FOCUS

09 SEPTEMBRE 2025

CARTOGRAPHIES DE RISQUES : DE SAPIN II À LA CSRD ET AU DEVOIR DE VIGILANCE, COMMENT PRÉSERVER L'ERM FACE AU PIÈGE DES SILOS?

Chaque rentrée offre aux risk managers une opportunité précieuse : celle de prendre du recul sur leurs pratiques, d'analyser les tendances de leur métier et de préparer les évolutions de leurs processus de gestion des risques à l'horizon 2026. Ces dernières années, la fonction a été profondément marquée par un environnement réglementaire foisonnant et exigeant, qui a bouleversé les approches traditionnelles.

Un cadre réglementaire toujours plus dense

Les obligations issues des lois nationales (Sapin II, loi Potier…), des directives européennes (CSRD, CS3D), mais aussi d'autres référentiels de bonnes pratiques (ISO, qualité, gestion de projet…), ont conduit les organisations à multiplier les exercices de cartographie des risques.

Chacun de ces cadres impose **ses spécificités méthodologiques, son périmètre et ses modalités propres**. Résultat : une prolifération de démarches parallèles, parfois redondantes, qui pèsent sur les équipes et sollicitent de manière répétée les mêmes contributeurs.

La fragmentation des cartographies : un défi croissant

Au fil des échanges avec nos clients et partenaires de l'écosystème des risques, un constat revient avec insistance : malgré l'existence de comités dédiés, **les démarches de cartographie tendent à se fragmenter et à s'organiser en silos de conformités**. Compliance, RSE, directions opérationnelles… chacun pilote son propre dispositif, avec ses propres échéances et ses propres exigences.

Cette fragmentation génère plusieurs difficultés :

- une mobilisation disproportionnée de ressources internes,
- un sentiment de lassitude chez les opérationnels,
- des résultats peu exploitables dans une logique consolidée,
- et, in fine, un affaiblissement du rôle de la gestion des risques comme outil de pilotage stratégique.

Préserver la cartographie des risques ERM dans son rôle de démarche fédérant les différentes approches d'évaluation de risques

Face à cette démultiplication, un enjeu central émerge : réaffirmer le rôle de l'Enterprise Risk Management (ERM) comme couche agrégative. L'ERM ne doit pas devenir un silo supplémentaire, mais bien l'ossature qui permet d'articuler les différentes démarches réglementaires et thématiques.

Un ERM consolidé permettrait :

- **de répondre aux exigences de cohérence** formulées dans les textes (Sapin II, CSRD, CS3D),
- **d'alimenter plus directement la prise de décision** grâce à une vision globale,
- et **d'optimiser les ressources** en évitant de solliciter plusieurs fois les mêmes acteurs pour des exercices similaires.

Vers une identification des risques plus transversale

Une piste de progrès réside dans la création de **grilles de lecture transverses**. Plutôt que de multiplier les cartographies spécifiques, les organisations peuvent **construire une bibliothèque élargie de risques majeurs** propres à l'ERM.

Cette bibliothèque intégrerait les thématiques réglementaires (conformité, climat, droits humains…), tout en conservant un niveau de granularité compatible avec une vision consolidée.

Ces risques peuvent ensuite être **tagués** selon leur pertinence pour tel ou tel cadre (CSRD, Sapin II, devoir de vigilance…), ou regroupés en **clusters thématiques** permettant d'articuler les différentes perspectives sans perdre la lisibilité globale.

FOCUS

09 SEPTEMBRE 2025

CARTOGRAPHIES DE RISQUES : DE SAPIN II À LA CSRD ET AU DEVOIR DE VIGILANCE, COMMENT PRÉSERVER L'ERM FACE AU PIÈGE DES SILOS?

Mutualiser, dans la mesure du possible, les sollicitations des contributeurs

Une démarche intégrée ouvre également la possibilité de **rationaliser la collecte d'informations**. Plutôt que de multiplier les réunions avec les contributeurs selon les projets, **un entretien ou atelier unique pourrait couvrir l'ensemble des thématiques**, en veillant à ce que les fonctions centrales (risk manager, responsable RSE…) se coordonnent pour assurer ensuite la classification et la consolidation.

Il sera toujours possible de compléter par des entretiens plus teintés "ERM", notamment pour développer sur des thématiques qui nécessitent un certain degré de confidentialité.

Cette approche permet non seulement de **gagner en efficacité**, mais aussi de **maintenir un engagement plus fort** des directions ou des opérationnels, moins exposés à la redondance des sollicitations.

Pour une mutualisation intelligente du pilotage des risques

La rationalisation peut également s'opérer au stade du traitement. Nombre de plans d'actions mis en œuvre par les organisations couvrent déjà plusieurs types de risques. **En rattachant une même action transverse à différents risques**, il devient possible de piloter plus efficacement et de **favoriser les synergies entre les métiers** (qualité, conformité, opérationnel, climat).

Les limites du décloisonnement : l'exemple de l'évaluation

Si les convergences sont possibles en identification et traitement, les méthodologies d'évaluation posent davantage de défis.

- Les seuils de matérialité de l'ERM et de la CSRD permettent certaines harmonisations, notamment en élargissant les impacts considérés dans une perspective de long terme. Le devoir de vigilance, quant à lui, pousse à intégrer de manière plus systématique les effets sur les tiers : salariés, chaîne de sous-traitance, clients, communautés riveraines… **L'enjeu pour les risk managers est donc d'adapter leurs échelles d'analyse afin d'englober ces dimensions complémentaires, tout en conservant une cohérence globale entre les différentes approches**.
- Mais certaines spécificités restent difficiles à contourner : Sapin II, par exemple, impose une évaluation brute et nette intégrant des facteurs aggravants, approche que l'on ne retrouve pas toujours dans les dispositifs ERM, climat ou droits humains. Une solution pragmatique pourrait consister à ajouter **une étape spécifique d'évaluation brute applicable uniquement à certains types de risques, afin de préserver l'harmonisation globale sans renoncer aux exigences réglementaires**.

Un enjeu aussi technologique

Au-delà des réflexions méthodologiques, l'outillage joue un rôle central. Les solutions de type GRC (Governance, Risk & Compliance) offrent la possibilité de consolider données et cartographies, **d'automatiser certains rapprochements et de faciliter le partage d'informations**. Mais ces outils ne sont efficaces que si l'organisation a défini en amont des référentiels communs et une gouvernance claire.

Conclusion : un défi collectif

La démultiplication des cartographies est un défi majeur pour les risk managers. Elle reflète un paradoxe : alors même que la gestion des risques devrait être un facteur de cohérence et de pilotage stratégique, elle se retrouve fragmentée par des exigences réglementaires de plus en plus nombreuses.

Réaffirmer l'ERM comme socle intégrateur, mutualiser les efforts d'identification et de traitement, accepter des spécificités là où elles sont incontournables, et s'appuyer sur des outils adaptés : telles sont les pistes pour transformer la contrainte en opportunité.

Car au-delà du respect des normes, l'objectif reste le même : doter l'organisation d'une vision claire et consolidée de ses risques, au service de sa résilience et de sa performance durable.

FANNY DREYFOUS-DUCAS
DIRECTEUR

ARENGI
RISK GOVERNANCE DIGITAL