COMMUNIQUE DE PRESSE

Les systèmes d'information restent insuffisamment pris en compte dans la démarche de *risk management* des entreprises françaises

Une enquête Mazars, « Audit des risques liés aux systèmes d'information : quelles pratiques au sein des entreprises françaises ? »

Après son enquête sur la gestion des risques en 2007, et la mise en évidence de l'importance qu'attachent les entreprises au contrôle de leurs systèmes d'information, Mazars a souhaité aller plus loin, et comprendre comment, et par qui, est appréhendée la gestion des risques informatiques.

En effet, au-delà des seules considérations techniques (sécurité des systèmes d'information, disponibilité des données, procédures de confidentialité etc.), les contraintes réglementaires imposent aux entreprises de maîtriser leur système d'information.

La maîtrise des SI sort donc aujourd'hui du seul domaine – technique – des Directions des Systèmes d'Information (DSI), et entre désormais dans celui du contrôle interne.

Pour comprendre la place actuelle de la maîtrise des risques liés aux systèmes d'information, une enquête a été menée auprès de 134 organisations afin de comprendre de quelle manière se sont structurées les entreprises en termes de contrôle des systèmes d'information et quelle place elles accordent à l'audit de ces derniers : le plan d'audit couvre-t-il les risques informatiques de façon suffisante ? Les entreprises disposent-elles en interne des ressources nécessaires ? Et dans l'affirmative quelles sont elles ? Autant de questions auxquelles l'enquête tente, entre autres, de répondre.

« *Cette enquête fait ressortir que la notion d'audit informatique est parfaitement identifiée et utilisée dans les entreprises qui intègrent ce sujet à leur plan d'audit, ou plus généralement à leur stratégie de contrôle dans plus de 60 % des cas. Pourtant la gestion du risque global lié aux systèmes d'information reste assez souvent confiée aux DSI, et aux directions qui les utilisent* » explique **Olivier Lenel, associé de la ligne de métier Management du Contrôle interne de Mazars**. « *Ce rattachement technique aux DSI – s'il semble paradoxal compte tenu des enjeux liés à la maîtrise du SI, s'explique probablement par le fait que la fonction d'audit interne des SI est encore jeune, et est en général constituée d'effectifs réduits : seules 18% des entreprises ont des effectifs dédiés à l'audit des SI, leur existence remonte à moins de 6 ans, et 80 % des équipes sont composées de moins de 4 personnes !* ».

« *L'enquête, si elle démontre une réelle sensibilité de l'entreprise aux questions de la maîtrise des risques relatifs aux systèmes d'information, confirme aussi assez largement le manque de moyens engagés pour donner aux dirigeants et administrateurs une assurance raisonnable quant à la maîtrise de ce risque global* »**, ajoute François Nogaret, associé de la ligne de métier Management du Contrôle interne de Mazars**.

A RETENIR

Les domaines clés de l'audit interne des SI

- Sécurité physique et logique
- Architecture des systèmes d'information
- Examen critique des processus informatiques
- Analyse de l'organisation de la fonction informatique
- Conformité réglementaire (Bâle II, SOX, Cnil, Solvency II, archivage fiscal, traçabilité, …) ou aux règles internes
- Evaluation des plans de secours
- Lutte contre la fraude
- Revue des projets informatiques transverses
- Analyse de données
- Analyse de migrations de systèmes

↳ L'audit des systèmes d'information – pierre angulaire de l'audit interne – couvre un champ d'investigation très large, et requiert des compétences spécifiques et très diversifiées. Conscientes du caractère stratégique de l'audit des SI, les entreprises, ne disposant pas de ressources dédiées suffisantes, recourent très souvent à des prestataires externes à même d'émettre une opinion sur la qualité et la maîtrise des risques de leur système d'information.

Principaux enseignements de l'enquête

- **Des entreprises inégalement soumises à une réglementation contraignante**

Les entreprises interrogées sont **à 34% soumises à une réglementation spécifique en matière de contrôle interne** (Bâle 2, Solvency 2, Sarbanes Oxley, etc.). Ces contraintes réglementaires concernent naturellement au premier chef les entreprises du secteur banque/assurance.

- **Des entreprises plutôt sensibles à la maîtrise des risques**

Les entreprises interrogées sont à **29% fortement sensibilisées** au sujet de la maîtrise des risques, et à **59% moyennement sensibilisées**. Par ailleurs, **61% des entreprises interrogées ont engagé une démarche de cartographie des risques.**

- **62% des entreprises interrogées intègrent un département d'audit interne**

La taille de l'entreprise conditionne nettement la création d'une fonction d'audit interne, avec un palier à 400M€ de chiffre d'affaires, seuil au-delà duquel cette fonction est quasiment systématiquement représentée. L'enquête démontre que les départements d'audit interne ont une vocation systématiquement généraliste, et, 61% d'entre eux ne disposent que d'un effectif inférieur ou égal à 5 auditeurs.

- **Une sensibilité avérée aux risques liés aux systèmes d'information…**

35% des entreprises perçoivent une forte exposition (et 47% une exposition modérée) aux risques liés aux systèmes d'information.

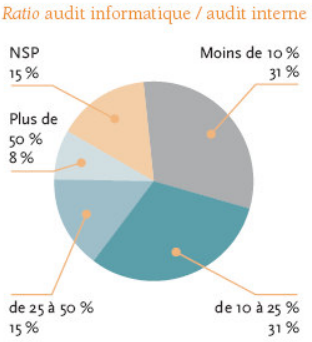
- **… mais une prise en compte inégale de l'informatique dans les plans d'audit**

38% des entreprises ne mettent pas en œuvre d'audit des systèmes d'information.

Parmi les freins à l'utilisation de ce type d'expertise mis en avant par les entreprises, on compte :

- la rareté des compétences d'auditeur des systèmes d'information au sein de l'entreprise
- la difficulté à convertir un objectif d'audit classique en objectif d'audit informatique
- l'ignorance que certains pans d'une mission d'audit peuvent être totalement délégués, ou dévolus, à des auditeurs des systèmes d'information.

La charge relative impartie aux systèmes d'information au cours des missions d'audit reste assez limitée :



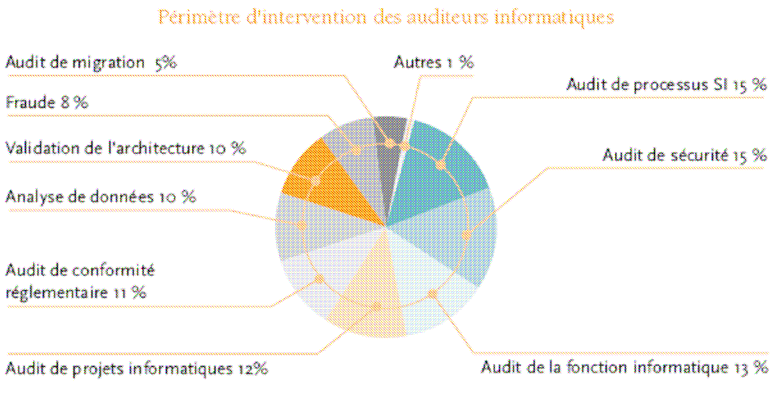
- **Auditeurs internes des systèmes d'information : une fonction en devenir ?**

Seulement 18% des entreprises ont choisi de mobiliser des effectifs dédiés à l'audit des systèmes d'information.

L'existence récente de cette fonction dans l'entreprise (moins de 6 ans en général) et **son effectif limité** (80 % des équipes sont composées de moins de 4 personnes), peuvent expliquer en partie son rôle encore restreint, et son rattachement parfois technique aux Directions des Systèmes d'Information.

Quant à la question de **l'autonomie** des auditeurs des systèmes d'information dans l'exercice de leur mission, elle semble a priori limitée. Plus de deux tiers des entreprises rattachent en effet systématiquement l'audit informatique à des missions d'audit plus larges.

Les compétences des auditeurs des systèmes d'information sont utilisées sur des sujets variés et les entreprises se focalisent manifestement plus sur l'audit ***des*** systèmes d'information que sur l'audit ***par*** les systèmes d'information.



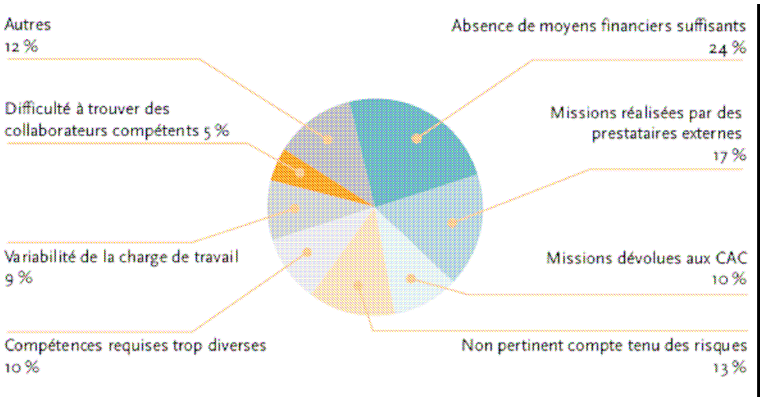
Le nombre annuel de missions d'audit de systèmes d'information reste faible (dans près de 70 % des cas le nombre des missions d'audit informatique réalisées sur un an est inférieur à 5). Cette situation ne contribue pas à faciliter la capitalisation et l'industrialisation du métier.

Les travaux des auditeurs des systèmes d'information intéressent un public assez large, et au premier chef le top management (Direction Générale, Comité d'audit, Direction de l'audit interne).

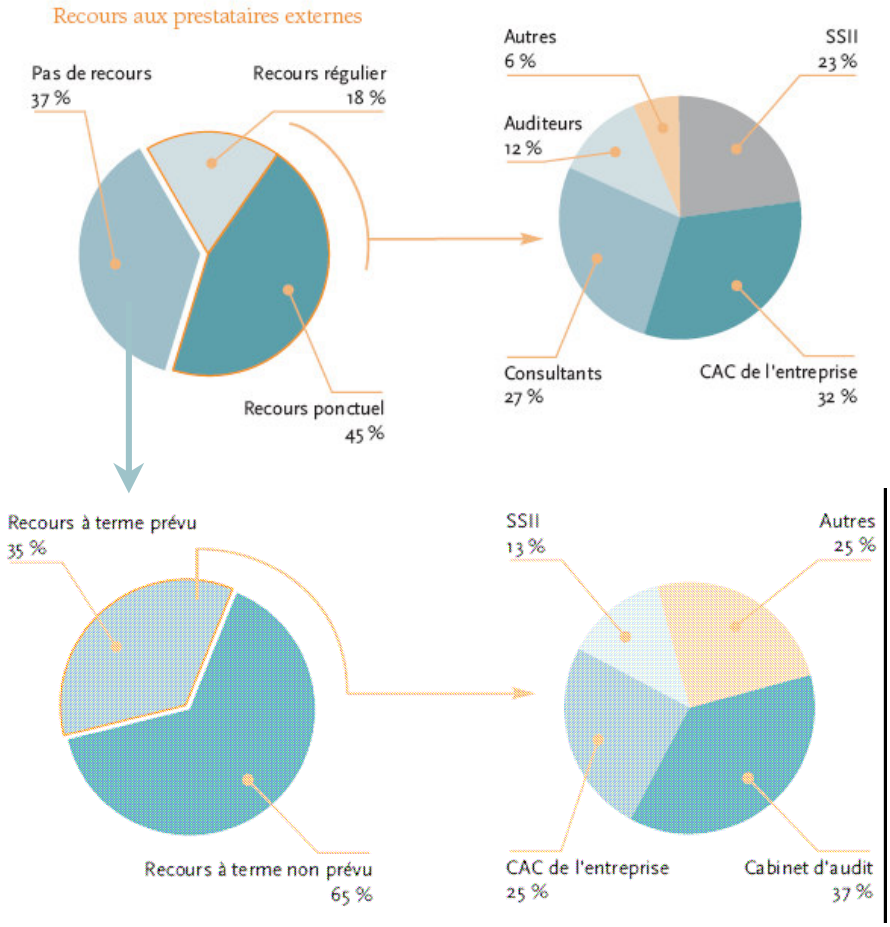
- **82% des entreprises ont fait le choix de ne pas avoir d'auditeurs dédiés aux systèmes d'information**

Pourquoi ?

La première raison semble triviale, mais c'est une réalité : parce que le coût est trop important. La deuxième, c'est que des prestataires externes en sont chargés, et que les bénéfices attendus de ce type de prestations semblent trop faibles face à l'investissement qu'elles nécessitent, si on souhaite les réaliser en interne.



Les entreprises qui n'ont, à l'heure actuelle, pas d'auditeurs des systèmes d'information dédiés ne prévoient pas de créer cette fonction dans 65% des cas. Ceci est caractéristique d'une demande d'expertise soit ponctuelle, soit très diversifiée et spécialisée, pour laquelle on préfère faire appel, chaque fois que nécessaire, à des ressources (ou à des prestations) externes.



Le **recours à des prestataires externes** répond à un besoin précis et immédiat. Il s'agit d'une attitude réactive, bien plus que préventive, face à d'éventuels risques liés aux systèmes d'information. Ainsi, il semblerait que dans la grande majorité des cas, il n'y ait pas de programmes d'audit spécifiques dans ce domaine ; la mise à disposition de ressources internes dédiées n'est donc pas justifiée.

Le recours à des prestataires externes se traduit indifféremment par une externalisation totale des travaux ou, de façon moins tranchée, par un apport technique aux équipes d'auditeurs internes.

Ces travaux « à la demande » auprès de prestataires externes couvrent principalement des prestations de trois natures distinctes :

- la validation de l'architecture des systèmes ;
- la validation de la sécurité logique ;
- la validation du plan de continuité.

Pour mieux interpréter cette situation, le recours à des prestataires externes, en dehors des commissaires aux comptes, semble être effectué chaque fois qu'une mutation importante intervient dans les systèmes d'information et que l'opinion d'un tiers apparaît indispensable

A propos de Mazars

Mazars est une organisation internationale spécialisée dans l'audit, l'expertise comptable, la fiscalité et le conseil aux entreprises. Son partnership intégré rassemble plus de 8 000 professionnels dans 46 pays. De plus, grâce à l'Alliance internationale Praxity dont il est membre fondateur, le groupe a accès aux compétences de 15 000 professionnels supplémentaires, dans 27 autres pays, tous unis par la même exigence de qualité et une détermination commune à aller au-delà des standards techniques et éthiques en vigueur. Mazars s'impose ainsi comme un véritable challenger international capable de proposer, grâce à son organisation multiculturelle et sa gamme complète de services, des solutions souples et sur mesure aux grandes sociétés internationales et aux PME qu'il accompagne dans leur développement.

www.mazars.com et www.mazars.fr

La ligne de métier **Management du Contrôle Interne** de Mazars se positionne comme le partenaire des entreprises dans la maîtrise globale de leurs risques. Ses équipes expertes et pluridisciplinaires s'attachent à construire pour chaque entreprise une solution durable et sur mesure. Elles conseillent et accompagnent les entreprises, dans la mise en place et l'optimisation de leur contrôle interne, de leur gouvernance, de la prévention contre la fraude, et de la maîtrise des risques liés aux systèmes d'information.