La mise en conformité avec une loi étrangère : le cas de l'application de la loi Sarbanes-Oxley par la direction des systèmes d'information d'une PME française cotée au New York Stock Exchange

Par Randa BEN ROMDHANE
Enseignant-chercheur à l'ISC Paris Business School
et Éric FIMBEL
Professeur à NEOMA Business School

La loi Sarbanes-Oxley (abrégée en Sox), en vigueur aux États-Unis depuis 2002, fait l'objet de nombreuses controverses depuis plus d'une dizaine d'années. Plusieurs des effets et des conséquences de cette loi ont été identifiés par la littérature. Toutefois, ses effets et ses conséquences au niveau des directions des systèmes d'information (DSI) des petites et moyennes entreprises n'ont pas encore été mis en évidence. Cet article a pour objet de comprendre ces effets à travers l'étude du cas de la DSI d'une PME française cotée au New York Stock Exchange (NYSE). Les résultats de notre analyse nous ont permis d'identifier quatre types de difficulté : des difficultés organisationnelles, techniques, économiques et culturelles.

Introduction

La loi Sarbanes-Oxley a été adoptée aux États-Unis en 2002 en réaction à plusieurs scandales comptables et financiers (en particulier à celui d'Enron). L'adoption de cette loi avait pour intention affichée de protéger les actionnaires et de rétablir la confiance du public. Elle se caractérise par son application extraterritoriale : ses dispositions s'étendent à toute entreprise même non américaine cotée aux États-Unis (COLLARD et *al.*, 2011). Elle impose à toute société cotée aux États-Unis que ses dirigeants évaluent l'efficacité de leur système de contrôle interne, les rendant, par ailleurs, responsables de sa mise en place et de son maintien à niveau.

La loi Sarbanes-Oxley (souvent abrégée en Sox ou Sarbox) implique plusieurs obligations de conformité qui impactent plusieurs fonctions de l'entreprise, en particulier sa direction des systèmes d'information (DSI), qui est responsable du niveau de sécurité et d'exactitude des données. Dans les grandes structures, la déclinaison de la politique de conformité à cette loi au niveau de leur DSI (qui englobe toutes les réglementations y compris la Sox) requiert des moyens financiers et humains assez importants. Toutefois, dans les PME concernées par cette loi, les DSI ne disposent pas des mêmes capacités que leurs homologues des grandes entreprises pour assurer la mise en place et la mise à niveau de telles exigences (MICHELSON et *al.*, 2009 ; WALLACE et *al.*, 2011).

Ce constat nous amène à formuler la question de recherche suivante : « Quelles difficultés les DSI des PME éprouvent-elles au regard de leur mise en conformité avec la loi Sarbanes-Oxley ? ».

Afin de répondre à notre question de recherche, nous avons structuré notre travail en trois parties. D'abord, une revue de littérature permettra de souligner les effets de la loi Sarbanes-Oxley sur les entreprises. Ensuite, après avoir présenté notre méthode d'investigation empirique, nous mettrons en évidence quatre types de difficulté découlant des procédures de mise conformité avec les exigences de la loi Sarbanes-Oxley (Sox) dans

les DSI de PME. Ces difficultés sont d'ordres organisationnel, technique, économique et culturel. Enfin, nous discuterons, dans une troisième partie, les résultats obtenus au regard de la littérature (ces résultats se situent dans le prolongement de la littérature qui traite des effets de la Sox dans les PME).

Mise en évidence des effets de la loi Sarbanes-Oxley par la littérature

Une analyse bibliométrique[1] nous a permis de constater une insuffisance de la littérature académique mettant en tension les problématiques de l'application de la loi Sarbanes-Oxley dans les DSI de PME. Nous avons réalisé plusieurs requêtes dans des bases de données académiques (du type EBSCO, IEEE, ACM, Sciences Directs) en utilisant plusieurs combinaisons possibles de mots clés.

Nous avons obtenu peu de résultats pertinents par rapport à notre problématique. À titre d'exemple, une requête réalisée sur la base de données EBSCO a donné un résultat de 2 470 articles de revues universitaires contenant le mot « Sarbanes-Oxley », dont environ une centaine contenant les items « information system », « CIO[2] », « IT Departement » et « Information Technology ». Très peu d'articles étaient directement liés à notre problématique.

Une recherche effectuée avec la combinaison « Compliance, information system, Sarbanes-Oxley » a donné 45 résultats, dont un seul était véritablement en lien avec ce que nous mettons en tension dans notre article. Les travaux proposés par la base se focalisaient sur la déclinaison des exigences de la loi Sarbanes-Oxley au niveau des DSI, mais ils ne montraient pas les effets et les difficultés rencontrées par celles-ci dans ce processus. Globalement, les problématiques traitées par les articles en lien avec Sarbanes-Oxley sont plutôt orientées vers les grands groupes. Les seuls articles contenant les mots clés « *small business* » ou « *small firm* » se focalisent sur les conséquences économiques de la Sox pour ces entreprises.

Le rôle des DSI dans la garantie de conformité

La mise en place et la vérification des procédures de conformité avec les exigences de la Sox se déclinent dans tout le tissu organisationnel. La DSI se trouve au cœur de cette obligation, en particulier à travers les sections 302, 404 et 409 du Sarbanes-Oxley Act de 2002, qui sont centrées sur les règles de contrôle interne (KAARST-BROWN et KELLY, 2005). Selon Challande et Lequeux (2009), cela impose aux DSI de :

• garantir la sécurité et l'exactitude des données capturées, stockées et mises à disposition par tous les systèmes informatiques de l'entreprise, et en particulier par des applications liées aux domaines financier et connexes ;
• mettre en œuvre un système d'archivage des données comptables et financières, un élément essentiel du contrôle interne exigé par la loi Sox.

Les DSI ont donc pour obligation de garantir la conformité des systèmes d'information. Elles doivent assurer la documentation, le suivi, l'évaluation, la communication et le *reporting* (ANISINGARAJU, 2003). Pour atteindre cet objectif, les DSI doivent établir les bases d'un environnement de contrôle interne rigoureux (DAMIANIDES, 2005). Ces exigences ont fait évoluer la fonction du directeur informatique, et du même coup les compétences requises pour occuper cette fonction (SUTTON et ARNOLD, 2005).

Bien que les DSI soient familiarisées avec le sujet de la conformité au travers de l'application d'autres réglementations propres à certains secteurs d'activité, la loi Sox constitue pour celles-ci un véritable défi, et ce pour plusieurs raisons :

• Tout d'abord, la mise en conformité avec les prescriptions de cette loi nécessite une organisation adaptée (KAARST-BROWN et KELLY, 2005). Ainsi, au sein de la DSI, le personnel doit avoir une connaissance suffisante de cette loi et disposer de compétences dans les domaines comptable et financier. Wallace et *al.* (2011) ont démontré que le niveau de formation et d'implication du personnel de la DSI a un impact significatif sur l'atteinte des objectifs de conformité avec la Sox.
• Par ailleurs, la réussite de la DSI dans l'atteinte de ces objectifs nécessite une définition claire des rôles de chacun et la mise en place d'une gouvernance informatique adéquate (KAARST-BROWN et KELLY, 2005). La DSI doit occuper une place importante au sein du conseil d'administration et le DSI (en tant que manager) doit travailler en étroite collaboration aussi bien avec le directeur financier qu'avec le directeur général (BRAGANZA et FRANKEN, 2007).
• Enfin, la complexité de cette loi implique des changements significatifs, qui requièrent d'importants moyens afin de mettre en place la structure technique et organisationnelle adéquate au sein de la DSI. Or, pour réussir cette opération, les PME ne disposent pas des mêmes leviers d'action que les grands groupes.

Les effets de la loi Sarbanes-Oxley

Plusieurs travaux ont démontré les apports de la loi Sarbanes-Oxley dans l'amélioration de la qualité des contrôles internes et de celle des informations publiées par les entreprises concernées (EPPS et GUTHRIE, 2010 ; FENG et *al.*, 2009 ; C. LI et *al.*, 2012 ; THORNTON, 2006). En effet, l'existence de faiblesses importantes au niveau des contrôles internes augmente le risque de manipulation et de malversation de l'information comptable, et en particulier des résultats (EPPS et GUTHRIE, 2010). La conformité à cette loi a permis aux entreprises concernées d'identifier et de corriger les déficiences de leurs contrôles (THORNTON, 2006) et d'améliorer, par conséquent, la qualité de l'information interne (FENG et *al.*, 2009). Selon C. Li et *al.* (2010), le

[1] Réalisée en avril 2016.

[2] *Chief Information Officier*, l'équivalent anglais de DSI (directeur des systèmes d'information).

niveau de qualité des contrôles internes informatiques exigés par la section 404 de la Sox affecte positivement celui des informations prévisionnelles produites par les systèmes de *reporting* financier (notamment les résultats prévisionnels).

Cependant, malgré l'amélioration de la qualité des contrôles internes apportée par la loi, de nombreuses critiques ont été faites à l'encontre de cette dernière, et pour cause : en effet, ses injonctions imposent aux entreprises des procédures lourdes et exigeantes en matière de contrôle interne et d'audit, qui produisent parfois des effets contradictoires avec l'esprit même de cette loi (VAKKUR et *al.*, 2010). X. Li (2014) a ainsi démontré que les effets pervers de cette loi l'emportent largement sur ses apports, dans les entreprises concernées. Ainsi, par exemple, l'un des objectifs majeurs de cette loi, en particulier de sa section 404, est d'obliger les entreprises à porter à la connaissance des investisseurs les faiblesses identifiées de leurs contrôles internes dans le but de renforcer la confiance de ces derniers. Mais, d'après Rice et *al.* (2015), le *reporting* des entreprises sur d'éventuelles faiblesses en matière de contrôle interne ne s'est pas amélioré, contrairement à ce qui était attendu de cette loi.

D'autre part, afin d'éviter les risques de non-conformité, les entreprises tendent vers des formes organisationnelles plus centralisées (VAKKUR et *al.*, 2010). En effet, la centralisation est perçue par les managers comme un facteur de réduction des coûts engendrés par la complexité du processus de mise en conformité. Toutefois, cette tendance nuit à la compétitivité des entreprises, en renforçant leur rigidité et en altérant leur capacité d'adaptation qui est pour elles stratégique (*op. cit.*). De la même manière, Zhang (2007) démontre que la Sox a conduit à une baisse de compétitivité des entreprises américaines, par comparaison avec les entreprises non américaines non soumises à cette loi. La complexité et les coûts d'agence engendrés par la mise en conformité avec celle-ci ont été à l'origine du retrait de nombreuses entreprises non américaines de la cotation au marché américain (HOSTAK et *al*., 2013).

Par ailleurs, Vakkur et *al.* (2010) ont démontré l'existence d'un effet significatif de la Sox sur le déclin du taux d'innovation dans les entreprises concernées en raison de la baisse des budgets alloués à la recherche et développement au profit de leurs dépenses de mise en conformité. La rigidité de la loi ainsi que la sévérité des mesures punitives induisent l'apparition d'un biais conservateur chez les dirigeants dans la sélection de nouveaux projets. Le déclin de l'innovation conduit à des pertes conséquentes de parts de marché et, de fait, à une baisse des bénéfices futurs (COHEN et *al*., 2008).

Ahmed et *al*. (2010) soulignent l'existence d'une baisse des *cash-flows* dans les entreprises soumises à cette loi. En sus des coûts directs liés aux missions d'audit et à la mise en place des contrôles internes, des coûts indirects supplémentaires sont induits par le temps improductif des managers, dont le temps et l'attention sont de plus en plus focalisés sur la mise en œuvre et le suivi des contrôles exigés par la Sox.

Ces coûts ont été un facteur dissuasif majeur pour nombre d'entreprises non américaines dans leur décision de renoncer à leur cotation boursière aux États-Unis (DUARTE et *al.*, 2014).

Ces conséquences sont encore plus significatives pour de petites et moyennes entreprises (AHMED et *al.*, 2010 ; MARTIN et COMBS, 2010). En effet, la baisse constatée des *cash-flows* « post-Sox » peut atteindre dans les PME 3 %, en comparaison des grandes entreprises où cette baisse n'est que de 0,5 % (MARTIN et COMBS, 2010). Il y aurait donc un effet négatif inversement proportionnel à la taille de l'entreprise, notamment en raison de seuils de coûts fixes insensibles à l'« effet taille ».

Terrain, données et méthodes

Afin d'instruire notre question de recherche, nous avons choisi d'étudier les difficultés de mise en conformité avec la Sox des DSI de PME à travers le cas d'une PME française cotée au NYSE (*New York Stock Exchange*). Ce terrain nous paraît représenter un cas extrême, au travers duquel le phénomène que nous étudions apparaît de manière claire et transparente, au sens de Pettigrew (1990). Notre choix de l'étude de ce cas unique découle de sa spécificité, qui est de favoriser la compréhension en profondeur d'une situation particulièrement éclairante pour une thématique des plus larges (HLADY RISPAL, 2002 ; YIN, 2009).

Présentation du cas

Le cas que nous avons sélectionné est une entreprise française[3] de taille moyenne spécialisée dans la fabrication et la commercialisation de semi-conducteurs pour la téléphonie mobile 4G destinés aux fabricants d'appareils mobiles à travers le monde. Elle compte un effectif de deux cent cinquante employés, dont la moitié est en France. Elle fait partie des cinq plus grands acteurs spécialisés dans la technologie des semi-conducteurs en Europe. En avril 2011, cette entreprise a été introduite au NYSE (avec un capital de 50 millions d'euros). Ce choix stratégique avait pour finalité d'attirer des investisseurs et des opérateurs spécialisés dans son activité. La viabilité de l'entreprise dépendait de son innovation technologique et de sa capacité à appréhender un marché caractérisé par l'évolution et l'obsolescence rapides de ses technologies et de ses normes industrielles.

Les choix opérationnels et organisationnels qui en ont découlé étaient donc destinés à soutenir ces orientations stratégiques. La DSI, qui joue un rôle fondamental dans cette démarche, devait par conséquent s'adapter en permanence à ce contexte évolutif afin de gérer et de piloter efficacement les processus SI qui soutiennent les activités de l'entreprise. Son directeur des Systèmes d'information dirigeait une équipe de dix personnes et travaillait en étroite collaboration avec la direction comptable et le service de contrôle de gestion sur les

[3] Le nom de cette entreprise n'est pas divulgué ici, pour des raisons de confidentialité.

sujets de conformité avec la Sox. Le management de l'équipe au quotidien reposait sur un mode de fonctionnement à la fois agile et informel. La plurivalence des équipes impliquait l'inexistence d'une définition précise des rôles individuels ainsi qu'une répartition aléatoire de la charge de travail.

Par ailleurs, les spécificités fonctionnelles et pratiques de cette PME l'ont amené à opter pour une infrastructure informatique légère et agile rendue possible par la technologie du *cloud computing*. Les solutions applicatives étaient apportées par un fournisseur de solutions logicielles grâce au modèle d'exploitation SaaS (*Software as a Service*)[4]. Cela impliquait la délégation de certaines responsabilités à l'éditeur, comme la maintenance ou la gestion des changements. Cette solution présentait deux avantages majeurs pour l'entreprise : la réduction des coûts et l'adaptabilité des services et des applications.

Les données recueillies

Afin de mettre à l'épreuve notre question de recherche, nous avons privilégié une étude qualitative reposant sur deux vagues d'entretiens approfondis (menés en novembre 2012 et en avril 2013) avec le DSI de l'entreprise retenue. Ces entretiens ont été semi-directifs/ouverts et se sont déroulés dans les locaux de l'entreprise. D'une durée d'une heure trente chacun, ils ont été intégralement enregistrés et retranscrits. Nous avons interrogé le DSI sur les difficultés rencontrées au quotidien par son service dans la gestion des procédures de mise en conformité avec la Sox. Le profil du DSI (un ancien consultant en organisation dans un grand cabinet d'audit américain) a été un élément central dans la réussite de ce contact. En effet, une proximité culturelle antérieure combinée à sa connaissance et à sa maîtrise du sujet nous ont permis d'aboutir à des axes d'analyse pertinents.

Les entretiens ont été utilement complétés par l'examen de documents internes (procès-verbaux de réunions, échanges de méls, notes de service, etc.), que nous avons consultés sur place, dans les locaux mêmes de l'entreprise. Nous avons également pu consulter les rapports d'activité annuels de l'entreprise (disponibles sur son site *Web*).

Nous avons enrichi notre dispositif empirique par des données secondaires décrivant les dispositions de la loi Sarbanes-Oxley et leur déclinaison dans la DSI étudiée.

Afin de traiter les données collectées, nous avons procédé à une analyse de contenu thématique en suivant les recommandations de Hlady Rispal (2002) et de Miles et Huberman (2003). À cet effet, nous avons tout d'abord effectué une pré-analyse à travers une lecture flottante afin de déterminer les règles de découpage du corpus. Nous avons ensuite identifié les catégories pertinentes pour cette étude. Nous avons privilégié une technique de codification inductive qui nous a semblé être en adéquation avec notre objectif exploratoire.

[4] Logiciel à la demande.

Les résultats

L'analyse des données nous a permis d'identifier quatre types de difficulté : les difficultés organisationnelles, techniques, économiques et culturelles. Ces difficultés contraignent le DSI à procéder à des arbitrages et à des interprétations afin d'arriver à un niveau de conformité acceptable.

Les difficultés organisationnelles

Selon le DSI, la difficulté majeure se situait au niveau organisationnel, à la fois à l'intérieur de la DSI (en raison de la taille réduite de l'équipe) et dans les autres fonctions, pour ce qui relevait de la mise en œuvre des contrôles informatiques. Le manque de personnel dédié et qualifié pour la certification Sarbanes-Oxley au sein de l'équipe informatique impliquait une surcharge de travail conséquente pour le DSI (manager), qui devait gérer tous les aspects liés à la mise en pratique des exigences formelles de la loi au niveau informatique. Pour une structure de cette taille, procéder à des recrutements supplémentaires au sein de la DSI aurait constitué un coût qui n'était pas justifié :

« *Ça, c'est problématique […]. Plus on est une petite structure, [et] plus le temps a de la valeur. Moi, je n'ai personne qui soit dédié pour que l'on soit "certifié Sarbanes-Oxley"…* ».

D'autre part, dans la mise en œuvre des contrôles informatiques, la DSI se trouvait confrontée à des situations conflictuelles opposant les singularités organisationnelles de l'entreprise aux exigences formelles de la Sox. En effet, la polyvalence et l'agilité de l'équipe sont les deux éléments clés pour le fonctionnement au quotidien de la DSI. Parmi les exigences de la Sox, toutes les communications entre les services doivent être formalisées par écrit. Or, pour le DSI, cela aurait été insensé, étant donné la proximité physique des responsables dans l'entreprise et d'un mode d'intercommunication à la fois informel et souple.

« *Cela génère une complexité au quotidien : ils sont à deux mètres, les services de contrôle de gestion et ceux de la finance ! […]. Mais, parler, cela ne suffit pas. Il faut formaliser un mél, etc. […]. Il y a beaucoup de sujets qui font que l'on passe plus de temps à écrire la demande qu'à y répondre…* ».

Par ailleurs, la mise en conformité avec la Sox impliquait une « ségrégation » dans les droits des utilisateurs, au niveau informatique. Cela était incompatible avec la nécessaire plurivalence des équipes dans les fonctions support (la DSI et le service comptable). Or, pour l'entreprise étudiée, la collaboration était une nécessité stratégique. Cette inapplicabilité de la Sox était encore plus manifeste dans le cas où l'absence d'un collaborateur nécessitait une délégation de droits afin de pouvoir assurer la continuité du travail :

« *Il faut que le travail continue à se faire […], ce qui oblige ces personnes à être multi-casquettes […]. Cela a un impact sur l'informatique puisque l'on met en œuvre les profils que l'on nous demande […]. On n'est pas assez nombreux pour le faire. Et ça ne se justifie pas, parce qu'au quotidien, ils s'en sortent très bien. On*

ne va pas recruter quelqu'un en plus « juste » pour que les droits d'accès soient séparés […] : ça n'a pas trop de sens… ».

Ce témoignage met en évidence la difficulté, pour la DSI, de concilier deux axes stratégiques pour l'entreprise : d'un côté, l'agilité organisationnelle indispensable au bon fonctionnement de l'entreprise et, de l'autre, la certification Sox, déterminante pour la politique de financement de l'entreprise :

« *Nos concurrents sont des grands groupes qui font des dizaines de milliards de chiffre d'affaires. Donc, ce n'est pas avec la taille que l'on va réussir à être meilleurs qu'eux. On peut être meilleurs qu'eux en étant plus réactifs, plus flexibles, plus agiles […]. Et si l'on ne respecte pas cette contrainte, c'est un enjeu financier énorme par rapport au marché financier. Donc, si l'on applique bêtement "les contraintes", et bien là on n'avance plus, on ne sait plus quoi faire […]. On sera certifiés certes, mais on ne bougera plus, on ne "saura"plus rien faire…* ».

Les difficultés d'ordre technique

L'une des exigences de la Sox n'est pas seulement de mettre en place des contrôles, il faut aussi les formaliser pour pouvoir apporter des preuves. Toutefois, dans le contexte technique de l'entreprise sous étude, il n'était pas toujours possible de fournir ces éléments. L'un des exemples les plus éloquents est celui des opérations de test des systèmes de production réalisées en mode *cloud computing*, c'est-à-dire sur une plateforme virtuelle accessible *via* une adresse URL[5] temporaire fournie par le prestataire : à la fin de cette opération, ce lien disparaît automatiquement, ne laissant aucune preuve tangible du déroulement des tests. Or, la loi Sarbanes-Oxley exige systématiquement des éléments incontestables pour prouver l'efficacité et la fiabilité de ces opérations.

« *Nos auditeurs nous disent : "qu'est-ce qui prouve que vous avez fait les tests ?" On a eu un URL temporaire, mais il n'est plus accessible. On ne peut pas aller vérifier, et voir les tests que l'on a faits – ou comment on les a fait, etc. On leur explique l'environnement de test, et les résultats…* ».

En plus de l'impossibilité de fournir ces preuves, la DSI doit formaliser toutes les étapes de réalisation des tests et restituer leurs résultats dans un compte rendu jugé sans valeur ajoutée en matière de preuve et de couverture de risque.

« *Donc, on fait ce compte rendu… Mais on pourrait le faire sans réaliser le test, donc, cela ne prouve rien […]. Mais il faut quand même faire ce rapport… qui n'a aucune valeur pour personne…, mais "il faut" le faire !...* ».

Pour tenter d'apporter une solution technique à cette problématique, la DSI suggère l'utilisation d'un outil de gestion de tickets[6] pour gérer la demande d'un environnement de test. Cela permet en effet de prouver, d'un côté, l'existence d'une demande d'environnement (URL) réellement formulée par l'utilisateur et, de l'autre, la clôture de cette demande, qui signifie la fin et le bon déroulement des tests. Toutefois, cette solution reste insuffisante, puisqu'elle se limite au suivi de la demande et ne donne en aucun cas de preuves de la réalisation effective des tests. Ce qui ne répond pas aux exigences de la Sox.

« *Et ça, ça ne leur suffisait pas [aux auditeurs]. C'est quand même le principal, si l'utilisateur dit, d'après ce qu'il a vu : "Vous pouvez y aller". […] Le problème, c'est que l'on ne pouvait pas voir ce que l'utilisateur avait vu...* ».

Malgré ses avantages en termes d'agilité et de réduction des coûts, la technologie du *cloud computing* ne semble pas compatible avec les exigences de la Sox. De plus, la délégation des responsabilités au prestataire *cloud* constitue un domaine de risque, selon les termes mêmes de cette loi. En effet, pour être conforme aux exigences de la Sox, une DSI doit fournir deux rapports semestriels d'audit certifiant la conformité du prestataire à une norme dénommée ISAE34. Le décalage de calendrier entre les dates de l'audit du prestataire et de celui réalisé par la DSI constituerait un motif de non-conformité, selon les auditeurs.

« *Donc, il a fallu trouver un contournement, pour – quand même – couvrir ce risque […]. Ce qui me manquait, c'était ces trois mois sur douze… Ce n'était pas six mois… : ce n'était pas énorme. Mais, pour eux, c'était trop […]. Donc, il a fallu travailler avec eux pour trouver une solution qui les satisfasse et qui, pour nous, était faisable.* »

Par ailleurs, l'une des exigences de cette loi en matière de sécurité consiste à mettre en place un outil de gestion de mots de passe présentant un certain degré de complexité. Selon le DSI, cela incite les utilisateurs à garder une trace écrite de leurs mots de passe dans des emplacements non sécurisés – ce qui est tout à fait contradictoire avec l'esprit de cette exigence. De plus, cet outil a engendré des problèmes d'incompatibilité avec les protocoles déjà existants.

« *Donc, il y avait des soucis techniques : ce n'était pas aussi trivial que ça… Donc, ça a été un projet qui est en train de s'achever, là… On ne met jamais des gens à 100 %, parce que l'on doit toujours être là : on fonctionne en mode polyvalent, souple, etc. Euh… donc… en charges, c'est un projet qui a coûté… trois mois [du CA]* ! ».

Les difficultés d'ordre économique

Les exigences de mise en conformité engendrent des coûts supplémentaires pour la DSI, qui, considérée comme une fonction support, ne dispose que d'un budget limité. Ces coûts sont principalement liés à la mise en place de contrôles internes informatiques adéquats, mais aussi aux temps improductifs nécessaires à cette mise en place. Ces temps improductifs découlent essentiellement de la nécessité de fournir des preuves et de formaliser, ce qui entraîne des coûts injustifiés.

(5) URL : de l'anglais *Uniform Resource Locator* (adresse *Web*).

(6) Un dispositif de gestion des tickets est un système permettant aux utilisateurs de soumettre leurs demandes d'assistance ou de signaler des incidents au personnel d'assistance informatique.

« *Donc, c'est beaucoup d'arbitrage – qui est d'ailleurs [lui aussi] du temps improductif, parce que le temps que l'on passe à faire ça, on ne le passe pas à faire notre travail (donc, ce serait aussi à ajouter dans le coût d'application de la procédure…)* ».

Ainsi, par exemple, la mise en place de l'outil de gestion des mots de passe a nécessité une charge de travail d'environ trois moisXhommes durant l'année 2012. Selon le DSI, il s'agit d'un projet n'ayant aucune valeur ajoutée pour l'entreprise. Un autre exemple est celui de la conception d'une matrice d'analyse des risques qui est exigée par les auditeurs. Ce projet a nécessité un temps de travail conséquent pour le DSI, qu'il n'a pas pu consacrer à son travail habituel. Il lui a fallu, en tout, six mois, en 2012, entre la création de cette grille d'analyse et sa validation.

Les difficultés d'ordre culturel

La loi Sox, qui est d'essence culturelle nord-américaine, est difficile à intégrer dans une entreprise française. Son niveau de rigidité impose un formalisme « inutile », qui n'a parfois aucun intérêt ni aucune valeur :

« *Mais il faut quand même faire ce rapport, donc… qui n'a aucune valeur pour personne..., mais bon, il "faut" le faire !...* ».

En fait, aux États-Unis, les entreprises sont plus familiarisées avec cette philosophie en raison de scandales répétés depuis 2000. Ces scandales ont été un déclic pour les communautés des dirigeants et des managers aux États-Unis dans leur prise de conscience des enjeux personnels de la réforme, notamment au regard des pénalités très lourdes qu'ils risquaient d'encourir. Cela n'est pas le cas en France, où le sujet de la conformité ne fait pas encore partie de la culture des managers, et encore moins de celle de communautés de pratiques professionnelles comme les DSI.

Face aux quasi-absurdités de cette loi par rapport au contexte réel, le DSI est amené à recourir à des arbitrages et à des interprétations afin de se rapprocher du niveau de conformité exigé :

« *Il faut négocier, parce que c'est une question d'interprétation. Eux [les auditeurs], ils sont plus dans le "noir et blanc" . Nous, on va essayer d'être dans… le gris !* ».

Par exemple, selon la Sox, les contrôles doivent avoir lieu trimestriellement. La loi manque de précision sur le concept de trimestrialité. Alors que la trimestrialité, pour la DSI, n'est pas liée à une contrainte calendaire, les auditeurs considèrent au contraire que le respect des dates est impératif. Pour éviter un jugement abusif dans le rapport final d'audit, le DSI est donc contraint de négocier ce niveau d'interprétation.

Par ailleurs, dans le cadre du contrat du *cloud*, le niveau de formalisme de la Sox implique pour la DSI l'obligation de prouver de façon formelle la manière dont elle gère sa relation avec son prestataire *cloud*. Les auditeurs exigent donc un compte rendu de réunion annuel pour montrer que cette relation est effective. Selon le DSI de l'entreprise que nous avons étudiée, ce protocole est complètement « inutile », étant donné les spécificités du contrat. De fait, le DSI considère qu'il s'agit d'exigences « absurdes » qui ne présentent aucun intérêt en matière de sécurité et de couverture des risques – qui sont précisément les deux principaux axes de la Sox. Pour lui, les interprétations et les négociations avec les auditeurs sont des moyens de « contourner » la rigidité et l'absurdité de certaines exigences liées à la Sox. Toutefois, cela rend le jugement assez subjectif, ce qui, là encore, est contradictoire avec l'esprit même de l'audit :

« *Pour eux [les auditeurs], il faut que ça rentre dans des cases. C'est compliqué... Et puis, à partir du moment où l'on parle d'interprétation, c'est subjectif – alors que l'audit doit être objectif (enfin, dans l'idéal – l'idéal utopique [...]). On est dans les négociations, parce que c'est un moyen, euh… de contourner, d'essayer de cacher, euh… ou de s'améliorer.* »

Discussion

Notre travail s'est efforcé d'identifier et de comprendre les difficultés de mise en conformité avec la Sox auxquelles ont été confrontées les DSI de PME. Dans la littérature existante, seuls ses effets et conséquences sur de grandes entreprises ont été mis en évidence. Ses conséquences pour les PME n'ont été abordées que de manière marginale et en se limitant au seul aspect économique. Cette étude de cas a permis d'identifier quatre types de difficulté (difficultés organisationnelles, techniques, économiques et culturelles), auxquelles ont été confrontées les DSI de PME.

Dans une PME, la taille réduite des équipes, la nécessaire plurivalence des personnes et la relativité des définitions formelles des rôles qui en découle sont incompatibles avec les exigences formelles de la Sox. L'atteinte des objectifs de la Sox nécessite des changements significatifs au sein de l'organisation des DSI (KAARST-BROWN et KELLY, 2005). Toutefois, ces changements nécessitent des investissements humains et financiers importants, ce qui est décourageant, voire dissuasif, pour la DSI d'une PME.

Par ailleurs, les contrôles informatiques exigés par la Sox sont impossibles à mettre en œuvre dans le contexte organisationnel d'une PME. La séparation des tâches imposée par la loi Sarbanes-Oxley implique en effet une ségrégation entre les droits des utilisateurs au niveau informatique. Des recrutements supplémentaires ainsi qu'une redéfinition de la structure organisationnelle pourraient être une solution pour sortir de cette impasse. Toutefois, le coût salarial supplémentaire est injustifié par rapport au défi économique réel de l'entreprise et à ses exigences de compétitivité. D'autre part, la séparation des tâches impliquerait une tendance à la centralisation. Or, cette tendance peut nuire aux entreprises, voire être dangereuse pour celles-ci du fait qu'elle en augmente la rigidité, portant de ce fait atteinte à leur performance et à leur compétitivité (VAKKUR et *al.*, 2010 ; ZHANG, 2007). Cette rigidité nuirait à la polyvalence des personnels et à la souplesse de l'organisation (qui sont des éléments clés de leur fonctionnement au quotidien) et à une capacité d'adaptation qui revêt une dimension stratégique pour une PME.

La mise en conformité de la DSI génère des coûts supplémentaires conséquents par rapport au budget de la DSI et, plus globalement, à celui de l'entreprise. Si les coûts liés directement aux missions d'audit et à la mise en place des contrôles nécessaires sont faciles à identifier, il n'en va pas de même pour les coûts indirects qui découlent de temps improductifs, mais rémunérés. Ces coûts engendrent une baisse de profitabilité des entreprises (VAKKUR et *al.*, 2010), voire leur retrait de la cotation boursière américaine (DUARTE et *al.*, 2014).

Par ailleurs, les dépenses liées à la mise en conformité de la DSI avec la Sox entraînent une baisse dans les budgets alloués à l'innovation (COHEN et *al.*, 2008). Cette baisse peut mettre en péril l'activité centrale de l'entreprise, surtout lorsque celle-ci évolue dans un marché fortement concurrentiel et qu'elle dépend d'un nombre limité de clients.

Les difficultés de mise en conformité rencontrées par les DSI rendent l'application réelle de la Sox plus complexe et passive. Face à la rigidité et à l'impossibilité de respecter certaines exigences, le DSI se voit obligé de recourir à une sorte de bricolage technico-administratif pour aboutir à une apparence de conformité. Cela ne favoriserait-il pas l'émergence de pratiques d'hybridation (PACHE et SANTOS, 2013), voire de découplage (MAINHAGU, 2015) ?

Ces résultats invitent à la réflexion et à l'ouverture de nouvelles pistes de recherche, notamment sur la multiplicité des normes et des référentiels dans les communautés de pratiques (comme les DSI) : nous pouvons suggérer un questionnement sur les effets et les conséquences des normes et des référentiels de bonnes pratiques dans les DSI, ou encore sur les facteurs permettant aux managers de faire face à des exigences normatives/légales potentiellement conflictuelles.

Conclusion

Cette étude de cas nous a permis de souligner les défis que les DSI de PME doivent relever pour mener à bien leurs démarches de mise en conformité avec les exigences de la loi Sarbanes-Oxley qui, plus de dix ans après son adoption, continue à être un objet de controverse sur les plans tant académique que professionnel. Notre principal apport se situe dans le prolongement des travaux soulignant les effets et les conséquences de la loi Sarbanes-Oxley dans les organisations, en particulier pour les DSI de PME. Nous avons souligné comment la manœuvre de mise en conformité, dans ce type de configuration organisationnelle, expose la DSI à des difficultés d'ordres organisationnel, technique, économique et culturel.

Malgré l'intérêt indéniable que représentent les résultats issus d'une étude de cas exploratoire, celui-ci reste toutefois limité. D'un côté, sur le plan empirique, notre exploration reste restreinte et ne peut de ce fait vraisemblablement pas mettre en évidence toutes les facettes du problème. D'un autre côté, l'unicité du cas étudié ne peut autoriser une généralisation des résultats que nous avons obtenus.

Bibliographie

AHMED (A.A.S.), McANALLY (M.M.L.), RASMUSSEN (S.) & WEAVER (C.D.), "How costly is the Sarbanes Oxley Act? Evidence on the effects of the Act on corporate profitability", *Journal of Corporate Finance*, 16(3), 2010, pp. 352-369.

ANISINGARAJU (S.), "The role of technology in the Sarbanes-Oxley Act compliance", in *Computer Technology Review*, 23 (10), 36, 2003.

BRAGANZA (A.) & FRANKEN (A.), *Sox Compliance, and power relationships*, Communications of the ACM, 50(9), 2007, pp. 97-102.

CHALLANDE (J.-F.) & LEQUEUX (J.-L.), *Le Grand Livre du DSI : mettre en œuvre la direction des systèmes d'information 2.0*, Eyrolles, Éditions d'Organisation, 2009.

COHEN (D.A.), DEY (A.) & LYS (T.Z.), "Real and accrual-based earnings management in the Pre- and Post-Sarbanes-Oxley Periods", *The Accounting Review*, 83(3), 2008, pp. 757-787.

COLLARD (C.), DELHAYE (C.), LOOSDREGT (H.-B.) & ROQUILLY (C.), *Risque juridique et conformité. Manager la Compliance*, Lamy, 2011.

DAMIANIDES (M.), *SARBANES–OXLEY and IT Governance, New guidance on IT control and compliance. Information Systems Management*, 22(1), 2005, pp. 77-85.

DUARTE (J.), KONG (K.), SIEGEL (S.) & YOUNG (L.), "The Impact of the Sarbanes-Oxley Act on Shareholders and Managers of Foreign Firms", in *Review of Finance*, 18(1), 2014, pp. 417-455.

EPPS (R.) & GUTHRIE (C.), ""Sarbanes-Oxley 404 material weaknesses and discretionary accruals", Accounting Forum, 34(2), 2010, pp. 67-75.

FENG (M.), LI (C.) & McVAY (S.), "Internal control and management guidance", in *Journal of Accounting and Economics*, 48(2-3), 2009, pp. 190-209.

HLADY RISPAL (M.), *La Méthode des cas : application à la recherche en gestion,* De Boeck Supérieur, 2002.

HOSTAK (P.), LYS (T.), YANG (Y.G.). & CARR (E.), "An examination of the impact of the Sarbanes–Oxley Act on the attractiveness of U.S. capital markets for foreign firms", in *Review of Accounting Studies*, 18(2), 2013, pp. 522-559.

KAARST-BROWN (M.) & KELLY (S.), "IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function?", in Proceedings of the 38th Hawaii International Conference on System Sciences, 2005 IEEE, 2005, p. 10.

LI (C.), PETERS (G.), RICHARDSON (V.J.) & WASTON (M. W.), "The consequences of information technology control weaknesses on management information

systems: The case of Sarbanes-Oxley internal control reports", in MIS Quarterly, 36(1), 2012, pp. 179-203.

LI (X.), "The Sarbanes–Oxley act and cross-listed foreign private issuers", in *Journal of Accounting and Economics*, 58(1), 2014, pp. 21-40.

MAINHAGU (S.), « Quand des professionnels contraignent leurs dirigeants à adopter une stratégie de découplage », in *Annales des Mines, Gérer et Comprendre*, n°121, septembre 2015, pp. 12-20.

MARTIN (J.) & COMBS (J.), "SARBANES-OXLEY, Does the Cost Knock Your Socks Off?", *The Academy of Management Perspectives*, 24(3), 2010, pp. 103-105.

MICHELSON (S.), STRYKER (J.) & THORNE (B.), "The Sarbanes-Oxley Act of 2002: what impact has it had on small business firms?", in *Managerial Auditing Journal*, 24(8), 2009, pp. 743-766.

MILES (M.B.) & HUBERMAN (A.M.), *Analyse des données qualitatives*, De Boeck Supérieur, 2003.

PACHE (A.C.) & SANTOS (F.), "Inside the Hybrid Organization: Selective Coupling as a Response to Competing Institutional Logics", in *Academy of Management Journal*, 56(4), 2013, pp. 972-1001.

PETTIGREW (A.M.), "Longitudinal Field Research on Change: Theory and Practice", in *Organization Science*, 1(3), 1990, pp. 267-292.

RICE (S.C.) WEBER (D.P.) & WU (B.), "Does SOX 404 Have Teeth? Consequences of the Failure to Report Existing Internal Control Weaknesses", in *The Accounting Review*, 90(3), 2015, pp. 1169-1200.

SUTTON (S.G.) & ARNOLD (V.), "The Sarbanes-Oxley Act and the changing role of the CIO and IT function – Information Systems", in *International Journal of Business Information Systems,* 1(1), 2005, pp. 118-128.

THORNTON (G.), "Getting business benefits from 404 compliance", *Grant Thornton Corporate Governor Series*, February, 20, 2006.

VAKKUR (N.), McAFEE (R.) & KIPPERMAN (F.), "The unintended effects of the Sarbanes-*Oxley Act of 2002",* in *Research in Accounting Regulation*, 22(1), 2010, pp. 18-28.

WALLACE (L.), LIN (H.) & CEFARATTI (M.), "Information security and Sarbanes-Oxley compliance: An exploratory study", in *Journal of Information Systems*, 25(1), 2011, pp. 185-211.

YIN (R.K.), *Case Study Research: Design and Methods*, London : SAGE Publications, 2009.

ZHANG (I.X.), "Economic consequences of the Sarbanes-*Oxley Act of 2002"*, in *Journal of Accounting and Economics*, 44(1-2), 2007, pp. 74-115.