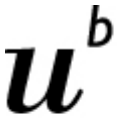

UNIVERSITÄT
BERN

Institut für Wirtschaftsinformatik
der Universität Bern

Arbeitsbericht Nr. 190

Compliance-Nachweise bei Outsourcing von IT-Aufgaben

Gerhard F. Knolmayer

August 2006

Institutsadresse: Engehaldenstrasse 8, CH-3012 Bern, Schweiz
Tel.: ++41 (0)31 631 38 09
Fax: ++41 (0)31 631 46 82
E-Mail: gerhard.knolmayer@iwi.unibe.ch

Compliance-Nachweise bei Outsourcing von IT-Aufgaben

1 Problemstellung

In den letzten Jahren haben sich Gesetzgeber und Regulatorenbeeinflusst vom Fehlverhalten einiger Unternehmen, veranlasst gesehen, teilweise sehr weit reichende Anforderungen zu formulieren. Die von den Regulationen betroffenen Unternehmen sollen bestimmte Anforderungen erfüllen, also "compliant" sein. Unter Compliance wird die Einhaltung von gesetzlichen und behördlichen Vorschriften, Richtlinien und internen Vorgaben verstanden.

Die neuen Regulierungen werden als "informationcentric" charakterisiert [Ecke06]. Um sie erfüllen zu können, müssen auch die eingesetzten IT-Systeme gewissen Anforderungen genügen. Aus diesem Grund finden Fragen der Compliance in IT-Bereichen und die damit eng verbundene IT Governance neuerdings große Beachtung. Auf Basis einer Umfrage wird der Anteil der in IT-Bereichen für Compliance-Nachweise aufgewendeten Zeiten auf 34% geschätzt [Hurl06, 11].

In Abschnitt 2 dieses Beitrags werden Formen von Outsourcing kurz zusammengefasst. Abschnitt 3 verweist auf einige besonders aktuelle Anforderungen an die Unternehmensführung, auf daraus an IT-Systeme resultierenden Vorgaben und auf (Quasi-)Standards zur Erfüllung dieser Vorgaben. Abschnitt 4 beschäftigt sich mit der Erfüllung dieser Anforderungen bei Auslagerung von IT-Aufgaben. Abschnitt 5 erörtert, ob diese neuen Compliance-Anforderungen ein Off- und Nearshoring von IT-Aufgaben eher fördern oder bremsen. Abschnitt 6 fasst die Überlegungen zusammen.

2 Off- und Nearshoring als Spezialformen des Outsourcings

Unter Outsourcing von Informationssystemen verstehen wir die mittel- und langfristige Auslagerung einzelner oder aller bisher innerbetrieblich erfüllter Aufgaben der Informationsverarbeitung an einen rechtlich unabhängigen Dienstleister [MeKn98, 17]. Offshoring kann definiert werden als eine Auslagerung von Geschäftsprozessen oder einzelner Prozessschritte an Dienstleister, die in Übersee domiliziert sind; Begriffe wie "Offshore Outsourcing" und Offsourcing machen deutlich, dass Offshoring als Spezialfall des Outsourcings verstanden wird. In West- und Mitteleuropa wird eine Auslagerung an räumlich näher positionierte Dienstleister, vor allem nach Osteuropa, als Nearshoring bezeichnet.

In den zahlreichen Darstellungen, die sich mit Vor- und Nachteilen von IT-Outsourcing beschäftigen (vgl. [KnMi00, 12 ff]), werden die mit der Erfüllung von Compliance-Nachweisen verbundenen Gesichtspunkte kaum thematisiert. Hingegen haben sich Aufsichtsbehörden und Wirtschaftsprüfer mit dieser Thematik bereits seit längerem auseinandergesetzt. In Verbindung mit dem in den USA 2002 beschlossenen und erstmals 2005 angewandten Sarbanes-Oxley Act (SOX) findet diese Thematik auch in der Wirtschaftsinformatik Aufmerksamkeit. Aktuelle Fragen sind: Wird der SOX bewirken, dass Outsourcing generell oder für bestimmte Aufgaben nicht mehr anwendbar ist? Erhöht er die Kosten des Outsourcings? Reduziert handkehrum Outsourcing die Kosten der Erfüllung der SOX-Nachweise? (Vgl. [MeGa04]).

Werden IT-Aufgaben ausgelagert, so leitet sich aus der Forderung nach IT Governance jene nach "Outsourcing Governance", im Fall der Auslagerung ins Ausland nach „Offshoring bzw. Nearshoring Governance“ ab, wobei unterschiedliche und verschieden gehandhabte Rechtsnormen relevant werden. Lagert der inländische Dienstleister Aufgaben ins Ausland aus, wie dies aktuell bei T-Systems diskutiert wird, oder wird er von einem ausländischen Unternehmen übernommen, so kann eine als "inländisches Outsourcing" konzipierte Auslagerung zu einer Off- oder Nearshoring-Beziehung werden.

3 Compliance-Anforderungen an Informationssysteme

3.1 Vorschriften

Im Folgenden stehen grundlegende Zusammenhänge, nicht aber die oft subtilen Unterschiede z.B. zwischen internationalen und nationalen Prüfungsstandards im Vordergrund. Die an IT-Systeme gestellten Anforderungen unterscheiden sich nach Branchen (vgl. [Cutl06, 9 ff]) und Rechtsordnungen. Sie können (wie z.B. Datenschutzvorschriften oder unternehmensinterne Regelungen über akzeptablen Umgang mit dem Internet) unmittelbaren Bezug zu IT-Systemen aufweisen. Da immer mehr Geschäftsprozesse computergestützt ablaufen, sind IT-Systeme aber auch mittelbar für den Nachweis der Einhaltung anderer Vorschriften (z.B. der Ordnungsmäßigkeit des Rechnungswesens oder der Qualitätskontrolle) von zentraler Bedeutung.

Bei Prüfung von Jahresabschlüssen hat der Wirtschaftsprüfer gemäß [IDW02] das IT-Umfeld, die IT-Organisation, die IT-Infrastruktur, die IT-Anwendungen, IT-gestützte Geschäftsprozesse, das IT-Überwachungssystem sowie IT-Outsourcing zu prüfen. Die Bestimmungen zur Jahresabschlussprüfung wurden z.B. in Deutschland durch das Gesetz über Kontrolle und Transparenz im Unternehmensbereich und für an US-Börsen notierte Gesellschaften im SOX verschärft. Darüber hinaus existieren viele weitere Vorschriften mit teilweise nur lokaler oder branchenspezifischer Bedeutung. Weitere Regulierungen wie Basel II, Solvency II, die EU-Richtline MiFID („Markets in Financial Instruments Directive“) und die mehr als 1000 Seiten umfassende EU-Verordnung zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH) werden demnächst wirksam.

Regulations- und Compliance-Fragen sind z.B. in Banken zu einem oder sogar *dem* zentralen Thema der Unternehmensführung geworden [NN05]. Unternehmen, die große Anstrengungen auf sich nehmen mussten, um zu einer Vielzahl neuer und oft unklarer Bestimmungen compliant zu werden, wissen nicht, ob ihre Vorgehensweisen korrekt sind [Kolo05, 3]. Was im Zusammenhang mit dem Health Insurance Portability and Accountability Act (HIPAA) formuliert wird, gilt auch für andere Anforderungen: "Unfortunately, the technical requirements are buried well within mountains of information found in the HIPAA legislation, the interpretation of various experts, and government and private websites" [NaBu03, 7]. Aus der Pharmaindustrie wird über einen erheblichen Zuwachs externer Prüfungen berichtet, der weder für die Pharma-Unternehmen noch für ihre Lieferanten zu bewältigen sei. Es gibt redundante Prüfungen, ihre Länge habe sich seit 1996 verdoppelt und die Kompetenz der Prüfer habe mit den technischen Weiterentwicklungen nicht Schritt gehalten [PDAS04].

Im Folgenden konzentrieren wir uns auf Compliance-Anforderungen an interne Kontrollsysteme und IT-Systeme. Gemäß American Institute of Certified Public Accountants (AICPA) sind Gegenstand der internen Kontrolle

- die Zuverlässigkeit der Finanzberichterstattung,
- die Effektivität und Effizienz der Geschäftsprozesse und
- die Compliance mit gesetzlichen und regulatorischen Vorschriften [AICP06, 1].

Bei Beurteilung des internen Kontrollsystems hat der Prüfer

- das Kontrollumfeld
- Risikobeurteilungen
- Kontrollaktivitäten
- Information und Kommunikationssysteme und
- die Überwachung des internen Kontrollsystems (Monitoring) [IDW01, 823; AICP06, 1]

zu berücksichtigen.

Besondere Aufmerksamkeit finden Compliance-Fragen derzeit in Zusammenhang mit dem SOX, der formal für alle an US-Börsen notierten Gesellschaften und ihre wesentlichen Beteiligungen gilt, de facto aber weit darüber hinaus von Bedeutung ist [TreuoJ; Arbe04; Enge04; KnWe06]. Eine Übersicht über verwandte Regelungen in anderen Staaten findet sich in [Maza06].

Bei hohen Strafandrohungen fordert Section 404 des SOX vom CEO und CFO im Rahmen der jährlichen Berichterstattung eine Beurteilung der Effektivität der "… company's internal control structure and procedures for financial reporting. Section 404 also requires the company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board" [SEC03]. Für den jährlichen Bericht des Managements über interne Kontrollsysteme sind folgende Inhalte vorgesehen:

- "a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;
- a statement identifying the framework used by management to evaluate the effectiveness of this internal control;
- management's assessment of the effectiveness of this internal control as of the end of the company's most recent fiscal year; and
- a statement that its auditor has issued an attestation report on management's assessment" [SEC03].

Alle Kontrollschritte, von denen rund 50-70% in IT-Systemen erfolgen [Schi05], sind zu dokumentieren, was die erheblichen Auswirkungen des SOX auf Gestaltung, Betrieb und Wartung der IT-Systeme erklärt (vgl. etwa [Sarb04; AuMa05; BuRi05; Dami05; LaPe05; Brew06; KnWe06]).

3.2 Orientierungshilfen

Das oben angesprochene Framework wird nicht spezifiziert, muss aber geeignet und breit akzeptiert sein, „… established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment" [SEC03]. Mehrere Frameworks, Vorgehensmodelle und Reifegradmodelle schlagen Norm-Prozesse und „best practices“ für verschiedene Aufgaben vor. Dazu gehören

- das vom Committee of Sponsoring Organizations of the Treadway Commission bereits 1992 entwickelte und bisher vor allem in den USA beachtete COSO-Framework, das sich insbesondere mit der Gestaltung interner Kontrollsysteme beschäftigt und sich im SOX-Umfeld zu einem "Quasi-Standard" zu entwickeln scheint,

- das von der ISACA ursprünglich 1995 veröffentlichte und derzeit in Release 4.0 vorliegende CobiT (Control Objectives for Information and related Technology)-Framework, das IT-Systeme detaillierter als COSO betrachtet und in den vier Domänen Planung und Organisation, Beschaffung und Einführung, Auslieferung und Unterstützung sowie Überwachung insgesamt 34 Prozesse definiert, zu denen u.a. „Monitor and Evaluate Internal Control“, „Ensure Regulatory Compliance“ und „Provide IT Governance“ gehören,
- die ursprünglich von der britischen Central Computer and Telecommunications Agency (CCTA) seit 1989 entwickelte Information Technology Infrastructure Library (ITIL), die einen Schwerpunkt auf das Service Management legt und insbesondere in Europa für diesen Bereich weite Beachtung findet,
- die auf ITIL bzw. British Standard 15000 aufbauenden Normen ISO/IEC 20000, die Anforderungen und Verfahrensregeln für IT-Dienstleister und deren Prüfer formulieren,
- Standards zu Information Security Management Systems (wie ISO/IEC 17799 oder 27001), die Anforderungen an die IT-Sicherheit und zugehörige Prozesse sowie rund 130 "Baseline Controls" definieren oder
- das vom Software Engineering Institute der Carnegie Mellon University entwickelte Capability Maturity Model (CMM), das 2001 durch das Integrationsbedürfnisse betonende CMMI weiter entwickelt wurde.

Unterschiede und inhaltliche Überschneidungen der Frameworks werden nicht einmal für einen bestimmten Zeitpunkt einhellig interpretiert (vgl. [Glen03; Gray04, 38; Sewe05]). Die damit verbundene Unsicherheit verstärkt sich noch durch die Weiterentwicklungen der Frameworks. So wurde etwa COSO zu einem „Enterprise Risk Management Framework“ erweitert [COSO04] und CobiT hat sich über mehrere Stufen von einem Prüfungskonzept zu einem Governance-Konzept weiter entwickelt [ISAC06, 47]. Die CobiT-Prozesse sind zudem so umfangreich, dass eine vollständige Umsetzung aller Prozessschritte meist kaum möglich und wirtschaftlich sein wird. Zur Relativierung der gestellten Anforderungen werden in CobiT sechsstufige Reifegradmodelle formuliert. Beispielsweise werden für den Prozess „Ensure regulatory compliance“ die Stufen

0 … Non-existent
1 … Initial/Ad hoc
2 … Repeatable but Intuitive
3 … Defined Process
4 … Managed and Measurable
5 … Optimised

unterschieden [ITGI05, 166]. Damit stellt sich die Frage, wie Management und Wirtschaftsprüfer die nur selten den maximalen Reifegrad erreichenden IT-Systeme hinsichtlich Compliance bewerten sollen: Wie viel Reife ist zur Erfüllung der Compliance-Anforderungen erforderlich?

Prüfungsgesellschaften haben eigene Vorgehensmodelle (z.B. KPMG: "Streamlining SOX 404 Compliance"; PWC: "Enterprise Risk Management - Integrated Framework") entwickelt. Dies kann z.B. bei der Zusammenarbeit mehrerer Prüfer (vgl. Abschnitt 4.3) zu Problemen führen, wenn auf Grund der unterschiedlichen Standards, Frameworks und Vorgehensmodelle Aussagen gemacht werden, die bei Anlegung eines anderen Maßstabes nicht relevant wären.

4 Auslagerung compliance-relevanter Aufgaben

4.1 Nachweispflichten trotz Auslagerung

Unternehmen können sich nicht durch Auslagerung ihren Nachweispflichten entziehen. So stellt die Eidgenössische Bankenkommission (EBK) bereits 1999 fest: "Die Unternehmung ist gegenüber der Aufsichtsbehörde auch für die ausgelagerten Geschäftsbereiche verantwortlich, wie wenn sie diese selbst betreiben würde" [EBK99, 3]. Analog formuliert das (auf Basis des SOX eingerichtete) Public Company Accounting Oversight Board (PCAOB) im Auditing Standard No. 2: "The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting" und "If the service organization's services are part of the company's information system …, then they are part of the information and communication component of the company's internal control over financial reporting" [PCAO04, 249].

Vor Verschärfung der Compliance-Anforderungen wurde oft davon ausgegangen, dass das auslagernde Unternehmen nur bestimme, *was* der Dienstleister zu erbringen habe, es aber diesem überlassen sei, *wie* diese Leistungen erbracht werden. Diese Sichtweise kann kaum aufrechterhalten werden, weil das auslagernde Unternehmen sicherstellen muss, dass die Vorgehensweisen des Dienstleisters den Ansprüchen des Gesetzgebers und der Regulatoren entsprechen: „... outsourcing normally results in greater, not less, scrutiny of the activity“ [MeGa04].

4.2 Einschränkungen und Voraussetzungen für Auslagerungen

Einschränkungen für Outsourcing und insbesondere für Verlagerungen ins Ausland gelten vor allem im Finanzdienstleistungssektor (vgl. [HaHS00; Stoc03]). In Deutschland unterscheiden der § 25a (2) Kreditwesengesetz und das zugehörige Rundschreiben 11/2001 der Bundesanstalt für Finanzdienstleistungsaufsicht unwesentliche und wesentliche Bereiche. Letztere sind sehr breit gefasst und umfassen u.a. alle Tätigkeiten, die unmittelbar für die Durchführung der Finanzdienstleistungen notwendig sind und Risiken nachhaltig beeinflussen können. Wesentlich sind auch Bereiche, die der Erfassung, Analyse, Begrenzung, Überwachung, Steuerung und Kontrolle der Risiken dienen sowie jene, die bestehen müssen, um den organisatorischen Mindestanforderungen zu genügen und eine lückenlose Aufsicht durch das Bundesaufsichtsamt zu gewährleisten. Für Weiterverlagerungen an Subunternehmer ist ein Zustimmungsvorbehalt für das auslagernde Institut vertraglich zu vereinbaren. Nicht auslagerungsfähig sind die Unternehmensplanung, -organisation, -steuerung und -kontrolle als originäre Leitungsaufgaben; bei größeren Banken darf auch die Interne Revision nicht vollständig ausgelagert werden. Zudem darf die Gesamtheit der bei Einzelbetrachtung auslagerbaren Bereiche die in der Bank verbleibenden an Umfang und Bedeutung nicht deutlich übertreffen [Bund01].

Die Prüfrechte der Internen Revision, der Abschlussprüfer und des Bundesaufsichtsamts müssen durch eine Duldungserklärung des Dienstleisters bestätigt werden. Bei Off- oder Nearshoring muss die Rechtsordnung des ausländischen Staates, in dem der Dienstleister domiziliert ist, solche Prüfungen erlauben. Manche ausländische Aufsichtsbehörden wollen hoheitliche Maßnahmen ausländischer Aufsichtsbehörden in ihrem Land nicht akzeptieren (vgl. [ZeHa98, 1115 f; Eyle00, 1232 f; HeSt00, 26 f]). Der Abschlussprüfer hat zur Ordnungsmäßigkeit der Auslagerung und zu jeder Auslagerungsmaßnahme Stellung zu nehmen [Bund01]. Da (im Gegensatz zu Funktionsausgliederungen in der Versicherungswirtschaft (vgl. [MiLa04])) keine Vorlage- oder Genehmigungspflicht von Auslagerungen vorgesehen ist, besteht für Banken Rechtsunsicherheit bezüglich des Ergebnisses späterer

Prüfungen [Tetz02].

Ein Rundschreiben der EBK verlangt u.a., dass Outsourcing-Lösungen den Erfordernissen einer angemessenen Organisation, des Bankgeheimnisses und des schweizerischen Datenschutzes entsprechen. Intern ist zu definieren, welche Stelle für die Kontrolle des Dienstleisters verantwortlich ist; dessen Leistungen sind fortlaufend zu überwachen und zu beurteilen, so dass allfällig notwendige Maßnahmen sofort ergriffen werden können. Die Bank muss die nötigen Einsichts-, Weisungs- und Kontrollrechte vertraglich vereinbaren. Prüftätigkeiten können an den Wirtschaftsprüfer des Dienstleisters delegiert werden, sofern dieser über die notwendigen Kompetenzen verfügt [EBK99].

4.3 Prüfung ausgelagerter compliance-relevanter Aufgaben

Das Institut der Wirtschaftsprüfer legte 2003 im Prüfungsstandard IDW PS 331 Regelungen für die Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen [IDW03] fest. Diese orientieren sich am International Standard on Auditing ISA 402 "Audit Considerations Relating to Entities Using Service Organizations" des International Auditing and Assurance Standards Boards.

Betrachtet man die Rechts- und Kommunikationsbeziehungen bei Auslagerung compliance-relevanter Aufgaben, so kann (in Anlehnung an die kompakte amerikanische Terminologie) zwischen

- der User Organization (der auslagernden Unternehmung; dem zu prüfenden „entity“)
- dem User Auditor (dem Wirtschaftsprüfer der auslagernden Unternehmung)
- der Service Organization (dem Dienstleister) und
- dem Service Auditor (dem Wirtschaftsprüfer des Dienstleisters; dem „anderen Prüfer“)

unterschieden werden [AICP06, xv] (vgl. Bild 1).

Grundsätzlich ist der User Auditor für die Prüfung des Gesamtsystems und damit auch der ausgelagerten Systeme der User Organization verantwortlich. Insbesondere obliegt ihm die Prüfung der Schnittstellen zwischen internen und ausgelagerten Informationssystemen z.B. hinsichtlich Vollständigkeit, Genauigkeit und Freigabe übertragener Inputs, der Sicherstellung der Vollständigkeit und Richtigkeit erhaltener Outputs sowie der Zugangskontrollen zu den ausgelagerten Systemen [GeBa03, 72].

Der Dienstleister kann die compliance-relevanten Aufgaben auf Basis strikter Anweisungen des Auftraggebers oder auf Grund eigener Entscheidungen so erfüllen, dass ein vertraglich mit dem Auftraggeber vereinbartes Ergebnis erzielt wird. Im ersten Fall kann es ausreichen, im internen Kontrollsystem der User Organization wirksame Regelungen zur Überwachung der Auslagerung einzurichten [IDW03, 1001]. Im anderen Fall muss sich die User Organization auf das interne Kontrollsystem des Dienstleisters verlassen, das damit für die Prüfung der User Organization relevant wird. Der User Auditor muss beurteilen, ob die Tätigkeit des Dienstleisters hinreichend durch das interne Kontrollsystem der User Organization oder des Dienstleisters überwacht wird. Deshalb hat die User Organization mit dem Dienstleister vertraglich Prüfungs- und Kontrollrechte zu vereinbaren, um sich von der Angemessenheit und Wirksamkeit des internen Kontrollsystems beim Dienstleister überzeugen zu können, soweit nicht ausreichende Prüfungsergebnisse Dritter vorliegen. Die Beurteilung kann auf

- Systemprüfungen der den Dienstleister betreffenden internen Kontrollen der User Organization,
- Verwertung des Berichts eines Service Auditors über die Wirksamkeit des internen Kontrollsystems des Dienstleisters und
- eigenen Prüfhandlungen beim Dienstleister

basieren. Ergänzend kann der User Auditor Prüfergebnisse des Service Auditors und Feststellungen der internen Revision des Dienstleisters, von Sachverständigen und Aufsichtsbehörden berücksichtigen (vgl. [IDW03, 1001]).

Werden Ergebnisse des Service Auditors verwertet, so hat der User Auditor dessen berufliche Qualifikation und fachliche Kompetenz sowie die Qualität, Verwertbarkeit und Angemessenheit seiner Berichte beurteilen. Insbesondere muss der Service Auditor nach Art, Umfang und Zeitpunkt ausreichende Funktionsprüfungen vorgenommen haben [IDW03, 1001]. Der User Auditor hat seine Einschätzungen im Prüfungsbericht darzulegen.

Reichen die Informationen Dritter nicht aus, so muss der User Auditor nach [IDW03, 1001] selbst Informationen beim Dienstleister beschaffen oder diesen auffordern, einen Service Auditor mit Prüfhandlungen zu betrauen. Im ersten Fall hat die User Organization den Dienstleister aufzufordern, ihrem Prüfer Zugang zu den notwendigen Informationen zu gewähren. Im zweiten Fall sind die erforderlichen Prüfhandlungen nach Abstimmung zwischen der User Organization und dem User Auditor durch den Dienstleister und den Service Auditor zu vereinbaren. Insbesondere hat der Service Auditor darzulegen, ob

- die Beschreibung des internen Kontrollsystems durch die gesetzlichen Vertreter richtig ist,
- die Kontrollen implementiert wurden und
- das interne Kontrollsystem angemessen ausgestaltet ist, um die angegebenen Ziele zu erreichen [IDW03, 1002].

Die oben angeführten Aktivitäten können bei einem für mehrere Kunden international tätigen Dienstleister erheblichen Aufwand bewirken. Aus diesem Grund hat das AICPA bereits 1992 ein Statement for Auditing Standard SAS No 70 verabschiedet, das sich mit der Prüfung von Dienstleistern auseinander setzt und vorsieht, dass ein Service Auditor „SAS 70“-Berichte erstellen kann [AICP06]. Ein (hier relevanter) SAS 70-Bericht vom Typ II bestätigt das Vorhandensein und die durch Tests festgestellte Effektivität der internen Kontrollen. Er soll die Basis dafür bilden, dass der User Auditor auf eigene Prüfhandlungen beim Dienstleister verzichten kann. Solche Berichte waren vor Inkrafttreten des SOX wenig verbreitet, gewinnen aber nun an Bedeutung. Manche Dienstleister waren nicht in der Lage, SAS 70-Berichte beizubringen; das Management der auslagernden Unternehmen musste darauf in den SEC Filings hinweisen [BaMc05; Meke05]. In der Schweiz knüpft der Prüfungsstandard PS 402 [Treu04, 237 ff] eng an SAS 70 an.

SAS 70-Berichte werden zuweilen kritisch beurteilt:

- Dieser „obscure auditing standard“ [Schn04a] würde neuere Entwicklungen bei der Prüfung interner Kontrollsysteme insbesondere im Zusammenhang mit dem SOX schon auf Grund seines Alters zu wenig berücksichtigen.
- SAS 70 kennt keine Maßnahmen- und Prüfungskataloge; das Prüfobjekt ist nicht präzise umschrieben, sondern wird vom Auftraggeber festgelegt (vgl. [AICP06, 34]). SAS 70 habe ein beschränktes Ziel und somit auch nur beschränkten Wert: "In a

SAS 70 audit, the service organization is responsible for describing its control objectives and control activities that might be of interest to auditors in user organizations" [Goss01]. Der Service Auditor berichtet nur über vorgefundene Fehler, nicht aber über den Umfang seiner Prüfungen. Gegebenenfalls muss der User Auditor seine Anforderungen an den SAS 70-Bericht zeitgerecht gegenüber dem Dienstleister spezifizieren (vgl. Bild 1).

- "Firms are … under pressure to demonstrate compliance with regulatory requirements that differ by country, state, locality and industries, and especially laws governing what kind of data must be kept, for how long, and when data can be destroyed" [Hurl06, 9]. Ein international und branchenübergreifend tätiger Dienstleister ist daher mit einer Vielzahl zumindest teilweise unterschiedlicher Anforderungen konfrontiert (vgl. [Apga05; Kolo05; Hurl06] und Bild 2). Der Dienstleister muss die Vereinigungsmenge aller gestellten Anforderungen erfüllen, wenn der Service Auditor einen allgemein verwendbaren SAS 70-Bericht vorlegen soll; die zweckmäßige Erfüllung multipler Compliance-Anforderungen wird als große Herausforderung angesehen [Kolo05, 6]. IBM hat einen Bericht über ihre SAS 70-Prüfung im Geschäftsbereich EMEA rund 200 Kunden zur Verfügung gestellt; einige Kunden hatten speziell auf ihre Situation zugeschnittene Berichte angefordert [Math05, 163].
- Es bestehen zeitliche Abhängigkeiten zwischen den Prüfungshandlungen des Service Auditors, dem Zeitpunkt der Berichterstattung der User Organization und dem Zeitpunkt ihrer Prüfung. Da die Wirtschaftsjahre der Kunden eines Dienstleisters voneinander abweichen können und die SAS 70-Berichte zeitnah sein sollen, kann der Fall eintreten, dass der zuletzt vorliegende SAS 70-Bericht (insbesondere bei Veränderungen im internen Kontrollsystem) den Aktualitätsanforderungen nicht entspricht (vgl. [Step03; Gazz04]). In diesem Zusammenhang wird erörtert, ob der Dienstleister zu Quartalsprüfungen oder sogar zu nahezu kontinuierlichen Prüfungen („Rolling audits“ [NNoJ]) verpflichtet ist, um seinen Kunden bzw. ihren Prüfern aussagefähige Berichte zur Verfügung stellen zu können.
- SAS 70 sei nicht IT-spezifisch, zu wenig technisch orientiert und Sicherheitsfragen würde zu wenig Aufmerksamkeit gewidmet [Leun03].
- Für eine umfassende Risikomanagement-Beurteilung sind Daten aus verschiedenen Quellsystemen zusammenzutragen, zu bereinigen, auszuwerten und zu interpretieren. In der Diskussion um Entwicklungstendenzen im Outsourcing wird zuweilen unterstellt, die auslagernden Unternehmen würden vermehrt „Best-of-Breed“-Konzepte umsetzen und mit verschiedenen Dienstleistern zusammen arbeiten. Dann resultieren die in Bild 3 dargestellten Leistungs- und Kommunikations-Beziehungen. Nehmen mehrere Dienstleister compliance-relevante Aufgaben wahr, so ergibt eine isolierte Berichterstattung über die Vorgehensweisen der einzelnen Dienstleister eventuell kein aussagefähiges Bild vom Gesamtsystem.
- Manche Outsourcing-Dienstleister übertragen compliance-relevante Aufgaben an "Subservice Organizations" (vgl. [AICP06, 59 ff]. Eine häufige Konstruktion ist, dass Vertragspartner der User Organization eine in ihrem Staat domizilierte Tochtergesellschaft des Offshore-Dienstleisters ist (vgl. [MoBl04, 210]). Werden mehrere Subservice-Gesellschaften hintereinander geschaltet, so entsteht eine "n-tier Supply Chain" von Dienstleistungen, für die eine Kette von SAS 70-Berichten notwendig sein könnte (Bild 4). Da die User Organization typischerweise keine Verträge mit den Subservice Organizations abschließt, sollte der (vertraglich gebundene) Tier-1-Dienstleister die Informationen über interne Kontrollen der Subservice Organizations gemäß der "carve-out method" oder der "inclusive method" bereitstellen; dies kann zu extensiven und komplexen Planungs- und Kommunikationsprozessen führen [AICP06, 61 ff]. Erforderlichenfalls muss der User

Auditor Prüfungshandlungen auch bei den Subservice Organizations vornehmen [AICP06, 61].
- Es können Unvereinbarkeiten zwischen User Auditor und Service Auditor im Hinblick auf die geforderte Unabhängigkeit der Prüfer bestehen [Schn04b].

Im Übrigen ist nicht auszuschließen, dass Aufgaben der Internen Revision z.B. an einen externen Prüfer teilweise ausgelagert werden [WiSo99; Lück00, 6 ff]. Da die Interne Revision ein Prüfobjekt des User Auditors darstellt, könnte auch über eine (teilweise) ausgelagerte Interne Revision ein SAS 70-Bericht durch einen Service Auditor erstellt werden. Gegebenenfalls hat dann ein Wirtschaftsprüfer das Vorgehen eines anderen Wirtschaftsprüfers zu beurteilen.

5 Auswirkungen von Compliance-Anforderungen auf den Umfang von Off- und Nearshoring

Im Umfeld des SOX werden widersprüchliche Thesen über die Auswirkungen der neuen regulatorischen Anforderungen auf den Umfang von Outsourcing-Aktivitäten vertreten. Empirische Evidenzen liegen noch kaum vor und sind auch schwierig zu gewinnen.

Die Auslagerung compliance-relevanter IT-Aufgaben an Dienstleister führt dazu, dass gewisse Infrastruktur-Anpassungen im Rechnungswesen, in den internen Kontrollsystemen und in der IT nicht vom auslagernden Unternehmen vorgenommen werden müssen. Der Dienstleister kann dann, wenn die Compliance-Anforderungen mehrerer Kunden und ihrer Wirtschaftsprüfer (weitgehend) übereinstimmen, Economies of Scale realisieren, wie sie für wissensintensive Prozesse bei Outsourcing charakteristisch sind [MeKn98, 22 ff]. Auf diese Weise können sich für die User Organization Kostenvorteile bei Compliance-Nachweisen auch dann ergeben, wenn der Dienstleister ein Entgelt für die Bereitstellung eines SAS 70-Berichts fordert (vgl. [Math05, 163]).

Eine gegenüber internen IT-Bereichen höhere Professionalität spezialisierter Dienstleister kann die Ausrichtung an den anspruchsvollen Frameworks erleichtern. Die Bedeutung von Zertifikaten haben die im Offshoring-Geschäft tätigen Dienstleister erkannt: Rund 75% der gemäß CMMI dem höchsten Reifegrad zugeordneten Unternehmen sind in Indien domiziliert [Deut05, 6].

Die skizzierten Beziehungen zwischen Geschäftsleitungen, IT-Verantwortlichen, Outsourcing-Dienstleistern, internen und externen Prüfern ergeben ein komplexes Beziehungsgefüge, das der mit Outsourcing angestrebten Komplexitätsreduktion widerspricht. Die Kommunikations- und Beurteilungsprozesse und die gegebenenfalls erforderlichen Systemprüfungen z.B. bei einem indischen Dienstleister können zu einem organisatorisch und fachlich anspruchsvollen und kostenintensiven Vorgang werden: User Auditors „... are packing their bags and heading off to places such as India and China“ [Doug03]. Einer User Organization wurde von ihren Prüfern mitgeteilt, dass der geplante Wechsel des Dienstleisters verschoben werden müsse, da andernfalls die Veränderungen in den internen Kontrollsystemen nicht zeitgerecht geprüft werden könnten [Meke05].

Gesetzgeber und Regulatoren wollen operationelle Risiken z.B. durch Verpflichtung zu einem Risiko-Management reduzieren. Diese Risiken steigen in vielen Fällen durch Outsourcing, insbesondere bei Auslagerung ins Ausland [Base01; Baka04; Djav05; AsMV06; CGHJ06]; dies kann nach Basel II auf eine höhere Kapitalbindung führen. Zu den Risiken bei Outsourcing von Finanzdienstleistungen zählt [Base05, 11] Compliance Risiken, insbesondere unzureichenden Datenschutz, mangelhafte Berücksichtigung von "consumer and

prudential laws" sowie unzureichende Compliance- und Kontrollsysteme des Dienstleisters. Die Einhaltung von Sicherheitsvorschriften werde durch Outsourcing erschwert [Bedn05]. Beschäftigen viele Unternehmen einer Branche den gleichen Dienstleister, so kommt es zu einer Risikokonzentration [Base05, 18 f]; das Federal Financial Institutions Examination Council widmet daher „Multi-Regional Data Processing Servicers“ besondere Aufmerksamkeit [Fede03, 15 ff]. Aus dieser Perspektive sind Outsourcing und insbesondere Off- und Nearshoring Vorgehensweisen, deren Zusatzrisiken durch umfangreichere Kontrollprozesse kompensiert werden müssen, um ein der internen Aufgabenerfüllung vergleichbares Sicherheitsniveau zu erreichen.

Umfragen zeigen, dass mehr als 80% sowohl der auslagernden Unternehmen als auch der Dienstleister befürchten, gesetzgeberische Maßnahmen oder politischer Druck könnten ein geplantes Offshoring verhindern [BrWi05, 5]. Restriktive gesetzliche bzw. aufsichtsrechtliche Rahmenbedingungen sind Ursache dafür, dass sich Unternehmen gegenüber Outsourcing zögerlich verhalten [PwC05, 25]. Für den Bankenbereich findet sich der Hinweis: "… outsourcing may affect adversely the supervisory authority’s powers to gather information or to require changes in the way that the outsourced activity is carried out” [Base01, 17]. Für manche kommt wegen der Vorschriften des SOX ein Outsourcing compliance-relevanter Aufgaben nicht in Betracht (vgl. etwa [Step03, 7]) oder es wird die Frage nach der Vereinbarkeit von Outsourcing und Compliance-Nachweisen erörtert [Brei06]. Unternehmen, die bereits Offshoring betreiben, “… can only hope that they don’t find themselves up the Ganges without a paddle” [Schn04b, 44].

Der Gesetzgeber und die Behörden hätten grundsätzlich die Möglichkeit, durch restriktive Maßnahmen und Anforderungen die Auslagerung von Aufgaben ins Ausland zu erschweren. Solche Maßnahmen werden zuweilen unter arbeitsmarktpolitischen Gesichtspunkten gefordert (vgl. [ErSa05, 111]). Allerdings sind Wettbewerbsnachteile für eine derart agierende Volkswirtschaft zu erwarten, wenn Off- bzw. Nearshoring die ihnen zugeschriebenen Vorteile besitzen; eine gesamtwirtschaftlich mögliche "Win-Win-Situation" [McKi03] würde dann nicht eintreten. Auf diese Weise würden die verstärkten Kontrollmechanismen neben ihren direkten Kostenfolgen weitere negative Auswirkungen besitzen und die Vermutung einer Überregulierung noch berechtigter erscheinen lassen.

6 Fazit

Neue regulatorische Vorschriften besitzen bisher weitgehend vernachlässigte Auswirkungen auf die Attraktivität von Outsourcing-Beziehungen. Dieser Beitrag zeigt die Komplexität, die bei Gestaltung compliance-relevanter IT-Systeme und ihrer Prüfung bei Outsourcing entsteht. Auch unter Compliance-Gesichtspunkten sind mit Outsourcing Vor- und Nachteile verbunden. Wie die neuen regulatorischen Anforderungen die Entwicklung von Outsourcing insbesondere in Form von Off- und Nearshoring beeinflussen, sollte in weiteren Forschungsarbeiten empirisch untersucht werden.

Literatur

[AICP06] *American Institute of Certified Public Accountants*: AICPA Audit Guide. Service Organizations: Applying SAS No. 70, as Amended. With Conforming Changes as of May 1, 2006. AICPA, New York 2006.

[Apga05] *Apgar, Chris:* Complying with multiple regulations and contending with conflicts. http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1120646,00.html, 2005-09-06, Abruf am 2006-08-10.

[Arbe04] *Arbeitskreis "Externe und Interne Überwachung der Unternehmung" der Schmalenbach-Gesellschaft für Betriebwirtschaft e.V.*: Auswirkung des Sarbanes-Oxley Act auf die Interne und Externe Unternehmensüberwachung. In: Betriebs-Berater 59 (2004) 44, S. 2399-2407.

[AsMV06] *Aspray, William; Mayadas, Frank; Vardi, Moshe Y.* (Hrsg): Globalization and Offshoring of Software. ACM, o.O. 2006.
http://www.acm.org/globalizationreport/pdf/fullfinal.pdf, Abruf am 2006-08-10.

[AuMa05] *Augenstein, Friedrich; Martin, Christoph:* Enterprise Compliance Management - reagiert oder agiert der CIO? In: Information Management & Consulting 20 (2005) 4, S. 13-19.

[Baka04] *Bakalov, Rudy:* Risk Management Strategies for Offshore Application and Systems Development. In: Information Systems Control Journal 5 (2004), S. 36-39.
http://www.isaca.org/Template.cfm?Section=Archives&Template=/ContentManagement/ContentDisplay.cfm&ContentID=21894, Abruf am 2006-08-10.

[BaMc05] *Baker & McKenzie*: SOX and Outsourcing: Material Weakness Due to Service Provider. http://www.technologyexecutivesclub.com/PDFs/ArticlePDFS/BMOutsourcing%20Alert_June2005.pdf, 2005-06, Abruf am 2006-08-10.

[Base01] *Basel Committee on Banking Supervision/Bank for International Settlements*: Internal audit in banks and the supervisor's relationship with auditors, Basel 2001.
http://www.bis.org/publ/bcbs84.pdf, 2001-08-28, Abruf am 2006-08-10.

[Base05] *Basel Committee on Banking Supervision/Bank of International Settlements*: Outsourcing in Financial Services, Basel 2005.
http://www.bis.org/publ/joint12.pdf, Abruf am 2006-08-10.

[Bedn05] *Bednarz, Ann:* Offsite security complicates compliance. In: Network World 21 (2005) 11, S. 27-28.
http://www.networkworld.com/news/2005/0318offsite.html, 2005-03-18, Abruf am 2006-08-10.

[Brei06] *Breitenbach, Thomas:* Outsourcing und Compliance: Ein Widerspruch?
Vortrag am BITKOM-Forum "Outsourcing & Sicherheit", Frankfurt, 2006-06-29.

[Brew06] *Brewer, Dennis C.:* Security Controls for Sarbanes-Oxley Section 404 IT compliance: Authorization, Authentication, and Access. Wiley, Hoboken 2006.

[BrWi05] *Brown, Douglas; Wilson, Scott:* The Black Book of Outsourcing. Wiley, Hoboken 2005.

[Bund01] *Bundesanstalt für Finanzdienstleistungsaufsicht*: Rundschreiben 11/2001, Auslagerung von Bereichen auf ein anderes Unternehmen gemäß § 25a Abs. 2 KWG, 2001.
http://www.bafin.de/rundschreiben/93_2001/rs11_01.htm, 2001-12-06, Abruf am 2006-08-10.

[BuRi05] *Butler, Charles W.; Richardson, Gary L.:* The Implications of Sarbanes-Oxley for the IT Community. In: Cutter Consortium (Hrsg.): Enterprise Risk Management and Governance Advisory Service, Executive Report 2 (2005) 3.

[CGHJ06] *Camp, L. Jean; Goodman, Seymour; House, Charles H.; Jack, William B.; Ramer, Rob; Stella, Marie:* Offshoring: Risks And Exposures. In: Aspray, W.; Mayadas, F.; Vardi, M.Y. (Hrsg.): Globalization and Offshoring of Software. ACM, o.O. 2006, S. 182-212.
http://www.acm.org/globalizationreport/pdf/fullfinal.pdf, Abruf am 2006-08-10.

[COSO04] *COSO* (Hrsg.): Enterprise Risk Management - Integrated Framework, Executive Summary, 2004 http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf, 2004-09, Abruf am 2006-08-10.

[Cutl06] *Cutler,* Jr., John M.: Rules of the Game: Legal and Regulatory Issues Facing the Supply Chain Manager. CSCMP, Oak Brook 2006.

[Dami05] *Damianides, Marios:* Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance. In: Information Systems Management 22 (2005) 1, S. 77-85.

[Deut05] *Deutsche Bank Research*: Outsourcing nach Indien: der Tiger auf dem Sprung; Frankfurt 2005. http://www.dbresearch.com/PROD/DBR_INTERNET_DE-PROD/PROD0000000000191727.pdf, 2005-10-11, Abruf am 2006-08-10.

[Djav05] *Djavanshir, G. Reza:* Surveying the Risks and Benefits of IT Outsourcing. In: IT Pro 7 (2005) 6, S. 32-37.

[Doug03] *Dougherty, Timothy R.:* Outsourcing becomes a Source of Concern. SAS 70 Reviews and Controls. In: KPMG (Hrsg.): FlashPoint 2003-09, S. 1-8.
http://www.kpmg.com/NR/rdonlyres/EFFA63FC-E4B9-4408-A60D-72DFE577A443/0/OutsourcingBecomesaSourceofConcern.pdf, Abruf am 2006-08-10.

[EBK99] *Eidgenössische Bankenkommission*: Rundschreiben der Eidg. Bankenkommission: Auslagerung von Geschäftsbereichen (Outsourcing).
http://www.ebk.admin.ch/d/publik/mitteil/1999/m14-99-2.pdf, 1999-08-26, Abruf am: 2006-08-10.

[Ecke06] *Eckerson, Wayne:* Compliance and BI: Same Mission, Different Approaches. In: SearchCIO.com. http://searchcio.techtarget.com/columnItem/0,294698,sid19_gci1201522,00.html?track=NL-48&ad=557666&asrc=EM_NNL_372796&uid=241980, 2006-07-19, Abruf am: 2006-08-10.

[Enge04] *Engelen, Klaus C.:* Sarbanes-Oxley setzt Europa unter Reformdruck. In: Finanz-Betrieb 6 (2004) 10, S. 690-697.

[ErSa05] *Erber, Georg; Sayed-Ahmed, Aida:* Offshore Outsourcing. In: Intereconomics 40 (2005) 2, S. 100-112.

[Eyle00] *Eyles, Uwe:* Funktionsauslagerung (Outsourcing) bei Kredit- und Finanzdienstleistungsinstituten. In: Zeitschrift für Wirtschafts- und Bankrecht 54 (2000) 25, S. 1217-1234.

[Fede03] *Federal Financial Institutions Examination Council* (Hrsg.): Supervision of Technology Service Providers. IT Examination Handbook, 2003.
http://www.occ.treas.gov/efiles/disk2/booklets/tsp/tech_ser_provider.pdf, 2003-03, Abruf am 2006-08-10.

[Gazz04] *Gazzaway, Trent:* SAS 70: New Life For an Old Audit Standard. In: Financial Executive 20 (2004) 3, S. 43-44.

[GeBa03] *Germano, Lisa; Baker, Anita:* Why an SAS 70 Review Will Benefit Your Organization. In: Journal of Pension Benefits 11 (2003) 1, S. 69-73.

[Glen03] *Glenfis*: ITIL-Cobit Mapping.
http://www.glenfis.ch/media/download/tools/ITIL-Cobit-Mapping_de.xls, Abruf am 2006-08-10.

[Goss01] *Gossels, Jonathan G.:* SAS 70: The Emperor Has No Clothes.
http://www.systemexperts.com/tutors/sas70.pdf, Abruf am 2006-08-10.

[Gray04] *Gray, Helen:* Is there a relationship between IT governance and corporate governance? What improvements (if any) would IT governance bring to the LSC?
http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=16236 Abruf am 2006-08-10.

[HaHS00] *Hadding, W.; Hopt, K.J.; Schimansky, H.:* Funktionsauslagerung (Outsourcing) bei Kreditinstituten. Bankrechtstag 2000. de Gruyter, Berlin-New York 2001.

[HeSt00] *Herring, Frank M.; Steck, Andreas:* Rechtliche Grenzen des Outsourcing – der neueste Entwurf eines BAKred-Rundschreibens. In: Zeitschrift für das gesamte Kreditwesen 53 (2000) 24, S. 1441-1445.

[Hurl06] *Hurley, Jim:* The Struggle to Manage Security Compliance for Multiple Regulations. White Paper http://www.bindview.com/resources/whitepapers/StruggleToManage_WP.pdf, 2006-01-17, Abruf am 2006-08-10.

[IDW01] *Institut der Wirtschaftsprüfer*: IDW Prüfungsstandard: Das interne Kontrollsystem im Rahmen der Abschlussprüfung (IDW PS 260). In: Die Wirtschaftsprüfung 54 (2001) 16, S. 821-831.

[IDW02] *Institut der Wirtschaftsprüfer*: IDW Prüfungsstandard: Abschlußprüfung bei Einsatz von Informationstechnologie (IDW 330). In: Die Wirtschaftsprüfung 55 (2002) 21, S. 1167-1179.

[IDW03] *Institut der Wirtschaftsprüfer*: IDW Prüfungsstandard: Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen (IDW PS 331). In: Die Wirtschaftsprüfung 56 (2003) 18, S. 999-1002.

[ISAC06] *ISACA Switzerland*: Zertifizierung als CISA oder CISM. http://www.isaca.ch/files/ISACA_Broschuere_06.pdf, 2006-04-20, Abruf am 2006-08-10.

[ITGI05] *IT Governance Institute*: COBIT 4.0, Rolling Meadows 2005.

[KnMi00] *Knolmayer, Gerhard; Mittermayer, Marc-André:* Quick Guide to Outsourcing. Entscheidungshilfe und Wegleitung bei Outsourcing-Projekten. ASC, Zürich 2000.

[KnWe06] *Knolmayer, Gerhard F.; Wermelinger, Thomas:* Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen. In: *Siegel, T.; Klein, A.; Schneider, D.; Schwintowski, H.-P. (Hrsg.):* Unternehmungen, Versicherungen und Rechnungswesen. Duncker & Humblot, Berlin 2006, im Druck.

[Kolo05] *Kolodgy, Charles J.:* Optimizing Your IT Controls Environment for Compliance with Multiple Regulations. IDC White Paper, Framingham 2005. http://database.ittoolbox.com/white-papers/pdfViewer.asp?r=http%3A%2F%2Fhosteddocs%2Eittoolbox%2Ecom%2FSymantec60706A%2Epdf&c=WhitePapers, 2005-12, Abruf am 2006-08-10.

[LaPe05] *Lahti, Christian B.; Peterson, Roderick:* Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools. Syngress, Rockland 2005.

[Leun03] *Leung, Linda:* Call in the security auditors. In: Network World 20 (2003) 30, S. 41.

[Lück00] *Lück, Wolfgang:* Die Zukunft der Internen Revision. Entwicklungstendenzen der unternehmensinternen Überwachung. Schmidt, Berlin 2000.

[Math05] *Mathews, B.:* Prüfung outgesourcter Informatikleistungen – Prüfprozessoptimierung im IT-Security Bereich, Diplomarbeit, Uni Zürich 2005. http://www.isaca.ch/files/Diplom_PruefungOutsourcingIT.pdf, 2005-16-09, Abruf am 2006-08-10.

[Maza06] *Mazars*: Sarbanes-Oxley Act - International Survey 2006. http://www.mazars.com/news/sarbanes-oxley-act.php, Abruf am 2006-08-10.

[McKi03] *McKinsey Global Institute*: Offshoring: Is It a Win-Win Game? San Francisco 2003. http://hei.unige.ch/~baldwin/ComparativeAdvantageMyths/IsOffshoringWinWin_McKinsey.pdf, 2003-08, Abruf am 2006-08-10.

[MeGa04] *Mensik, Michael S.; Garesis, Robert:* The Sarbanes-Oxley/Outsourcing Intersection: An Introduction. In: Baker & McKenzie (Hrsg.), U.S. Outsourcing Client Alert, 2004. http://www.bakernet.com/NR/rdonlyres/53BC9F5D-47A1-4E85-88C3-27E152D85509/0/CAOutsourcing0904.pdf, Abruf am 2006-08-10.

[Meke05] *Mekechuk, Bryan:* The Compliance Imperative. In: Optimize (2005) 45. http://www.optimizemag.com/article/showArticle.jhtml?articleId=164902258, Abruf am 2006-08-10.

[MeKn98] *Mertens, Peter; Knolmayer, Gerhard:* Organisation der Informationsverarbeitung. 3. Aufl., Gabler, Wiesbaden 1998.

[MiLa04] *Michaels, Bernd; Langheid, Theo:* Funktionsausgliederungen zur Entlastung des Unternehmens. In: Versicherungswirtschaft 59 (2004) 11, S. 800-807.
http://bld.de/fileadmin/bld/txt_pdf/Michaels-Langheid-11-2004.pdf, Abruf am 2006-08-10.

[MoBl04] *Morstead, Stuart; Blount, Greg:* Offshore Ready. 2. Aufl., APQC: Houston 2004.

[NaBu03] *Nanda, Arup; Burleson, Donald K.:* Oracle Privacy Security Auditing. Includes Federal Law Compliance with HIPAA, Sarbanes-Oxley & The Gramm-Leach-Bliley Act GLB. Rampant Tech Press, Kittrell 2003.

[NN05] *NN*: Compliance Is Bankers' Top Concern. In: Community Banker 14 (2005) 9, S. 70.

[NNoJ] *NN*: Frequently Asked Questions.
http://www.sas70solutions.com/SAS70-FAQ.html, Abruf am 2006-08-10.

[PCAO04] *PCAOB*: Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, 2004 (As of 2006-05-12)
http://www.pcaob.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf, Abruf am 2006-08-10.

[PDAS04] *PDA Supplier Auditing & Qualification Task Group*: Auditing of Suppliers Providing Computer Products and Services for Regulated Pharmaceutical Operations. In: PDA Journal of Pharmaceutical Science and Technology 58 (2004) 5, Technical Report 32, Release 2.0.

[PwC05] *PwC Deutsche Revision*: Entwicklung von Branchen-Standards im Investmentgeschäft. In: PwC Deutsche Revision (Hrsg.): PwC, Frankfurt am Main 2005, S. 24-25.
http://www.pwc.com/de/ger/ins-sol/publ/mandantenmagazin/2005-02.pdf, Abruf am 2006-08-10

[Sarb04] *Sarbanes Oxley Group*: The Sarbanes-Oxley G*ui*de For Finance And Information Technology Professionals. Booksurge/CLA, o.O. 2004.

[Schi05] *Schirmbrand, Michael:* IT Governance - Aktuelle Entwicklungen.
http://www.lsz-consulting.at/pdf/summit_6u7_9_05/03_schirmbrand.pdf, 2005-09, Abruf am 2006-08-10.

[Schn04a] *Schneider, Craig:* Stuck in the SAS 70s. In: CFO.com.
http://www.cfo.com/printable/article.cfm/3011799, 2004-02-23, Abruf am 2006-08-10.

[Schn04b] *Schneider, Craig:* A World of Trouble. In: CFO 20 (2004) 4, S. 41-44.
http://www.cfoeurope.com/displayStory.cfm/2569824, 2004-04, Abruf am 2006-08-10.

[SEC03] *U.S. Security and Exchange Commission*: SEC Implemen*ts I*nternal Control Provisions of Sarbanes-Oxley Act; Adopts Investment Company R&D Safe Harbor, 2003.
http://www.sec.gov/news/press/2003-66.htm, 2003-05-27, Abruf am 2006-08-10.

[Sewe05] *Sewera, Sonja:* Referenzmodelle im Rahmen von IT-Governance. CobiT ITIL MOF.
http://wwwai.wu-wien.ac.at/~koch/lehre/inf-sem-ss-05/referenzmodelle, Abruf am 2006-08-10.

[Step03] *Stephenson, Mark:* Does SAS 70 Suffice for SOA? In: Protiviti KnowledgeLeader 2003-12-15. Wiederabgedruckt in: ISACA San Francisco Chapter (2004) 1, S. 6-7.
http://www.sfisaca.org/download/2004-q1_lan.pdf, Abruf am 2006-08-10.

[Stoc03] *Stocker, Christoph:* Regulatorische Anforderungen an IT-Outsourcing: Finanzmarktbereich. In: *Weber, R.H.; Berger, M.; Auf der Maur, R. (Hrsg.):* IT-Outsourcing. ICT: Rechtspraxis I, Schulthess, Zürich et al. 2003, S. 227-253.

[Tetz02] *Tetzel, Wolfgang:* Aufsichtsrechtliche Probleme des Outsourcing unter besonderer Berücksichtigung von § 25 a KWG, Leipzig 2002.
http://www.uni-leipzig.de/bankinstitut/dokumente/2002-02-20-06.pdf, Abruf am 2006-08-10.

[TreuoJ] *Treuhand-Kammer* (Hrsg.): Was bedeutet der Sarbanes-Oxley Act of 2002 für Schweizer Unternehmen? Eine Orientierungshilfe zum neuen US-Gesetz. Zürich o.J. http://www.treuhand-kammer.ch/pix/files/Oxley_de2.pdf, Abruf am 2006-08-10.

[Treu04] *Treuhand-Kammer* (Hrsg.): Schweizer Prüfungsstandard: Unternehmen, die Dienstleistungsorganisationen in Anspruch nehmen – Auswirkung auf die Abschlussprüfung (PS 402). In: Schweizer Prüfungsstandards (PS), Ausgabe 2004, Zürich 2004, S. 237-243. http://www.auditcommittee.ch/Schweizer_Pruefungsstandards.pdf, Abruf am 2006-08-10.

[WiSo99] *Widener, Sally K.; Selto, Frank H:* Management Control Systems and Boundaries of the Firm: Why Do Firms Outsource Internal Auditing Activities? In: Journal of Management Accounting Research 11 (1999), S. 45-73.

[ZeHa98] *Zerwas, Herbert; Hanten, Mathias:* Outsourcing bei Kredit- und Finanzdienstleistungsinstituten – Zum neuen § 25a Abs. 2 KWG. In: Wertpapier-Mitteilungen - Zeitschrift für Wirtschafts- und Bankrecht 52 (1998) 22, S. 1110-1118.

Abbildungen

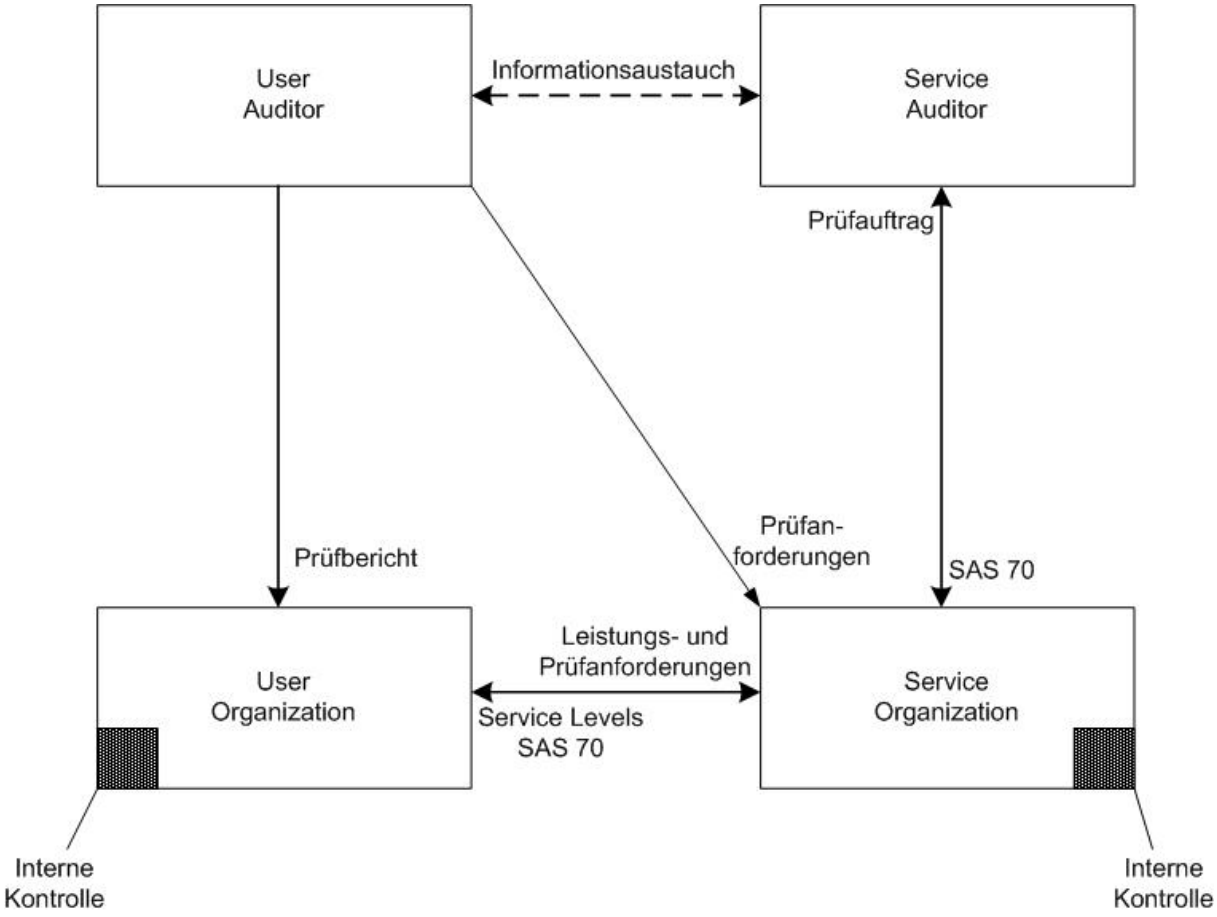

Bild 1 Rechts- und Kommunikationsbeziehungen bei Outsourcing compliance-relevanter Aufgaben

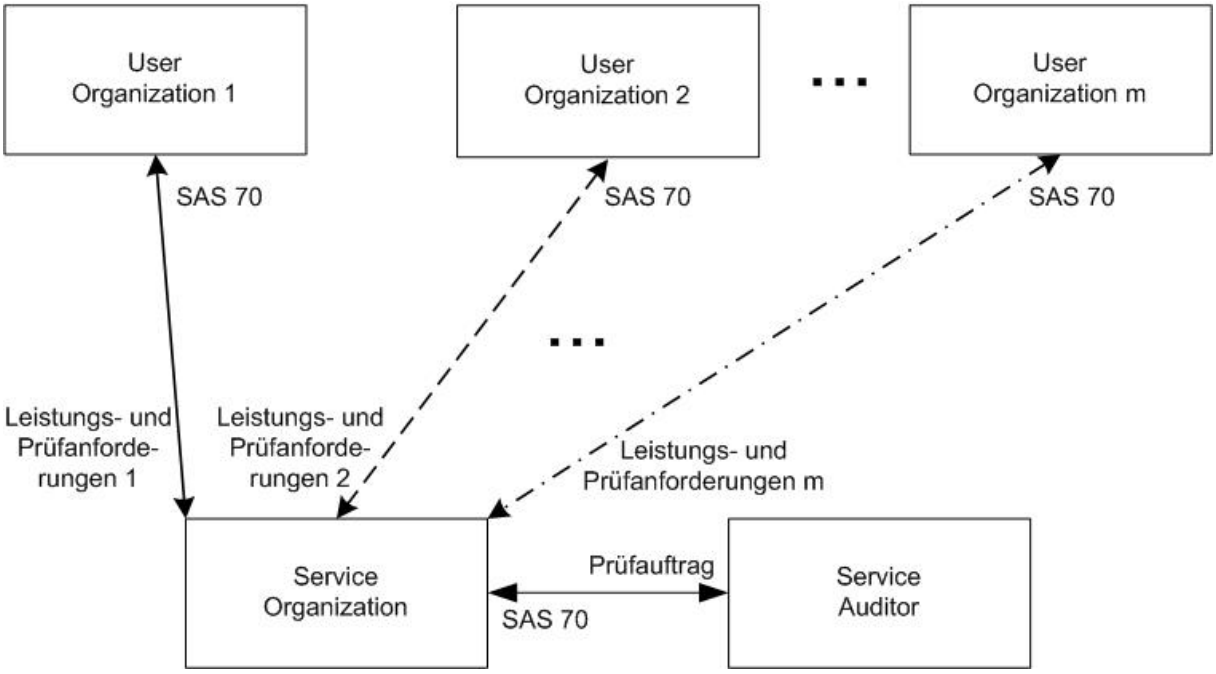

Bild 2 Erfüllung multipler Anforderungen an SAS 70-Berichte

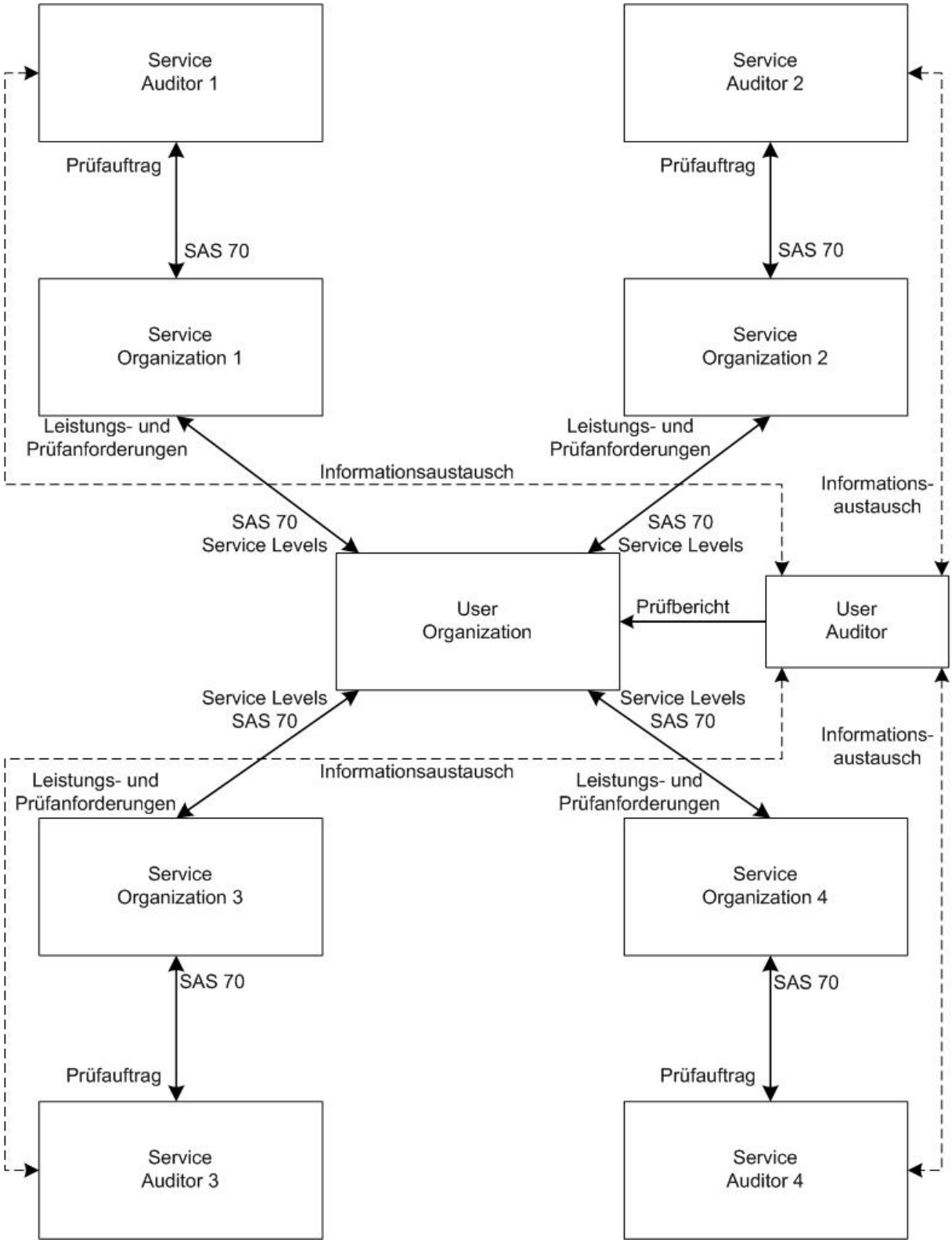

Bild 3 Compliance-Beurteilung bei Beschäftigung mehrerer Dienstleister nach dem Best-of-Breed-Konzept

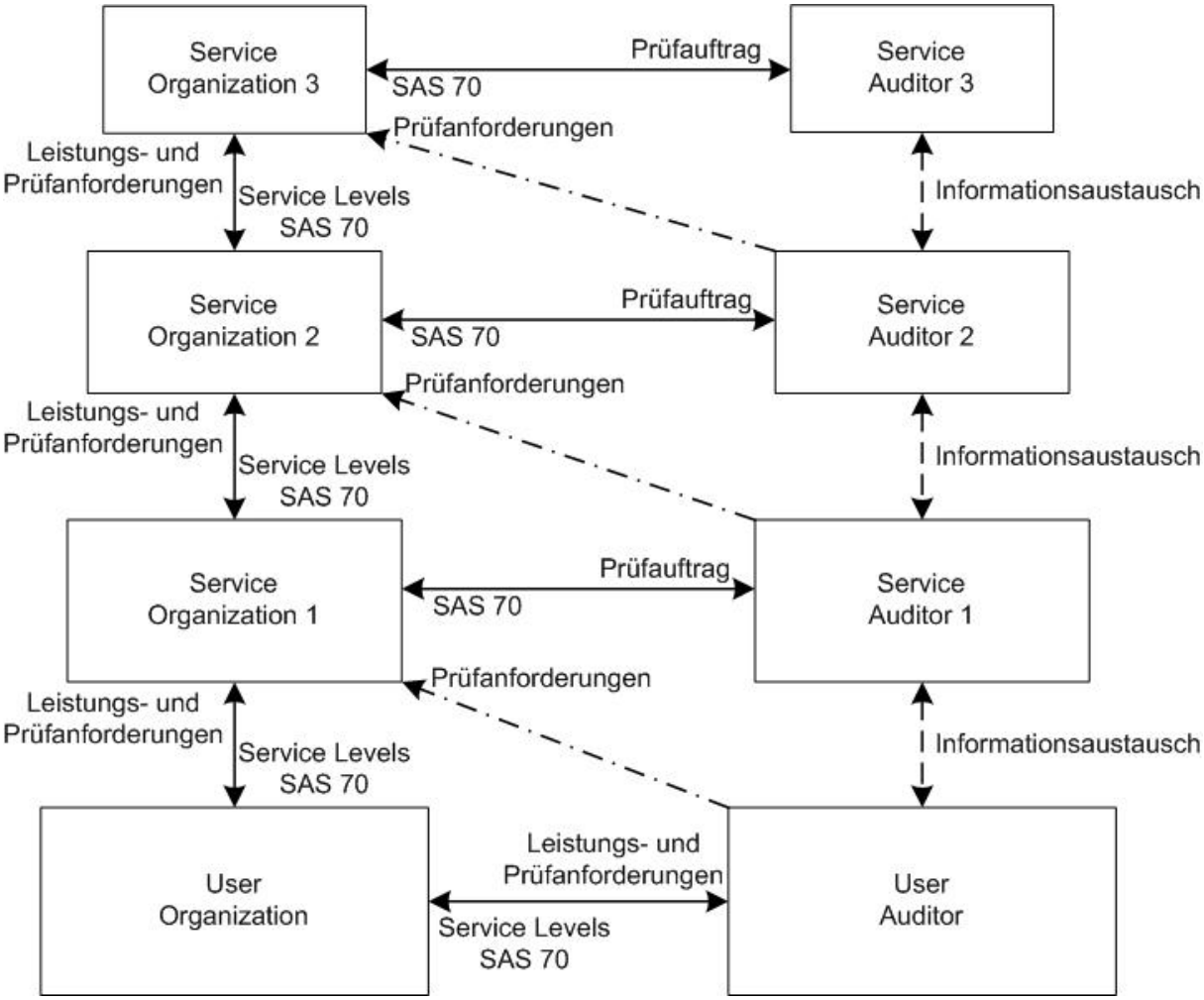

Bild 4 Rechts- und Kommunikationsbeziehungen bei Outsourcing compliance-relevanter Aufgaben an Subservice Organizations