Michel Huissoud

CobiT 4.0 apporte-t-il une réponse aux attentes du PCAOB ?

Oui, mais…! CobiT 4.0 est l'instrument privilégié pour concevoir et auditer les contrôles informatiques. Mal utilisé, il peut cependant conduire à des audits surdimensionnés. Il doit en outre être complété par une analyse des contrôles applicatifs. Ce domaine réserve encore et toujours des surprises qu'un auditeur averti devrait découvrir avant la presse spécialisée…

L'audit du système de contrôle interne (SCI) est revenu en force et c'est tant mieux. La mise en œuvre des règles du PCAOB[1], l'organe de surveillance de la Bourse américaine chargé de faire respecter les exigences de la loi Sarbanes-Oxley (SOX), montre cependant que l'intégration de l'informatique dans le SCI pose encore de nombreuses questions. Il serait faux de penser que ces questions qui nous viennent des Etats-Unis ne concernent qu'une petite minorité de sociétés suisses cotées à la bourse américaine. Que ce soit par le biais des futures directives européennes, des nouvelles dispositions du Code des Obligations ou finalement sous la pression des bailleurs de fonds de l'entreprise, les entreprises vont devoir porter dans le futur une plus grande attention aux risques informatiques et à leur prise en compte correcte dans le SCI.

Il est pour la discussion utile de suivre la typologie adoptée par le Standard d'audit no 2[2] édicté par le PCAOB. Celui-ci distingue :

- les contrôles généraux établis à l'échelon de l'entreprise (*company-* ou *entity-level controls*),
- les contrôles applicatifs (*application controls*) et
- les contrôles généraux informatiques (*IT general controls*).

L'illustration 1[3] montre que seule la seconde catégorie est directement liée aux processus métiers de l'entreprise.

[1] Public Company Accounting Oversight Board
[2] Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, état février 2005
[3] extraite de l'ouvrage « IT Control Objectives for Sarbanes-Oxley », IT Governance Institute (www.itgi.org), 2004

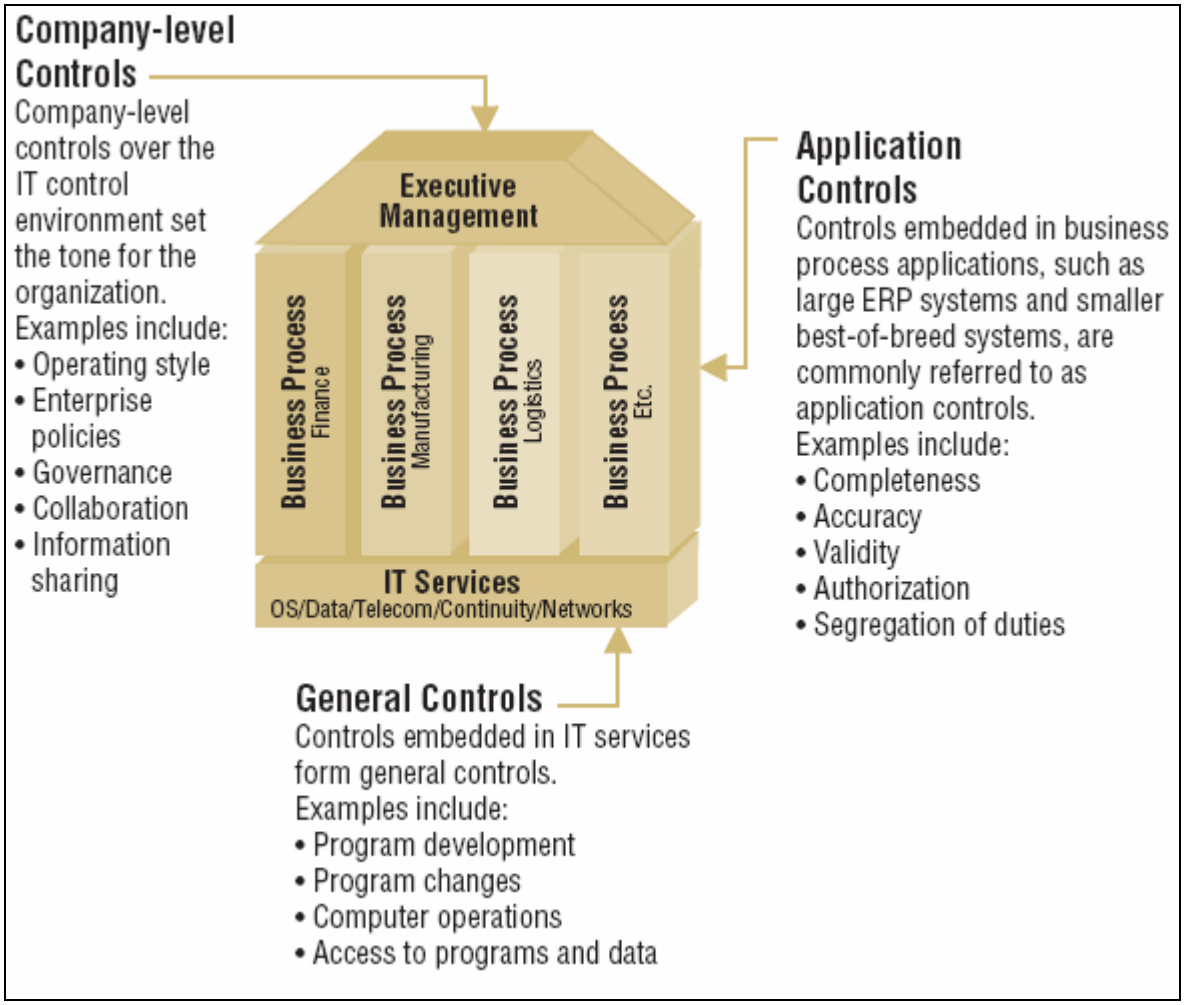

Illustration 1 : les différentes catégories de contrôles selon la typologie du PCAOB

1 *Premier constat : CobiT 4.0 permet de prendre en compte les contrôles informatiques, mais à l'exception des contrôles applicatifs*

La publication en décembre 2005 de la version 4.0 de CobiT[4] a été l'occasion de procéder à quelques remaniements (voir illustration 2) et d'aligner systématiquement ce référentiel sur les règles du PCAOB.

CobiT 3	CobiT 4.0
Le Guide du management et les objectifs de contrôle font l'objet de deux ouvrages séparés	Un ouvrage rassemble pour chacun des 34 processus informatiques, les objectifs de contrôle, les niveaux de maturité, ainsi que les facteurs et les indicateurs de succès
Certains contrôles applicatifs sont compris dans les processus DS5 « gestion de la sécurité » et DS11 « gestion des données »	18 contrôles applicatifs ont été identifiés (numérotés AC1 à AC18), extraits des processus DS05 et DS11, et font l'objet d'une brève description en introduction de CobiT. Ils ne sont par la suite plus traités

[4] "Control Objectives for Information and related Technology (COBIT®)", IT Governance Institute (www.itgi.org)

	dans CobiT (voir illustration 3 ci-dessous).
Le processus PO04 traite de l'organisation générale de la fonction informatique	Le nouveau processus PO04 aborde en détail le thème de la « propriété » des applications et des données informatiques. Pour chacun des 34 processus informatiques, CobiT ne se limite plus à la division informatique mais définit les rôles au sein de l'ensemble de l'entreprise en recourant à un modèle RACI (*who is Responsible, Accountable, Consulted and/or Informed*).
Les 34 processus sont placés sur un même niveau leurs liens ne sont pas explicites	CobiT 4.0 indique les liens de continuité entre tous les processus, en mentionnant par exemple qu'un rapport sur les coûts d'une application, produit dans le cadre du processus PO5 (gérer les investissements informatiques), peut conduire à l'acquisition d'une nouvelle application (processus AI2) qui va nécessiter une adaptation du concept de sécurité (processus DS5).
Illustration 2 : quelques importants changements entre les versions 3 et 4.0 de CobiT	

Tant la Commission européenne[5] que l'Institute of Internal Auditors (IIA) le confirment : CobiT est aujourd'hui l'outil de référence privilégié pour la prise en compte de la gouvernance de l'informatique dans la mise en œuvre des directives européennes ou pour une démarche SOX.

Il est cependant nécessaire de prendre en compte les trois règles suivantes :

1.1 Intégrer directement l'informatique dans toute l'analyse des contrôles à l'échelon de l'entreprise (*company-* ou *entity-level controls*)

Les contrôles établis à l'échelon de l'entreprise ne sont efficaces que s'ils sont globaux. Il est donc essentiel que les systèmes de contrôle adoptent une démarche intégrante :

- ils doivent par exemple comprendre une analyse des risques qui porte sur l'ensemble des risques de l'entreprise, y compris les risques de panne informatique,
- les règles déontologiques doivent traiter aussi bien la lutte anti-corruption que l'interdiction d'accéder aux sites pédophiles,
- la répartition des compétences doit régler tant la conclusion des contrats que la responsabilité des données et des applications,
- la surveillance de l'entreprise doit détecter aussi bien les réclamations des clients que les tentatives d'intrusion dans un serveur informatique,
- etc.…

Plusieurs processus des domaine Planning et organisation (PO) et Surveillance et évaluation (ME) de CobiT sont parfaitement adaptés à ce type de contrôles.

[5] Voir par exemple, la décision prise en mars 2005 reconnaissant CobiT comme un des instruments agréés pour assurer la sécurité des données des agences chargées du payement des aides agricoles.

Les travaux d'audit peuvent se limiter à des vérifications superficielles, fondées sur des autoévaluations, des interviews et la consultation de documents. L'auditeur doit cependant vérifier quelques questions essentielles, dont celle de la définition de la propriété d'une application, qui mérite d'être abordée ici plus en détail.

Comme relevé dans un article précédent (Expert-comptable 2004/10), la maîtrise de l'informatique implique que les utilisateurs connaissent et assument leurs responsabilités. Les utilisateurs (les maîtres d'ouvrage) sont les propriétaires des données et des applications informatiques qui traitent celles-ci. A ce titre ils doivent par exemple valider par des tests adéquats toute modification apportée à leurs logiciels. Deux exemples montrent que l'évolution technologique vient malheureusement singulièrement compliquer cette répartition des tâches :

a) EAI/SOA

Les démarches d'intégration (Enterprise Application Integration, EAI) ou d'architecture orientée service (Service oriented Architecture, SOA) présentent le même défaut. Dans un louable but de simplification et d'efficacité, elles brisent les anciennes barrières entre applications. Des tâches identiques, présentes dans plusieurs applications, comme les routines de calcul des intérêts, l'édition et l'impression des factures, ou plus simplement le transfert de données entre logiciels, sont extraites des application et placées dans un espace commun auquel accèdent l'ensemble des applications (middleware dans l'approche EAI). Si les avantages en terme de simplification de la maintenance sont incontestables, la pratique montre que la « propriété » de ce middleware est plus problématique. Une modification de ces routines devrait en principe être testée dans l'ensemble des applications qui y ont recours et formellement acceptée par les responsables de toutes ces applications. Une exigence complexe à remplir, tant techniquement (difficulté à simuler en environnement de tests) qu'organisationellement (difficulté à rassembler un pool de représentants d'application).

b) Patch Management[6]

Le recours à des logiciels standard apporte incontestablement un gain d'efficacité pour l'entreprise. La pratique montre que les versions misent sur le marché comportent encore de nombreuses erreurs qui sont corrigées ultérieurement par des programmes livrés par le fournisseur (patches). Le problème réside là aussi dans la difficulté pour les utilisateurs d'être associés à ces travaux de maintenance. Vu la difficulté de réaliser des tests à grande échelle, ces patches passeront souvent en production sans que les utilisateurs en soient conscients. Les informaticiens auront en effet tendance à considérer que ces opérations ne présentent pas de risques et n'ont pas d'impact sur la disponibilité ou le bon fonctionnement des applications. Cela est probablement vrai dans 99% des cas mais la pratique montre que dans les rares cas où ces travaux entraînent une panne, celle-ci peut se révéler dramatique pour l'entreprise. D'où la recommandation de tester les patches avant de les charger, de les passer en production en période calme, d'effectuer un monitoring étroit les premières heures ou les premiers jours et dans tous les cas d'informer les utilisateurs de l'augmentation des risques.

Ces exemples montrent que l'auditeur sera bien inspiré de vérifier en détail que l'entreprise a pris les mesures nécessaires pour atteindre les objectifs de contrôle selon CobiT PO4.6 à 4.9, en particulier la détermination des responsabilités pour l'assurance qualité, pour la gestion des risques, ainsi que pour les données et les systèmes.

[6] Voir sur ce thème l'excellent guide « Global Technology Audit Guide Change and Patch Management Controls: Critical for Organizational Success », The Institute of Internal Auditors, 2005

1.2 Comprendre les processus métiers et identifier les contrôles applicatifs (*application controls*)

Il est important de savoir que CobiT mentionne les contrôles applicatifs (voir illustration 3) mais ne les intègre pas dans les 34 processus informatiques de base. Ces contrôles relèvent en effet des processus métiers. Ils ne sont donc compris ni dans les Objectifs de contrôle, ni dans le Guide du management.

„Therefore, the COBIT IT processes cover general IT controls, but not application controls, because these are the responsibility of business process owners and, as described previously, are integrated into business processes."

	DATA ORIGINATION/ AUTHORISATION CONTROLS
AC1	Data Preparation Procedures
AC2	Source Document Authorisation Procedures
AC3	Source Document Data Collection
AC4	Source Document Error Handling
AC5	Source Document Retention
	DATA INPUT CONTROLS
AC6	Data Input Authorisation Procedures
AC7	Accuracy, Completeness and Authorisation Checks
AC8	Data Input Error Handling
	DATA PROCESSING CONTROLS
AC9	Data Processing Integrity
AC10	Data Processing Validation and Editing
AC11	Data Processing Error Handling
	DATA OUTPUT CONTROLS
AC12	Output Handling and Retention
AC13	Output Distribution
AC14	Output Balancing and Reconciliation
AC15	Output Review and Error Handling
AC16	Security Provision for Output Reports
	BOUNDARY CONTROLS
AC17	Authenticity and Integrity
AC18	Protection of Sensitive Information during Transmission and Transport

Illustration 3: les 18 contrôles applicatifs identifiés par CobiT

Ils doivent absolument faire l'objet d'une démarche complémentaire centrée sur l'identification des risques liés aux processus, démarche pour laquelle CobiT n'est pas d'une grande utilité.

Le chiffre 2 ci-dessous revient en détail sur ce type de contrôles.

1.3 Ne traiter les contrôles généraux informatiques (*IT general controls*) que dans la mesure où ils conditionnent le bon fonctionnement d'applications sensibles des processus métiers

Des articles spécialisés se sont fait l'écho d'audits de conformité SOX qui avaient perdu toute proportionnalité avec les objectifs à atteindre. L'épaisseur du blindage de la porte d'accès à un centre de calcul a-t-elle réellement une influence sur la fiabilité des états financiers d'une compagnie internationale ? On peut en douter et de tels excès contribuent à discréditer le travail des auditeurs. Certaines critiques doutent à juste titre de la valeur ajoutée de tels audits et relèvent que SOX a de facto transformé les dividendes autrefois versés aux actionnaires en honoraires versés aux cabinets d'audit.

Ces excès peuvent être évités en adoptant la démarche rétrograde (ou « *Top-down Approach* ») préconisée par le PCAOB:

1) identifier les positions importantes des états financiers,

2) identifier les processus qui génèrent ou conditionnent ces positions,

3) identifier les applications informatiques sensibles pour ces processus,

4) n'auditer que les contrôles généraux informatiques essentiels au bon fonctionnement de ces applications.

Si l'entreprise ne réalise par exemple qu'une part infime de son chiffre d'affaires avec une application e-commerce découplée de ses autres ressources informatiques, l'auditeur devrait avoir le « courage » d'ignorer purement et simplement ce domaine. Si en revanche, l'ensemble de la facturation est externalisée, c'est toute la fiabilité des interfaces (conditionnée par des contrôles tant applicatifs que généraux) qui devra par exemple être examinée.

L'audit des contrôles généraux informatique ne peut se limiter à des interviews mais doit comprendre des vérifications de l'efficacité des contrôles. Ceux-ci sont essentiellement compris dans les domaines Acquisition et implémentation (AI) et Distribution et support (DS) de CobiT, qui fournit avec son Guide d'audit[7] une aide précieuse.

2 Second constat : les contrôles applicatifs demeurent aujourd'hui le principal gap

Un fait divers a récemment illustré l'importance de ces contrôles applicatifs : un négociant en titres a saisi un ordre en inversant le nombre de titre et leur valeur. Il a ainsi vendu 610'000 actions pour 1 Yen au lieu d'en vendre une pour 610'000 Yens. Une erreur qui a coûté 290 millions de francs à la banque et qu'une simple plausibilisation à la saisie (comparaison avec les valeurs précédentes, avertissement vu le nombre d'actions offertes, etc.…) aurait permis d'éviter.

Deux exemples montrent que ces risques importants sont aujourd'hui encore trop souvent négligés, aussi bien par les entreprises que par certains auditeurs.

2.1 Le programme standard de comptabilité des assurances suisses

Depuis le 1er janvier 2005, les assurances privées actives dans le domaine de la prévoyance professionnelle doivent établir à l'attention de l'autorité de surveillance (l'Office fédéral des assurances sociales) une comptabilité annuelle (Betriebsrechnung) permettant de délimiter ce type d'assurances du reste de leurs affaires. Une exigence raisonnable si l'on considère que le total de ces engagements s'élève fin 2004 à 118 milliards de francs à répartir entre 2,3 millions d'assurés…

Cette comptabilité constitue un instrument essentiel à la surveillance étatique, mais regroupe également les données qui pour la plupart des assurances permettent de justifier l'attribution au fonds d'excédents et la distribution des parts excédents. Elle doit donc être considérée comme un système alimentant les états financiers des assurances.

En outre, et selon l'article 140 (devoir d'information) de la nouvelle Ordonnance sur la surveillance des assurances privées en vigueur dès le 1.1.2006 , « *L'entreprise d'assurance transmet aux preneurs d'assurance, dans les cinq mois qui suivent la date du bilan: (a.) la comptabilité des assurances de prévoyance professionnelle, (b.) les indications concernant l'attribution au fonds d'excédents et la distribution des parts excédents, …* ».

[7] Pas encore disponible en version 4,0

Il est réjouissant d'apprendre que l'autorité de surveillance et ses partenaires ont mis au point à l'échelon national une comptabilité standard.

Erfolgsrechnung - Teil 1 — Zahlen in Tausend CHF, BJ = Berichtsj

a	b	c	d
	Gesamtgeschäft		+/- in %
	BJ	BJ-1	
1 **Bruttoprämien gebucht**	0	0	
2 Veränderung Bruttoprämienüberträge (Zunahme = +)	0	0	
3 **Bruttoprämien verdient = 1 - 2**	0	0	
4 Anteil Rückversicherer an den verdienten Prämien	0	0	
5 **Verdiente Prämien für eigene Rechnung = 3 - 4**	0	0	
6 Sonstige versicherungstechnische Erträge	0	0	
7 Zahlungen für Versicherungsfälle	0	0	
8 Leistungsbearbeitungsaufwendungen	0	0	
9 Anteil Rückversicherer an Aufw. für Versicherungsfälle	0	0	
10 **Total Zahlungen netto für Versicherungsfälle = 7 + 8 - 9**	0	0	
11 Veränderung Deckungskapital (Zunahme = +)	0	0	
12 Veränderung der Verstärkungen	#VALEUR!	#VALEUR!	########
13 Veränderung sonstige versicherungstechn. Rückstellungen	12'345	0	
14 Veränderung der Rückstellung für eingetretene, noch nicht erledigte Versicherungsfälle (+=Zunahme)	0	0	
15 Anteil Rückversicherer an Veränd. der vt. Rückstellungen	0	0	
16 **Veränderung der versicherungstechn. Rückstellungen (netto) = 11 + 12 + 13 + 14 - 15**	#VALEUR!	#VALEUR!	########

Illustration 4 : le programme de comptabilité standard (Betriebsrechnung) des assurances privées suisses, réalisé provisoirement avec EXCEL

Il est revanche pour le moins préoccupant de constater qu'il est prévu dans un premier temps de tenir cette comptabilité standard grâce à des tableaux EXCEL.

Comment l'organe externe de révision considérera-t-il les données émanant de ces tableaux EXCEL, qui pour certaines influencent directement certaines positions au bilan des sociétés ? Quelle augmentation des honoraires sera-t-elle nécessaire pour donner une assurance raisonnable sur ces chiffres ? La situation sera-t-elle appréciée différemment si la compagnie d'assurance est soumise à SOX ? On peut dans tous les cas penser que les compagnies d'assurance suisses, qui devraient être les premières intéressées à disposer de données fiables, auraient été mieux inspirées de développer directement leur standard dans un langage de programmation sérieux permettant de mettre en place les contrôles applicatifs appropriés.

2.2 Une fréquente absence de contrôles applicatifs dans les processus de bouclement comptable et d'établissement des comptes

Les auditeurs ont vérifié que les processus métiers alimentent correctement les logiciels de comptabilité et que ceux-ci digèrent et traitent avec fiabilité les informations reçues. Les contrôles appropriés sont en place, tant dans les applications essentielles aux processus métiers que dans les logiciels de comptabilité. Tout est donc pour le mieux.

Ce serait oublier d'une part que le bouclement va nécessiter un certain nombre d'écritures et d'opération dans l'application comptable et, d'autre part, qu'un logiciel comptable n'est généralement pas en mesure de livrer à un imprimeur une version imprimable des comptes annuels. En pratique, les données vont passer à travers de nombreuses opérations

informatiques : elles sont extraites de l'application comptable, transitent éventuellement par un tableur (en particulier s'il s'agit d'établir les comptes consolidés d'un groupe…), sont ensuite reprises dans un programme du type PageMaker ou InDesign, retravaillées en vue de leur publication et finalement transmises à l'imprimerie. Tous ces produits informatiques ont en commun une absence de gestion sérieuse des droits d'accès et de traçabilité des modifications. Compte tenu de cette absence de contrôles applicatifs, ce processus présente donc au moins autant de risques de fraudes et d'erreurs de présentation comptable que l'ensemble des processus situés en amont.

Le PCAOB confirme à cet égard dans une évaluation de novembre 2005[8] que « *Some auditors did not perform sufficient testing of the controls over preparing financial statement disclosures. The controls in this area are among the most important in the financial reporting process because of the relatively high risk of material misstatement or omission due to fraud or error.* »

3 Efficacité du contrôle interne, qui doit auditer quoi et quand?

Le malentendu relevé par le PCAOB vient-il d'une interprétation trop rigide de la notion de « période » ? Le PCAOB est-il lui-même suffisamment clair[9] ? Les Normes d'audit suisses[10] partent de l'idée qu'un audit du système de contrôle interne couvre l'exercice sous revue, alors que la réalité montre qu'en terme de risques de fraudes et d'erreurs c'est le laps de temps couvrant le bouclement et la préparation à la publication des comptes qui est la période de tous les dangers, donc bien après la fin de l'exercice.

En situation d'externalisation de services, quelle valeur accorder à un rapport d'audit (par exemple SAS70) qui n'étant pas daté du 31 décembre ne démontre pas que le prestataire de service disposait d'un SCI efficace durant toute la période ? Dans le même contexte, comment interpréter l'opinion de l'AICPA[11], qui semble admettre que les vérifications chez le prestataire de service ne puissent porter que sur six mois[12] ? Ces questions du périmètre temporel des contrôles mériteront probablement d'être encore approfondies.

La seconde question, toujours plus sensible dans l'audit du SCI, est la délimitation des tâches incombant à l'audit interne. Si le PCAOB règle de manière relativement précise les tâches que l'auditeur externe peut déléguer à l'audit interne[13], la délimitation des tâches entre la ligne et l'audit interne est plus floue.

L'IIA a récemment plaidé pour un renforcement de la surveillance continue de l'efficacité des contrôles en place. Il s'agit en réalité de mettre en place et d'institutionnaliser sous la responsabilité des auditeurs internes une batterie de contrôles détectifs, souvent développés en recourant à des logiciels d'audit[14]. On doit cependant se poser la question : les contrôles détectifs relèvent-ils de la surveillance du SCI ou sont-ils partie intégrante du SCI ? L'avenir nous montrera si les auditeurs internes auront pu éviter que la direction de l'entreprise

---

[8] « Report on the initial implementation of Auditing Standard no 2», PCAOB, 30 novembre 2005

[9] Voir par exemple le chiffre 101 de AS2: "*For controls over significant nonroutine transactions, controls over accounts or processes with a high degree of subjectivity or judgment in measurement, or controls over the recording of period-end adjustments, the auditor should perform tests of controls closer to or at the "as of" date rather than at an interim date*."

[10] Voir par exemple le chiffre 37 de la NAS 400 : « *L'auditeur doit déterminer si les contrôles internes ont été appliqués tout au long de la période* »

[11] American Institute of Certified Public Accountants

[12] "*Testing should be applied to controls in effect throughout the period covered by the report. To be useful to user auditors, the report should ordinarily cover a minimum reporting period of six months*.", AICPA Professional Standards, AU 324.02

[13] Voir par exemple l'annexe E (chiffres 29 à 50) de AS2

[14] L'entreprise ACL est le sponsor officiel du Guide (GTAG 3) publié par l'IIA sur ce thème

saisisse cette perche tendue pour se débarrasser de la responsabilité du contrôle interne et la transférer aux auditeurs. Ce risque ne devrait pas être négligé.

Michel Huissoud, CISA, CIA

Vice-président ISACA (Suisse)