

JOURNEES DES COMMISSIONS
16 octobre 2008



**Commission Systèmes d'Information – Organisation de la
Gestion des Risques**

**" Les systèmes d'information de gestion des risques,
supports d'une démarche globale de gestion des
risques : partage d'expériences »**

Modérateur :

François BEAUME, Responsable risk management de Dalkia

Intervenants :

Julien CAMUS, SCHLUMBERGER, Deputy risk & insurance manager,

Michel POZZO DI BORGO, Banque de France, Responsable du pôle risque

SCHLUMBERGER

Ce retour d'expérience porte sur la problématique de l'intégration des Systèmes d'Information (SI).

Les acquis : Une gestion des risques forte et historiquement opérationnelle

Schlumberger est le leader mondial des services d'exploration et de production de l'industrie pétrolière. La dangerosité de son métier et son exposition à des risques spécifiques en dommages, RC et Transport, l'a conduit à mettre en place depuis de nombreuses années une organisation atypique caractérisée par :

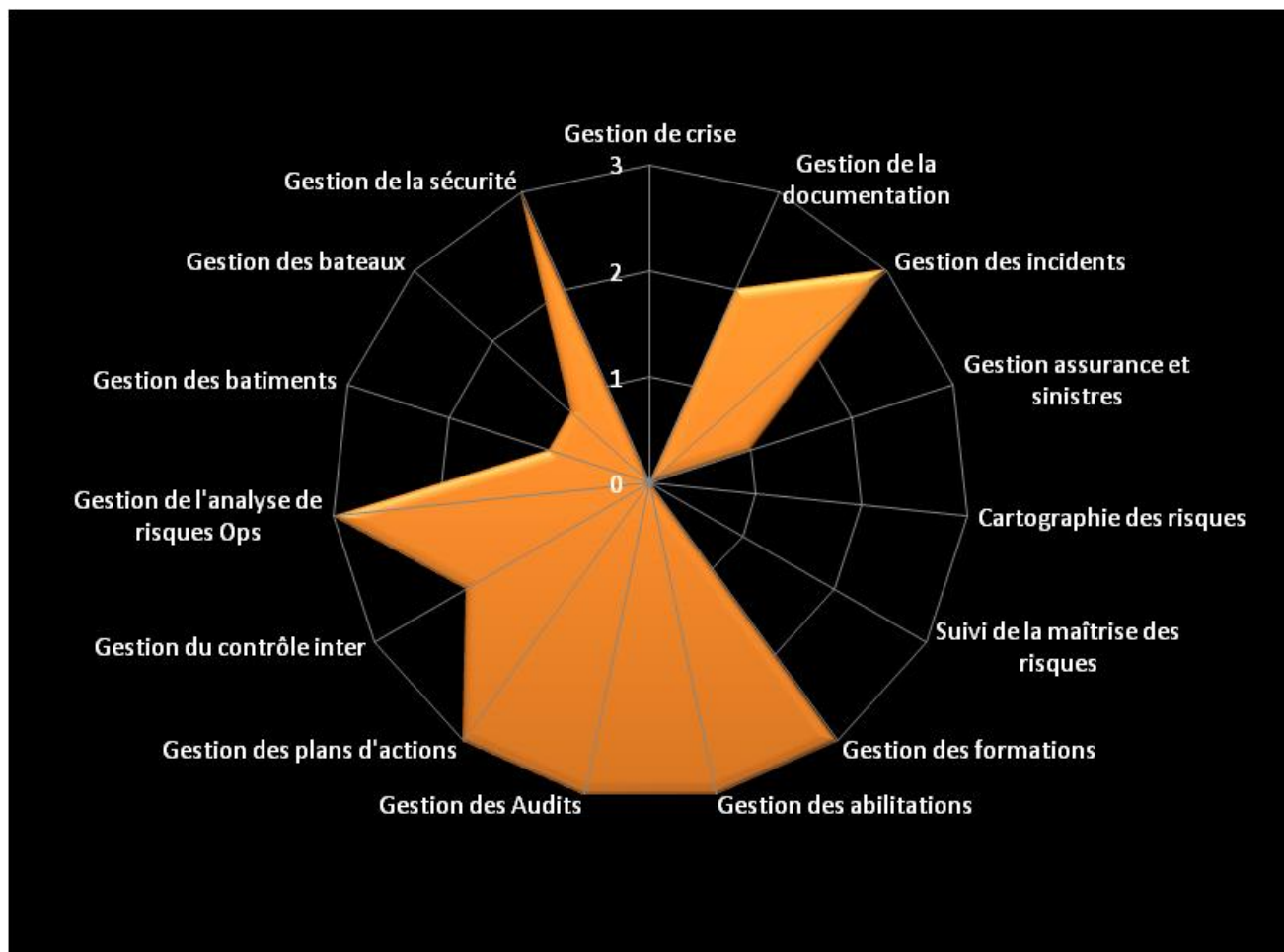
- Une fonction Quality & HSE (santé, sécurité & environnement) comme régulateur des risques opérationnels. Cette fonction est directement rattachée au CEO et ses processus sont intégrés au management du groupe dans le monde entier.
- Un Risk Management corporate centralisé, historiquement axé sur les assurances, et rattaché aujourd'hui à la Finance mais aussi à la fonction Quality & HSE.
- Un fort lien avec le Contrôle Interne (reporting).

Grace à cette organisation, le groupe a acquis une maturité récente au niveau corporate qui se traduit en termes :

- *de documentation* : mise au point de standard BCP (Business continuity Plans), CMP (Crisis Management Plans) et EMP (Emergency Management Plans),
- *d'organisation* : création d'un Comité des risques et d'une CMT (Crisis Management Team),
- *de Risk Mapping* : réalisation d'une première cartographie des risques en 2006,
- *de suivi et traitement des risques* : gestion efficace des plans d'actions pour réduire les risques opérationnels.

Des fonctions variablement couvertes

Schlumberger dispose d'un système d'information centralisé développé en interne à partir de la base « incidents », base de gestion documentaire historique du groupe qui contient plus d'un million d'informations. Ce système d'information appelé QUEST est exclusivement réservé à la gestion des plans d'actions concernant les risques opérationnels. Il est composé des modules de gestion suivants :



QUEST est très puissant. Ainsi :

- Le module de « gestion des incidents » permet aussi bien de gérer les plans d'actions sur des risques avérés que sur des risques potentiels. Il gère aussi les observations qui peuvent conduire à des actions d'amélioration de la qualité opérationnelle du groupe (formation des personnels ou, réaménagement d'un site ou d'une installation...). Cette base ne permet toutefois pas de recherches par processus.
- Le module « gestion de la sécurité », par exemple, contient une base de données sur les risques pays et le risque terroriste et gère les autorisations de déplacement et de séjours de salariés dans plus de 130 pays.
- Le module de « gestion des formations » propose, par exemple, un cours de pilotage d'hélicoptère ou une formation à la sécurité des passagers.

Pour efficace qu'il soit, ce système n'intègre pas des fonctions corporate comme :

- le suivi de la maîtrise des risques,
- la cartographie des risques, la gestion des assurances et des sinistres indemnisés,
- la gestion de la documentation sur les risques,
- la gestion des bateaux, des bâtiments, des équipements sur les puits, ...

Ces différentes fonctions reposent sur des outils bureautiques ou sur des sites web non connectés au SI. Par exemple :

- *Crisis Management* : sharepoint portal
- *Business Continuity Plans* : sharepoint portal
- *Risk Mapping* : Excel spreadsheet

Forces et faiblesses de la situation actuelle

Un système non intégré peut avoir des vertus :

- Souplesse et simplicité d'utilisation,
- Autonomie et rapidité,
- Coût marginal,
- Autorité du top management / culture du résultat

Mais des faiblesses aussi :

- Pas de gestion en mode projet,
- Des besoins insuffisamment définis car la fonction de risk management est encore peu mature,
- Pas d'intégration des systèmes¹,
- Communication insuffisante sur les systèmes non intégrés,
- Output (livrables) décevant sur la forme comparé aux standards du groupe en termes de qualité.

Les trajectoires possibles

A partir de cette situation, quelles sont les évolutions possibles ? Le choix semble devoir se faire entre trois solutions différentes :

- Mettre en place un produit spécialisé intégrant les fonctions Crisis Management, Risk Mapping et Suivi des plans d'actions et l'interfacer avec QUEST. Le problème est alors une perte de cohérence des produits achetés dans la mesure où seules certaines fonctionnalités de ces produits seraient intégrées.
- Intégrer les fonctions manquantes dans QUEST par développement interne. Le problème est ici la disponibilité des équipes.
- Continuer avec les différents modules existant et harmoniser / interfacer quand cela est possible. Mais est-il envisageable d'intégrer une feuille de calcul Excel dans un système de l'envergure de QUEST ?

Pour le moment, ces différentes hypothèses sont toujours en discussion chez Schlumberger.

¹ Dommage de ne pouvoir relier la base « gestion des incidents » à un système de gestion des assurances ou à la cartographie des risques.

BANQUE DE FRANCE (BDF) LE PROJET SIRIS

CONTEXTE

Le contexte macro-économique

La Banque de France a un grand nombre d'activités et, par conséquent, de risques liés à ces activités. Ainsi, la BDF :

- est un fabricant. Elle imprime de la monnaie papier, en concurrence avec les autres banques centrales de la zone euro,
- est garante de la circulation fiduciaire. La BDF assure le recyclage et la destruction des billets usés,
- injecte des liquidités. En tant que banquier de l'Etat, elle est la banque des banques,
- assume des missions régaliennes,
- assure des services au profit de la profession bancaire,
- garantit la sécurité des systèmes de paiement,
- met en œuvre la politique monétaire qui est décidée au niveau du système européen des banques centrales.

Le contexte spécifique

La démarche de risk management de BDF et l'outil utilisé visent à couvrir le risque opérationnel qui, dans le monde bancaire, répond à une définition précise du Comité de Bâle (l'autorité de supervision des banques européennes). Cette définition est la suivante : « Le risque opérationnel est le risque de perte résultant d'une inadéquation ou de la défaillance de systèmes, de procédures ou de personnes, ou résultant d'éléments extérieurs ». Le risque opérationnel bancaire est donc tout sauf les risques financiers (risque de crédit, de liquidité ou le risque de marché).

Lorsque BDF s'est engagé dans le projet, une première génération de SI existait. Il s'agissait d'un outil assez simple que chaque responsable « risque » utilisait sur son PC de manière totalement autonome. Le partage et l'agrégation des informations étaient donc un problème, ce qui explique la demande très forte qui a conduit au projet SIRIS.

L'encadrement du projet

La BDF a été la première banque centrale européenne à initier un projet de système d'information de gestion des risques opérationnels. Lancé dès 2003, ce projet était très encadré :

- Dès l'origine, il y avait une volonté affirmée d'embarquer l'intégralité de la méthodologie de gestion des risques dans l'outil. Tous les éléments référentiels de cette méthodologie (typologie des risques, classification, impacts, etc ...) devaient être intégrés dans l'outil afin d'obtenir une cohérence parfaite des plans d'actions.
- Afin de garantir un environnement technique encadré et commun à tous, BDF impose un partenariat obligatoire avec l'informatique. Au sein de BDF, aucune entité n'a la possibilité de choisir son outil informatique de manière autonome. Toute initiative doit entrer dans un cadre général strictement défini par l'organisation informatique, aussi bien en termes de méthode de conduite de projet qu'en termes d'implémentation de l'outil. Quel que soit le projet SI (comptabilité, finance, politique monétaire, risques), il y a des jalons à respecter, des étapes à franchir, des instances de suivi, de pilotage et de reporting à mettre en place. Ainsi, le projet Siris est-il placé sous la responsabilité de deux chefs de projet, l'un issu de l'organisation informatique, l'autre du pôle « risque ».
- La BDF doit appliquer pour ses projets une procédure d'appel d'offres européen.
- L'approche se faisant dans l'esprit du contrôle interne, sa démarche est très détaillée parce qu'elle implique de nombreux acteurs et objets de risque qui tous doivent trouver leur compte dans l'outil final. Il y a donc de sérieuses contraintes en termes de volumétrie (ce qui exclut les outils bureautiques ou même les bases « access »). C'est pourquoi le projet est géré par une maîtrise d'œuvre centrale œuvrant pour l'ensemble des lignes opérationnelles.
- Enfin, la BDF a évolué en excluant désormais tout développement interne d'un SI et en préconisant le choix d'un progiciel. Cet abandon du « Home made » représente un revirement culturel fort qui n'est pas encore totalement assimilé par les collaborateurs de BDF.

FONCTIONNALITES ATTENDUES

Le cahier des charges de l'outil comprenait plusieurs fonctionnalités majeures. Les principales étaient les suivantes :

- La description de l'arborescence des processus des métiers. L'outil doit être capable de décrire l'ensemble des lignes d'activités opérationnelles de la BDF.
- La description et l'évaluation des risques, des dispositifs de contrôle interne et des plans d'action.
- Le recensement des incidents des métiers.
- L'établissement automatisé de nombreux rapports. Ce point est délicat car il est difficile d'obtenir des éditeurs un outil disposant d'une souplesse graphique répondant aux nombreuses demandes des dirigeants et des lignes opérationnelles destinataires des rapports. Néanmoins, aujourd'hui, l'outil mis en place à la BDF est en mesure d'éditer une soixantaine de rapports différents.
- L'émission et la gestion des questionnaires d'autoévaluation sur des sujets variés et selon différentes périodicités. Cette fonction implique des temps de réponses très bref du système sous peine de démotivation des

correspondants interrogés qui peuvent être plusieurs centaines à se connecter simultanément.

- Le calcul statistique sur les risques opérationnel est désormais imposé par Bâle II aux banques commerciales. Bien que les banques centrales ne soient pas soumises à cette obligation, la BDF a souhaité intégrer le calcul statistique dans son outil. Concrètement, cela veut dire que l'outil dispose d'un moteur qui traite à la fois les populations d'incidents dans le cadre d'une logique actuarielle pour établir des courbes de distribution d'une part, et la cartographie pour simuler l'apparition d'un certains nombre de risques. Toutefois, en raison de sa complexité, cette fonctionnalité est encore en phase expérimentale.

Après l'examen de plusieurs offres, le choix de BDF s'est porté sur la société E-Front qui disposait d'un produit standard appelé Front GRC² qui, après paramétrage pour BDF, a pris en interne le nom de SIRIS (pour système d'information des risques opérationnels).

DIFFICULTES RENCONTREES

... liées au fournisseur :

- A l'origine, la clientèle pour ce type de produits était limitée. Le risque de défaillance du fournisseur était donc réel sur ce micromarché.
- Difficulté de faire respecter par une petite société dont la culture est très éloignée des contraintes d'une exploitation informatique industrialisée, les procédures et les standards de recettes de la BDF.
- Le fournisseur est porteur de risque opérationnel en lui-même (confidentialité des informations confiées³).
- Fournisseur non spécialiste de la gestion du risque opérationnel au sein d'une banque centrale (difficulté de comprendre les besoins et l'environnement métier).

... en interne :

- Les difficultés dans la mise en œuvre du projet avec l'organisation informatique (compréhension du cahier des charges. Exemple : modélisation de données).
- Une culture « Home Made » des domaines opérationnels (tendance à aller au-delà du paramétrage pour réformer le progiciel).
- Le manque de maturité des correspondants (RM) face aux spécificités techniques et fonctionnelles d'un SI (adaptation des besoins aux contraintes du système).
- La reprise de l'existant pose toujours un problème crucial (nettoyage préalable du premier outil pour faciliter la reprise dans le nouvel outil). Sur ce point, la

² GRC : Global Risk Compliance.

³ Sur ce point, les mesures de sécurité d'usage ont été appliquées : clauses de confidentialité annexée au contrat fournisseur, stricte interdiction de tout accès à distance, interdiction absolue de sortir toute information, y compris à des fins de test ou de recette, ...

simultanéité de la méthodologie et de l'implémentation de l'outil est indispensable pour éviter tout décalage.

FACTEURS CLES DU SUCCES

... vis-à-vis du fournisseur :

- Engager un réel partenariat avec son fournisseur et assurer sa promotion en communiquant sur la réalisation du projet pour limiter le risque de défaillance.
- Mise en place de réunions permettant au fournisseur de mieux comprendre le contexte fonctionnel et les besoins du client.
- Mise en place et prise du « leadership » d'un club utilisateurs afin de mieux maîtriser les évolutions d'un produit standard (logiciel).

... vis-à-vis des opérationnels de la BDF :

- « Être dur » sur la reprise de l'existant,
- Veiller à la simultanéité entre le déploiement de l'outil et de la méthodologie.
- Clarté du management quand au choix de la politique de gestion des systèmes d'information (« Home Made » ou Progiciel).
- Mise en place d'un processus itératif à travers des ateliers permettant une meilleure prise en compte des besoins et des changements de la maîtrise d'œuvre vis-à-vis de l'organisation informatique.

POINT DE ROUTE

En 2008, environ un millier de collaborateurs utilise SIRIS. Pour la plupart, il s'agit d'une utilisation occasionnelle (notamment lors de la documentation des questionnaires d'évaluation). Sur l'ensemble de cette population, une soixantaine de collaborateurs ayant des responsabilités au niveau central (pôle risque, contrôle interne) disposent de tous les droits d'accès et utilisent le système quotidiennement.

SIRIS a permis de sortir progressivement d'une logique de conformité pour entrer dans une logique de gestion des risques. Ainsi, grâce à la mise en place des questionnaires d'évaluation, la pertinence et l'efficacité du contrôle interne a été examiné pour la première fois. La question de savoir s'il fallait systématiquement reconduire tous les contrôles s'est posée, ce qui représentait un changement de culture important dans une banque bicentenaire où le réflexe des opérationnels est traditionnellement l'observation scrupuleuse des consignes de sécurité et non leur évaluation.

DALKIA

Un contexte, des spécificités

Division énergie de Veolia Environnement, Dalkia est un groupe de 55 000 personnes implanté dans 38 pays qui a réalisé un chiffre d'affaires d'environ 8 milliards d'euros en 2007. Son métier est l'optimisation des performances techniques, économiques et environnementales d'installations confiées par ses clients (collectivités publiques, entreprises, etc.). A noter que Dalkia est rarement propriétaire des installations sur lesquels le groupe intervient.

Si la démarche de gestion des risques n'est pas une nouveauté pour Dalkia, elle se pratiquait jadis de manière dispersée. Le déploiement d'une filière Risk Management organisée et de ses outils au sein des unités opérationnelles du groupe est apparue comme nécessaire. Au niveau SI, le projet consistait à concevoir un outil central mis à la disposition des différents acteurs (Risk Management Groupe, Risk Managers d'Unités opérationnelles, courtiers, etc) pour instaurer un cadre homogène de gestion des risques, de reporting et de suivi des actions.

Le déploiement de ce projet a démarré en 2005 et le perfectionnement de la démarche et de l'outil centralisé se poursuit aujourd'hui pour finaliser ou améliorer certains modules.

La conduite de cette opération répondait à plusieurs spécificités propres au groupe Dalkia :

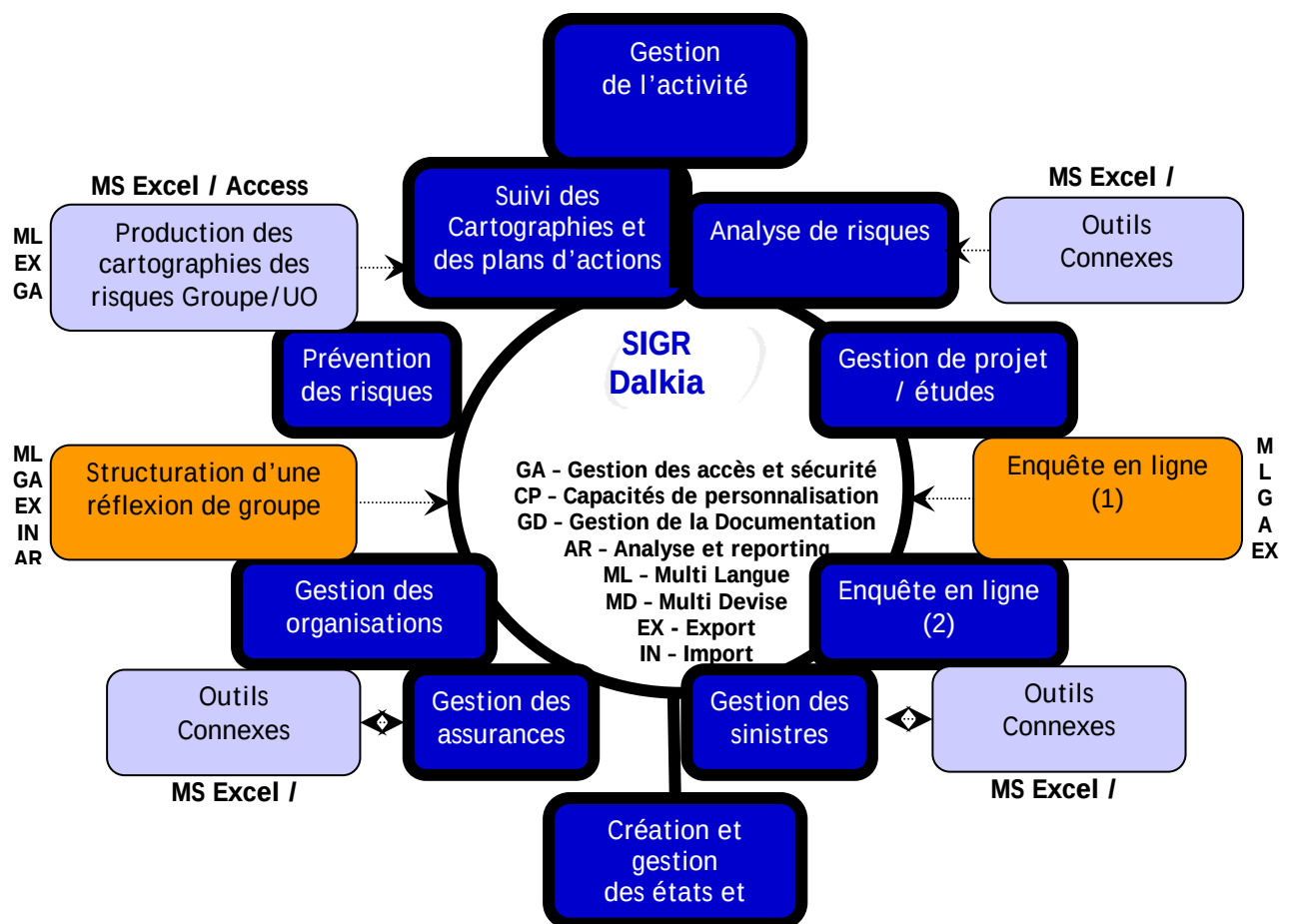
- la reconnaissance de l'importance des outils en tant que support méthodologique et opérationnel de la démarche globale de gestion des risques,
- la volonté de rompre avec des pratiques ne favorisant pas l'agrégation et la communication des données pour se doter d'un outil de gestion centralisateur avec des facilités d'import, complété par des outils connexes de différentes natures,
- le choix de ne pas développer cet outil en interne mais de se procurer un progiciel du marché avec une volonté initiale de rester dans le standard tout en promouvant des capacités d'utilisation maximisées,
- la conscience que le déploiement de l'outil devrait tenir compte de la complexité inhérente au métier et du modèle d'organisation Dalkia,
- la nécessité d'impliquer et de satisfaire une pluralité d'acteurs tant au niveau central que local⁴.
- la décision de favoriser une appropriation de l'outil par ses utilisateurs en réalisant un déploiement en langue locale facilité par des modules d'import de traductions,
- le souci d'intégrer dans les fonctionnalités de l'outil des problématiques locales spécifiques,

⁴ A noter qu'il, s'agit aussi bien d'acteurs internes (correspondant risk management, responsables techniques de centre,, etc) que d'acteurs externes (courtiers groupe ou locaux, autres prestataires).

- la volonté de disposer d'un outil capable de créer les états (reporting, analyse, communication) en interne.

Des fonctionnalités multiples

L'outil est doté de différents modules qu'illustre ce graphique :



Quelques remarques :

- L'outil central ne gère pas tout. Il existe d'autres outils centraux par métiers comme l'outil utilisé par la direction juridique pour suivre les sociétés et participations. Il y a donc nécessité de pouvoir communiquer avec ces outils. Par ailleurs, il y a parfois un déficit d'outil centralisateur. Par exemple, bien que les missions de Dalkia concernent plus de 1200 000 installations dans le monde, il n'existe pas aujourd'hui d'outil centralisé permettant de réaliser l'inventaire exhaustif de ces sites sur la base des critères discriminant du risk

management. Cet inventaire est fait séparément pour certains pays sur des outils locaux. La capacité d'importer des données produites sur d'autres outils dans le système d'information de gestion des risques est donc une commodité indispensable.

- L'outil central dialogue avec des *outils connexes* propres à la filière Risk Management (production des cartographies des risques, outil de structuration d'une réflexion de groupe utilisé pour animer des séminaires ou des sessions de formation interne, outil permettant de réaliser des enquêtes en ligne : questionnaires d'évaluation, remontée d'informations).
- *Gestion des assurances* : ce module permet d'avoir une vue globale ou locale des assurances du groupe. Il permet notamment de gérer et suivre les parcs et valeurs, les primes et leur historique, les programmes mondiaux et les polices locales,
- *Gestion des sinistres* : module où sont répertoriés et instruits les sinistres déclarés ou non. En revanche, les incidents sont gérés par les outils dédiés à l'exploitation et à la maintenance.
- *Gestion de projet/études* : ce module permettra de suivre les études sur des projets de contrats ou d'acquisitions. Y seront réunies les nécessaires à pour réaliser l'étude. En cas de concrétisation, l'étude est alors transférée dans le module gestion des organisations et/ou gestion des assurances.
- *Analyse de risques* : ce module permet de faire le point sur une activité, une entité, ou une installation en termes de gestion des risques (modèles de contrats utilisés, typologie des engagements, ...).
- *Suivi des cartographies et des plans d'actions* : dissociation volontaire de la phase de production d'une cartographie (au niveau du groupe et au niveau Unité Opérationnelle) de la phase d'historisation et de suivi des plans d'actions. Seule les cartographies validées sont intégrées dans l'outil qui prend en charge le suivi des plans d'actions.
- *Gestion de l'activité* : module en cours d'amélioration afin de remplir sa fonction de support de l'activité.

Forces et faiblesses du système

Les forces sont nombreuses mais certaines ont aussi leur revers. Dans ce registre, on peut mentionner :

- Un déploiement synchronisé de l'organisation et des outils Risk Management (*versus* – un degré de maturité inégal des correspondants qui vivent parfois difficilement les délais qu'impose cette démarche).
- Un déploiement d'outils de gestion incluant le reporting (*versus* - relégué au second plan, le reporting doit néanmoins être fait, ce qui pose un problème de disponibilité et de moyens).
- Une forte maîtrise interne des outils, permettant une réactivité optimale.
- Une vision prospective et extensive des objectifs dès le début du projet
- Une vision industrialisée intégrant les besoins de tous les utilisateurs en amont.

- Utilisation d'outils connexes, développés en interne, comme laboratoire d'idées intégrables à terme dans l'outil centralisateur.
- De réels partenariats avec les fournisseurs.
- Des moyens en interne pour gérer et suivre le projet dans toutes ses phases (*versus* – Ces moyens peuvent être réduits).

D'incontestables faiblesses ont affectée le déploiement du projet :

- Difficultés techniques, notamment problèmes importants d'accès réseau lors du lancement du nouveau SIGR (avec pour conséquence l'utilisation de l'outil en mode dégradé pendant un an et des retards dans son déploiement).
- Intégration encore trop faible avec les autres systèmes Groupes.
- Une connotation "France" encore trop marquée sur certains sujets (en cours de correction grâce à une implication croissante des risk managers d'unités opérationnelles).
- Un vrai challenge pour gagner durablement l'adhésion de tous les acteurs (il faut convaincre de l'intérêt de l'outil).

Aujourd'hui ? Demain ?

Les objectifs sont les suivants :

- Densifier la communication notamment sur les résultats obtenus au moyen du système d'information de gestion des risques.
- Améliorer l'ergonomie en développant des assistants spécifiques centrés sur un processus (déclaration de sinistres par exemple).
- Interfaçage avec les outils Groupes.
- Etendre le périmètre traité par le système d'information (suivi des plans d'actions issus des cartographies, gestion du risque automobile, ...) en intégrant dans l'outil tous les processus Risk Management.
- Impliquer les risk managers d'unités opérationnelles dans la vie de l'outil (Définition commune des besoins et cahier des charges pour les développements futurs, internalisation de certains outils développés en local, ...).
- Animer la communauté des utilisateurs (L'inégale maturité et la diversité des profils utilisateurs nécessite une gestion rigoureuse des besoins mais est aussi un facteur de progrès qui repose sur le partage des idées et des bonnes pratiques).