

**CADRE D'ÉVALUATION
DES SYSTÈMES DE
CONTRÔLE INTERNE**

Comité de Bâle sur le contrôle bancaire

**Bâle
Janvier 1998**

Table des matières

| | Page |
|--|-------------|
| Introduction | 1 |
| I. Contexte général | 6 |
| II. Objectifs et rôle du cadre de contrôle interne | 8 |
| III. Principaux éléments d'un processus de contrôle interne | 10 |
| A. Surveillance par la direction et culture de contrôle | 10 |
| 1. Conseil d'administration | 10 |
| 2. Direction générale | 11 |
| 3. Culture de contrôle | 12 |
| B. Évaluation des risques | 13 |
| C. Activités de contrôle | 14 |
| D. Information et communication | 17 |
| E. Activités de surveillance | 19 |
| IV. Évaluation des systèmes de contrôle interne par les autorités prudentielles | 22 |
| V. Rôles et responsabilités des auditeurs externes | 25 |
| Annexe Enseignements prudentiels fournis par les cas de défaillances des contrôles internes | 26 |

Cadre d'évaluation des systèmes de contrôle interne

INTRODUCTION

1. Dans le sens de l'action qu'il poursuit pour résoudre les questions prudentielles et renforcer le contrôle des banques par des recommandations encourageant l'application de saines pratiques de gestion des risques, le Comité de Bâle sur le contrôle bancaire¹ sollicite les commentaires des autorités de contrôle et autres parties concernées sur le présent projet de cadre d'évaluation. Ce cadre a été conçu pour être utilisé par les autorités prudentielles dans leur évaluation des systèmes de contrôle interne des banques. Un système de contrôle interne efficace est une composante essentielle de la gestion d'un établissement et constitue le fondement d'un fonctionnement sûr et prudent d'une organisation bancaire. En se dotant de contrôles internes rigoureux, une banque pourra mieux réaliser ses buts et ses objectifs de rentabilité à long terme, en assurant également la fiabilité de sa communication financière tant externe qu'à sa direction. Un tel système peut aussi garantir que la banque agit dans le respect des lois et réglementations ainsi que de ses politiques, programmes, règles et procédures internes; il atténue, en outre, le risque de pertes imprévues ou d'atteinte à la réputation de l'établissement. Ce document décrit les éléments clés d'un système de contrôle interne sain, en se fondant sur l'expérience enregistrée dans les pays membres et sur les principes précisés dans les publications antérieures du Comité. Il entend définir certains principes destinés aux autorités prudentielles dans leur évaluation des systèmes de contrôle interne des banques.

2. Le Comité de Bâle, conjointement avec les autorités de contrôle bancaire du monde entier, insiste de plus en plus sur l'importance de contrôles internes sains. Cet intérêt accru s'explique en partie par les pertes substantielles subies par plusieurs organisations bancaires. L'analyse des problèmes liés à ces pertes montre qu'elles auraient probablement pu être évitées si les banques avaient été dotées de systèmes de contrôle interne efficaces. De tels systèmes auraient, en effet, empêché l'apparition de ces problèmes ou permis de les détecter, limitant ainsi les dommages causés aux organisations bancaires. En élaborant ces principes, le Comité a tiré des enseignements des situations des banques en difficulté dans les divers pays membres.

3. Ces principes se prêtent donc à une application générale, et les autorités de contrôle devraient s'y référer pour évaluer les méthodes et procédures qu'elles emploient pour voir comment les banques structurent leurs systèmes de contrôle interne. L'approche exacte

¹ Le Comité de Bâle sur le contrôle bancaire, institué en 1975 par les gouverneurs des banques centrales des pays du Groupe des Dix, rassemble les autorités de contrôle des banques. Il est composé de hauts représentants des autorités de contrôle bancaire et banques centrales d'Allemagne, de Belgique, du Canada, des États-Unis, de France, d'Italie, du Japon, du Luxembourg, des Pays-Bas, du Royaume-Uni, de Suède et de Suisse. Ses réunions ont habituellement pour cadre la Banque des Règlements Internationaux, à Bâle, siège de son Secrétariat permanent.

retenue par les divers responsables prudents sera fonction, bien entendu, de nombreux facteurs, dont leurs techniques de contrôle sur place et sur pièces, et de la part prise par les auditeurs externes dans l'exercice de la surveillance; néanmoins, **tous les membres du Comité de Bâle reconnaissent que les principes établis dans ce document devraient être utilisés pour évaluer le système de contrôle interne d'une banque.**

4. Le Comité de Bâle adresse ce document à l'ensemble des autorités de contrôle dans le monde, étant convaincu que les principes qu'il contient fourniront un cadre utile pour une surveillance efficace des systèmes de contrôle interne. D'une manière plus générale, le Comité désire souligner que des contrôles internes sains sont un élément essentiel à la conduite prudente de l'activité bancaire et qu'ils favorisent également la stabilité globale du système financier.

5. Les recommandations diffusées antérieurement par le Comité de Bâle comportaient généralement des analyses des contrôles internes portant sur des domaines spécifiques de l'activité bancaire, tels que le risque de taux d'intérêt et les opérations de négociation et sur instruments dérivés. Cette fois, cependant, elles présentent un cadre que le Comité encourage les autorités prudentielles à utiliser pour évaluer les contrôles internes sur l'ensemble des activités de bilan et de hors-bilan des organisations bancaires. Ces recommandations ne se concentrent pas sur des secteurs ou activités spécifiques au sein d'une banque, et leur application exacte dépend de la nature et de la complexité des opérations effectuées ainsi que des risques qu'elles comportent. Dans les sections III et IV, le Comité énonce quatorze principes à appliquer par les autorités de contrôle bancaire pour évaluer les systèmes de contrôle interne des banques. L'annexe, pour sa part, fournit des enseignements prudents tirés de cas antérieurs de contrôles internes insuffisants.

Principes pour l'évaluation des systèmes de contrôle interne

Surveillance par la direction et culture de contrôle

Principe 1:

Le conseil d'administration devrait être chargé d'approuver les stratégies et politiques, d'apprécier les risques encourus par la banque, de fixer des niveaux acceptables en regard de ces risques en s'assurant que la direction générale prend les dispositions nécessaires pour identifier, surveiller et contrôler ces risques, d'approuver la structure organisationnelle et de s'assurer que la direction générale surveille l'efficacité du système de contrôle interne.

Principe 2:

La direction générale devrait être chargée de mettre en œuvre les stratégies approuvées par le conseil, de définir des politiques de contrôle interne appropriées et de surveiller l'efficacité du système de contrôle interne.

Principe 3:

Le conseil d'administration et la direction générale sont chargés de promouvoir des critères élevés d'éthique et d'intégrité et d'instaurer, au sein de l'organisation bancaire, une culture qui souligne et démontre, à tous les niveaux du personnel, l'importance des contrôles internes. Tous les niveaux du personnel de l'organisation doivent comprendre leur rôle dans le contrôle interne et s'impliquer activement dans ce processus.

Évaluation des risques

Principe 4:

La direction générale devrait s'assurer qu'il est procédé à l'identification et à l'évaluation des facteurs internes et externes qui pourraient compromettre la réalisation des objectifs de la banque. Cette évaluation devrait couvrir l'ensemble des divers risques encourus par l'établissement (par exemple, risque de crédit, risque-pays et risque de transfert, risque de marché, risque de taux d'intérêt, risque de liquidité, risque opérationnel, risque juridique et risque de réputation).

Principe 5:

La direction générale devrait s'assurer que les risques affectant la réalisation des stratégies et objectifs de la banque font l'objet d'une évaluation permanente. Un réexamen des contrôles internes peut s'avérer nécessaire pour prendre en compte de manière appropriée tout risque nouveau ou jusque-là non contrôlé.

Activités de contrôle

Principe 6:

Les activités de contrôle devraient faire partie intégrante des opérations quotidiennes de la banque. La direction générale doit mettre en place une structure de contrôle appropriée pour garantir des contrôles internes efficaces, en définissant les activités de contrôle à chaque niveau opérationnel. Ces activités devraient inclure les éléments suivants: examens effectués au niveau supérieur; contrôles d'activité appropriés pour les différents départements ou unités; contrôles physiques; vérification périodique du respect des plafonds d'engagement; système d'approbation et d'autorisation; système de vérification et

de contrôle par rapprochement. La direction générale doit s'assurer régulièrement que tous les domaines de la banque se conforment aux politiques et procédures établies.

Principe 7:

La direction générale devrait s'assurer qu'il existe une séparation appropriée des tâches et que des responsabilités conflictuelles ne sont pas confiées à des membres du personnel. Les secteurs présentant des conflits d'intérêts potentiels devraient être identifiés, circonscrits aussi étroitement que possible et surveillés avec attention.

Information et communication

Principe 8:

La direction générale devrait s'assurer de l'existence de données internes adéquates et exhaustives – d'ordre financier, opérationnel ou ayant trait au respect de la conformité – ainsi que d'informations de marché extérieures sur des événements et conditions intéressant la prise de décision. Ces données et informations devraient être fiables, récentes, accessibles et présentées sous une forme cohérente.

Principe 9:

La direction générale devrait instituer des voies de communication efficaces pour garantir que l'ensemble du personnel est parfaitement informé des politiques et procédures affectant ses tâches et responsabilités et que les autres informations importantes parviennent à leurs destinataires.

Principe 10:

La direction générale doit s'assurer de l'existence de systèmes d'information appropriés couvrant toutes les activités de la banque. Ces systèmes, notamment ceux qui contiennent et utilisent des données informatisées, doivent être sûrs et faire l'objet de tests périodiques.

Surveillance

Principe 11:

La direction générale devrait surveiller en permanence l'efficacité globale des contrôles internes de la banque pour favoriser la réalisation des objectifs fixés. La surveillance des principaux risques devrait faire partie des opérations quotidiennes de la banque et comporter, au besoin, des évaluations spécifiques.

Principe 12:

Un audit interne efficace et exhaustif du système de contrôle interne devrait être effectué par un personnel bien formé et compétent. La fonction d'audit interne, en tant qu'élément de la surveillance du système de contrôle interne, devrait rendre compte directement au conseil d'administration, ou à son comité d'audit, ainsi qu'à la direction générale.

Principe 13:

Les carences détectées dans les contrôles internes devraient être notifiées dans les meilleurs délais au niveau de direction approprié et faire l'objet d'un traitement rapide. Les déficiences importantes devraient être signalées à la direction générale et au conseil d'administration.

Évaluation des systèmes de contrôle interne par les autorités prudentielles

Principe 14:

Les autorités prudentielles devraient exiger que toutes les banques, quelle que soit leur dimension, disposent d'un système efficace de contrôle interne qui corresponde à la nature, à la complexité et au degré de risque de leurs activités de bilan et de hors-bilan et réagisse aux modifications de l'environnement et des conditions d'activité de la banque. Dans les cas où les autorités prudentielles constatent que le système de contrôle interne n'est pas adéquat (s'il ne prend pas en compte, par exemple, tous les principes contenus dans ce document), elles devraient intervenir auprès de la banque pour s'assurer que des améliorations sont apportées immédiatement.

6. Toutes les parties concernées sont invitées à faire part de leurs commentaires sur les divers aspects de ce document, dont l'annexe, jusqu'au 30 mars 1998.

I. Contexte général

1. Le Comité de Bâle a analysé certains cas récents de banques en difficulté, afin d'identifier les principales sources des problèmes de contrôle interne. Les problèmes mis à jour renforcent l'idée qu'il est important que les administrateurs et la direction des banques, les auditeurs internes et externes ainsi que les autorités de contrôle bancaire consacrent une attention soutenue au renforcement des systèmes de contrôle interne et à l'évaluation permanente de leur efficacité. Plusieurs de ces cas montrent que des contrôles internes insuffisants peuvent entraîner des pertes bancaires substantielles.

2. Les formes de déficiences des contrôles observées généralement dans les banques en difficulté peuvent être classées en cinq grandes catégories.

- ***Défaillances dans la surveillance et l'exercice des responsabilités de la part de la direction et absence d'une forte culture de contrôle au sein de la banque.*** Les cas de pertes importantes reflètent tous, sans exception, un manque d'attention et de rigueur de la direction envers la culture de contrôle dans la banque, une orientation et une surveillance insuffisantes de la part du conseil d'administration et de la direction générale ainsi que l'absence d'un exercice clair de ses responsabilités de la part de la direction dans l'attribution des rôles et des tâches. Ces cas révèlent également des incitations insuffisantes à exercer une surveillance hiérarchique rigoureuse et à maintenir un niveau élevé de conscience du contrôle au sein des divers secteurs d'activité.
- ***Évaluation inadéquate du risque inhérent à certaines activités bancaires, tant de bilan que de hors-bilan.*** De nombreuses organisations bancaires ayant subi des pertes substantielles négligeaient d'évaluer en permanence les risques liés aux nouveaux produits et activités ou de revoir leurs estimations des risques en fonction des modifications notables de l'environnement ou des conditions d'activité. Plusieurs cas récents montrent clairement que des systèmes de contrôle efficaces pour des produits traditionnels ou simples sont inopérants pour des instruments plus sophistiqués ou complexes.
- ***Absence ou déficience d'éléments clés du contrôle, tels que séparation des tâches, approbations, vérifications, concordances, analyses des résultats d'exploitation.*** La non-séparation des tâches, en particulier, a joué un rôle majeur dans les pertes sensibles enregistrées par les banques.
- ***Mauvaise communication de l'information entre les niveaux de direction dans la banque, spécialement vers le haut pour signaler les problèmes.*** Pour être efficaces, les politiques et procédures doivent être communiquées de manière effective à l'ensemble du personnel associé à une activité. Certaines pertes bancaires ont été dues au fait que des agents directement concernés ne connaissaient pas ou ne comprenaient pas les

politiques de l'établissement. Dans plusieurs cas, des informations sur des activités inappropriées qui auraient dû être transmises à la direction par la voie hiérarchique n'ont été notifiées au conseil d'administration ou à la direction générale que lorsque les problèmes étaient devenus graves. Dans d'autres cas, le contenu des rapports à la direction était insuffisant ou inexact, donnant ainsi une impression favorable sur la situation d'une activité qui était, en fait, problématique.

- ***Programmes d'audit et autres activités de surveillance inadéquats ou inefficaces.*** Très souvent, les audits effectués n'étaient pas suffisamment rigoureux pour déceler et notifier les insuffisances du contrôle dans les banques en difficulté. Dans d'autres cas, même si les auditeurs ont fait part des problèmes, ceux-ci n'ont pas été corrigés par la direction.

3. Le cadre de contrôle interne qui sous-tend ces recommandations est fondé sur les pratiques suivies actuellement dans de nombreuses grandes banques, entreprises d'investissement et sociétés non financières ainsi que par leurs auditeurs. En outre, ce cadre d'évaluation va dans le sens de l'importance accrue donnée par les autorités de contrôle bancaire à l'examen des processus de gestion du risque et de contrôle interne dans une organisation bancaire. Il importe de souligner que le conseil d'administration et la direction générale sont chargés de s'assurer de l'existence de contrôles internes adéquats et de promouvoir un environnement dans lequel les individus comprennent et assument sérieusement leurs responsabilités dans ce domaine. Les autorités de contrôle bancaire, pour leur part, ont mission d'évaluer l'engagement du conseil d'administration et de la direction de la banque à l'égard du processus de contrôle interne.

II. Objectifs et rôle du cadre de contrôle interne

4. Le contrôle interne est un *processus* mis en œuvre par le conseil d'administration², la direction générale et tous les niveaux du personnel. Il ne s'agit pas simplement d'une procédure ou d'une politique appliquée à un certain moment, mais plutôt d'un système qui fonctionne en continu à tous les niveaux de la banque. Le conseil d'administration et la direction générale sont chargés d'instaurer la culture appropriée capable de favoriser un processus de contrôle interne efficace et d'en vérifier en permanence l'efficacité; il importe toutefois que tous les membres du personnel y participent activement. Les principaux objectifs du processus de contrôle interne³ peuvent être classés en trois groupes:

1. efficacité et efficacie des opérations (objectifs opérationnels);
2. fiabilité et exhaustivité des données financières et des informations destinées à la direction (objectifs d'information);
3. conformité aux lois et réglementations applicables (objectifs de conformité).

5. Les *objectifs opérationnels* de contrôle interne concernent l'efficacité et l'efficacie de la banque dans l'utilisation de ses actifs et autres ressources ainsi que dans sa protection en cas de pertes. Le processus de contrôle interne cherche à s'assurer que l'ensemble du personnel œuvre avec droiture à la réalisation des objectifs, sans occasionner des coûts imprévus ou excessifs ni privilégier d'autres intérêts (tels que ceux d'un employé, d'un fournisseur ou d'un client) que ceux de l'établissement.

6. Les *objectifs d'information* portent sur la préparation de rapports fiables et aussi récents que possible, indispensables à la prise de décision au sein de l'organisation bancaire. Ils recouvrent également la nécessité d'établir des comptes annuels, états financiers et autres communications financières qui soient fiables, qu'il s'agisse des informations destinées aux autorités prudentielles ou à d'autres usages externes. Les données reçues par la direction, le conseil d'administration, les actionnaires et les autorités de contrôle devraient être d'une qualité et d'une intégrité suffisantes pour que leurs bénéficiaires puissent s'y référer pour fonder leurs décisions. Le terme fiable, appliqué aux états financiers, se rapporte à la

² Ce document se réfère à une structure de gestion composée d'un conseil d'administration et d'une direction générale. Le Comité est conscient de l'existence de différences notables entre les cadres législatifs et réglementaires des divers pays, en ce qui concerne les fonctions de ces deux instances. Dans certains pays, le conseil est chargé principalement, mais non exclusivement, de superviser l'organe exécutif (direction générale), afin de s'assurer qu'il s'acquitte de ses tâches; il est parfois appelé, pour cette raison, conseil de surveillance et n'a pas de rôle exécutif. Dans d'autres, en revanche, il détient une autorité plus large, en ce sens qu'il élabore le cadre général de gestion de la banque. Du fait de ces différences, les notions de conseil d'administration et de direction générale sont utilisées dans ce document non pas pour identifier des structures juridiques, mais plutôt pour désigner deux niveaux de prise de décision au sein d'une banque.

³ Il inclut les contrôles internes sur la préservation des actifs et autres ressources contre une acquisition, un usage ou un transfert non autorisé ou en cas de pertes.

préparation de documents établis sur une base sincère à partir de principes et règles comptables exhaustifs et bien définis.

7. Les *objectifs de conformité* garantissent que toute l'activité bancaire est conduite en conformité avec les lois ou réglementations et exigences prudentielles applicables ainsi qu'avec les politiques et procédures internes. Cet objectif doit être satisfait pour préserver les droits et la réputation de la banque.

III. Principaux éléments d'un processus de contrôle interne

8. Le processus de contrôle interne, qui visait traditionnellement à réduire la fraude, les détournements de fonds et les erreurs, a récemment pris une dimension plus vaste et recouvre l'ensemble des risques encourus par les organisations bancaires. Il est reconnu à présent qu'un processus de contrôle interne sain est essentiel pour qu'une banque puisse réaliser les objectifs qu'elle s'est fixés et maintenir sa viabilité financière.

9. Le contrôle interne consiste en cinq éléments étroitement liés:

1. Surveillance par la direction et culture de contrôle
2. Évaluation des risques
3. Activités de contrôle
4. Information et communication
5. Activités de surveillance.

Les problèmes rencontrés dans les cas récents de pertes bancaires importantes entrent dans ces cinq catégories. Le fonctionnement efficace de ces éléments est capital pour la réalisation des objectifs opérationnels, d'information et de conformité d'une banque.

A. Surveillance par la direction et culture de contrôle

1. Conseil d'administration

Principe 1: Le conseil d'administration devrait être chargé d'approuver les stratégies et politiques, d'apprécier les risques encourus par la banque, de fixer des niveaux acceptables en regard de ces risques en s'assurant que la direction générale prend les dispositions nécessaires pour identifier, surveiller et contrôler ces risques, d'approuver la structure organisationnelle et de s'assurer que la direction générale surveille l'efficacité du système de contrôle interne.

10. Le conseil d'administration a une mission de gouvernance, d'orientation et de surveillance vis-à-vis de la direction générale. Il est chargé de fixer les grandes stratégies et les principales politiques de l'organisation et d'approuver sa structure organisationnelle globale. Il lui incombe en dernier ressort de veiller à la mise en place et à l'application d'un système adéquat de contrôle interne. Pour être efficaces, ses membres doivent être objectifs, compétents et scrupuleux et connaître les activités de la banque ainsi que les risques qu'elle encourt. Un conseil d'administration fort et actif, surtout lorsqu'il est associé à des canaux de communication faisant bien remonter l'information et à des organes financiers, juridiques et d'audit interne efficaces, est souvent le mieux en mesure de résoudre les problèmes qui pourraient amoindrir l'efficacité du système de contrôle interne.

11. Le conseil d'administration devrait inclure dans ses activités 1) des discussions régulières avec la direction sur l'efficacité du système de contrôle interne, 2) un examen, dans les délais les plus brefs, des évaluations sur les contrôles internes effectuées par la direction et les auditeurs internes et externes, 3) des actions répétées pour s'assurer que la direction a pris en compte de manière appropriée les recommandations et préoccupations exprimées par les auditeurs et autorités de contrôle au sujet des carences du contrôle interne.

12. Une option utilisée par les banques de nombreux pays consiste à instaurer un comité d'audit indépendant pour assister le conseil dans l'exercice de ses responsabilités. Cela permet d'examiner dans le détail des informations et rapports sans devoir mobiliser tous les administrateurs et d'apporter toute l'attention nécessaire à certaines questions particulières. Le comité d'audit est généralement responsable du suivi du processus de communication financière et du système de contrôle interne. Dans le cadre de cette responsabilité, il est attentif aux opérations du département d'audit interne de la banque, auquel il sert de contact direct; il engage également les auditeurs externes et en est l'interlocuteur privilégié. Dans les pays optant pour un comité d'audit, celui-ci devrait être entièrement composé d'administrateurs extérieurs (c'est-à-dire de membres du conseil qui ne sont employés ni par la banque ni par l'un de ses établissements affiliés) possédant une compétence en matière de communication financière et de contrôle interne. Il convient de noter que la constitution d'un comité d'audit ne devrait en aucun cas décharger le conseil plénier de ses tâches, lui seul étant juridiquement mandaté à prendre des décisions.

2. Direction générale

Principe 2: La direction générale devrait être chargée de mettre en œuvre les stratégies approuvées par le conseil, de définir des politiques de contrôle interne appropriées et de surveiller l'efficacité du système de contrôle interne.

13. Il incombe à la direction générale de mettre en œuvre les directives approuvées par le conseil d'administration, en appliquant notamment les stratégies et politiques de la banque et en instaurant un système de contrôle interne efficace. Pour l'élaboration des politiques et procédures de contrôle interne plus spécifiques, les membres de la direction générale délèguent habituellement leur responsabilité aux personnes chargées des activités ou fonctions d'une unité particulière. Il est donc important que la direction générale s'assure que ces personnes établissent et conduisent les politiques et procédures appropriées.

14. Le respect de la conformité à un système de contrôle interne passe en grande partie par une structure organisationnelle parfaitement transparente et connue de l'ensemble du personnel, montrant clairement les niveaux de responsabilité et d'autorité en matière de notification et permettant une communication adéquate dans l'ensemble de l'organisation. La répartition des tâches et responsabilités devrait garantir l'absence de ruptures dans la chaîne

hiérarchique et l'exercice d'un degré de contrôle efficace par la direction à tous les niveaux de la banque et dans toutes ses activités.

15. Il importe que la direction générale prenne des mesures pour garantir que les activités sont conduites par du personnel qualifié possédant l'expérience et les capacités techniques requises. Le personnel devrait bénéficier d'une rémunération appropriée ainsi que d'une remise à niveau périodique de sa formation et de ses compétences. La direction générale devrait instaurer des politiques de rémunération et de promotion récompensant les comportements adéquats et réduisant au maximum les incitations, pour les agents, à ignorer ou à contourner les mécanismes de contrôle interne.

3. Culture de contrôle

Principe 3: Le conseil d'administration et la direction générale sont chargés de promouvoir des critères élevés d'éthique et d'intégrité et d'instaurer, au sein de l'organisation bancaire, une culture qui souligne et démontre, à tous les niveaux du personnel, l'importance des contrôles internes. Tous les niveaux du personnel de l'organisation doivent comprendre leur rôle dans le contrôle interne et s'impliquer activement dans ce processus.

16. L'un des éléments essentiels d'un système de contrôle interne efficace réside dans une culture de contrôle forte. Il incombe au conseil d'administration et à la direction générale de souligner, dans les termes utilisés et les actions entreprises, l'importance du contrôle interne; cela passe notamment par les valeurs éthiques mises en avant par la direction dans son comportement professionnel, tant à l'intérieur qu'à l'extérieur de l'organisation. Les termes, actes et attitudes de ces deux instances affectent l'intégrité, l'éthique et les autres aspects de la culture de contrôle d'un établissement.

17. À des degrés divers, le contrôle interne relève de la responsabilité de chacun. Presque tous les employés produisent des informations utilisées dans le système de contrôle interne ou effectuent d'autres actions indispensables à l'exercice du contrôle. Un élément clé d'un système de contrôle interne fort est la conscience, pour chaque employé, de la nécessité d'assumer ses tâches de manière efficace et de notifier au niveau de direction approprié tout problème rencontré dans le cadre des opérations, toute infraction au code de conduite ainsi que toute violation des politiques établies ou action illégale constatée. L'idéal, à cet effet, est que les procédures opérationnelles soient clairement précisées par écrit et mises à la disposition de l'ensemble du personnel concerné. Il est essentiel que tous les agents de la banque comprennent l'importance du contrôle interne et s'impliquent activement dans ce processus.

18. En renforçant les valeurs éthiques, les organisations bancaires devraient éviter des politiques et pratiques pouvant engendrer par mégarde des incitations ou des tentations à

effectuer des activités inappropriées: importance exagérée donnée aux objectifs de performance ou autres résultats opérationnels, particulièrement à court terme; gratifications élevées liées aux performances; séparation inefficace des tâches ou d'autres fonctions de contrôle pouvant conduire à mal utiliser les ressources ou à dissimuler des performances médiocres; sanctions minimales ou excessives en cas de comportement incorrect.

19. Si l'existence d'une forte culture de contrôle interne ne garantit pas à une organisation d'atteindre ses objectifs, son absence augmente les risques d'erreurs non décelées ou d'irrégularités.

B. Évaluation des risques

20. Dans la perspective du contrôle interne, l'évaluation des risques devrait déceler et apprécier les facteurs internes et externes pouvant compromettre la réalisation des objectifs opérationnels, d'information et de conformité d'une organisation bancaire. Cette analyse devrait prendre en compte des risques tels que le risque de crédit, le risque de marché, le risque de liquidité et le risque opérationnel (lequel inclut le risque de fraude, de détournement d'actifs et d'informations financières douteuses). Il existe une différence notable entre l'évaluation des risques dans le contexte du processus de contrôle interne et le concept plus large de «gestion des risques» dans l'activité globale d'une banque. Dans une organisation bancaire, cette gestion des risques consiste à établir des objectifs organisationnels et autres (en matière de rentabilité, par exemple) et à déterminer, mesurer et fixer les plafonds d'engagement que la banque acceptera pour les atteindre. L'objet du contrôle interne est alors de s'assurer que les objectifs et politiques sont communiqués et appliqués, que le respect des plafonds est soumis à surveillance et que les déviations sont corrigées dans le sens des politiques de la direction. Par conséquent, le concept de gestion des risques s'étend, mais ne se limite pas, à l'évaluation des risques et à la fixation d'objectifs opérationnels tels qu'ils sont définis aux fins du contrôle interne.

Principe 4: La direction générale devrait s'assurer qu'il est procédé à l'identification et à l'évaluation des facteurs internes et externes qui pourraient compromettre la réalisation des objectifs de la banque. Cette évaluation devrait couvrir l'ensemble des divers risques encourus par l'établissement (par exemple, risque de crédit, risque-pays et risque de transfert, risque de marché, risque de taux d'intérêt, risque de liquidité, risque opérationnel, risque juridique et risque de réputation).

21. Une évaluation efficace des risques recense et analyse les facteurs internes (nature des activités de la banque, qualité du personnel, modifications organisationnelles et mouvements d'effectifs) et externes (évolution des conditions économiques, changements au sein de la profession et progrès technologique) pouvant compromettre la réalisation des

objectifs de la banque. Cette évaluation devrait être effectuée au niveau de chaque département opérationnel ainsi que pour l'ensemble des activités et filiales de l'organisation bancaire consolidée et peut s'opérer par diverses méthodes. Pour être efficace, elle doit porter à la fois sur les risques mesurables (risque de crédit, risque de marché et risque de liquidité) et non mesurables (risque opérationnel, risque juridique et risque de réputation).

22. Le processus d'évaluation des risques nécessite également de déterminer ceux qui sont contrôlables par la banque et ceux qui ne le sont pas. Pour les premiers, la banque doit établir si elle accepte ces risques ou si elle préfère les limiter au moyen de procédures de contrôle. Pour ceux qui ne peuvent pas être contrôlés, la banque doit décider soit de les accepter, soit de se désengager, soit encore de réduire le niveau de l'activité concernée.

Principe 5: La direction générale devrait s'assurer que les risques affectant la réalisation des stratégies et objectifs de la banque font l'objet d'une évaluation permanente. Un réexamen des contrôles internes peut s'avérer nécessaire pour prendre en compte de manière appropriée tout risque nouveau ou jusque-là non contrôlé.

23. Pour que l'évaluation des risques et, par conséquent, le système de contrôle interne demeurent efficaces, la direction générale doit considérer en permanence les risques pouvant entraver la réalisation des objectifs de la banque et réagir aux modifications des circonstances et des conditions d'activité. Il peut s'avérer nécessaire de revoir les contrôles internes, afin de bien prendre en compte des risques nouveaux ou jusque-là non contrôlés. Par exemple, avec l'innovation financière, une banque doit évaluer les nouveaux instruments financiers et opérations de marché et examiner les risques qu'ils font encourir. Souvent, la meilleure façon de comprendre ces risques est de voir comment divers scénarios (économiques ou autres) affectent les flux de trésorerie et le rendement des transactions et instruments financiers. Un examen attentif de l'éventail des problèmes possibles, allant des malentendus avec la clientèle aux défaillances opérationnelles, soulignera certains aspects importants en matière de contrôle.

C. Activités de contrôle

Principe 6: Les activités de contrôle devraient faire partie intégrante des opérations quotidiennes de la banque. La direction générale doit mettre en place une structure de contrôle appropriée pour garantir des contrôles internes efficaces, en définissant les activités de contrôle à chaque niveau opérationnel. Ces activités devraient inclure les éléments suivants: examens effectués au niveau supérieur; contrôles d'activité appropriés pour les différents départements ou unités; contrôles physiques; vérification périodique du respect des plafonds d'engagement; système d'approbation et

d'autorisation; système de vérification et de contrôle par rapprochement. La direction générale doit s'assurer régulièrement que tous les domaines de la banque se conforment aux politiques et procédures établies.

24. Les activités de contrôle sont conçues et mises en œuvre pour faire face aux risques décelés par la banque par le biais du processus d'évaluation des risques décrit précédemment. Ces activités comportent trois étapes: 1) l'établissement des politiques; 2) la performance des procédures au regard de ces politiques; 3) la vérification du respect de la conformité aux politiques. Les activités de contrôle se situent à tous les niveaux du personnel de la banque, y compris la direction générale et les personnels directement en contact avec le marché. Voici différents exemples d'activités de contrôle.

- *Examens effectués au niveau supérieur* – Le conseil d'administration et la direction générale demandent souvent des présentations et comptes rendus de résultats qui leur permettent d'évaluer les progrès réalisés par la banque vers ses objectifs. Par exemple, la direction générale peut vouloir consulter des rapports indiquant les résultats financiers effectifs en cours d'exercice par rapport au budget. Les questions de la direction générale qui en résultent et les réponses fournies par les niveaux hiérarchiques inférieurs constituent une activité de contrôle qui peut mettre en évidence des problèmes, tels que carences du contrôle, erreurs dans la communication financière interne ou fraudes.
- *Contrôles d'activité* – La direction, au niveau d'un département ou d'une unité, reçoit et examine des comptes rendus normaux ou exceptionnels sur une base quotidienne, hebdomadaire ou mensuelle. Les examens fonctionnels sont plus fréquents que ceux effectués au niveau supérieur et sont habituellement plus détaillés. Par exemple, le responsable du secteur des prêts commerciaux consulte des rapports hebdomadaires sur les défauts de paiement, les paiements reçus et les revenus d'intérêts produits par le portefeuille, tandis que le responsable du crédit au sein de la direction générale a connaissance de documents similaires une fois par mois et sous une forme plus condensée couvrant toutes les catégories de prêts. Comme pour les examens au niveau supérieur, les questions qui résultent de l'analyse des rapports et les réponses qu'elles amènent représentent l'activité de contrôle.
- *Contrôles physiques* – Les contrôles physiques portent en général sur les limitations d'accès aux actifs physiques, dont les titres et autres actifs financiers. Les activités de contrôle incluent les restrictions physiques, la double conservation et les inventaires périodiques.

- *Conformité aux plafonds d'engagement* – L'établissement de limites prudentes sur les engagements constitue un élément majeur de la gestion des risques. Par exemple, la conformité aux limites fixées pour les emprunteurs et les autres contreparties réduit la concentration du risque de crédit de la banque et permet de diversifier son profil de risque. Par conséquent, un aspect important des contrôles internes réside dans la vérification, à intervalles réguliers, du respect de telles limites.
- *Approbaton et autorisation* – La nécessité de solliciter une approbation et une autorisation pour les transactions dépassant certaines limites garantit qu'un niveau de direction approprié a connaissance de la transaction ou de la situation, ce qui aide à établir les responsabilités.
- *Vérification et concordance* – La vérification des caractéristiques détaillées des transactions ainsi que des diverses activités et des résultats fournis par les modèles de gestion des risques utilisés par la banque constitue une activité de contrôle importante. La concordance périodique, par exemple entre les flux de trésorerie et les rapports et états financiers, peut mettre en évidence des activités et enregistrements comptables exigeant d'être amendés. Par conséquent, les conclusions de ces contrôles devraient être notifiées régulièrement aux niveaux de direction appropriés.

25. Les activités de contrôle ont leur efficacité optimale lorsque la direction et l'ensemble du personnel les considèrent comme faisant intrinsèquement partie, et non comme un complément, des opérations quotidiennes de la banque. Lorsque les contrôles sont vus comme un complément des opérations de chaque jour, ils sont souvent jugés moins importants et peuvent ne pas être réalisés dans des situations où des agents s'estiment pressés par le temps pour effectuer leurs activités. En outre, les contrôles qui sont véritablement intégrés aux opérations quotidiennes permettent de réagir rapidement à des modifications des conditions et évitent des coûts inutiles. Dans le cadre de l'action visant à instaurer la culture de contrôle appropriée au sein d'une banque, la direction générale devrait s'assurer que les activités de contrôle adéquates font véritablement partie des fonctions quotidiennes de l'ensemble du personnel concerné.

26. La direction générale ne doit pas se contenter de définir des politiques et procédures appropriées pour les diverses activités et unités de la banque. Elle doit s'assurer périodiquement que tous les domaines de la banque opèrent en conformité avec ces politiques et procédures et faire en sorte également que les politiques et procédures existantes demeurent adéquates. Cette fonction entre habituellement dans les attributions du département d'audit interne.

Principe 7: La direction générale devrait s'assurer qu'il existe une séparation appropriée des tâches et que des responsabilités conflictuelles ne sont pas confiées à des membres du personnel. Les secteurs présentant des conflits d'intérêts potentiels devraient être identifiés, circonscrits aussi étroitement que possible et surveillés avec attention.

27. Dans les cas de pertes bancaires importantes dues à un contrôle interne insuffisant, les autorités prudentielles constatent en général que l'une des causes principales réside dans l'absence de séparation adéquate des tâches. Le fait de confier à la même personne des responsabilités conflictuelles (par exemple, celles des fonctions de marché et de postmarché d'une unité de négociation) lui donne la possibilité d'avoir accès à des actifs de valeur et de manipuler des données financières en vue d'un profit personnel ou de dissimuler des pertes. C'est pourquoi, au sein d'une banque, certaines tâches devraient être réparties entre plusieurs individus, afin de réduire le risque de manipulation de données financières ou de détournement d'actifs.

28. La séparation des tâches ne concerne pas seulement des situations où la même personne contrôle à la fois la salle des marchés et le postmarché. En l'absence de contrôles appropriés, de sérieux problèmes peuvent également se poser lorsqu'un individu est chargé:

- de l'approbation du décaissement de fonds et de leur décaissement effectif;
- des comptes clientèle et des comptes propres;
- des transactions au titre du portefeuille bancaire et du portefeuille de négociation;
- de la fourniture informelle d'informations à des clients sur leurs positions et de la relation commerciale avec ces mêmes clients;
- de l'évaluation du caractère adéquat des dossiers de crédit et de la surveillance des emprunteurs après l'octroi des crédits;
- de tout autre domaine où des conflits d'intérêts notables apparaissent et ne sont pas atténués par d'autres facteurs.

29. Les domaines de conflits potentiels devraient être identifiés, circonscrits aussi étroitement que possible et surveillés avec attention. Des examens périodiques des responsabilités et fonctions des personnes détenant les postes clés devraient être également effectués pour s'assurer que ces responsables ne sont pas en mesure de dissimuler des agissements inappropriés.

D. Information et communication

Principe 8: La direction générale devrait s'assurer de l'existence de données internes adéquates et exhaustives – d'ordre financier, opérationnel ou ayant trait au respect de la

conformité – ainsi que d'informations de marché extérieures sur des événements et conditions intéressant la prise de décision. Ces données et informations devraient être fiables, récentes, accessibles et présentées sous une forme cohérente.

30. Une information adéquate et une communication efficace sont deux éléments essentiels au bon fonctionnement d'un système de contrôle interne. S'agissant des banques, pour que l'information soit utile, elle doit être pertinente, fiable, récente, accessible et présentée sous une forme cohérente. Il peut s'agir de données internes d'ordre financier, opérationnel ou ayant trait au respect de la conformité ainsi que d'informations de marché extérieures sur des événements et conditions intéressant la prise de décision. L'information interne fait partie d'un processus d'enregistrement qui devrait comporter des procédures définies pour la conservation des supports d'enregistrement.

Principe 9: La direction générale devrait instituer des voies de communication efficaces pour garantir que l'ensemble du personnel est parfaitement informé des politiques et procédures affectant ses tâches et responsabilités et que les autres informations importantes parviennent à leurs destinataires.

31. En l'absence d'une communication efficace, l'information est inutile. La direction générale d'une banque doit instaurer des voies effectives de communication, afin que les informations nécessaires parviennent à leurs destinataires. Ces informations portent à la fois sur les politiques et procédures opérationnelles de l'établissement ainsi que sur les résultats d'exploitation réels.

32. La structure organisationnelle de la banque devrait faciliter la libre circulation – horizontale et verticale – de l'information dans toute l'organisation. Une telle structure garantit que les informations remontent et permet au conseil d'administration et à la direction générale de connaître les risques encourus dans le cadre de l'activité et les résultats d'exploitation. L'information qui redescend à travers l'organisation garantit que les objectifs, les stratégies, et aussi les attentes, de la banque ainsi que les politiques et procédures établies sont communiqués au niveau de direction inférieur et au personnel chargé des opérations. Cette communication est essentielle pour obtenir un effort commun de tous les employés vers les objectifs de la banque. Enfin, la communication horizontale dans l'organisation est nécessaire pour que l'information parvenant à une unité ou un département puisse être connue des autres unités ou départements concernés.

Principe 10: La direction générale doit s'assurer de l'existence de systèmes d'information appropriés couvrant toutes les activités de la banque. Ces systèmes, notamment ceux qui contiennent et utilisent des données informatisées, doivent être sûrs et faire l'objet de tests périodiques.

33. Un élément essentiel des opérations d'une banque réside dans la mise en place et la maintenance de systèmes d'information de la direction couvrant toute la gamme des activités. Cette information est habituellement fournie sous forme à la fois électronique et non électronique. Les banques doivent être tout particulièrement informées des exigences organisationnelles et de contrôle interne liées au traitement électronique de l'information.

34. Les systèmes électroniques et l'utilisation de l'informatique présentent des risques qui doivent être efficacement contrôlés par les banques, afin d'éviter des dysfonctionnements et des pertes potentielles. Les contrôles sur les systèmes et la technologie informatiques devraient être à la fois généraux et spécifiques aux applications. Les contrôles généraux portent sur le système informatique (c'est-à-dire ordinateur central et terminaux d'utilisateur) et en assurent un fonctionnement correct en continu. Ils incluent notamment des procédures de sauvegarde et de reprise, des politiques de développement et d'acquisition de logiciels, des procédures de maintenance et des contrôles de sécurité d'accès. Les contrôles liés aux applications sont des étapes informatisées au sein des applications logicielles et d'autres procédures manuelles qui examinent le traitement des opérations. Ils comprennent, entre autres, les questions de réconciliations et de concordances. En l'absence de contrôles adéquats sur les systèmes et la technologie informatiques, y compris ceux qui sont en cours de développement, les banques pourraient subir des pertes de données et de programmes résultant de dispositions inappropriées en matière de sécurité physique et électronique, de défaillances des équipements ou systèmes et de procédures inadéquates de sauvegarde et de reprise. Au niveau de la direction, la prise de décision pourrait être faussée par des informations non fiables ou erronées fournies par des systèmes mal conçus et insuffisamment contrôlés. Le traitement de l'information pourrait être entravé, voire totalement stoppé, s'il n'est pas possible, en cas de défaillance prolongée de l'équipement, de recourir à des installations de secours compatibles. Dans des situations extrêmes, de tels problèmes pourraient causer de sérieuses difficultés aux banques et même compromettre leur capacité d'effectuer leurs activités essentielles.

E. Activités de surveillance

Principe 11: La direction générale devrait surveiller en permanence l'efficacité globale des contrôles internes de la banque pour favoriser la réalisation des objectifs fixés. La surveillance des principaux risques devrait faire partie des opérations quotidiennes de la banque et comporter, au besoin, des évaluations spécifiques.

35. L'activité bancaire est un secteur dynamique, où tout évolue rapidement. Les banques doivent en permanence surveiller et évaluer leurs systèmes de contrôle interne en

fonction des modifications des conditions internes et externes et les renforcer, au besoin, pour en garantir l'efficacité.

36. Surveiller l'efficacité des contrôles internes devrait faire partie des opérations quotidiennes de la banque mais commande également de procéder à des évaluations périodiques spécifiques de l'ensemble du processus de contrôle interne. La fréquence de la surveillance des différentes activités devrait être fonction des risques encourus ainsi que du rythme et de la nature des changements affectant l'environnement opérationnel. Un processus de surveillance en continu peut permettre de découvrir et de corriger rapidement les déficiences du système de contrôle interne; il atteint son efficacité maximale lorsque le système de contrôle interne est intégré à l'environnement opérationnel et donne lieu à des rapports réguliers qui font l'objet d'un examen. Dans le cadre de la surveillance en continu figurent, par exemple, l'examen et l'approbation des enregistrements courants ainsi que la consultation et l'approbation par la direction des rapports sur des faits exceptionnels.

37. En revanche, les évaluations spécifiques ne détectent généralement les problèmes qu'après coup; elles permettent cependant à une organisation d'avoir un aperçu récent et global de l'efficacité du système de contrôle interne et de celle, en particulier, de ses activités de surveillance. Ces évaluations du système de contrôle interne prennent souvent la forme d'autoévaluations, lorsque les personnes chargées d'une fonction précise déterminent le degré d'efficacité des contrôles pour leurs activités. Les documents et résultats concernant les évaluations sont ensuite soumis à l'attention de la direction générale. Les examens effectués à tous les niveaux devraient être étayés par une documentation adéquate et communiqués dans les meilleurs délais à l'échelon de direction approprié.

Principe 12: Un audit interne efficace et exhaustif du système de contrôle interne devrait être effectué par un personnel bien formé et compétent. La fonction d'audit interne, en tant qu'élément de la surveillance du système de contrôle interne, devrait rendre compte directement au conseil d'administration, ou à son comité d'audit, ainsi qu'à la direction générale.

38. La fonction d'audit interne constitue un élément majeur de la surveillance en continu du système de contrôle interne, parce qu'elle fournit une évaluation indépendante du caractère adéquat des contrôles instaurés et du respect de la conformité à ces derniers. En rendant compte directement au conseil d'administration ou à son comité d'audit ainsi qu'à la direction générale, les auditeurs internes procurent des informations objectives sur les différentes activités. En raison de l'importance de cette fonction, l'audit interne doit être assuré par un personnel compétent et bien formé ayant une parfaite compréhension de son rôle et de ses responsabilités. La fréquence et l'ampleur des examens et tests des contrôles internes effectués au sein d'une banque par les auditeurs internes devraient correspondre à la nature et à la complexité des activités de l'organisation et aux risques associés. Dans tous les cas, il est

capital que la fonction d'audit interne soit indépendante du fonctionnement de la banque au quotidien et qu'elle ait accès à toutes les activités conduites par l'organisation bancaire.

39. Il est important que la fonction d'audit interne rende compte directement au plus haut niveau de l'organisation bancaire, habituellement le conseil d'administration ou son comité d'audit, et à la direction générale. Cela permet à la gouvernance d'entreprise de s'exercer correctement, le conseil bénéficiant d'informations qui ne sont altérées en aucune façon par les niveaux de direction couverts par ces comptes rendus. Le conseil devrait également renforcer l'indépendance des auditeurs internes, en faisant en sorte que des questions ayant trait, par exemple, à leur rémunération ou aux affectations budgétaires les concernant soient traitées par le conseil ou par les niveaux de direction supérieurs plutôt que par des responsables qui sont affectés par les travaux des auditeurs internes.

Principe 13: Les carences détectées dans les contrôles internes devraient être notifiées dans les meilleurs délais au niveau de direction approprié et faire l'objet d'un traitement rapide. Les déficiences importantes devraient être signalées à la direction générale et au conseil d'administration.

40. Les déficiences des contrôles internes, ou les politiques ou procédures inefficaces, devraient être signalées dès leur détection à la ou aux personnes appropriées, les problèmes graves étant portés à l'attention de la direction générale et du conseil d'administration. Lorsque ces insuffisances ont été notifiées, il est important que la direction y remédie dans les meilleurs délais. Les auditeurs internes devraient en effectuer le suivi et informer immédiatement la direction générale ou le conseil de toute insuffisance non corrigée. Pour faire en sorte que toutes les déficiences soient traitées au plus tôt, la direction devrait prévoir un système pour suivre les faiblesses du contrôle interne ainsi que les actions destinées à y remédier.

IV. Évaluation des systèmes de contrôle interne par les autorités prudentielles

Principe 14: Les autorités prudentielles devraient exiger que toutes les banques, quelle que soit leur dimension, disposent d'un système efficace de contrôle interne qui corresponde à la nature, à la complexité et au degré de risque de leurs activités de bilan et de hors-bilan et réagisse aux modifications de l'environnement et des conditions d'activité de la banque. Dans les cas où les autorités prudentielles constatent que le système de contrôle interne n'est pas adéquat (s'il ne prend pas en compte, par exemple, tous les principes contenus dans ce document), elles devraient intervenir auprès de la banque pour s'assurer que des améliorations sont apportées immédiatement.

41. Bien que le conseil d'administration et la direction générale soient responsables en dernier ressort de l'efficacité du système de contrôle interne, les autorités prudentielles devraient évaluer, dans le cadre de leurs activités de contrôle permanent, les systèmes dont sont dotées les diverses banques. Elles devraient également s'assurer que la direction de chaque établissement accorde sans tarder l'attention requise à tout problème détecté par le processus de contrôle interne.

42. Les autorités prudentielles devraient exiger des banques soumises à leur contrôle qu'elles aient une culture de contrôle forte et opter, dans l'exercice de leur surveillance, pour une approche centrée sur le risque, incluant d'examiner l'adéquation des contrôles internes. Il importe que les autorités prudentielles évaluent non seulement l'efficacité du système global de contrôle interne, mais aussi les contrôles sur les secteurs à haut risque (ceux, par exemple, qui présentent des caractéristiques telles qu'une rentabilité inhabituelle, une croissance rapide ou une activité nouvelle). Elles devraient donner une place particulière aux documents précisant les politiques et procédures en tant que mécanisme clé de communication.

43. Dans l'évaluation des systèmes de contrôle interne des banques, les autorités prudentielles peuvent choisir d'accorder une attention spéciale directe à des activités ou situations traditionnellement associées à des défaillances de contrôle interne ayant entraîné des pertes substantielles. Certaines modifications de l'environnement de la banque devraient faire l'objet d'une considération particulière pour déterminer si des révisions parallèles sont nécessaires dans le système de contrôle interne. Ces modifications englobent notamment: 1) un environnement opérationnel modifié; 2) un personnel nouveau; 3) des systèmes d'information nouveaux ou transformés; 4) des domaines ou activités enregistrant une croissance rapide; 5) une technologie nouvelle; 6) des secteurs, produits ou activités nouveaux (ceux surtout de nature complexe); 7) des restructurations, fusions et acquisitions d'entreprises; 8) une expansion ou acquisition d'opérations à l'étranger (y compris l'incidence des modifications de l'environnement économique et réglementaire correspondant).

44. Pour évaluer la qualité des contrôles internes, les autorités prudentielles ont le choix entre diverses approches. Elles peuvent examiner le travail du département d'audit

interne de la banque à partir de ses documents de travail, y compris sa méthode d'évaluation du risque. Si elles sont satisfaites des prestations de l'audit interne, elles peuvent utiliser les rapports des auditeurs internes comme premier élément d'identification des problèmes de contrôle dans la banque ou pour détecter des domaines de risque potentiel qui n'ont pas été passés en revue récemment par les auditeurs. Les autorités prudentielles peuvent opter pour un processus d'autoévaluation, par lequel la direction examine les contrôles internes secteur par secteur et certifie à l'autorité prudentielle que les contrôles sont adéquats pour les activités de la banque. D'autres peuvent exiger des audits externes périodiques des domaines clés, dont elles déterminent elles-mêmes l'ampleur. Enfin, les autorités prudentielles peuvent associer une ou plusieurs de ces méthodes à leurs propres examens sur place des contrôles internes.

45. Dans de nombreux pays, les autorités prudentielles effectuent des examens sur place qui comportent une révision des contrôles internes. Un tel examen pourrait inclure à la fois une analyse de tout le processus d'activité et un contrôle approprié des transactions sous forme de sondages, afin d'avoir une vérification indépendante des processus de contrôle interne de la banque.

46. Un contrôle approprié des transactions devrait être effectué sous forme de sondages pour vérifier:

- l'adéquation des politiques, procédures et limites internes et leur respect;
- l'exactitude et l'exhaustivité des rapports à la direction et documents financiers;
- la fiabilité (c'est-à-dire un fonctionnement conforme aux attentes de la direction) des contrôles spécifiques considérés comme essentiels pour l'élément de contrôle interne faisant l'objet de l'évaluation.

47. Pour apprécier l'efficacité des cinq éléments de contrôle interne d'une organisation bancaire (ou de l'une de ses unités ou activités), les autorités prudentielles devraient:

- déterminer les objectifs de contrôle interne adaptés à l'organisation, l'unité ou l'activité examinée (par exemple, prêts, placements, comptabilité);
- évaluer l'efficacité des éléments de contrôle interne, non pas par un simple examen des politiques et procédures, mais en consultant également l'ensemble des documents, en discutant des opérations avec divers niveaux du personnel de la banque, en observant l'environnement opérationnel et en contrôlant par sondages les transactions;
- faire part, dans les meilleurs délais, au conseil d'administration et à la direction de leurs préoccupations prudentielles au sujet des contrôles internes et des recommandations visant à les améliorer;
- s'assurer, pour les carences détectées, qu'une action corrective est mise en œuvre sans tarder.

48. Les autorités de contrôle bancaire qui ne procèdent pas à des examens de routine sur place recourent généralement aux travaux des auditeurs externes. Ceux-ci devraient alors

effectuer l'examen du processus d'activité et le contrôle par sondages des transactions précisés précédemment.

49. Dans tous les cas, les autorités de contrôle bancaire devraient examiner les observations et recommandations des auditeurs externes concernant l'efficacité des contrôles internes et s'assurer que la direction et le conseil d'administration de la banque ont donné suite aux préoccupations et recommandations exprimées par les auditeurs externes. Le niveau et la nature des problèmes de contrôle rencontrés par les auditeurs devraient être pris en compte dans l'évaluation, par les autorités prudentielles, de l'efficacité des contrôles internes de la banque.

50. Les autorités prudentielles devraient également encourager les auditeurs externes de la banque à planifier et à conduire leurs audits de manière à bien prendre en considération l'éventualité d'indications erronées résultant de manipulations frauduleuses des états financiers. Tout cas de fraude détecté par les auditeurs externes, quelle qu'en soit la gravité, devrait être signalé au niveau de direction approprié. Une fraude impliquant la direction générale et une fraude ayant de graves conséquences pour l'établissement devraient être notifiées au conseil d'administration et/ou à son comité d'audit. Dans certaines circonstances (en fonction des exigences nationales), les auditeurs externes peuvent avoir à signaler les fraudes à des autorités prudentielles ou à d'autres instances extérieures à la banque.

51. En examinant l'adéquation du processus de contrôle interne dans chaque organisation bancaire, les autorités prudentielles devraient également s'assurer de l'efficacité du processus au niveau des divers secteurs d'activité et filiales. Il est important qu'elles évaluent le processus de contrôle interne non seulement pour chaque établissement ou entité juridique, mais aussi pour tout l'éventail des activités et filiales au sein de l'organisation bancaire consolidée.

V. Rôles et responsabilités des auditeurs externes

52. Bien que, par définition, les auditeurs externes ne fassent pas partie d'une organisation bancaire et ne soient donc pas un élément de son système de contrôle interne, ils ont une incidence importante sur la qualité des contrôles internes à travers leurs activités d'audit, et notamment leurs discussions avec la direction et leurs recommandations pour améliorer les contrôles internes. Les auditeurs externes fournissent en retour des informations utiles sur l'efficacité du système de contrôle interne.

53. Si l'objet principal de la fonction d'audit externe est de donner un avis sur les comptes annuels d'une banque, ou de les certifier, l'auditeur externe doit choisir de s'en remettre ou non à l'efficacité du système de contrôle interne de l'établissement. Pour cette raison, il doit évaluer ce système, afin de voir dans quelle mesure il peut s'y fier pour déterminer la nature, la fréquence et la portée de ses propres procédures d'audit.

54. Le rôle exact des auditeurs externes et les processus qu'ils utilisent varient d'un pays à l'autre. Dans de nombreux pays, les normes d'audit professionnelles requièrent que les audits soient planifiés et exécutés de manière à obtenir l'assurance raisonnable que les états financiers ne comportent aucune erreur sérieuse. Les auditeurs vérifient également par sondage les transactions et écritures servant de base à l'établissement des états financiers et de la communication financière. Ils évaluent les principes comptables utilisés ainsi que les estimations significatives effectuées par la direction et jugent la présentation globale des états financiers. Dans certains pays, ils sont tenus par les autorités prudentielles de fournir une évaluation spécifique de la portée, de l'adéquation et de l'efficacité du système de contrôle interne des banques, y compris de leur fonction d'audit interne.

55. Un trait commun à tous les pays, cependant, est que l'on attend des auditeurs externes qu'ils aient une idée claire du processus de contrôle interne d'une banque. L'ampleur de l'attention accordée au système de contrôle interne varie selon l'auditeur et l'établissement; toutefois, on escompte généralement que les auditeurs externes détectent les carences notables existantes et signalent à la direction ainsi que, dans de nombreux pays, à l'autorité de contrôle celles qui sont sérieuses soit oralement, soit par courrier confidentiel. En outre, les auditeurs externes peuvent être soumis à des exigences prudentielles particulières précisant la manière d'évaluer les contrôles internes et d'en rendre compte.

Enseignements prudents fournis par les cas de défaillances des contrôles internes

A. Surveillance par la direction et culture de contrôle

1. De nombreux cas de défaillances des contrôles internes ayant entraîné des pertes bancaires substantielles auraient pu être nettement moins graves, ou même évités, si le conseil d'administration et la direction générale des établissements avaient instauré une culture de contrôle forte. Les cultures de contrôle insuffisantes présentaient souvent deux éléments communs. Tout d'abord, la direction générale n'était pas parvenue à souligner l'importance d'un système de contrôle interne solide à travers les termes utilisés et les actions entreprises et, surtout, par le biais des critères déterminant les rémunérations et promotions. Deuxièmement, la direction générale n'avait pas réussi à mettre en place une structure organisationnelle et des responsabilités de direction bien définies. Elle n'avait pas pu, par exemple, exiger un contrôle adéquat des principaux preneurs de décisions ni la notification, dans les meilleurs délais, de la nature et du déroulement des activités.

2. La direction générale peut affaiblir la culture de contrôle en promouvant et récompensant des responsables efficaces pour produire des bénéfices mais qui négligent d'appliquer les politiques de contrôle interne ou de traiter les problèmes décelés par l'audit interne. L'impression qui prévaut alors dans l'organisation est que les contrôles internes sont considérés comme secondaires par rapport aux autres objectifs, ce qui affecte l'engagement à l'égard de la culture de contrôle ainsi que sa qualité.

3. Certaines banques ayant connu des problèmes de contrôle étaient dotées de structures organisationnelles dans lesquelles les responsabilités n'étaient pas clairement définies, de sorte qu'une unité n'avait pas à rendre directement des comptes à un membre de la direction générale. Autrement dit, aucun membre de la direction ne surveillait les résultats de cette unité de manière suffisamment rigoureuse pour observer des activités inhabituelles, financières ou autres, et personne, au sein de la direction générale, n'avait une vision globale des opérations ni de la façon dont les bénéfices étaient réalisés. Si la direction avait compris les opérations de l'unité, elle aurait été en mesure de déceler des signes avant-coureurs (tels qu'un pourcentage inhabituel de profit par rapport aux niveaux de risques), d'analyser les transactions et de prendre des mesures pour réduire les pertes éventuelles. Ces problèmes auraient pu également être évités si le supérieur hiérarchique avait examiné les opérations ainsi que les rapports à la direction et s'était enquis auprès du personnel compétent de la nature des transactions effectuées. De telles approches fournissent aux supérieurs

hiérarchiques un aperçu objectif de la manière dont les décisions sont prises et garantissent que le personnel clé opère en respectant les critères fixés par la banque et le cadre de contrôle interne.

B. Évaluation des risques

4. Dans un passé récent, l'évaluation inadéquate des risques a été en partie à l'origine des problèmes de contrôle interne et des pertes qui en ont résulté dans certaines banques. Parfois, les rendements potentiels élevés liés à divers prêts, placements et instruments dérivés ont fait oublier à la direction la nécessité d'évaluer parfaitement les risques inhérents aux transactions et de dégager des ressources suffisantes pour surveiller et examiner en permanence les engagements. Des pertes ont également eu lieu lorsque la direction n'est pas parvenue à adapter le processus d'évaluation des risques aux modifications de l'environnement opérationnel. Par exemple, quand des produits plus complexes ou sophistiqués apparaissent dans un secteur d'activité, il peut arriver que les contrôles internes ne soient pas renforcés pour tenir compte de ces éléments. Un second exemple concerne la mise en place d'une activité nouvelle sans une évaluation complète et objective des risques encourus. En l'absence de cette réévaluation des risques, le système de contrôle interne peut ne pas traiter les risques de manière adéquate dans cette activité nouvelle.

5. Comme examiné précédemment, les organisations bancaires ont à fixer des objectifs pour l'efficacité et l'efficacité opérationnelles, la fiabilité de la communication financière et le respect de la conformité aux lois et réglementations. L'évaluation des risques comporte l'identification et la détermination des risques inhérents à la réalisation de ces objectifs. Ce processus aide à s'assurer que les contrôles internes de l'établissement correspondent à la nature, à la complexité et au degré de risque de ses activités de bilan et de hors-bilan.

C. Activités de contrôle

6. Dans les cas de pertes bancaires importantes dues à un contrôle interne insuffisant, les autorités prudentielles constatent en général que les établissements concernés ont négligé certains principes essentiels du contrôle interne. Il s'agit le plus souvent de la séparation des tâches, qui est l'un des piliers d'un système de contrôle interne sain. Fréquemment, la direction générale a confié à une personne très appréciée la responsabilité de la surveillance de deux ou plusieurs secteurs présentant des intérêts conflictuels. Ainsi, dans de nombreux cas, la même personne supervisait à la fois la salle des marchés et le postmarché d'une unité de négociation; elle pouvait alors contrôler l'engagement de la transaction (par exemple, l'achat ou la vente de titres ou de produits dérivés) ainsi que la fonction d'enregistrement correspondante. Attribuer

de telles tâches conflictuelles à une même personne lui donne la possibilité de manipuler des données financières pour réaliser un profit personnel ou de dissimuler des pertes.

7. La séparation des tâches ne concerne pas seulement des situations où la même personne contrôle à la fois la salle des marchés et le postmarché. De sérieux problèmes peuvent également apparaître lorsqu'un même individu est chargé:

- de l'approbation du décaissement de fonds et de leur décaissement effectif;
- des comptes clientèle et des comptes propres;
- des transactions au titre du portefeuille bancaire et du portefeuille de négociation;
- de la fourniture informelle d'informations à des clients sur leurs positions et de la relation commerciale avec ces mêmes clients;
- de l'évaluation du caractère adéquat des dossiers de crédit et de la surveillance des emprunteurs après l'octroi des crédits;
- de tout autre domaine où des conflits d'intérêts notables apparaissent et ne sont pas atténués par d'autres facteurs⁴.

8. Les insuffisances des activités de contrôle reflètent toutefois l'échec des multiples efforts destinés à voir si l'activité est conduite selon les attentes, depuis les examens effectués au niveau supérieur jusqu'au bon fonctionnement de mécanismes régulateurs spécifiques dans un processus d'activité. Dans plusieurs cas, par exemple, la direction n'a pas réagi comme il le fallait aux informations qu'elle recevait. Ces informations figuraient dans des rapports périodiques sur les résultats des opérations de toutes les unités de l'organisation, qui informaient la direction des progrès réalisés par chacune vers les objectifs et lui permettaient de poser des questions si les résultats n'étaient pas conformes aux attentes. Souvent, les unités qui ont enregistré par la suite des pertes notables avaient commencé par dégager des bénéfices – nettement supérieurs à ce qu'on attendait compte tenu du niveau de risque apparent – qui auraient dû alerter la direction générale. Si des examens au niveau supérieur avaient eu lieu, la direction générale aurait pu se pencher sur les résultats anormaux et déceler puis traiter certains des problèmes, limitant ainsi ou empêchant ces pertes. Cependant, comme les différences par rapport aux attentes étaient positives (sous forme de bénéfices), aucune question n'était posée et les enquêtes n'ont été entreprises que lorsque les problèmes avaient pris une ampleur incontrôlable.

⁴ À titre d'illustration d'un conflit d'intérêt potentiel atténué par d'autres contrôles, l'examen indépendant d'un prêt, dans le cadre des activités de surveillance du système de classification des crédits d'une banque, peut compenser le conflit d'intérêt potentiel qui se présente lorsqu'une personne chargée d'évaluer le caractère adéquat d'un dossier de crédit surveille également la cote de crédit de l'emprunteur après l'octroi du crédit.

D. Information et communication

9. Certaines banques ont enregistré des pertes parce que l'information au sein de l'organisation n'était ni fiable ni complète et que la communication n'avait aucune efficacité. L'information financière peut être communiquée de façon erronée sur le plan interne; des séries de données incorrectes émanant de sources extérieures peuvent être utilisées pour évaluer des positions financières; de même, des activités modestes, mais à haut risque, peuvent ne pas figurer dans les rapports à la direction. Parfois, les banques avaient négligé de faire connaître de manière adéquate les tâches des employés et leurs responsabilités en matière de contrôle ou faisaient part des politiques de l'établissement par des canaux, tels que la messagerie électronique, qui ne garantissaient pas que ces politiques étaient lues et retenues. Par conséquent, sur des périodes de temps assez longues, d'importants aspects des politiques de la direction n'étaient pas appliqués. Dans d'autres cas, aucune voie de communication adéquate ne permettait aux employés de rendre compte de présomptions d'irrégularités. Si de telles voies avaient été établies pour signaler les problèmes à travers la structure hiérarchique, la direction aurait été en mesure d'identifier et de corriger beaucoup plus tôt les irrégularités.

E. Activités de surveillance

10. De nombreuses banques ayant enregistré des pertes dues à des problèmes de contrôle interne ne surveillaient pas de manière efficace leurs systèmes de contrôle interne. Souvent, ces systèmes ne comportaient pas les processus de surveillance en continu indispensables et les évaluations spécifiques étaient inadéquates ou traitées de façon inappropriée par la direction.

11. Dans certains cas, l'absence de surveillance a commencé par l'incapacité de prêter attention ou de donner suite aux informations transmises jour après jour aux supérieurs hiérarchiques ainsi qu'à d'autres membres du personnel qui indiquaient une activité inhabituelle, telle que dépassements des plafonds d'engagement, utilisation de comptes clientèle pour des opérations propres ou absence d'états financiers courants émanant des emprunteurs. Dans une banque, les pertes associées aux activités de négociation étaient dissimulées au sein d'un compte clientèle fictif. Si l'organisation avait été dotée d'une procédure exigeant que des situations des comptes soient adressées à la clientèle chaque mois et que les comptes clientèle soient périodiquement confirmés, les pertes dissimulées auraient vraisemblablement été découvertes bien longtemps avant d'être suffisamment lourdes pour entraîner la faillite de l'établissement.

12. Dans plusieurs autres cas, l'unité ou l'activité qui était à l'origine de pertes massives présentait de nombreuses caractéristiques indiquant un niveau de risque accru, tel qu'une rentabilité inhabituelle pour le niveau de risque perçu et une croissance rapide dans une activité nouvelle géographiquement distante de la banque mère. Toutefois, en raison d'une

évaluation de risque inadéquate, les établissements n'avaient pas dégagé suffisamment de ressources additionnelles pour contrôler ou surveiller les activités à haut risque. En fait, dans quelques exemples, les activités à haut risque étaient moins suivies que d'autres qui présentaient des profils de risque nettement inférieurs – plusieurs avertissements des auditeurs internes et externes au sujet des activités de l'unité avaient d'ailleurs été ignorés de la direction.

13. Si l'audit interne peut constituer une source efficace d'évaluations spécifiques, son efficacité était nulle dans de nombreuses organisations bancaires en difficulté. Trois facteurs contribuaient à ce dysfonctionnement: le fait de procéder à des audits fragmentés, le manque de compréhension globale des processus d'activité et le suivi inadéquat des problèmes après leur détection. L'approche d'audits fragmentés venait essentiellement de ce que les programmes d'audit interne étaient structurés en séries d'audits partiels sur des activités spécifiques au sein de la même unité ou du même département, de secteurs géographiques ou encore d'entités juridiques. Du fait de cette fragmentation, les processus d'activité n'étaient pas pleinement compris par le personnel de l'audit interne. Une conception d'audit qui aurait permis aux auditeurs de suivre les processus et fonctions du début jusqu'à la fin (c'est-à-dire en prenant la même transaction de son point de départ jusqu'à sa notification dans les comptes rendus financiers) leur aurait permis de mieux comprendre la situation; en outre, elle aurait fourni l'occasion de vérifier et de tester l'adéquation des contrôles à chaque étape du processus.

14. Dans certains cas, les problèmes d'audit interne ont également résulté d'une connaissance et d'une formation inadéquates du personnel d'audit interne sur les produits et marchés, les systèmes d'information électronique et d'autres domaines hautement sophistiqués. Comme ce personnel ne possédait pas les compétences nécessaires, il hésitait souvent à poser des questions lorsqu'il entrevoyait des problèmes et, quand les questions étaient posées, avait tendance à accepter une réponse plutôt qu'à la remettre en cause.

15. L'audit interne peut également devenir inefficace lorsque la direction n'assure pas un suivi approprié des problèmes décelés par les auditeurs. Des délais ont pu intervenir à cause d'un manque de reconnaissance par la direction du rôle et de l'importance de l'audit interne. En outre, l'efficacité de l'audit interne est compromise lorsque la direction générale et les membres du conseil d'administration (ou, le cas échéant, le comité d'audit) ne reçoivent pas en temps voulu et de manière régulière des rapports de suivi signalant les problèmes critiques et les actions correctives prises ensuite par la direction. Un tel suivi périodique peut aider la direction générale à traiter les questions importantes dans les meilleurs délais.