Les ateliers Risques de l'EIFR

1- Gouvernance de l'information

20 janvier 2015 - Avec Atos Consulting et RSD

I- Contexte : une multitude de régulations impactant in fine les données elles-mêmes

Les entreprises du secteur financier sont soumises à une série d'obligations légales et réglementaires de mise en œuvre d'un cadre robuste de gouvernance de l'information. Outre la réglementation relative à la protection des données personnelles s'appliquant à toute entreprise, de nombreuses règles financières nationales, européennes ou étrangères exigent en effet une conservation organisée de divers types de données, parmi lesquelles : les Directives MIF (I et II) qui prévoient la conservation pendant une durée de 5 ans des données relatives aux transactions financières et au cadre de réalisation de celles-ci afin de pouvoir démontrer une pratique de bonne exécution ; les directives bâloises qui imposent la conservation des données sur les transactions financières et les risques pendant une période définie, avec une obligation renforcée dans le cas d'une utilisation de modèles internes ; les standards de sécurité de l'information dans l'industrie des paiements qui obligent les émetteurs de cartes à conserver un historique de la piste d'audit pendant une période cohérente avec la durée d'utilisation ; mais aussi les lois américaines Bank Secrecy, Dodd-Franck ou Sarbanes-Oxley qui obligent les entreprises ayant des activités ou une cotation aux Etats-Unis à maintenir un enregistrement de différents types de transactions.

La protection des données personnelles constitue assurément un domaine d'attention et de contrainte particulière dans un secteur fortement utilisateur d'informations nominatives. Le principe général établissant que ces données ne peuvent être détenues que pendant une durée justifiée par rapport à leur utilisation vient parfois en opposition avec certaines obligations de conservation des données, comme dans le cadre de MiFID (données personnelles clients à conserver pour la démonstration de la meilleure exécution mais à effacer à la demande ou si la nécessité n'est plus clairement établie) ou encore celui de la titrisation (difficulté à constituer des bases de données historiques de défaut si le droit à l'oubli conduit à effacer des informations sur la défaillance d'entreprises). L'année 2015 apportera dans ce domaine une actualité très forte avec un nouveau règlement européen renforçant notamment le droit à l'oubli et les sanctions en cas de dispositif de conservation insuffisant, et avec en France la Loi Numérique en début d'année.

II- Enjeux : un degré de risques et de complexités certain

En toute hypothèse, un établissement financier ne peut plus se reposer sur une conservation systématique de l'information pour une donnée indéterminée. La conformité aux règles de conservation des données constitue pour tout établissement une problématique complexe nécessitant une bonne appréhension d'enjeux de natures différentes : enjeux réglementaires globaux mais également locaux ; enjeux organisationnels, avec un volume d'information important et croissant, des utilisateurs nombreux et une organisation en silos (métiers, géographie) ; et enfin enjeux techniques, dans un contexte de diversité de supports et de variété de solutions de stockage.

III- Une gouvernance spécifique s'impose

La gouvernance de l'information vise à s'assurer de la conformité des dispositifs de gestion et de conservation des données, quel que soit le support utilisé (fichiers, enregistrements, messagerie, données physiques), aux exigences réglementaires générales et locales, au travers d'outils, politiques, procédures, processus et bien sûr de contrôles. Il s'agit en pratique de définir précisément le domaine respectif de **responsabilité des nombreuses parties prenantes** à cette matière (responsables métiers, filières conformité et juridique, direction informatique, …), et de garantir la mise en œuvre cohérente de bonnes pratiques adaptées. A chaque acteur de la gouvernance de l'information son rôle qui peut se trouver synthétisé dans un **workflow simple** : la Conformité en lien avec le Juridique va définir et

faire évoluer les politiques générales à décliner localement, les Records managers au sein des métiers vont déployer la gestion du calendrier de rétention de l'information, l'IT va appliquer ces politiques sur l'ensemble des entrepôts de données, et les Business managers au sein des métiers auront ainsi un accès sécurisé à l'information.

Le programme de gouvernance de l'information dans une entreprise visera **à aligner la valeur de l'information** (qui constitue globalement un actif de l'entreprise, même si la question de la propriété juridique effective de l'information personnelle est complexe), **les risques** (au travers notamment d'un recours plus ou moins important un dispositif de Cloud) et **les coûts de traitement**, **avec les objectifs de l'établissement**, et devra préciser pour chaque catégorie d'information les règles de conservation, de partage interne, de gestion des accès et de sécurité, et de traçabilité d'utilisation.

- ➔ **Plusieurs défis d'envergure sont à surmonter**, comme la nécessité d'avoir une vision globale des traitements et de systèmes de conservation résultant souvent d'évolutions historiques de restructurations ou d'acquisitions, la définition de règle d'archivage selon le domaine d'application, l'interface avec les applicatifs métiers, …

Le dispositif de gouvernance de l'information trouvera avantage à reposer sur une seule plateforme centrale permettant la diffusion des règles et politiques internes vers les différentes solutions de conservation (disques partagés, solutions d'ECM, ou archives physiques), et s'appuyant sur les systèmes IT existants. Même si toutes les fonctions de l'entreprise sont concernées, le sponsor de cette plateforme sera typiquement celui qui aura ultimement à répondre d'éventuelles irrégularités ou de dysfonctionnements dans le dispositif, c'est-à-dire le responsable de la conformité. Dans certains groupes, une fonction spécifique nouvelle a cependant été mise en place, celle de **Chief Data Officer** garant du respect des obligations réglementaires ainsi que de la sécurité de l'information.

De tels outils de type plateforme centralisée pour la gouvernance des informations s'imposent et existent. Ils peuvent permettre, sans manipulation des données métiers, une gestion complète des règles issues de la politique de conservation des informations de l'entreprise sur la base des lois en vigueur, leur application selon les lignes de métier dans les systèmes en place, et l'obtention d'indicateurs de performance et de risques (rapports de contrôle et d'audits, tableaux de bord).

Dans cette matière, comme classiquement dans les domaines des risques ou de la conformité, une **cartographie des informations, des traitements et des systèmes, de même que le recensement des règles générales et locales applicables, constituent un préalable** à la démarche de bonne gouvernance. L'objectif ultime est de **coupler une donnée et une règle** (d'accès, d'utilisation, de conservation et d'archivage), en intégrant bien sûr la modularité nécessaire pour tenir compte de situations opérationnelles particulières telles que le gel de la suppression de données si une situation de litige conduit à devoir conserver des données plus longtemps que normalement prévu. L'avènement de l'ère du «Big data » ne modifie pas substantiellement la nature de cette problématique, même s'il met en lumière la masse d'informations à prendre en compte, particulièrement dans le domaine financier.

De façon générale, tout établissement a intérêt à une démarche proactive dans le domaine de la gestion des données, pour se prémunir d'irrégularités opérationnelles comme de sanctions éventuelles en cas de contrôles de régulateurs ou de plaintes de particuliers pouvant s'estimer malmenés par une utilisation indue des données les concernant. La protection des données personnelles ne constitue toutefois qu'un aspect de cette problématique bien plus large de gouvernance de l'information, qui mêle des considérations de respect de règles, de gestion de coûts

(on estime que près de 30 % des données détenues par les entreprises seraient inutiles car périmées ou en doublon, ce qui conduit à des coûts de conservation en moyens physiques et humains largement indus) et aussi d'efficacité opérationnelle. Une démarche de mise en place d'une gouvernance de l'information peut ainsi conforter tant la sécurité réglementaire que la rentabilité et l'efficience globale de l'entreprise.