Les nouvelles pratiques de la gouvernance informatique

La loi Sarbanes-Oxley (SOX) votée par le Congrès américain au mois de juillet 2002 pour répondre aux scandales Enron et Worldcom pose essentiellement trois grands principes : l'exactitude et l'accessibilité de l'information ; la responsabilité pénale des gestionnaires ; l'indépendance des auditeurs (voir à ce sujet : www.sarbanes-oxley.com).

En France, la Loi de Sécurité Financière (Loi n°2003-706 du 1er août 2003, J.O. du 2 août 2003), dont le périmètre est plus large que la SOX, a également pour objectif de limiter les catastrophes financières en accroissant la responsabilité des dirigeants et en renforçant le contrôle interne.

Les implications de la SOX

L'article 404 de la SOX, intitulé "Management assessment of internal control" exige, pour les entreprises cotées aux Etats-Unis, la mise en place d'un contrôle interne efficace sur le reporting financier. Un rapport sur le contrôle interne exercé sur le reporting financier doit être déposé par chaque société cotée auprès de la SEC (Commission américaine des opérations de bourse). Les exigences de la SOX et ses implications s'étendent à toute société française qui serait cotée aux Etats-Unis et à toute filiale française d'une société américaine cotée aux Etats-Unis.

Ces nouvelles contraintes obligent à : l'auto-évaluation des contrôles internes ; la mise en place de procédures de reporting financier ; la traçabilité de tous les mouvements financiers. Cette nécessité d'un contrôle interne efficace du reporting financier impose donc de contrôler également le système d'information de l'entreprise. L'entreprise et notamment le Directeur des Systèmes d'Information (DSI), disposent d'un modèle de référence en matière d'audit et de maîtrise des systèmes d'information, la norme COBIT (Control Objectives for Business and related Technology), qui s'inscrit dans la lignée des nouvelles pratiques de la gouvernance informatique.

Ces "bonnes pratiques" sont proposées par l'IT Governance Institute (voir http://www.itgi.org) pour permettre à l'entreprise de mieux gérer les risques liés à l'informatique, en tenant compte notamment des contraintes liées à la mise en œuvre des dispositions des articles 302 et 404 de la loi Sarbanes-Oxley. La première édition de cette norme date de 1996 et a été créée par l'association ISACA (Information Systems Audit and Control Association). L'IT Governance Institute a été créé par l'ISACA en 1998, afin de promouvoir la mise en place de normes de direction et de contrôle de la tech-

Benoît de Roquefeuil
Avocat - Directeur
du département de gestion
Alain Bensoussan Avocats

La loi Sarbanes-Oxley a modifié les règles de gouvernance des sociétés cotées notamment en ce qui concerne la gestion de leurs données financières. Elle oblige ces sociétés à appliquer des règles strictes de gouvernance sur leurs systèmes d'information.

CV Benoît de ROQUEFEUIL

Avocat à la Cour d'appel de Paris, il a rejoint le Cabinet Alain BENSOUSSAN en 1991 où il dirige le département "contentieux informatique" spécialisé dans l'évaluation des risques projets, le suivi des situations pré-contentieuses et la gestion judiciaire et extra-judiciaire d'actions contentieuses.
Il est auteur de nombreux articles traitant de l'actualité du droit des nouvelles technologies dont notamment certains relatifs aux logiciels libres, aux jeux vidéo ou encore sur les mesures de protection des oeuvres numériques.

nologie de l'information des entreprises. Une régie de "Technologies de l'information" (TI) efficace aide les entreprises à atteindre leurs objectifs, à maximiser leur investissement dans les TI et à en gérer les risques et les possibilités. De nombreuses entreprises utilisent la norme CobiT pour l'audit de leur système d'information. Suite aux exigences de la SOX, l'IT Governance

Les normes constituent un facteur de progrès considérable.

Institute a lancé en 2004 une version interactive de CobiT en ligne qui regroupe plus de 300 objectifs détaillés pour la gouvernance des technologies de l'information. Un Institut français pour la Gouvernance du Système d'information a été créé en janvier 2004 (IGSI) afin de promouvoir cette méthode auprès des DSI et des auditeurs informatiques.Le Directeur des Systèmes d'Information joue un rôle fondamental dans ce processus de mise en conformité des systèmes d'information. C'est lui qui doit en garantir la sécurité et les contrôles. Ces derniers portent sur : la gestion électronique et l'archivage des documents ou des courriers électroniques ; l'amélioration des systèmes financiers et la conduite du changement ; la sécurité des bases de données et des réseaux.

COBIT, un référentiel de gouvernance

COBIT définit un ensemble de bonnes pratiques pour mesurer l'efficacité des systèmes d'information au regard des objectifs de l'entreprise et des risques technologiques associés. L'intégration des outils de mesure COBIT dans le contrôle de pertinence des approvisionnements, le contrôle de conformité des fournitures (matérielles ou intellectuelles) et l'analyse des qualités de service présentent en effet un double avantage. En premier lieu, COBIT permet d'optimiser et d'harmoniser les processus de mesure de la conformité pour toute évolution des systèmes d'information. En second lieu, l'adoption des systèmes d'évaluation COBIT autour des 34 processus d'évaluation liés aux technologies de l'information confère également une "lisibilité" à l'entreprise, en vue d'éventuels audits auxquels elle pourrait être soumise. La difficulté réside principalement dans le fait que l'adoption des normes COBIT suppose l'adhésion en parallèle à un processus qualitatif contraignant et le recours à d'autres processus normatifs qui sont fortement structurants pour l'entreprise, ce qui implique une conduite du changement de grande envergure.

Par ailleurs, il est possible que, dans certaines organisations, l'utilisation des modèles de gouvernance COBIT pour le contrôle des systèmes d'informations induise des exigences de normalisation à la charge des fournisseurs de l'entreprise. Ainsi, pour l'acquisition et/ou la mise en œuvre de logiciels ou de progiciels, il pourrait être exigé que ces produits aient été développés suivant des normes de type CMMI (ou unified process) qui correspondent à autant de modèles ou référentiels de processus de production logicielle. De même, pour les services, les règles de gouvernance COBIT pourraient conduire à exiger des prestataires qu'ils respectent les processus de production des services informatiques définis par les "bonnes pratiques" ITIL (Information Technology Infrastructure Librairy) qui sont associées aux normes (processus de certification BS15000 ET BD0005) du British Standard Institute. Enfin, la gouvernance COBIT peut encore induire l'exigence du respect de normes de gestion de projet, telles que notamment PMI ou PRINCE2. Une telle exigence de normalisation transverse permet sans doute de faciliter les convergences entre les processus des organisations amenées à travailler ensemble, pour des périodes plus ou moins longues, sur des opérations concernant les systèmes d'informations (contrat d'externalisation, d'intégration de systèmes, de tierce maintenance applicative...). De ce fait, le recours à des "bonnes pratiques" communes est de nature à optimiser la sécurité et la conformité.

Pour autant, il est nécessaire de prêter attention à ce que l'optimisation de la sécurité par le recours à des processus normés ne soit pas un facteur de rigidité trop important qui pourrait priver l'entreprise de la possibilité d'avoir recours à des produits ou services dont la conception et l'exécution ne seraient pas certifiées suivant les normes et les règles jugées compatibles par les règles de gouvernance adoptées en interne.

Les normes sont donc de plus en plus précises et efficaces et constituent un facteur de progrès considérable, notamment en termes de mesure de la conformité, mais elles doivent cependant être implémentées et appliquées avec discernement. Ainsi, il conviendra de veiller à ce que, à périmètre qualitatif égal, les normes régissant les processus de production et/ou d'organisation des fournisseurs de services soient substituables les unes aux autres, afin d'éviter un appauvrissement de l'offre concurrentielle d'une part, et que s'impose un standard unique d'autre part.

Information & Systèmes accueille
des opinions d'auteurs qui n'engagent pas sa rédaction.