BASEL COMMITTEE ON BANKING SUPERVISION

BANK FOR INTERNATIONAL SETTLEMENTS

Risques liés aux systèmes informatiques et de télécommunications

(Juillet 1989)

La vitesse de l'innovation technologique liée aux ordinateurs et aux télécommunications, ces dernières années, et l'intégration d'opérations automatisées rendent les banques de plus en plus dépendantes de la fiabilité et de la continuité de leurs systèmes informatiques.

Les banques ont toujours été exposées à des risques tels qu'erreurs et fraudes, mais leur importance et la rapidité avec laquelle ils peuvent survenir se sont modifiées de manière spectaculaire. En outre, avec des systèmes de règlement informatisés, les relations de crédit interbancaires couvrent désormais le monde entier sous forme de réseaux interconnectés. À partir du moment où une banque est dans l'incapacité de faire face à ses obligations de paiement, du fait de difficultés propres aux systèmes, d'une défaillance ou d'autres raisons, les prêts accordés par des établissements créanciers à cette banque se transforment en créances douteuses, et la défaillance se propage, par réaction en chaîne, à tout le système, menaçant d'investir et de paralyser l'ensemble du système de règlement.

Les types de risques qui caractérisent un environnement informatique et les procédures de sécurité et de contrôle nécessaires requièrent toute l'attention des autorités de surveillance. On examinera ici les catégories suivantes de risques: diffusion non autorisée d'informations, erreurs, fraudes, interruption de l'activité par suite d'une défaillance du matériel ou du logiciel, planification inefficace et risques liés aux opérations d'informatique individuelle.

Le présent document est un outil de référence élaboré à l'intention des autorités de contrôle dans un vaste domaine d'activité. Il n'est pas conçu comme un document technique pour des experts en la matière et s'efforce plutôt de mettre l'accent sur les principaux problèmes devant retenir l'attention des autorités de contrôle.

Diffusion non autorisée d'informations

La plupart des informations bancaires sont créées par traitement informatique ou liées directement à ce dernier. Les données et documents sont généralement acheminés à l'intérieur d'une banque ou entre une banque et ses correspondants et clients par des réseaux publics de communication (lignes téléphoniques et satellites, par exemple). Un grand nombre d'usagers, dont les employés et clients des banques, peuvent accéder directement à ces informations par l'intermédiaire de terminaux et de téléphones informatiques. Tout en améliorant les services à la clientèle et les opérations internes, ces activités ont accru les risques d'erreur et d'utilisation abusive des informations des banques.

Une grande partie de ces informations sont confidentielles; elles pourraient nuire aux relations avec la clientèle ainsi qu'à la réputation de l'établissement et entraîner des demandes de dommages et intérêts si elles tombaient entre de mauvaises mains. On peut citer parmi ces informations les soldes des comptes privés, les plafonds des découverts et les modalités d'exécution des opérations. La création et le stockage de la correspondance et des stratégies bancaires s'effectuent également par traitement de texte. Le danger particulier que représente la divulgation d'informations confidentielles avec les systèmes informatiques, par rapport aux systèmes manuels, réside dans le fait que l'on peut prélever plus facilement, et sous une forme pouvant être traitée par ordinateur (telles que copies sur bande ou disquette), une quantité beaucoup plus importante d'informations et que l'accès non autorisé peut intervenir sans laisser de traces.

Il convient donc de mettre en place des procédures adéquates de sécurité et de contrôle pour protéger la banque. C'est en fonction du degré de risque encouru par l'établissement et de l'incidence des pertes (ou de la diffusion non autorisée d'informations) qu'il faut fixer le niveau de contrôle requis.

Les contrôles techniques effectués aux fins de la sécurité de l'information pourraient inclure: le chiffrement, processus par lequel le texte en clair est converti en une série de symboles dénués de

sens; l'utilisation de codes d'authentification des messages, qui protègent contre toute altération non autorisée les transactions électroniques de données au cours de la transmission ou du stockage; enfin, le recours à du logiciel d'application de mesures de sécurité, en vue de restreindre l'accès aux données, fichiers, programmes, utilitaires et commandes de systèmes informatiques. De tels systèmes permettent de contrôler l'accès par utilisateur, par transaction et par terminal. Les violations ou tentatives de violation de la sécurité doivent être signalées.

Erreurs

Les erreurs se produisent en général lors de l'entrée des données ainsi que durant le développement et la modification des programmes. Des erreurs importantes peuvent également se glisser au cours de la conception des systèmes, des procédures routinières de gestion des systèmes et de l'utilisation de programmes spéciaux destinés à corriger d'autres erreurs. Les erreurs sont habituellement imputables à une défaillance humaine, et très rarement aux composants électroniques ou mécaniques internes. Elles peuvent aussi être introduites dans les programmes de logiciel lorsque ces derniers sont «personnalisés» et adaptés aux besoins d'un utilisateur particulier. Il faudrait veiller, lors de l'acquisition de programmes de logiciel standards, à limiter les modifications à un strict minimum.

Fraudes

Les flux de données bancaires représentent des actifs ou des instructions qui donnent lieu finalement à un déplacement d'actifs. La vitesse avec laquelle les actifs peuvent être transférés par les systèmes électroniques de paiement et de commutation de messages complique le contrôle interne. Les fraudes réussies ne se traduisent pas seulement par une perte financière directe pour l'établissement; elles portent aussi atteinte, lorsque les médias en prennent connaissance, à la confiance placée dans l'établissement et le système bancaire en général. Vu les nombreuses possibilités d'accès aux documents informatiques, les risques de fraude sont multiples. En voici quelques exemples:

- introduction de transactions non autorisées dans le système informatique;
- modification non autorisée des programmes lors d'opérations courantes de développement et de maintenance, de sorte que ceux-ci risquent d'engendrer automatiquement des transactions frauduleuses, de ne pas tenir compte des tests de contrôle effectués sur certains comptes ou d'éliminer l'enregistrement de transactions spécifiques;
- utilisation de programmes spéciaux pour modifier sans autorisation des documents informatiques en contournant les dispositifs normaux de contrôle et les pistes de vérification intégrés dans les systèmes informatiques;
- extraction physique des fichiers d'un ordinateur, qui seront modifiés ailleurs par insertion de transactions ou de soldes frauduleux avant d'être remis en place pour le traitement;
- introduction ou interception aux fins de leur modification de transactions lors de leur transmission par l'intermédiaire des réseaux de télécommunications.

À l'heure actuelle, on assiste à la mise en place de nouvelles formes de paiement qui permettent à des tiers d'initier des paiements au moyen d'un équipement électronique. La probabilité de voir se produire certains de ces types de fraudes par le biais d'un accès non autorisé aux systèmes de télécommunications s'en trouve accrue.

La plupart des systèmes bancaires comportent des dispositifs de contrôle et fournissent des informations destinées à faciliter la prévention ou la détection de ces types de fraudes. Toutefois, ces informations courent, elles aussi, le risque d'être manipulées par des personnes ayant accès aux terminaux ou aux fichiers informatiques.

Pour mettre sur pied des systèmes de contrôle interne efficaces, il est essentiel de déterminer tous les points vulnérables de chaque système. Les programmes et enregistrements sensibles doivent être protégés tout spécialement contre des modifications non autorisées. Il faut également veiller à donner

une formation adéquate au personnel œuvrant dans les domaines sensibles et à répartir convenablement les tâches.

Interruption d'activité par suite d'une défaillance du matériel ou du logiciel

Les systèmes informatiques sont constitués, au niveau du matériel comme du logiciel, de multiples éléments et la défaillance de l'un d'entre eux suffit pour bloquer tout le système. Ces éléments sont souvent concentrés en un seul ou en un nombre limité d'endroits, ce qui en accroît la vulnérabilité.

Le remède classique contre une panne du système consistait auparavant à revenir aux procédés manuels que le système informatique avait remplacés. Dans la plupart des cas, cette façon de procéder n'est plus réaliste et peu de banques pourraient fonctionner sans systèmes informatiques. Le traitement et la fourniture de l'information au moyen d'une technologie améliorée ont accru la dépendance des utilisateurs à l'égard de la disponibilité et de la fiabilité des systèmes automatisés. La disponibilité continue du système d'information d'une banque fait partie intégrante d'une prise de décisions efficace.

Lorsque les systèmes informatiques sont hors d'usage, les effets préjudiciables qui en résultent pour les services bancaires en temps réel aux clients sont immédiats et prennent rapidement des proportions alarmantes. Les retards s'accumulent et, si la défaillance dure plusieurs heures, leur élimination peut durer des jours entiers. Ces effets sont particulièrement dévastateurs dans le cas des systèmes électroniques et de paiement, ceux notamment qui garantissent un règlement le jour même, lorsque les bénéficiaires sont tributaires de la réception de fonds pour faire face à leurs engagements. Les coûts engendrés par une panne sérieuse des systèmes peuvent dépasser de loin les frais de remplacement du matériel, des données ou du logiciel endommagés.

L'existence de plans de secours efficaces peut permettre aux utilisateurs de réduire l'incidence des problèmes d'exploitation de ce genre. Ces plans devraient prolonger le système de contrôle interne et de sécurité physique d'une banque. Ils devraient comporter des dispositions pour la poursuite de l'activité et des procédures de relance en cas d'interruption ou de non-fonctionnement des systèmes, c'est-à-dire un dispositif de sauvegarde, sis hors du lieu d'installation, des fichiers sensibles, du logiciel et du matériel, ainsi que des procédures de remplacement du traitement de l'information. Les plans de secours devraient être testés périodiquement pour s'assurer que leur efficacité demeure intacte. Une banque qui s'en remet à des services informatiques externes pour le traitement de ses données devrait veiller à ce que les plans de secours de ces services complètent les siens.

Planification inefficace

Une saine planification est d'une importance capitale. L'efficacité et la qualité des services bancaires sont désormais tellement tributaires des systèmes informatiques que toute défaillance dans la planification ou le développement de nouveaux systèmes peut avoir de sévères conséquences commerciales. Toute défaillance dans l'installation de nouveaux systèmes et la fourniture de nouveaux services peut pénaliser lourdement une banque par rapport à ses concurrents. Inversement, l'informatisation à outrance, dans les cas notamment où les avantages sont faibles, s'est souvent révélée erronée du point de vue des coûts.

Quelques établissements financiers ont rencontré de sérieux problèmes en essayant d'introduire des systèmes financiers hautement intégrés. Un système de logiciel intégré est une structure dans laquelle les programmes concernant différentes applications – prêts, dépôts, clientèle de particuliers ou de grandes entreprises – qui sont conçus et exploités normalement de manière autonome sont élaborés dès le départ dans le cadre d'une structure globale. Cette approche vise à accroître la disponibilité réelle de l'information, améliorer l'efficacité de l'exploitation et faciliter l'implantation de nouveaux produits. Dans certains cas, le coût, le temps et les ressources en personnel nécessaires pour assurer le succès d'une installation de systèmes intégrés ont été sous-estimés. Des projets développés pendant de nombreuses années ont dû être abandonnés avec des coûts énormes.

Étant donné la complexité des systèmes informatiques et leur incidence sur l'ensemble de l'organisation, il importe que la direction s'engage à assurer le succès de chaque projet. Elle devrait

attacher une grande attention à la planification (stratégique) à long terme des systèmes informatiques, à l'équipement, au logiciel, aux études de faisabilité, à la détermination des spécifications des systèmes, au choix des fournisseurs et à la conduite du projet.

Risques liés à l'informatique individuelle

Les ordinateurs personnels, micro-ordinateurs et équipements informatiques mis à la disposition de l'utilisateur final ont joué jusqu'à une date récente un rôle relativement minime dans le traitement informatique central. À l'heure actuelle, compte tenu des avantages techniques, de la rapidité et du rapport coût/bénéfice de l'informatique individuelle, le recours à ces équipements s'est considérablement renforcé; l'informatique individuelle prend ainsi à son compte une partie du traitement des données relevant du contrôle centralisé. Les risques informatiques touchent maintenant de nouveaux domaines bancaires et, dans bien des cas, ces activités n'ont fait l'objet d'aucune mesure de contrôle ou de surveillance. La question la plus préoccupante à propos de l'informatique individuelle est que la mise en place des contrôles ne s'est pas faite au même rythme que le développement de ces nouveaux réseaux de fourniture et de traitement des informations.

Les risques sont généralement les mêmes que ceux liés aux unités centrales, mais il faut accorder une attention particulière à l'éventualité d'une altération ou d'une perte de données ou de logiciel susceptible d'entraver le fonctionnement efficace de tout le réseau d'exploitation de l'établissement. Les micro-ordinateurs sont utilisés aujourd'hui non seulement pour le traitement de texte, mais aussi en tant que terminaux de communication avec d'autres ordinateurs et d'autres processeurs autonomes. Comme ces systèmes sont, le plus souvent, extrêmement personnalisés et indépendants, une seule personne étant souvent chargée du développement, des tests, de la réalisation et de l'exploitation d'un jeu de programmes, on voit s'accroître la possibilité d'un recours à des procédures et à des méthodes de traitement de données différentes et incompatibles avec les normes adoptées par ailleurs dans l'établissement.

Tâches des responsables

C'est aux dirigeants de l'établissement qu'il incombe de veiller à ce que les activités soient protégées efficacement contre les risques mentionnés précédemment. Il convient en premier lieu d'instaurer des *mesures préventives* adéquates, destinées à réduire au minimum la probabilité d'une apparition de ces problèmes. Au nombre de ces mesures figurent une conception et une localisation minutieuses des centres informatiques, la mise en place de contrôles pour la saisie des données et de dispositifs de sécurité visant à prévenir l'accès non autorisé à l'équipement informatique, ainsi que l'utilisation de mots de passe pour limiter l'accès aux programmes et aux données.

Comme une action préventive ne peut jamais être totalement efficace, il est nécessaire que les responsables mettent également au point des systèmes de *mesures correctives*. Celles-ci doivent viser à déceler et limiter les effets sur l'activité d'événements qui échappent au contrôle préventif et menacent les opérations des banques. Elles doivent comprendre un doublement des capacités des réseaux de télécommunications et d'ordinateurs pour faire face au risque de panne ainsi que des procédures de rapprochement destinées à détecter les erreurs et des plans de secours pour les catastrophes de grande ampleur. En outre, toute politique informatique soigneusement élaborée devrait comporter une assurance contre les pertes liées aux fraudes des employés, aux coûts de remplacement des données et à la destruction de logiciel ou de matériel.

Audit interne

Il appartient également aux dirigeants et administrateurs de revoir, surveiller et tester les systèmes de contrôle informatique pour s'assurer de leur efficacité quotidienne et de leur utilité du point de vue de l'activité de l'établissement. Il est nécessaire de mettre en place un programme régulier de tests indépendants des procédures de sécurité et de contrôle par des inspecteurs, des auditeurs ou des

consultants. Ce programme devrait permettre de déceler les insuffisances des contrôles avant qu'elles ne compromettent sérieusement les opérations bancaires. La fréquence et l'importance des tests d'audit réalisés dans tout secteur doivent refléter le risque auquel les banques sont exposées si les procédures de sécurité et de contrôle se révèlent défaillantes.

Rôle des autorités de contrôle

Du point de vue des autorités de contrôle, il est nécessaire d'évaluer tant la pertinence de la politique suivie par un établissement en matière informatique que l'efficacité de son système de contrôle et d'audit informatiques internes. L'un des moyens dont elles disposent pour s'acquitter de cette tâche est d'évaluer la situation par le biais de *questionnaires* ou de rapports, mais ces fonctions relèvent le plus souvent de la compétence des inspecteurs et auditeurs externes. Un simple questionnaire ou rapport permet habituellement de donner des indications préliminaires aux autorités de contrôle, mais ne peut être considéré comme un substitut à l'analyse détaillée de spécialistes de la sécurité ou de l'audit informatiques. Le sujet est techniquement complexe et, dans chaque banque, les systèmes et le matériel présentent des différences considérables en ce qui concerne les causes de perturbations et les techniques de contrôle mises en œuvre.

Dans un domaine aussi spécialisé, il serait particulièrement utile que les autorités de contrôle mettent à profit les compétences des *auditeurs externes*. Il faudrait les inciter à consacrer les ressources nécessaires à cette partie de leurs responsabilités.

Les banques devraient attirer l'attention des auditeurs externes sur cette question, en insérant dans la lettre d'engagement une clause stipulant que l'auditeur externe évalue périodiquement la solidité des procédures informatiques qui sont vitales pour les activités de l'établissement ainsi que l'efficacité des contrôles informatiques internes. Par ailleurs, les auditeurs externes devraient mentionner, dans leur compte rendu annuel aux dirigeants, les insuffisances et imperfections qu'ils ont décelées au cours de l'examen effectué dans ce domaine particulier.

Si les autorités de contrôle s'acquittent de leur tâche essentiellement par le biais d'*inspections sur place,* les inspecteurs procèdent également à des interviews, à l'examen de la documentation et à des tests au hasard. Néanmoins, il leur sera sans doute difficile, du fait de leur nombre restreint ou de la limitation de leurs qualifications, sans parler des contraintes budgétaires et autres, de suivre l'évolution des nouveaux systèmes informatiques. Il est indispensable aujourd'hui que le corps d'inspecteurs comprenne des spécialistes en informatique, dont la formation corresponde au degré de perfectionnement des systèmes des banques soumises à inspection.

Tant les inspecteurs que les auditeurs utilisent normalement pour leur travail dans le domaine informatique des aide-mémoire ou des guides de référence élaborés par les autorités de contrôle avec l'assistance d'institutions spécialisées; ces outils se révèlent extrêmement précieux.