Assurances

Assurances

Le vol, l'ordinateur et le contrôle comptable

Claude C. Bismuth et Yves Giard

Volume 49, numéro 3, 1981

Introduction à l'informatique

URI : https://id.erudit.org/iderudit/1104137ar
DOI : https://doi.org/10.7202/1104137ar

Aller au sommaire du numéro

Éditeur(s)

HEC Montréal

ISSN

0004-6027 (imprimé)
2817-3465 (numérique)

Découvrir la revue

Citer ce document

Bismuth, C. & Giard, Y. (1981). Le vol, l'ordinateur et le contrôle comptable. *Assurances*, *49*(3), 230–238. https://doi.org/10.7202/1104137ar

Résumé de l'article

Electronic processing has opened the door to many frauds unheard of until today. Chartered accountants have thus had to work closely with clients in an attempt to prevent and to detect quickly computer frauds. In their article, Messrs. Bismuth and Giard point out the need for management to exercise over the operations and access to their systems, and for the auditors to conduct a periodic review of the computer systems as part of their annual audit. Computer security reviews can be the subject of a special assignment whereby the auditor can use his knowledge.

Le vol, l'ordinateur et le contrôle comptable

par

CLAUDE C. BISMUTH, M.B.A., C.A., C.I.S.A.,
associé responsable de la vérification informatique
de H. Marcel Caron & Associés et Clarkson Gordon

et

YVES GIARD, C.A., Cert. Info., chef d'équipe en
vérification informatique - H. Marcel Caron
& Associés et Clarkson Gordon

Electronic processing has opened the door to many frauds unheard of until today. Chartered accountants have thus had to work closely with clients in an attempt to prevent and to detect quickly computer frauds. In their article, Messrs. Bismuth and Giard point out the need for management to exercise over the operations and access to their systems, and for the auditors to conduct a periodic review of the computer systems as part of their annual audit. Computer security reviews can be the subject of a special assignment whereby the auditor can use his knowledge.

~

Traditionnellement, l'expert-comptable a été appelé de par sa fonction de vérificateur à rendre compte de la fiabilité des registres comptables à partir desquels les états financiers sont produits. Pour cela, il doit étudier les contrôles internes des systèmes dont l'aboutissement se retrouve dans les registres comptables.

Cette étude du contrôle interne vise principalement à assurer le vérificateur que les méthodes en vigueur permettent un contrôle suffisant de la garde et de la comptabilisation des biens de l'entreprise; sinon, elle vise à lui permettre d'évaluer l'incidence des faiblesses de contrôle qu'il aurait identifiées sur les états financiers.

Avec l'arrivée des ordinateurs, qu'y a-t-il de vraiment changé? De nouveaux intermédiaires sont venus se greffer aux registres comptables maintenant mécanisés.

Les activités de ces intermédiaires doivent être contrôlées comme dans les systèmes traditionnels.

Puisqu'il s'agit d'activités nouvelles telles que l'exploitation des ordinateurs, le développement et l'entretien des systèmes, de nouvelles techniques de contrôle doivent être utilisées. Ces contrôles peuvent être programmés de sorte que le système oblige, par exemple, l'opérateur à effectuer des tâches bien spécifiques et nous avise à l'aide de rapports automatisés, de toutes autres tâches que l'opérateur a pu effectuer. Autrefois, les techniques de contrôle des systèmes manuels étaient relativement simples: la répartition des tâches, l'autorisation d'une personne responsable sur un document ou tout simplement l'activité de supervision. En ce qui concerne les systèmes informatiques, les techniques de contrôle manuelles ou mécanisées sont complémentaires et parfois interchangeables. Par exemple, l'ordinateur peut effectuer la validation des données, produire des rapports d'exception, contrôler l'usage de mots de passe et faire une vérification des calculs manuels tels que les totaux de contrôle.

Cependant, selon le système manuel, une même opération était totalisée deux fois, soit lors de l'enregistrement au registre de transactions et de l'inscription à l'auxiliaire de contrôle tenu par deux personnes différentes, et conciliée au moyen du grand livre général. Selon le système mécanisé, la transaction n'est vue qu'une seule fois par l'ordinateur et elle pourrait servir de base à plusieurs calculs subséquents. Cette dualité des contrôles de traitement qui existe dans les systèmes manuels ne se retrouvant plus dans les nouveaux systèmes, les techniques de contrôle doivent assurer que la prise initiale de la transaction s'effectue de façon exacte. Ces contrôles de traitement initiaux des transactions ont une importance primordiale et sont d'autant plus essentiels aux systèmes informatiques.

Le traitement informatique pose un problème de contrôle: l'augmentation considérable du volume de l'information traitée. En effet, lors de la conversion sur ordinateur, on cherche à bénéficier de la capacité extraordinaire de traitement de l'ordinateur. Ceci rend impraticable ou illusoire la vérification manuelle ou l'utilisation de la capacité «humaine» aux fins de la vérification ou

du contrôle du traitement informatique. Il s'ensuit que certaines décisions doivent être prises par les concepteurs du système ou les usagers afin d'effectuer plutôt une vérification par exception des transactions traitées. Par conséquent, on se fie automatiquement au traitement électronique quant à l'exactitude des rapports produits.

D'autre part, l'exactitude des décisions prises par l'ordinateur dépend strictement de la qualité du travail de programmation effectué par l'équipe d'élaboration. Le contrôle exercé sur ces

particuliers s'effectue généralement par le biais des sondages d'acceptation du système qu'effectue l'usager. Cependant, le «cerveau» de l'ordinateur a la particularité d'être modifiable dans sa logique non pas sous l'effet de l'hypnose, mais par la simple intervention d'un programmeur. Ce type d'activité engendre beaucoup de problèmes de contrôle et nécessite une grande vigilance de la part du service informatique.

D'ailleurs, depuis l'avènement du terminal et des réseaux de télécommunication, ce problème a pris une dimension nouvelle et, de la notion de contrôle interne, on est passé véritablement à la notion de sécurité du milieu informatique. Ce problème provient non seulement de la grande accessibilité à l'information et au logiciel mais aussi de la concentration d'importants biens représentés par l'ordinateur ainsi que de l'information qui est emmagasinée. La croissance de l'usage de l'ordinateur dans la gestion quotidienne a suscité une plus grande dépendance du gestionnaire vis-à-vis cet outil devenu indispensable. On sait que l'entreprise engage des frais substantiels pour le développement d'une banque de données à la fois utile et fiable. L'information même devient souvent l'actif principal de l'entreprise.

Vu la problématique de l'ordinateur vis-à-vis les contrôles comptables et de gestion, que peut faire le gestionnaire afin de protéger ces éléments d'actif importants, de maintenir la fiabilité de l'information et d'assurer la continuité des opérations suite à un désastre? Comment l'expert-comptable peut-il lui venir en aide? Comment ses assureurs réagissent-ils aux risques reliés à l'informatique?

D'abord sur le plan des applications, l'expert-comptable doit conseiller son client à la suite de sa revue des systèmes, sur les méthodes à prendre pour améliorer le contrôle interne.

Participation à la revue des systèmes pendant leur élaboration

Il arrive souvent que les recommandations du vérificateur nécessitent une refonte importante du système en vigueur. Dans ce cas, les recommandations sont parfois laissées en suspens pour des raisons dites «économiques». La seule façon de remédier à ce problème est que le vérificateur participe vraiment à l'élaboration du système. Cette participation se justifie du fait que les usagers sont souvent plus enclins à définir leurs besoins fonctionnels du système informatique qu'à implanter des contrôles internes satisfaisants. D'autre part, le service informatique est souvent jugé sur la rapidité avec laquelle il répond aux besoins informatiques des usagers. De plus, les responsables de l'informatique ne sont souvent pas bien formés ou motivés par les aspects du contrôle interne par rapport à l'efficacité et à la rapidité des traitements des systèmes qu'ils conçoivent. De même, il est difficile pour le personnel de l'informatique d'entrevoir ou d'imaginer les conséquences de pertes informatiques au niveau global de l'entreprise.

Cela permet aussi d'évaluer la qualité des contrôles internes que l'on se propose d'implanter afin de donner à la direction une assurance raisonnable que les éléments essentiels d'un bon contrôle interne dans un milieu informatique sophistiqué seront mis en oeuvre.

D'autre part, cette revue peut être effectuée de façon beaucoup plus rapide et bénéfique avant l'implantation des systèmes puisque l'équipe d'élaboration a alors toute la cohésion et la formation nécessaire pour répondre facilement aux questions du vérificateur sur les nouveaux systèmes informatiques.

L'équipe d'élaboration est généralement multi-disciplinaire et constituée de personnes responsables. Ce groupe est bien informé des détails prévus aux systèmes et son activité prend fin lors de l'acceptation et de la mise en application de ces systèmes.

Par la suite, les systèmes sont changés périodiquement selon les besoins et bien souvent, quand ils atteignent une certaine maturité, leur transformation fait qu'on ne les reconnaît plus.

Il est donc important de recourir à l'expert-comptable lors de l'élaboration afin que le système englobe tous les aspects de contrôle nécessaires et que l'entreprise établisse des procédés bien structurés quant aux changements qui seront effectués aux systèmes par la suite. De plus, cette participation donne à la direction l'occasion d'améliorer certains contrôles ou d'en ajouter au cours
 de l'élaboration et avant la finalisation des systèmes.

Cette forme de participation assure une protection des applications elles-mêmes, mais qu'en est-il du centre informatique, du système d'exploitation, du réseau de télécommunication, des banques de données et de toutes les fonctions du centre informatique qui ne sont pas particulières aux applications mais partagées par elles et que l'on désigne souvent sous le vocable de «milieu informatique»?

Il ne s'agit pas ici simplement d'assurer la sécurité physique des ordinateurs, mais de prévenir les intrusions perpétrées à partir de terminaux par un programmeur ou un opérateur malhonnête cherchant à outrepasser les mécanismes de protection de fichiers de données. Il est, malheureusement, reconnu que les installations informatiques sont bien fragiles lorsqu'on songe à tous les incidents qui ont gravement compromis leur fonctionnement pendant des périodes prolongées. Avec l'évolution des techniques informatiques sont apparues de nouvelles possibilités de crime et une incroyable série de problèmes tant pour les experts de cette discipline que pour les cadres supérieurs.

Plusieurs articles et quelques livres ont été publiés au cours de la dernière décennie décrivant des crimes perpétrés à l'aide de l'informatique[1]. Il en est souvent conclu que la plupart de ces crimes ne sont jamais publiés, mais nous savons déjà que le sensationalisme d'une telle nouvelle permet à ce sujet de faire la manchette. Les banques américaines qui sont victimes de tels crimes

[1] À lire: "Crime by computer" de Donn B. Parker (New York: Charles Scribner's Sons, 1976).

sont obligées par la loi d'en publier l'occurrence. Ainsi, on pourrait être porté à croire qu'elles seules sont les victimes d'assaut fructueux des systèmes informatisés. La direction de l'entreprise n'est pas toujours à l'aise quant à la prise des décisions nécessaires pour assumer sa responsabilité vis-à-vis du centre informatique. L'expert-comptable est donc appelé à jouer un rôle actif dans l'évaluation et la mise en place d'un programme de sécurité pour l'ensemble des sections fonctionnelles et organisationnelles du service informatique. Ce programme d'évaluation sert surtout à faire le point sur les différentes mesures préventives en place. Notre expérience démontre que ces mesures ont souvent été mises en place sans plan global de sécurité. Il va sans dire que toute entreprise a donc certaines mesures préventives mais que le manque de planification et de coordination laisse des failles dans le système de prévention.

Ce programme devrait englober les secteurs critiques suivants:

1) La protection des installations informatiques contre les possibilités de catastrophes matérielles, de défaillance du matériel ou de malveillance de la part des employés.
2) Les règles et les procédés de secours et de reprise permettant d'assurer la continuité des opérations en cas de catastrophe matérielle.
3) La prévention de la manipulation des systèmes permanents aux fins de vol, fraude, détournement ou autres activités illégales.
4) Les règles et les procédés informatiques permettant de concevoir de nouveaux systèmes sécuritaires et contrôlables.
5) Le programme interne de sécurité, afin de prévenir ou de minimiser les risques et d'assurer l'intégrité des données et des systèmes informatiques.

En vue de cette évaluation, il est possible d'avoir recours à des experts de différentes disciplines: directeurs de l'informatique et des installations, conseillers pour le logiciel, les machines et les télécommunications et vérificateurs chevronnés en matière de contrôles informatiques et d'analyse des risques.

On devra commencer par un examen de l'ensemble du programme de sécurité qui porte sur divers aspects touchant l'administration et la gestion des contrôles et de la sécurité, entre autres:

- Quels sont les procédés permettant l'élaboration, la diffusion, la mise à jour et l'application des contrôles et mesures de sécurité?
- Quelle est la formation du personnel de l'informatique en ce qui concerne les contrôles et la sécurité?
- Quel est le mode de révision des règles, politiques et procédés de sécurité informatiques?

Chaque secteur fonctionnel du milieu informatique devrait être passé en revue en considérant les questions suivantes:

- Existe-t-il un contrôle et une politique de sécurité officiels pour le secteur en question?
- Des règles et des procédés documentés ont-ils été distribués au personnel concerné?
- Ces procédés sont-ils mis en application?
- Sont-ils appropriés et complets sans être trop coûteux ou préjudiciables à la souplesse opérationnelle?
- Peuvent-ils être améliorés sans trop de frais?
- Si les opérations du secteur étudié étaient touchées par une catastrophe, combien de temps faudrait-il pour qu'il recommence à fonctionner normalement?

~

À la suite de cette revue, l'expert-comptable, aidé de conseillers engagés dans d'autres disciplines, sera en mesure d'émettre un rapport englobant tous les aspects de la sécurité informatique et il appartiendra alors à la direction d'en exiger l'implantation et le suivi.

Cependant, ce programme de sécurité est axé davantage sur la prévention et la détection sans toutefois assurer en lui-même la protection après le fait, c'est-à-dire lorsqu'une panne majeure est survenue.

Ce plan de recouvrement est une étape supplémentaire du programme de protection et vise à assurer la continuité de l'exploitation de l'entreprise en cas de défaillance majeure des installations informatiques.

Les principales étapes d'élaboration du plan sont:

- Définir les fonctions d'affaires critiques.
- Établir des systèmes qui y sont reliés.
- Déterminer les besoins d'équipement minimums.
- Revoir les possibilités de recouvrement des systèmes reliés.
- Revoir et sélectionner les possibilités de traitement:
  — contrat d'aide mutuelle
  — centres:
    — espace seulement
    — tout équipé
  — centre de traitement à façon.

L'étape suivant l'identification de l'outil de recouvrement sera l'élaboration du plan détaillé visant à:

a) Rétablir les fonctions d'affaires critiques;

b) Au coût minimum;

c) Avec le minimum de remue-ménage.

La première étape sera caractérisée par l'identification des mesures d'urgence propres à assurer la survie des individus et des installations matérielles.

Dans un deuxième temps, on devra préparer un plan global de recouvrement propre à l'ensemble des installations informatiques. Ces activités dépendent du mode de traitement utilisé et concernent les procédés de transfert et de mise en place ainsi que les activités de recouvrement des installations.

Enfin, les procédés de recouvrement devraient être prévus pour chacun des systèmes critiques établis. Ces procédés doivent comprendre:

- le recouvrement des fichiers;
- le recouvrement de l'état au moment du désastre;

- le traitement dans le nouveau milieu;
- la distribution des rapports;
- l'implantation des procédés manuels.

Enfin, l'étape finale consistera à prévoir des moyens d'assurer que les méthodes prévues sont viables et à jour. À cette fin, on devra prévoir des essais dans le cadre de simulation de désastres afin d'apporter des améliorations au programme prévu.

Nous avons voulu démontrer comment l'expert-comptable
 pouvait aider son client à mieux maîtriser son milieu et ses applications informatiques. Il va sans dire que le succès de ces méthodes sera fonction de la volonté du client et de son entreprise à bien les maîtriser et à les mettre pleinement en vigueur.

~

Le manque de sécurité est, en effet, l'un des principaux points faibles du service informatique moderne. Nous trouvons à un extrême les entreprises qui n'ont presque rien fait pour assurer la sécurité du service informatique et qui s'exposent donc à de très grands risques et à l'autre, les entreprises ayant investi des capitaux considérables au chapitre de la sécurité, sans avoir suffisamment analysé si les mesures prises assureront véritablement le degré de protection souhaité.

Il serait souhaitable que cet exposé fasse réfléchir le gestionnaire, et qu'il accorde plus d'importance à l'évaluation du contrôle interne dans un cadre informatique. L'usager apprécierait sûrement les avantages d'un bon système préventif et détecteur, qui servirait à amoindrir les risques auxquels fait face l'entreprise. Par ailleurs, l'assureur voudra sûrement considérer davantage la qualité des mesures préventives de sécurité mises en place par ses clients dans l'évaluation des risques reliés aux polices d'assurance couvrant l'interruption des affaires. Ainsi, le client pourra espérer recevoir, par le biais d'une remise de prime, un geste reconnaissant de ses efforts financiers et l'assureur y gagnera sans doute en redoublant de précautions et en améliorant le processus suivi dans la catégorisation et la quantification du risque.