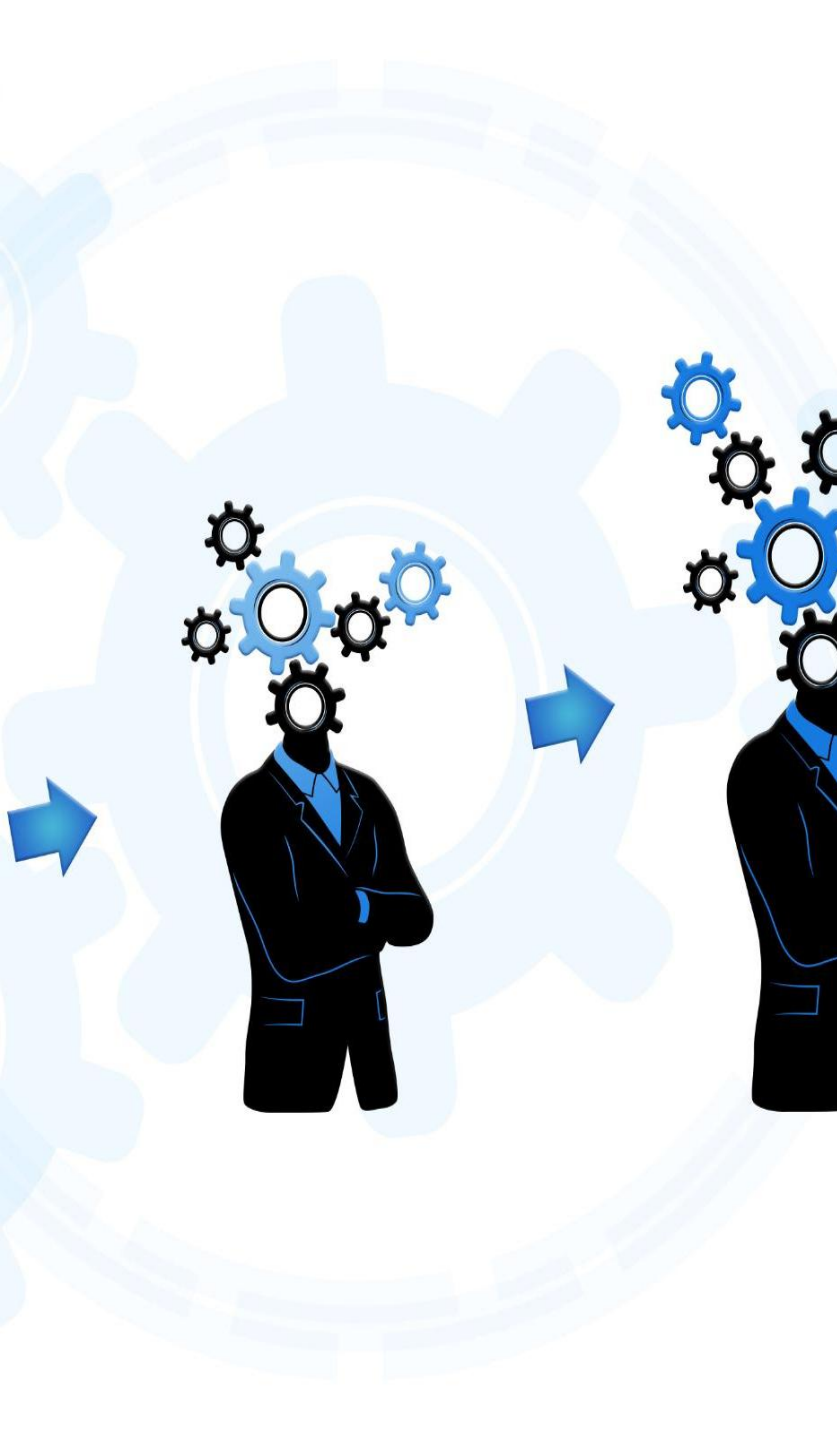
La réorganisation des processus limite les points de friction et les situations à risque exceptionnelles.

Externalisation et mutualisation

Transférer certaines activités à un tiers peut réduire l'exposition mais nécessite une gestion des risques fournisseurs.

Limitation des accès et habilitations

Restreindre les accès limite le nombre de personnes exposées aux risques opérationnels.





Prévenir la survenance des événements par le renforcement des capacités humaines

Formation et maintien des compétences

La formation continue est essentielle pour garantir des compétences adaptées aux évolutions des activités et des normes.

Polyvalence et back-up

Mettre en place des dispositifs de polyvalence réduit la dépendance aux personnes clés dans l'organisation.

Clarification des rôles

Définir clairement les responsabilités et règles de fonctionnement limite les erreurs liées aux ambiguïtés.

Gestion du stress et vigilance

Gérer la charge de travail et sensibiliser aux risques favorise une culture de vigilance et réduit les incidents.



Renforcer la résilience et la capacité de réaction de l'organisation

Plans de continuité d'activité

Mettre en place des plans pour maintenir ou reprendre rapidement les activités critiques en cas d'indisponibilité des ressources.

Détection rapide et escalade

Utiliser des dispositifs de détection rapide et des mécanismes d'escalade clairs pour réduire les délais de réaction aux incidents.

Contrôles et amélioration continue

Effectuer des contrôles de second niveau pour identifier les anomalies et appliquer les retours d'expérience pour progresser.

Priorisation et scénarios de dégradation

Prioriser les activités essentielles et définir des scénarios de dégradation contrôlée pour concentrer les efforts.



Conclusion

Ce qu'il faut retenir et les questions à se poser

Importance des risques RH

Les risques liés aux ressources humaines impactent directement la performance et la résilience des organisations.

Trois leviers de maîtrise

Réduire l'exposition, prévenir les causes et limiter les impacts sont essentiels pour une gestion efficace des risques.

Questions clés à poser

Identifier dépendances, erreurs humaines, et capacités de réaction aide à piloter les risques opérationnels.

Risque maîtrisé et assumé

L'objectif est un risque compris, assumé et piloté, pas un risque nul impossible à atteindre.



ROLE DES KRI DANS LE PILOTAGE DU RISQUE

Les KRI sont au cœur du **risk management** (gestion des risques).

Ils permettent de :

- ❑ **Surveiller** les zones à risque
- ❑ **Alerter** en cas de dérive (seuils)
- ❑ **Aider à la décision** (priorisation des actions)
- ❑ **Communiquer** avec la direction

On distingue souvent :

- ❑ ● KRI de **détection** (indicateurs de problèmes déjà présents)
- ❑ ● KRI de **prévention** (indicateurs prédictifs)



COMMENT CONSTRUIRE UN BON KRI

Choisir un **bon KRI (Key Risk Indicator)**, ce n'est pas prendre "un chiffre intéressant" c'est sélectionner **un signal utile pour piloter un risque réel.**



COMMENT CONSTRUIRE UN BON KRI

Bonnes pratiques

- ☐ 5 à 10 KRI max par périmètre
- ☐ Automatiser via Excel
- ☐ Mettre à jour régulièrement
- ☐ Revoir les seuils périodiquement



COMMENT CONSTRUIRE UN BON KRI

Un bon KRI doit être :

- ❑ **Pertinent** → lié à un risque critique
- ❑ **Mesurable** → basé sur des données fiables
- ❑ **Actionnable** → déclenche une décision
- ❑ **Suivi dans le temps** → avec des seuils (vert / orange / rouge)

Exemple concret :

- ❑ Risque : cyberattaque
- ❑ KRI : % de systèmes non patchés
- ❑ Seuil critique : > 10 %



- ❑ **KPI (Key Performance Indicator)** → mesure la performance
- ❑ **KRI** → mesure le niveau de risque

- ❑ KPI : chiffre d'affaires
- ❑ KRI : dépendance à un seul client



COMMENT CONSTRUIRE UN BON KRI

Bonnes pratiques

- ❑ Limiter le nombre de KRI (éviter la surcharge)
- ❑ Automatiser la collecte des données
- ❑ Définir des seuils clairs
- ❑ Réviser régulièrement les indicateurs
- ❑ Relier KRI → plans d'actions



- ❑ ● **Vert** → sous contrôle
- ❑ ● **Orange** → vigilance requise
- ❑ ● **Rouge** → action immédiate

L'objectif n'est pas seulement de mesurer, mais de **déclencher des décisions.**



- ❑ un responsable
- ❑ une fréquence de mise à jour
- ❑ un plan d'action associé



COMMENT CONSTRUIRE UN BON KRI

Exemple par domaine

RH

- ❑ Taux d'absentéisme
- ❑ Turnover postes clés
- ❑ Engagement collaborateurs



COMMENT CONSTRUIRE UN BON KRI

2. Identifier les “drivers” du risque

Pose-toi la question :

Qu’est-ce qui fait augmenter ce risque ?



COMMENT CONSTRUIRE UN BON KRI

3. Vérifier que le KRI est “bon”

Un bon KRI doit passer ce test

✓ Les 5 critères essentiels

- ❑ **Pertinent** → directement lié au risque
- ❑ **Mesurable** → données disponibles
- ❑ **Précoce** → alerte avant incident
- ❑ **Actionnable** → déclenche une action
- ❑ **Compréhensible** → clair pour le management

Si un indicateur ne déclenche **aucune décision**, ce n'est pas un bon KRI.



COMMENT CONSTRUIRE UN BON KRI

4. Choisir le bon type de KRI

KRI prédictif (le meilleur) anticipe le problème

- ❑ % de contrôles non réalisés
- ❑ charge de travail excessive

KRI de detection constate le problème

- ❑ nombre d'incidents
- ❑ pertes financières

Idéal = combiner les deux



COMMENT CONSTRUIRE UN BON KRI

5. Définir des seuils utiles

Sans seuil = pas de pilotage

Exemple :

☐ Vert → < 5%

☐ Orange → 5–10%

☐ Rouge → > 10%

Les seuils doivent être :

☐ réalistes

☐ alignés au niveau de risque accepté (appétence)



- ❑ Risque : cyberattaque
- ❑ Incident réel : faille exploitée
- ❑ Test : le % de systèmes non patchés avait-il augmenté ?



TESTER UN KRI

2. Tester le pouvoir prédictif

Un bon KRI doit **anticiper**, pas seulement constater

✓ Méthode

- ❑ Analyse historique (3–12 mois)
 - ❑ Regarde si le KRI dérive **avant** les incidents
- Sinon = indicateur de constat, pas de pilotage



TESTER UN KRI

4. Tester les seuils

Les seuils doivent déclencher des actions utiles

5. Tester l'actionnabilité

Question clé :

“Quand c’est rouge, que fait-on ?”

✓ Vérifie

- Existe-t-il une action définie ?
- Un responsable ?
- Un délai ?

Sinon → ce n’est pas un KRI, juste un chiffre





TESTER UN KRI

8. Tester la stabilité

Un bon KRI doit être :

- ☐ stable (pas trop volatile)
- ☐ mais sensible aux dérives

Sinon :

- ☐ trop stable → inutile
- ☐ trop volatil → bruit



COMMENT CONSTRUIRE UN BON KRI

Les KRI s'intègrent dans un dispositif plus large :

1. Identification des risques

Cartographie des risques

2. Définition des indicateurs

Lien entre risques ↔ KRI

3. Suivi régulier

Tableaux de bord (mensuels/trimestriels)

4. Gouvernance

Comités risques, reporting à la direction



QUESTIONS ?