dans quelle branche de l'organisation ces faiblesses ont été constatées et quelles sont les rubriques qui subissent un risque significatif du fait de cette lacune. Il en résultera, selon le cas, une réserve (3.7.2.) ou une déclaration d'abstention (3.8.1.). » (Modification, Rapport annuel 1997, *p.* 341*)*.

La mention d'une faiblesse significative dans le système de contrôle interne n'est requise que dans la mesure où le réviseur n'a pas pu se satisfaire des éléments probants recueillis par d'autres moyens. Lorsque les procédures de validation (*compliance tests*) ont permis au réviseur de conclure que l'information est fiable, la mention de cette faiblesse n'est pas requise dans la partie du rapport consacrée à l'attestation des états financiers. Le réviseur pourrait cependant juger utile d'en faire état dans son rapport s'il subsiste un risque significatif d'apparition de fraudes ou erreurs.

2.3. Révision dans un environnement automatisé (3 octobre 1997)[63]

1. Introduction

*1.1.*La présente recommandation s'appuie sur les normes générales de révision de l'I.R.E. et applique la norme ISA 401 de l'IFAC « Auditing in a Computer Information Systems Environnement ». Par ailleurs, elle tient également compte des principes formulés dans la recommandation de révision 2.1 sur « Le risque de révision » (3 décembre 1993).

La présente recommandation a pour but de fournir les directives sur la mise en œuvre de la révision lorsque la mission de vérification est menée dans un environnement automatisé.

Pour l'application de la présente recommandation, on parlera d'environnement automatisé lorsqu'une entité a recours à un ordinateur, quelle que soit sa capacité, pour le traitement de l'information financière soumise à contrôle indépendamment du fait que le traitement a lieu dans l'entité elle-même ou chez un tiers.

La stratégie de révision concernée par la présente recommandation aura pour objectif d'identifier et d'évaluer, dans un environnement automatisé, les risques inhérents et les risques de contrôle interne qui peuvent avoir une influence sur l'interprétation des comptes annuels.

*1.2.*Le réviseur doit évaluer l'incidence de l'environnement informatique sur la révision.

*1.3.*L'existence d'un environnement informatique ne modifie pas l'objectif ni l'étendue de la révision. Par contre, l'utilisation d'un ordinateur modifie le traitement,

---

[63] Avis du Conseil Supérieur du Revisorat d'Entreprises et de l'Expertise Comptable d.d. 1 juillet 1997 (Rapp. annuel CSR, 1997, p. 25- 26).

l’accumulation des données et la communication des informations financières et peut avoir une incidence sur les systèmes comptables et de contrôle interne de l’entité. En conséquence, un environnement informatique peut avoir une influence sur :

- Les procédures appliquées par le réviseur pour obtenir une connaissance suffisante des systèmes comptables et de contrôle interne.
- La prise en compte du risque inhérent et du risque lié au contrôle permettant au réviseur d’évaluer le risque d’audit.
- La conception et l’exécution par le réviseur de tests de procédures et de contrôles de validation nécessaires en la circonstance pour atteindre l’objectif de l’audit.

2. Capacités et compétences

*2.1.*Le réviseur doit posséder une connaissance suffisante de l’environnement informatique pour planifier, diriger, superviser et revoir le travail effectué. Le réviseur doit évaluer si des compétences informatiques particulières s’imposent pour réaliser la révision. Elles peuvent être nécessaires pour :

- Obtenir une compréhension suffisante des systèmes comptables et de contrôle interne influencés par ‘environnement informatique.
- Déterminer l’incidence de l’environnement informatique sur l’évaluation générale du risque et sur le risque relatif au solde des comptes et aux catégories de transactions.
- Concevoir et mettre en œuvre des tests de procédures et des contrôles de validation appropriés.

Si des compétences spéciales sont requises, le réviseur demandera l’aide d’un professionnel possédant ces compétences; il peut s’agir d’un collaborateur du réviseur ou d’un spécialiste externe à l’entité. Si le recours à ce professionnel est envisagé, le réviseur doit rassembler suffisamment d’éléments probants montrant que le travail effectué permet de répondre à l’objectif de la révision, selon la recommandation de révision 3.4 relative à l’« Utilisation des travaux d’un expert ».

3. Planification

*3.1.*Dans la planification des aspects de la révision susceptibles d’être influencés par l’environnement informatique du client, le réviseur doit tenir compte de l’importance et de la complexité des systèmes informatiques et de la disponibilité des données pouvant être utilisées pour la révision, en particulier :

- De l’importance et de la complexité du traitement informatisé pour chaque application comptable importante. L’importance désigne le caractère significatif des assertions sous-tendant l’établissement des états financiers affectées par le traitement informatisé. Une application peut être considérée comme complexe si, par exemple :

- Le volume des opérations est tel qu'il est difficile aux utilisateurs d'identifier et de corriger des erreurs de traitement.
- L'ordinateur génère automatiquement des opérations ou des écritures importantes directement dans une autre application.
- L'ordinateur exécute des calculs complexes d'informations financières et/ ou génère automatiquement des opérations ou des écritures importantes qui ne peuvent être (ou ne sont pas) validées indépendamment.
- Des opérations font l'objet d'un échange électronique avec d'autres entités (comme dans les systèmes d'échange électronique de données) sans contrôle manuel de la pertinence ou de la nécessité de ces échanges.

- De l'organisation des activités informatiques du client et du degré de concentration ou de décentralisation du traitement informatique dans l'entité, notamment lorsqu'ils ont une influence sur la séparation des tâches.
- De la disponibilité des données. Les documents source, certains fichiers informatiques et d'autres éléments probants nécessaires au réviseur existent parfois pendant une courte période seulement ou uniquement sur un support lisible par une machine. L'environnement informatique du client peut générer des rapports internes utiles pour les contrôles substantifs (en particulier les procédures analytiques). Le potentiel d'utilisation de techniques d'audit assistées par ordinateur peut accroître l'efficacité des procédures d'audit, ou permettre au réviseur d'appliquer certaines procédures à une population entière de comptes ou d'opérations à un moindre coût.

*3.2.*Dans un environnement informatique utilisant de gros systèmes, le réviseur doit également acquérir la connaissance de cet environnement et déterminer s'il peut influencer l'évaluation du risque inhérent et du risque lié au contrôle. La nature des risques et les caractéristiques du contrôle interne dans un environnement informatique comprennent :

- Le manque de trace matérielle supportant les transactions. Dans certains environnements informatiques, il est possible que des traces matérielles complètes nécessaires pour la révision n'existent que pendant une courte période ou uniquement sur un support lisible par la machine. Dans le cas où un programme d'application complexe exécute un grand nombre de tâches dans le processus de traitement, l'existence de traces matérielles exhaustives n'est pas évidente. C'est pourquoi des erreurs contenues dans le programme d'application peuvent être difficiles à détecter en temps voulu par des procédures manuelles (par l'utilisateur).
- L'uniformité du traitement des opérations. L'ordinateur applique le même traitement à toutes les opérations similaires en utilisant les mêmes instructions. Ceci permet d'éliminer quasiment toutes les erreurs humaines qui se produisent lors d'un traitement manuel. En revanche, les erreurs de programmation (ou les autres erreurs dans les logiciels de base ou les programmes d'application) entraînent en général un traitement incorrect de toutes les opérations.
- La séparation insuffisante des tâches. De nombreuses procédures de contrôle exécutées en général par plusieurs personnes dans un système manuel peuvent être

centralisées dans un système informatique. Ainsi, une personne ayant accès à des programmes, à des traitements ou à des données informatiques est en mesure d'exécuter des opérations non contrôlées.

- Le risque d'erreurs et d'irrégularités. Le risque d'erreur humaine dans la conception, la maintenance et la mise en œuvre d'un système informatique est supérieur à celui d'un système manuel, à cause du niveau de détail inhérent à ces systèmes. De même, le risque que des utilisateurs non autorisés accèdent à des données ou les modifient sans trace visible est plus grand dans un système informatique.

  En outre, la diminution de l'intervention humaine dans le traitement informatisé d'opérations contribue à réduire les possibilités de détection d'erreurs ou d'irrégularités. Les erreurs ou irrégularités se produisant lors de la conception ou de la modification de programmes d'application ou de logiciels risquent de passer longtemps inaperçues.
- Le lancement ou l'exécution des opérations. L'environnement informatique peut lancer ou exécuter automatiquement certains types d'opérations. L'autorisation de ces opérations ou procédures n'est pas toujours aussi bien documentée que dans un système manuel, et l'autorisation par la direction peut être implicite et résulter de son acceptation de l'environnement informatique et de ses modifications ultérieures.
- La dépendance vis-à-vis d'autres contrôles du traitement informatisé. Le traitement informatisé peut générer des rapports ou d'autres documents utilisés pour les procédures de contrôle manuel. L'efficacité de ces procédures peut dépendre de l'efficacité des contrôles d'exhaustivité et d'exactitude du traitement informatisé. Par contre, l'efficacité et la cohérence des contrôles du traitement d'opérations dans les applications informatisées sont souvent tributaires de l'efficacité des contrôles informatiques généraux.
- Le renforcement potentiel de la supervision de la direction. Un environnement informatique peut offrir à la direction une palette d'outils analytiques permettant d'examiner et de superviser les activités de l'entité. S'ils sont disponibles et utilisés, ces outils peuvent améliorer la structure de contrôle interne.
- L'utilisation potentielle de techniques d'audit assistées par ordinateur. Le traitement et l'analyse de grandes quantités de données par informatique peuvent permettre au réviseur d'appliquer des techniques d'audit informatisé générales ou spécialisées pour l'exécution des contrôles d'audit. Les risques et les contrôles mis en œuvre du fait des caractéristiques de l'environnement informatique ont une incidence potentielle sur l'évaluation du risque par le réviseur, et sur la nature, le calendrier et l'étendue des procédures d'audit.

4. Evaluation du risque

*4.1.*Les risques inhérents et les risques liés au contrôle dans un environnement informatique peuvent avoir un effet diffus et un effet spécifique à un type de comptes sur la probabilité d'anomalies significatives dans les circonstances suivantes :

- Les risques peuvent résulter de déficiences dans plusieurs des activités informatiques telles que : développement et maintenance de programmes, support logiciel, opérations, sécurité physique des équipements informatiques, contrôle d'accès à des utilisateurs privilégiés. Ces déficiences ont un effet diffus sur toutes les applications traitées par l'ordinateur.
- Les risques peuvent accroître le potentiel d'erreurs et de fraudes dans des applications spécifiques, des bases de données, des fichiers maîtres ou des traitements spécifiques. Ainsi, les erreurs sont relativement fréquentes dans des systèmes exécutant des opérations logiques ou des calculs complexes, ou qui gèrent un nombre élevé d'exceptions. De même, les systèmes qui contrôlent les sorties de fonds ou d'autres liquidités peuvent faire l'objet de fraudes de la part des utilisateurs ou du personnel informatique.

*4.2.*Les clients recourent fréquemment aux nouvelles technologies pour développer des systèmes informatiques de plus en plus complexes qui peuvent comporter des liaisons micro-gros systèmes, des bases de données distribuées, des traitements utilisateur final et des systèmes de gestion qui transfèrent directement des informations dans les systèmes comptables. Ces systèmes augmentent le degré de sophistication global de l'environnement informatique et la complexité des applications concernées. En conséquence, ils peuvent accroître le risque et nécessiter une attention particulière.

5. Stratégie de contrôle dans un environnement de traitement automatisé

5.1.Schéma de travail

La figure ci-après donne un aperçu général des différentes étapes que l'on peut distinguer lors de l'exécution des travaux de contrôle dans un environnement automatisé.<beeld_H:\verwerking\framemaker\frameExport\verwerking\figuren\fig1 [Converted].tif>

L'exécution des travaux dans un environnement automatisé s'effectue selon les phases suivantes :

Phase 1 : collecte d'informations de base et planification des travaux de contrôle.

Phase 2 : exécution d'une étude préalable comprenant les tâches suivantes :

- établissement d'un diagnostic général axé sur les contrôles clés prévus dans

l'environnement automatisé;
- évaluation des risques inhérents et de contrôle interne induits par le traitement automatisé, avec un accent particulier sur l'intégrité et la permanence des méthodes.

Phase 3 : prise de décision sur la stratégie de révision sur base de l'information disponible à ce stade :

- soit le réviseur décide de se fier au dispositif du contrôle interne;
- soit le réviseur y substitue des tests de validation appropriés et passe en phase 7.

Lorsque le système informatique est géré par une autre entité du groupe ou par un tiers, et que le réviseur n'est pas en mesure d'effectuer les travaux de contrôle nécessaires dans cette entité, il devra alors adopter une approche de validation.

Phase 4 : exécution d'un examen détaillé des contrôles généraux informatiques.

Phase 5 : prise de décision sur le passage aux contrôles des applications : si les contrôles généraux informatiques s'avèrent déficients, le réviseur peut décider de ne pas procéder aux contrôles des applications et de passer à la phase 7.

Phase 6 : l'examen détaillé des mécanismes de contrôle interne qui ont été instaurés dans et autour des diverses applications automatisées.

Phase 7 : adaptation de la stratégie de révision en ce qui concerne la revue analytique et les tests de validation.

Chacune des phases citées est développée ci-après.

5.2. Collecte des informations de base et planification des travaux de contrôle (phase 1)

Le réviseur doit se renseigner sur les éléments de l'environnement automatisé qui peuvent avoir une incidence sur la planification de ses travaux, et réunir, en particulier, des informations de base sur :

a) la stratégie et la planification d'automatisation adoptées par l'entreprise, l'organisation et les méthodes de travail du département informatique, la politique interne de sécurité, l'existence de procédures internes au département informatique;
b) les technologies utilisées par l'entité, en ce compris les réseaux de télécommunication et les procédures s'y rapportant, notamment en ce qui concerne la communication avec des tiers, tels que les banques, fournisseurs et clients;
c) l'architecture propre à chaque application : sa genèse, la nature du traitement, le schéma d'intégration des applications;
d) les méthodes adoptées pour la conception, le développement et la maintenance des

applications;

e) les changements significatifs survenus au cours de la période contrôlée, l'historique des problèmes significatifs rencontrés et les solutions apportées.

Cette information permet au réviseur d'évaluer l'importance de l'environnement automatisé et de déterminer le cadre de ses travaux ultérieurs.

5.3.Etude préalable (phase 2)

En vue d'élaborer sa stratégie de révision, le réviseur doit :

a) déterminer le niveau de risques inhérents liés à l'environnement automatisé;
b) effectuer une évaluation préalable des contrôles généraux ainsi que des programmes d'application; sont seulement visés ici les contrôles sur lesquels il considère qu'il sera efficace de s'appuyer. Cette analyse permet de déterminer le risque de contrôle interne en identifiant les faiblesses potentielles de la structure de contrôle et du système informatique;
c) le cas échéant, prévoir l'intégration de techniques de révision automatisées.

5.4.Fixation de la stratégie de révision (phase 3)

Les contrôles généraux informatiques peuvent avoir des répercussions sur la qualité et la fiabilité des traitements réalisés par les applications. En outre, l'absence de contrôles adéquats peut nuire à l'intégrité des données à traiter.

Pour élaborer sa stratégie de révision, le réviseur dispose de deux options :

a) s'il décide de s'appuyer sur le contrôle interne, il doit examiner les contrôles généraux du fonctionnement de l'ensemble du système informatique (« contrôles généraux informatiques ») ainsi que ceux intégrés ou exercés autour de chaque application (« contrôles applicatifs »). Si ces contrôles se révèlent insuffisants, le réviseur peut décider d'en revenir à des procédures manuelles compensatoires;
b) s'il décide de ne pas s'appuyer sur le contrôle interne, il doit alors procéder à des tests de validation étendus.

L’option retenue sera conditionnée à titre principal par des considérations d’efficacité et sera notamment basée sur les résultats de l’analyse préalable. Le choix sera correctement justifié dans les documents de travail.

5.5.L’examen détaillé des contrôles généraux informatiques (phase 4)

Les contrôles généraux informatiques visent l’ensemble des activités automatisées. Ils permettent d’acquérir une conviction raisonnable que les objectifs globaux du contrôle interne sont atteints dans l’environnement automatisé. Ces contrôles généraux peuvent être classés selon les catégories suivantes :

- contrôles liés à la gestion et à l’organisation du département informatique;
- contrôles de la mise en œuvre des applications;
- contrôles d’exploitation;
- contrôles d’accès logique;
- contrôles sur les dispositifs liés à la sécurité physique et au plan de secours.

Pour plus de détails, on se référera à l’annexe A.

Le réviseur doit prendre en considération l’impact de ces contrôles sur les applications automatisées lorsque ces dernières fournissent une information qui présente de l’importance pour la révision des comptes annuels.

5.6. Décision sur l’opportunité de procéder à l’examen des contrôles applicatifs (phase 5)

Lorsque les contrôles généraux informatiques sont satisfaisants, le réviseur passera à l’examen des contrôles applicatifs (phase 6).

Si le réviseur arrive à la conclusion que les contrôles généraux informatiques présentent des lacunes importantes, il ne pourra s’appuyer sur ces contrôles pour la suite de sa mission. Il en prendra acte dans ses documents de travail et examinera dans quelle mesure il est censé poursuivre son examen du contrôle interne. S’il ne peut s’appuyer sur le contrôle interne, il examinera dans quelle mesure il peut mettre en œuvre des procédures alternatives de révision permettant de valider les comptes annuels, conformément à la recommandation de révision relative aux effets du contrôle interne sur les travaux de révision.

5.7.Examen des contrôles applicatifs (phase 6)

On entend par « contrôles applicatifs », d’une part, les procédures de contrôle automatisées insérées dans l’application et, d’autre part, les procédés manuels de vérification sur lesquels se fonde une entité pour contrôler son traitement de données.

Ces deux types de contrôle seront évalués par le réviseur aussi bien pris isolément

qu’en complémentarité et en interaction. Ensemble, ils permettront d’assurer l’exhaustivité, l’exactitude, le caractère autorisé et l’adéquation dans le temps des informations financières et opérationnelles.

Avec la mise en œuvre des nouvelles technologies, on constate de plus en plus un glissement des contrôles effectués précédemment par l’utilisateur final vers des contrôles automatisés.

De plus amples détails relatifs aux contrôles applicatifs figurent en annexe B.

5.8.Adaptation de la stratégie de révision (phase 7)

Son examen détaillé des contrôles généraux informatiques et des mesures de contrôle interne qui ont été instaurées au sein et autour des différentes applications permettra au réviseur de juger si le contrôle interne, considéré comme un ensemble, donne satisfaction.

Si ses investigations révèlent que le contrôle interne souffre de lacunes importantes, il devra renforcer ses tests de validation et ses travaux de revue analytique. Par contre, si ces contrôles sont satisfaisants, il pourra réduire ses tests de validation de façon substantielle.

***

Annexe A : Contrôles généraux informatiques

Définition

Les contrôles généraux informatiques concernent l’ensemble des mécanismes qui interviennent dans un environnement automatisé. Ils permettent d’acquérir une conviction raisonnable quant au fait que les objectifs globaux du contrôle interne sont atteints. Ces contrôles peuvent être classés en 5 catégories :

- contrôles liés à la gestion et à l’organisation du département informatique;
- contrôles d’implantation et de maintenance des applications;
- contrôles d’exploitation;
- contrôles d’accès logique;
- sécurité physique et plan de secours.

1. Contrôles liés à la gestion et à l'organisation du département informatique

Dans ce contexte, les aspects suivants seront évalués :

- la place du département informatique dans l'organigramme général de l'entreprise;
- l'existence et la qualité du schéma directeur, du plan informatique, et du budget informatique;
- l'existence, la composition, le rôle, les responsabilités et la manière dont fonctionne le comité informatique;
- la manière dont la direction suit les projets informatiques et son niveau d'intervention dans l'allocation des moyens informatiques;
- l'implication et le rôle du département d'audit interne dans les questions relatives à l'environnement automatisé;
- l'existence d'un équilibre entre les moyens informatiques disponibles et les besoins tels que formulés et découlant du plan informatique;
- les relations entre les utilisateurs finaux et le département informatique;
- la structure du département informatique, la description des fonctions et la séparation des tâches (développement, gestion des données, exploitation);
- l'existence et la qualité de la politique du personnel au département informatique (engagement, licenciement, évaluation, promotion, formation);
- l'existence, le contenu, la qualité, et l'application d'une politique de sécurité informatique;
- le respect des législations spécifiques aux environnements automatisés (loi concernant la protection à l'égard des traitements de données à caractère personnel, loi sur la protection des droits d'auteurs relative aux progiciels,...)[64].

2. Contrôles d'implantation et de maintenance des applications

Ces contrôles sont relatifs à la manière dont les applications informatiques sont développées ou acquises et entretenues. Ils ont un impact important sur la qualité des applications qui sont mises en place. Dans cette catégorie de contrôles, une distinction sera faite entre :

- le travail à façon par développement interne ou effectué par un fournisseur externe;
- l'achat, la paramétrisation, l'adaptation éventuelle et la mise en place de progiciels;
- l'entretien des applications.

---

[64] Si cette législation n'est pas respectée par le client, le réviseur en fera état dans une lettre d'observation aux dirigeants.

2.1. Travail à façon par développement interne ou effectué par un tiers externe à l'entité

La réussite de projets informatiques de développement importants est largement dépendante de la qualité de la gestion du projet. Une gestion de projet adéquate suppose entre autres :

- un engagement clair et une collaboration active de la direction;
- l'intervention de gestionnaires de projet expérimentés;
- une méthodologie adaptée, complétée par des procédures et des standards de développement appropriés;
- un environnement de contrôle de qualité;
- des budgets détaillés;
- un planning détaillé des tâches;
- une définition claire des responsabilités;
- un suivi systématique écrit destiné à toutes les parties et notamment à la direction.

En outre, les facteurs suivants sont importants du point de vue du réviseur :

- l'existence d'environnements techniques séparés pour le développement, l'expérimentation de l'application et pour l'exploitation;
- la justification formelle du projet de développement sur base d'une étude de faisabilité et de spécifications formelles des besoins des utilisateurs;
- l'intégration claire du projet dans l'architecture des applications existantes;
- la prise en considération des mesures de contrôle et de sécurité nécessaires à chaque étape du processus de développement;
- la mise en œuvre de tests des modules individuels, des tests d'intégration et d'acceptation en cas de nouvelles applications pour veiller à ce que les programmes fonctionnent correctement du point de vue technique et répondent aux besoins des utilisateurs;
- l'existence, avant mise en production, d'une acceptation formelle du projet par les utilisateurs;
- la vérification que les applications ont été développées et documentées selon les normes en vigueur;
- l'existence d'une procédure contrôlée pour le transfert d'une phase de développement à la phase de production;
- parallèlement à la mise en place technique, les aspects d'organisation et de procédure du système administratif doivent être réexaminés;
- les utilisateurs doivent recevoir une formation adéquate. Une documentation complémentaire doit être, le cas échéant, élaborée en vue d'assurer une bonne intégration du progiciel dans l'environnement administratif.

Au cas où le développement est réalisé par un tiers, il faut prêter attention aux clauses du contrat, entre autres, en ce qui concerne la propriété du logiciel et de maintenance ultérieure.

2.2.L'achat, la paramétrisation et la mise en place de progiciels

L'achat, la paramétrisation et la mise en place d'un progiciel se gèrent comme tout autre projet. En outre, il faut tenir compte des aspects suivants :

- les progiciels doivent être sélectionnés sur base d'une définition claire des besoins. De plus, les méthodes de travail et les procédures doivent être revues et les objectifs reformulés si nécessaire;
- le contrat d'achat doit clairement spécifier les performances attendues du progiciel, ses fonctionnalités, la documentation à livrer par le fournisseur, les modalités de propriété ou de dépôt des sources, le support technique nécessaire lors de la mise en place, les modalités de mise à jour future et de formation des utilisateurs. Il doit aussi faire référence aux documents de travail et aux échanges de courrier préalables à la sélection du progiciel;
- en sélectionnant un progiciel, il y a lieu notamment de tenir compte des facteurs suivants :
    - les caractéristiques fonctionnelles, de contrôle et de sécurité du progiciel;
    - la réputation et la fiabilité du fournisseur;
    - la qualité du support futur garanti par le fournisseur;
    - la qualité de la documentation destinée aux utilisateurs;
    - la disponibilité d'une documentation technique de base;
    - les garanties contractuelles proposées pour assurer la continuité du produit;
- chaque progiciel doit être testé, avant sa mise en production;
- le progiciel doit être intégré dans l'architecture des applications existantes et cette intégration doit être documentée;
- le suivi des versions successives du progiciel doit être assuré de manière systématique.

Enfin, notons que toute adaptation importante des programmes doit s'effectuer dans le respect des règles de développement énoncées ci-dessus (2.1).

2.3.La maintenance

Les règles relatives aux nouveaux développements s'appliquent également à la maintenance. Bien que les modifications mineures ne se gèrent normalement pas comme un projet complet, les principes de base restent valables. Dans ce contexte, il faut noter l'importance d'un système clair de constat, d'évaluation, de fixation des priorités et d'exécution des changements demandés. Il est essentiel également de mettre à jour la documentation lors de l'exécution de ces changements.

3. Les contrôles d'exploitation

Les contrôles d'exploitation garantissent que les traitements automatisés journaliers se déroulent de manière fiable et mettent l'entité en mesure de réagir de manière adéquate aux incidents d'exploitation éventuels. Dans ce cadre, les aspects suivants sont, entre

autres, examinés :

3.1.Management opérationnel technique

Les activités reprises sous ce titre portent, d'une part, sur le maintien des performances du système et, d'autre part, sur la coordination et la planification de l'évolution de l'environnement automatisé.

3.2.Management du niveau de service attendu

Ceci se traduit par des accords passés entre les diverses parties intervenant dans le traitement automatisé (utilisateur final, développeur, exploitation,...) et qui sont concernées par le niveau de qualité du service à atteindre.

3.3.Management de l'évolution technologique

Il s'agit des procédures mises en place pour organiser les changements apportés à l'environnement automatisé (matériel, système, réseau, etc.).

3.4.Management de la configuration automatisée

Ceci concerne l'identification et la gestion du parc de matériels et logiciels de base.

3.5.Management des incidents

Ces procédures décrivent la manière dont les incidents intervenant dans le centre informatique sont traités (journalisation des problèmes et situations anormales, renvoi vers la hiérarchie du problème, suivi et action de correction, interaction avec les développeurs et les utilisateurs...).

3.6.Procédures d'exploitation

En plus, des procédures générales liées à la gestion du système (copies de sécurité, restauration, démarrage et arrêt du système) des procédures d'exploitation spécifiques aux applications sont nécessaires.

3.7.Procédures de sauvegarde et de restauration

Régulièrement, des copies de sécurité doivent être prises tant des fichiers de données que des programmes et de l'environnement système. Ces copies de sécurité doivent être stockées dans un endroit protégé. Une partie de celles-ci doivent être gardées à l'extérieur du site.

3.8.Procédures d'archivage et de désarchivage

Des procédures formelles d'archivage doivent exister; les options prises dans ce domaine doivent tenir compte des périodes légales de conservation ainsi que des besoins opérationnels en la matière.

3.9.Procédures de gestion des supports

Des indications claires doivent exister en matière de gestion des supports de données (inventaire, réutilisation, identification,...).

3.10.Planification des travaux d'exploitation

Les traitements par lots doivent être planifiés, paramétrés et mis en œuvre selon des directives clairement établies par avance.

3.11.Journalisation (logging-audit trail)

Une trace de contrôle de tous les processus automatisés internes importants doit être disponible.

4. Les contrôles d'accès logique

Les contrôles d'accès logique permettent de limiter l'accès aux seuls utilisateurs autorisés. On utilisera le plus souvent une combinaison de procédés d'identification des utilisateurs (User Ids) et de gestion de mots de passe pour atteindre cet objectif.

Certains contrôles indispensables doivent être mis en place afin de garantir l'efficacité du système, dont notamment :

- l'identification individuelle des différents utilisateurs;
- des procédures claires pour la gestion des profils de l'utilisateur (la définition des nouveaux utilisateurs, la « désactivation » du personnel ayant quitté l'entité contrôlée, la modification du profil lorsqu'une personne change de fonction, etc.);
- des lignes directrices et des mesures de contrôle concernant la confidentialité, la structure et la gestion des mots de passe (la longueur du mot de passe, son changement périodique,...);
- le contrôle des profils utilisateurs ayant des autorisations d'accès importantes « security officer »...);
- l'intégrité du logiciel de sécurité et du système d'exploitation en lui-même.

En outre, des mesures spécifiques doivent être prises pour interdire aux utilisateurs l'accès à des programmes, transactions, fichiers, données et utilitaires qui sont directement liés à leur fonction dans l'entité. Une trace de tous les traitements effectués doit être disponible.

De plus, des procédures de détection doivent être mises en œuvre pour garantir le fonctionnement du système de sécurité et permettre, le cas échéant, de signaler et de suivre les tentatives de violation.

Enfin, en cas d'existence d'un réseau, l'accès à celui-ci doit également être contrôlé de manière spécifique. Des contrôles supplémentaires sont nécessaires si des entités externes à la société peuvent se connecter au réseau (p. ex. connexion dial-up).

5. La sécurité physique et le plan de secours

5.1.La sécurité physique

Des mesures de prévention et de détection doivent être prises pour protéger tout système contre les dangers tels que incendie, dégât des eaux, pannes de courant, intrusions,...
Une sécurité physique adéquate est basée sur les principes suivants :

Situation
Lors de la mise en place d'une salle informatique, il doit être tenu compte des menaces externes potentielles telles que la présence d'activités industrielles, de réserves d'eau, d'entreposages de matériaux inflammables, etc.

Contrôle d'accès
L'accès au matériel (ordinateurs, matériel de télécommunication, etc.), doit être limité.

Sécurité contre l'incendie
Des mesures spécifiques de détection et de lutte contre le feu s'imposent.

Fourniture d'énergie
La continuité dans la distribution du courant électrique doit être assurée. Les mesures les plus fréquentes sont l'installation de stabilisateurs de courant et de batteries de secours, etc.

Environnement de travail
Des mesures adaptées doivent aussi être prises pour l'aménagement de la salle informatique (température, hygrométrie, etc.).

Réseau
Des mesures doivent être prises pour garantir la disponibilité du réseau (triangulation, liaisons alternatives,...).

5.2.Plan de secours

Un plan de secours efficace doit suivre une méthodologie prenant en compte les éléments suivants :

- identification des fonctions essentielles de l'entreprise sur base d'une analyse de risque; décision des liaisons et des dépendances entre ces fonctions;
- définition de la stratégie alternative en cas de sinistre;
- analyse des menaces potentielles;
- description des solutions possibles et des coûts y afférents;
- documentation du plan et des procédures de secours;
- développement et documentation des procédures alternatives pour les utilisateurs;
- tests du plan de secours;
- définition des responsabilités par la mise à jour du plan;
- formation du personnel concerné.

6. End user computing (traitement par l'utilisateur final)

L'on entend par « end user computing », l'utilisation des moyens informatiques par

tous les utilisateurs finaux dans l'entreprise (notamment par les utilisateurs n'appartenant pas au département informatique). Les moyens peuvent être mis à disposition aussi bien de façon centralisée que décentralisée (micro-ordinateurs).

Certains contrôles et mesures de sécurité applicables (ou même essentiels) pour de grands systèmes ne sont guère utilisables quand il s'agit de micro-ordinateurs. En pratique, ceci donnera lieu à un déplacement des priorités dans l'environnement de contrôle.

Le seuil d'accès étant très bas et les traitements s'effectuant sur un ordinateur « quelconque », on court aussi le risque d'une confiance illimitée des utilisateurs finaux dans l'information financière stockée et générée dans ces systèmes. Vu que ces terminaux sont surtout conçus pour les besoins des utilisateurs individuels, le degré d'exactitude et la fiabilité de l'information sera dans une très large mesure fonction des mesures de contrôle interne imposées par le management et appliquées par les utilisateurs.

Nous reprenons ci-dessous quelques points qui contribueront à déterminer l'approche de contrôle dans des environnements de cette espèce et qui visent à garantir la disponibilité, la confidentialité et l'intégrité des possibilités offertes par les systèmes informatiques basés sur le traitement par l'utilisateur final :

- l'existence d'instructions formelles du management relatives à l'utilisation et au contrôle des micro-ordinateurs dans l'entreprise;
- des mesures relatives à la sécurité physique : réduction du risque de vol, de dommages accidentels ou d'utilisation inappropriée;
- contrôle sur l'utilisation des logiciels (obligations en matière de licence, contrôle d'accès, exigences de formation, etc.);
- contrôle de l'accès aux applications et données développées par l'utilisateur final : mesures qui visent à prévenir des modifications non autorisées;
- instructions relatives à la protection et à l'utilisation de médias de stockage externes (disquettes, bandes, disques durs amovibles,...);
- contrôle de la fiabilité des applications développées par l'utilisateur final;
- contrôle sur la réalisation de copies de sauvegarde des logiciels, des applications développées, des données;
- des mesures de prévention contre l'infection des ordinateurs par des virus;
- des mesures de contrôle et des instructions relatives au branchement sur des réseaux.

***

Annexe B : Contrôles applicatifs

Définition

On entend par « contrôles applicatifs », d'une part, les procédures de contrôle automatisées insérées dans l'application et, d'autre part, les procédures manuelles sur lesquelles se fonde une entité pour contrôler son traitement de données.

L'ensemble de ces contrôles doit garantir que l'information tant financière que opérationnelle disponible dans le système est exhaustive, exacte, autorisée et validée.

1. Procédures de contrôle automatisées

On retrouve ci-dessous une liste non exhaustive de procédures de contrôle automatisées :

- contrôles de validité : ces contrôles sont relatifs au format, à l'exactitude, à l'existence et au caractère adéquat des données à traiter. Ils permettent de rejeter les données erronées;
- vérification de la séquence numérique : un contrôle de ce type doit permettre de vérifier si toutes les données ont été saisies. Il s'agit d'un contrôle portant sur le caractère exhaustif et complet;
- réconciliation automatisée si des données introduites peuvent être comparées à d'autres données enregistrées dans le système, il est possible d'en vérifier le caractère adéquat;
- systèmes d'autorisation : dans bon nombre d'applications, les transactions sont permises sur la base du profil de l'utilisateur. Ceci permet d'assurer la séparation des fonctions.

2. Procédures manuelles de contrôle

Cette catégorie comprend l'ensemble des contrôles effectués manuellement. Il s'agit entre autres :

- de l'analyse de l'information destinée à la gestion; du suivi des rapports d'exceptions;
- de la mise en œuvre de recoupements;
- de la confrontation entre les données fournies par l'environnement automatisé et la réalité (inventaires, recoupement avec les extraits de compte clients ou fournisseurs, etc.);
- de l'approbation formelle des transactions.

3. Interactions entre les contrôles applicatifs et les contrôles généraux informatiques

Les contrôles applicatifs et les contrôles généraux informatiques sont étroitement liés. Les contrôles généraux informatiques sont indispensables pour garantir la fiabilité des contrôles applicatifs qui se basent sur des traitements automatisés.

Les exemples suivants illustrent ce propos :

- si les contrôles relatifs à l'implantation, au développement et à la maintenan- ce des applications sont peu développés, il est possible que l'information destinée au management ne soit pas fiable, que les contrôles de validité ne fonctionnent pas correctement et que les listes de contrôle soient incomplètes et comportent des erreurs. Si les contrôles manuels se fondent sur des rapports peu fiables, l'efficacité du système de contrôle interne sera compromise;
- si les contrôles d'accès logiques relatifs au système présentent des lacunes importantes, la séparation de fonctions prévue au sein de l'entreprise peut être compromise.

2.4. Objectifs du contrôle des comptes annuels (5 janvier 1987)[65]

1. Introduction

Aux termes du paragraphe 1.3.1 des normes générales de révision : « La révision des comptes annuels a pour but de déterminer :

- si la comptabilité et les comptes annuels sont tenus et présentés en conformité avec les dispositions légales et réglementaires;
- si les comptes annuels (bilan, compte des résultats en annexe) donnent une image fidèle du patrimoine, de la situation financière et des résultats de l'entreprise compte tenu des dispositions légales et réglementaires qui les régissent et si les justifications données dans l'annexe sont adéquates. »

De façon plus précise, le contrôle des comptes annuels devra permettre au réviseur d'attester :

- en ce qui concerne *le bilan* : que tous les biens, créances et droits apparaissent à l'actif : qu'ils figurent sous es rubriques appropriées et que leur évaluation a été faite avec la sincérité, la prudence et la permanence nécessaires; que toutes les dettes et tous les engagements apparaissent au passif pour leur montant encore réellement dû et que les provisions nécessaires ont été comptabilisées en vue de

[65] Avis du Conseil Supérieur du Revisorat d'Entreprises d.d. 18 décembre 1986 (Rapp. annuel CSR, 1986-1987, non paginé).