Michel Huissoud

Wie kann man die Informatikrevision integrieren?

Der Wechsel von ISA 401 zu ISA 315, 330 und 500*

Die Schweiz hat beschlossen, sämtliche ISA [1]-Normen der IFAC [2] unverändert zu übernehmen. Ein aufgrund des internationalen Umfelds nicht ganz freiwilliger Entscheid, sicher aber ein Schritt in die richtige Richtung. Um die neusten ISA-Standards der IFAC von Oktober 2003 gebührend umzusetzen, wird man aber noch zwei Probleme lösen müssen: Einerseits sind wichtige Lücken bei den Normen für die Buchführung und den internen Kontrollsystemen zu schliessen, und andrerseits ist in der Revisionsbranche die Kommunikation zwischen Finanz- und Informatikrevision zu verbessern.

1. Rechnungslegungsnormen verdrängen ordnungsmässige Buchführung

Vielfach sind steuerliche Überlegungen oder die Wahrung von Aktionärsinteressen der Grund dafür, dass die Diskussion um die Normen zur Rechnungslegung seit Jahren im Vordergrund steht. US GAAP, Swiss GAAP FER, IAS/IFRS: Alle diese Normen lassen den Problemkreis von Buchführung und internen Kontrollsystemen unbeachtet, um sich auf die Bilanzerstellung oder die Ermittlung der Jahresergebnisse eines Unternehmens zu konzentrieren.

Mit andern Worten: Man beschäftigt sich stark mit der Bilanz und der Tresorerie eines Unternehmens und vergisst dabei, zu berücksichtigen, dass die Zuverlässigkeit dieser Daten direkt von der Qualität der vorgelagerten Prozesse abhängt. Ein Versäumnis, das noch für einige Überraschungen sorgen könnte, erfährt man doch aus einer neueren Studie [3] folgendes: «Die Tabellenkalkulationsprogramme sind selbst bei wichtigen Treasury-Aufgaben noch immer das dominierende Instrument.»

Michel Huissoud, lic. iur., CISA, CIA, Mitglied Fachstab für Informatik der Treuhand-Kammer, Vizepräsident ISACA-Schweiz, Vizedirektor bei der Eidgenösischen Finanzkontrolle, Bern

Dasselbe gilt auch für den Gesetzgeber: Man musste bis zum 24. April 2002 warten, bis mit der *Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV)*[4] eine zögerliche Ergänzung von Artikel 957 des Obligationenrechts erfolgte. Der Verordnungstext wurde übrigens auf Druck der Eidgenössischen Steuerverwaltung eingeführt, was erklärt, warum er sich mehr auf die Aufbewahrung als die Führung der Geschäftsbücher konzentriert [5].

Eine gesetzliche Verankerung der Internen Kontrolle besteht erst seit kurzem und ist noch im Entwicklungsstadium. Wir sehen uns mit einem Sarbanes-Oxley Act 2002 konfrontiert, der die Bereitstellung von «an adequate internal control structure and procedures for financial reporting» [6] fordert. Ferner ist am 17. Juli 2003 ein französisches Gesetz über Finanzsicherheit verabschiedet worden, in dem von «procédures de contrôle interne mises en place par la société» [7] die Rede ist. Zudem wurde vom Bundesrat die Gesetzesänderung zum Obligationenrecht zuhanden des eidgenössischen Parlaments verabschiedet. Sie sieht im neuen Artikel 728a vor, dass «die Revisionsstelle prüft: … ob ein funktionierendes internes Kontrollsystem existiert». In keinem dieser Texte wird indessen ausgeführt, was ein *internes Kontrollsystem (IKS)* umfassen soll. Es gibt zu diesem Thema reichlich Literatur, doch fehlt es an einer Norm, die sich – nach dem Muster des IFRS – an die Adresse der Finanzchefs der Unternehmen richtet und die Buch-

*Traduction de l'article paru dans l'EC 9/04, p. 742.

führung im allgemeinen und die Mindestanforderungen an ein IKS im besonderen festlegt (vgl. *Abbildung 1).*

An dieser Stelle sei erwähnt, dass Prüfungsnormen wie die ISA oder Werke wie das Schweizer Handbuch der Wirtschaftsprüfung keinen Ersatz für solche Standards bieten können, selbst wenn sie die IKS-Prüfung behandeln. Sie sind nämlich an die Wirtschaftsprüfer gerichtet und können nicht direkt bei den Unternehmen durchgesetzt werden.

Diese Lücke führt zu den ewig gleichen Fragen an die Wirtschaftsprüfer: Wer zwingt mich, ein IKS einzurichten? Was bezweckt ein IKS? Worin besteht ein IKS? Um eine Antwort auf diese Fragen zu geben, hat die eidgenössische Finanzkontrolle kürzlich eine Broschüre zu diesem Thema herausgegeben, die sich am Modell COSO orientiert und an die Kader der Bundesverwaltung gerichtet ist [8].

Abbildung 1
Das Problem fehlender Normen in der Buchführung

Der Grundsatz der Ordnungsmässigkeit		
Umfasst folgende Begriffe:	Buch- und Kontenführung, internes Kontrollsystem, elektronische Datenverarbeitung usw.	Rechnungslegung der Erfolgsrechnung, der Bilanz und von deren Anhängen
Geregelt durch:	Es fehlen anerkannte Normen	OR, Normen wie Swiss GAAP FER, IFRS, IPSAS usw. …

2. Ignorieren Finanzrevisionen die IT-Dimension?

Leider ja. Und selbst der Bankensektor, bekannt für die Gewissenhaftigkeit seiner Wirtschaftsprüfer, ist davon nicht ausgenommen. Die Eidgenössische Bankenkommission deckt in ihrem letzten Bericht [9] die Veruntreuungen von zwei Verantwortlichen eines Vermögensverwaltungsinstituts auf. Dieses hat fast die Hälfte seiner Eigenmittel verloren, vor allem als Folge der während mehrerer Jahre begangenen Veruntreuungen, die möglich waren aufgrund «der fehlenden strikten Trennung der Funktionen und der übermässigen Kompetenzen auf IT-Ebene». Hätte der Wirtschaftsprüfer der Bank diese Mängel feststellen müssen? Mit der ISA-Norm 315 «Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement» wird man diese Frage klar beantworten können. Sie regelt nämlich in Ziffer 52, dass «die Verwaltung der Zugriffskontrolle zur Begrenzung des Zugangs zu auszahlungswirksamen Daten und Programmen – z.B. mittels Passwörtern – eine entscheidende Frage bei der Revision der Jahresrechnung sein kann».

«Finanzprüfer und Informatikprüfer müssen lernen, besser miteinander zu kommunizieren.»

Wie steht es um die Prüfung der allgemeinen Kontrollen, die einen reibungslosen Betrieb der IT-Umgebung gewährleisten? Obschon heutzutage im allgemeinen unbestritten ist, dass die Informatikprüfung auch die Existenz und Wirksamkeit von integrierten Kontrollmechanismen in Finanzapplikationen umfassen muss, so ist die Frage einer Prüfung von allgemeinen Kontrollmechanismen eher noch umstritten. Die neuen Normen der IFAC geben auch hier eine klare Antwort. In der ISA-Norm 330 «The Auditor's Procedures in Response to Assessed Risks» sind die Prüfungsverfahren definiert, und in Ziffer 32 [10] werden die integrierten automatisierten Kontrollen in Informatikanwendungen behandelt. Eine solche Kontrolle kann nur dann als wirksam beurteilt werden, wenn sie als Ganzes, d.h. im Zusammenhang mit der Wirksamkeit von allgemeinen Betriebskontrollen (im vorliegenden Fall der Verfahren zum Programmunterhalt) erfolgt. Dieses Beispiel zeigt, dass die Prüfung nicht bei den betrieblichen Arbeitsabläufen enden darf, sondern dass sie auch die Informatikabläufe einschliessen muss, die zum reibungslosen Funktionieren des internen Kontrollsystems beitragen.

Machen wir uns aber nichts vor: Der Weg ist noch lang. Die Schweiz hat heute lediglich die ehemalige ISA-Norm 401 übernommen: «Prüfung im Umfeld computerisierter Informationssysteme», die – aus nicht mehr erklärbaren Gründen – noch nicht Einzug in die Schweizer Normen gehalten hatte. Mit diesem PS 401 wird der Grundsatz der Eingliederung der Informatik in die Prüftätigkeit verankert. Man wird indessen die Übernahme der im Oktober 2003 von der IFAC verabschiedenen Standards, nämlich ISA 315, 330 und 500 «Audit Evidence», abwarten müssen, um effektiv von einer Integration des Informatikaspekts in die Revision der Jahresrechnung sprechen zu können.

Bedauerlicherweise hat die Branche die Sensibilisierung beim Wechsel zum Jahr 2000 nicht genutzt, um eine Integration vorzunehmen. Wie man weiss, mussten damals die Unternehmen und Revisoren auf Druck der IFAC [11] und der Treuhand-Kammer umfassen-

de Inventare über die IT-Anwendungen und -Infrastruktureinrichtungen erstellen, um bei den Unternehmen die Kapazität für eine Fortführung des Geschäftsbetriebs prüfen zu können. Die Erfahrungen aus dem Jahr 2000 sind heute in Vergessenheit geraten, und die Prüfnorm ISA 570 «Fortführung der Unternehmenstätigkeit (Going Concern)», die in der Schweiz ab 2005 die Norm 13 ersetzen wird, ignoriert in der Liste der «Risikofaktoren, welche die Unternehmensfortführung in Frage stellen», grosszügig die Informatikrisiken.

Der Druck von seiten der zukünftigen Aufsichtsbehörde für die Revision könnte diese Entwicklung beschleunigen, sofern die amerikanische Gesetzgebung unseren helvetischen Rhythmus nicht erneut durcheinanderbringt. Die Abgeordnetenkammer behandelt nämlich demnächst ein Projekt über den Corporate Information Security Accountability Act, das die börsenkotierten Unternehmen verpflichten soll, «to hire an independent auditor to assess existing information security controls and ensure that they meet basic standards that the U.S. Securities and Exchange Commission has yet to determine».

3. Integrierte Prüfung, wer macht was?

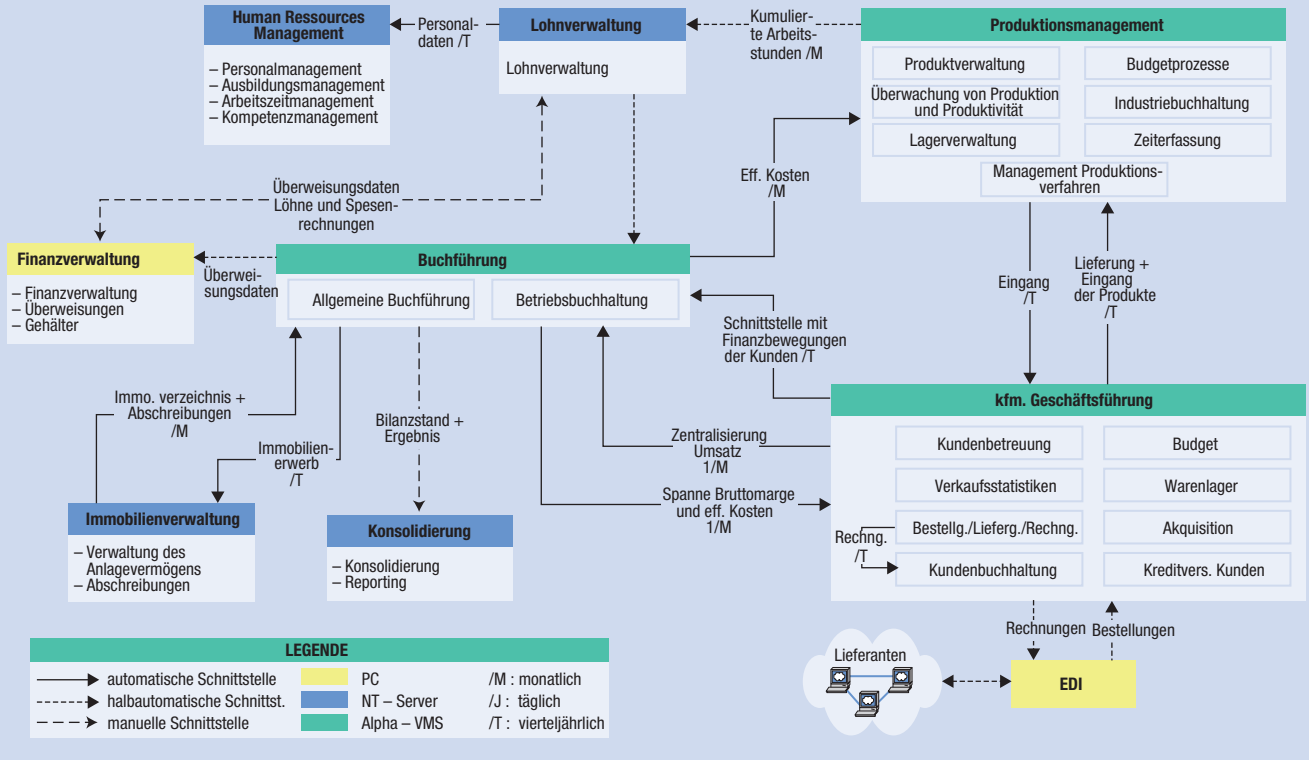
Die Integration der Informatikprüfung in die Finanzprüfung ist eine zentrale Frage, die viele Wirtschaftsprüfer beschäftigt.

Eine erste Feststellung: Finanzprüfer und Informatikprüfer müssen lernen, besser miteinander zu kommunizieren. Tatsächlich kann man feststellen, dass bei der Revision ähnliche Kommunikationsprobleme existieren wie in den Unternehmen selbst. Die Informatiker (Auftragnehmer/MOE [maîtrise d'œuvre] für unsere französischen Kollegen resp. Erbringer von Informatikdienstleistungen) haben grosse Schwierigkeiten, einen verantwortlichen und qualifizierten Partner bei den Dienstleistungsbenutzern (Auftraggeber/MOA [maîtrise d'ouvrage], sponsors für unsere angelsächsischen Kollegen resp. Leistungsempfänger) zu finden. Für ein geprüftes Unternehmen besteht tatsächlich die Gefahr, dass die mit dieser schlechten Kommunikation verbundene Risiken nicht erkannt werden, weil sich im Revisionsteam die gleichen Probleme nochmals ergeben. Der Informatikprüfer hat mit dem Informatikverantwortlichen zu tun, der Finanzprüfer mit den Finanzverantwortlichen, ohne dass die einen und die anderen ihre Feststellungen effektiv miteinander austauschen.

Damit ein Austausch stattfindet, braucht die Branche Verfahren und Instrumente, die den Dialog zwischen Finanzprüfern und Informatikprüfern fördern. Ein Beispiel dafür ist die Kartographierung der Informatikanwendungen eines Unternehmens.

In der Praxis geht es darum, den goldenen Mittelweg zwischen der wörtlichen Beschreibung eines Ablaufs und (als

Abbildung 2
Beispiel einer Kartographierung von Anwendungen
Auszug aus dem Leitfaden der CNCC



Extrembeispiel) einem Schaltschema in einem Gebäude zu finden. Die französische *Compagnie nationale des commissaires aux comptes (CNCC)* hat mit ihrem hervorragenden Leitfaden «Prise en compte de l'environnement informatique et incidence sur la démarche d'audit» (erhältlich unter www.cncc.fr) Pionierarbeit geleistet. Man findet darin insbesondere realistische Beispiele für die Darstellung der Anwendungslandschaft eines Unternehmens, die es den Prüfern ermöglichen sollten, eine identische Wahrnehmung der Probleme zu erlangen.

«Es müssen Anstrengungen unternommen werden, damit die Rechnungsrevisoren die Informatikaspekte besser in ihren Arbeitsplan integrieren können.»

Um ein solches Schema zu erstellen (vgl. *Abbildung 2),* muss man in einem interdisziplinären Approach die wichtigsten Anwendungen und Schnittstellen definieren. Anschliessend kann die Bestandesaufnahme wie folgt ergänzt werden:

Jede Anwendung mit

- den wichtigsten Funktionen,
- einer Schätzung des verarbeiteten Volumens,
- der technischen Umgebung,
- der Art der Zugriffskontrolle und
- der für die Anwendung verantwortlichen Person.

Jede Schnittstelle mit

- der Art von Schnittstelle (automatisch, manuell),
- den vor- und nachgelagerten Anwendungen,
- den Häufigkeiten (täglich, monatlich, jährlich) und
- dem Vorhandsein von Kontrollen zur Erkennung von Abweichungen.

Eine solche Bestandesaufnahme ist eine unerlässliche Arbeitsgrundlage, die den Informatik- und Finanzprüfern erlaubt, ihre Risikoanalysen zusammenzulegen, den Datenfluss aufzuzeigen und die erforderlichen Kontrollen festzulegen. Es sollte damit auch möglich sein, die durch die Informatikprüfung festgestellten Schwächen nötigenfalls bis in den Revisionsbericht zu verfolgen. Man wird noch weitere Instrumente entwickeln müssen, um diesen interdisziplinären Approach zu stimulieren.

4. IKS-Prüfung und ungelöste Fragen

4.1 Wie soll man Standardsoftware behandeln?

Wie versichert man sich der Zuverlässigkeit von Standardsoftware, ob zertifiziert oder nicht? Die Treuhand-Kammer hat vor einiger Zeit mitgeteilt, dass die Fachmitteilungen nicht mehr gültig seien. Die Mitteilung Nr. 9, «Zertifizierung der Software», verschwindet somit von der Bildfläche und hinterlässt eine Lücke, die man irgendwann schliessen muss. Einmal abgesehen von der Problematik der Firma, welche die Software zertifiziert, bleibt der Prüfer mit dem Problem einer Standardsoftware konfrontiert. Was soll er tun? Soll er sich erkundigen, ob das Produkt eventuell zertifiziert ist, welche Vorbehalte man bei der Zertifizierung angebracht hat, welche Parameter von der zertifizierten Version abweichen? Soll er sich über «Bugs» in dieser Software informieren? Soll er Auskunft über die Tests einholen, die vor der Einführung der Standardsoftware durchgeführt worden sind? Soll er selber die Tests durchführen, die nicht vorgenommen wurden? Die Erfahrung zeigt, dass Standardsoftware-Produkte Fehler enthalten, die sich im Rahmen der Revision materiell auswirken können, wie aber soll man einen Kunden davon überzeugen, solche Tests zu finanzieren?

4.2 Wie kann man Lieferanten und andere Geschäftspartner in die Schnittstellenprüfung einbeziehen?

Die ISA-Norm 402 liefert die Grundlagen für die Prüfung im Outsourcing-Verhältnis und bestimmt insbesondere, dass der Prüfer die «Interaktion zwischen dem Rechnungswesensystem und der Internen Kontrolle des Kunden und den Systemen der Dienstleistungsorganisation» berücksichtigen muss. Im Gegenzug existieren nur wenige Empfehlungen zur Prüfung der Schnittstellen, seien diese innerhalb oder ausserhalb des Unternehmens. Ist eine Zusammenarbeit mit dem Revisionsorgan eines Lieferanten, eines Kunden oder einer Pensionskasse ebenfalls Vorschrift? Zu welchen Bedingungen? Ein Bereich, wo alles oder fast alles noch offen ist.

Die CNCC bietet in Frankreich seit 2004 das Ausbildungsprogramm «Visa pour l'audit en environnement informatisé» [Befähigung für die Wirtschaftsprüfung im Informatikumfeld]. Es handelt sich dabei um einen Weiterbildungskurs im Umfang von 100 Stunden, bestehend aus einem 5tägigen Seminar (mit Schwerpunkt Anwendungsleitfaden, wie oben erwähnt), 5 Tagen Betreuung, in denen der Teilnehmer während eines seiner Mandate begleitet wird, und 20 Stunden Selbststudium. Der Fachstab für Informatik der Treuhand-Kammer prüft die Durchführung eines Ausbildungszyklus in Genf.

4.3 Was tun, wenn es kein IKS gibt?

Es ist interessant, aus der Botschaft des Bundesrats zu erfahren: «Sollte die Revisionsstelle feststellen, dass das in-

terne Kontrollsystem ungenügend ist, muss sie ersatzweise selber Kontrollen durchführen». Die Praxis wird zeigen, wie weit die Kundenfirmen bereit sind, diese Zusatzarbeiten zu entschädigen. Sofern sie sich weigern, bleibt der Revisionsstelle nichts anderes übrig, als ungeachtet der Vorbehalte eine Genehmigung der Rechnung vorzuschlagen oder aber das Mandat zu kündigen. Ein ungenügendes IKS scheint nach Auffassung der Lehre bis heute kein Grund zu sein, die Rückweisung der Rechnung zu beantragen [12]. Und doch könnte eine solche Lösung ein wirksames Druckmittel sein, um die Unternehmen zu zwingen, Schwachstellen durch nachträgliche und angemessene Kontrollen zu beheben.

5. Treuhand-Kammer: Rolle des Fachstabs für Informatik?

Die grossen Treuhandfirmen verfügen schon heute über Spezialisten und sind von der Entwicklung kaum betroffen. Problematisch könnte die Umsetzung von neuen Standards dagegen für kleinere Revisionsfirmen sein, die nicht über eine kritische Masse verfügen, um Spezialisten anzustellen. Denkbar wäre indessen, dass ihnen die Treuhand-Kammer ein Spezialistenteam für die Informatikprüfung zur Verfügung stellt, das – gegen Entschädigung – beraten und unterstützen resp. für die kleinen Revisionsfirmen gewisse Arbeiten im Auftragsverhältnis ausführen könnte. Ein solches Projekt, das die Gründung einer privaten Unternehmung voraussetzt, wird in Frankreich gegenwärtig von der «Compagnie nationale des commissaires aux comptes» geprüft.

Ohne so weit gehen zu wollen, müssen Anstrengungen unternommen werden, damit die Rechnungsrevisoren die Informatikaspekte besser in ihren Arbeitsplan integrieren können. Sie brauchen Hilfsmittel für die Darstellung, die Analyse und schliesslich die Prüfung der Arbeitsabläufe, ferner Verfahren für die Prüfung von Informatikanwendungen, einen Leitfaden für den Einsatz der Prüfinstrumente sowie Weiterbildungskurse, die über das übliche Angebot hinausgehen. Diese Erfordernisse rufen nach einer teilweisen Professionalisierung des bestehenden Fachstabs für Informatik der Treuhand-Kammer.

Anmerkungen

1 International Standard on Auditing.

2 International Federation of Accountants, die Normen wurden vom International Auditing and Assurance Standards Board (IAASB) der IFAC vorbereitet.

3 «Corporate Treasury in Deutschland», PricewaterhouseCoopers, Oktober 2003.

4 SR 221.431.

5 Ein weiteres Beispiel für den Einfluss von Steuerfragen liefert die Verordnung des Eidgenössischen Finanzdepartements vom 30. Januar 2002 betreffend die elektronisch übermittelten Daten und Informationen EIDI-V, SR 641.201.1, welche die Anforderungen bezüglich der Mehrwertsteuer behandelt.

6 Sarbanes-Oxley Act of 2002, Sec. 404 Management assessment of Internal Controls.

7 Art. 117, in Abänderung zu Artikel 225-37 des Handelsgesetzbuches (Code de Commerce).

8 www.efk.admin.ch.

9 Bericht 2003, Ziffer 2.1.2.

10 «32. In the case of an automated application control, because of the inherent consistency of IT processing, audit evidence about the implementation of the control, when considered in combination with audit evidence obtained regarding the operating effectiveness of the entity's general controls (and in particular, change controls) may provide substantial audit evidence about its operating effectiveness during the relevant period.»

11 Die für diese Gelegenheit die Weisung IFAC 1011 «Folgen des Jahr-2000-Wechsels für die Revisoren» erlassen hatte.

12 Vgl. z. B. das Schweizer Handbuch der Wirtschaftsprüfung (Band 2, Ziffer 4.41).