ISACA®
Trust in, and value from, information systems
Nr. 04 | Dezember 2014 | www.isaca.ch
Switzerland Chapter NEWSLETTER

Outsourcing
Der Artikel zeigt auf, welche Standards für welchen Zweck angewendet werden.
Seite 59

Ausbildung IT-Audit
Das CISA-Zertifikat der ISACA vermittelt ein umfassendes und breites Wissen im Bereich des IT-Audits
Seite 62

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder
Seite 62

Outsourcing Berichte: Welcher Standard passt?

Verschiedene Standards stehen für die Berichterstattung von Outsourcing-Dienstleistungen bereit. Diese haben jedoch verschiedene Vor- und Nachteile. Welcher Standard soll für welchen Zweck verwendet werden?

Von Raffael Schweitzer

Immer mehr Unternehmen lagern einen Teil ihrer Leistungserbringung an Service-Provider aus, um sich auf ihre Kernkompetenzen zu konzentrieren beziehungsweise Kosten in unterstützenden Bereichen zu sparen. Insbesondere auch die Erbringung von Informatikdienstleistungen wird immer häufiger durch externe Partner unterstützt oder sogar ganz übernommen. Aus Sicht der Revision stellt sich dabei nicht zuletzt die Frage, wie ein Unternehmen ausreichende Sicherheit über die ausgelagerte Leistungserbringung gewinnt und wie diese sinnvoll überprüft werden kann.

Heute wird dabei vor allem der ISAE 3402 Standard für die finanzielle Berichterstattung verwendet. Jedoch ist die Verwendung dieses Standards auf die Prüfungen des internen Kontrollsystems im Rahmen der Finanzberichterstattung limitiert. Gerade bei Auslagerungen im IT Umfeld interessieren ein Unternehmen jedoch vielfach nicht nur finanzrelevante Aspekte sondern insbesondere auch Fragen der Verfügbarkeit oder der Einhaltung von regulatorischen Vorgaben. Insbesondere letztere können aufgrund ihrer Natur oftmals nicht durch den ISAE 3402 Standard abgedeckt werden.

Dabei existieren heute verschiedene Alternativen zu einem ISAE 3402 Bericht, welche diesen Anforderungen gerecht werden. Sie werden in diesem Artikel vorgestellt.

Von SAS 70 zu ISAE 3402

Insbesondere durch den Sarbanes-Oxley Act, ein amerikanisches Gesetz zur Verstärkung des internen Kontrollsystems von Unternehmen, hat sich nach der Jahrtausendwende der amerikanische SAS 70 Standard zur Erstellung von sogenannten Attestation Reports zum globalen Standard für die Kontrolle von ausgelagerten Dienstleistungen im Rahmen der Finanzberichterstattung entwickelt. Der SAS 70 Standard wurde im Juni 2011 vom neuen globalen ISAE 3402 Standard beziehungsweise dessen amerikanischer Variante (SSAE 16) abgelöst – inhaltlich hat sich aber kaum etwas geändert.

Diese Standards sind deshalb einzig für die finanzielle Berichterstattung zu verwenden und somit primär für die finanzielle Revision (auch nach dem Schweizer Prüfstandard PS 402[1]) relevant. Bezüglich der Abdeckung von IT Komponenten einer Auslagerung sind sie geeignet, Prüfresultate bezüglich der IT Anwen-

dungskontrollen in den ausgelagerten Geschäftsbereichen sowie bezüglich der diese unterstützenden Generellen IT Kontrollen wiederzugeben. Letztere stellen das korrekte Funktionieren der typischen IT Unterstützungsprozesse wie Änderungswesen, Zugriffschutz sowie IT Betrieb sicher.

Berichte nach dem ISAE 3402 Standard – sowie der meisten anderen später diskutierten Berichtsformate - können entweder nur die Ausgestaltung und Implementation der beschriebenen Kontrollen (Type I) oder aber auch deren operative Effektivität (Type II) beurteilen.

ISAE 3000: Alle Freiheiten

Neben dem ISAE 3402 Standard existiert auch der grundlegende ISAE 3000 Standard, welcher für sämtliche Bestätigungen mit Ausnahme der finanziellen Berichterstattung verwendet werden kann. Dies beinhaltet beispielsweise Wirksamkeit des internen Kontrollsystems oder Einhaltung von regulatorischen Vorgaben oder von Vertragsbestimmungen. In der Schweiz wird der Standard durch den Prüfstandard PS 950 der Treuhandkammer umgesetzt, welcher den ISAE 3000 in die lokalen Prüfstandards einbettet.[2)]

Grundlage einer Prüfung nach ISAE 3000 ist in der Regel ein zu beurteilender Sachverhalt bzw. andere Kriterien, gegen welche geprüft werden kann. Im Unterschied zu Bestätigungen bezüglich finanzieller Berichterstattung müssen diese klar definiert sein, da der Prüfumfang nicht durch weitere Prüfungsstandards festgelegt ist. In der Regel erfolgt die Bestätigung wie bei einem ISAE 3402 Report indirekt über durch das Unternehmen implementierte Massnahmen und Kontrollen, welche bezüglich ihrer Wirksamkeit beurteilt werden.

ISAE 3000 erlaubt nicht nur die Bestätigung eines Sachverhalts mit hinreichender Sicherheit („reasonable assurance engagement") sondern auch mit eingeschränkter Sicherheit („limited assurance engagement"). Letzteres stellt ein Urteil mit geringerer Sicherheit dar, welches durch eingeschränkte Prüfungshandlungen gestützt wird. Entsprechend der gewählten Prüftiefe wird ein positiv oder negativ formuliertes Prüfurteil abgegeben.

Diese Unterscheidung macht in der Schweiz insbesondere im Bereich von regulatorischen Prüfungen im FINMA Umfeld Sinn, da deren Rundschreiben[3)] ebenfalls zwischen den Prüftiefen „Prüfung" und „kritischer Beurteilung" unterscheiden, welche ein positives bzw. ein negatives Prüfurteil beinhalten.

Bezüglich Berichterstattung orientieren sich Bestätigungen nach dem ISAE 3000 Standard heute oft an den Berichtsformaten wie sie für ISAE 3402 Bestätigungen verwendet werden.

SOC Reporting: Trust Services Principles

Nach der Ablösung von SAS 70 durch ISAE 3402 bzw. SSAE 16 wurde ebenfalls durch die amerikanische Vereinigung der Wirtschaftsprüfer (American Institute of Certified Public Accountants, AICPA) ein Standard für die Berichterstattung über die Kontrollen bei Outsourcing-Dienstleistern herausgegeben: Service Organization Control (SOC) Reports.[4)] Man unterscheidet dabei zwischen SOC 1, SOC 2 sowie SOC 3 Berichten.

Erstere entsprechen der bestehenden Anwendung von ISAE 3402 bzw. SSAE 16 für Berichte über die internen Kontrollen bezüglich der finanziellen Berichterstattung und sollen hier deshalb nicht weiter diskutiert werden. Es gelten dieselben Aussagen wie für ISAE 3402 Berichte generell, die AICPA regelt dabei insbesondere das Berichtsformat.

SOC 2 Berichte fokussieren sich genau auf die Bestätigung von Sachverhalten ausserhalb der finanziellen Berichterstattung. Dies geschieht in der Regel ebenfalls basierend auf dem vorher diskutierten ISAE 3000 Standard. Der Unterschied besteht jedoch darin, dass von der AICPA definierte Kriterien bestehen, welche als Grundlage des zu beurteilenden Sachverhalts dienen. Diese Kriterien sind in die so genannten Trust Services Principles gegliedert:

- Sicherheit,
- Verfügbarkeit,
- Vertraulichkeit,
- Integrität in der Verarbeitung, sowie
- Datenschutz.

Ein Outsourcing-Dienstleister kann einen Bericht über mindestens einen der Grundsätze erstellen lassen. Die Kriterien für die gewählten Grundsätze sind jedoch vorgegeben und bestimmen, was durch den Bericht abgedeckt wird.

Als Konsequenz besteht ein SOC 3 Bericht dann in einer Zertifizierung von einem oder mehreren der Grundsätze in einem vergleichsweise kürzeren Bericht, welcher nicht mehr auf die tatsächlich durchgeführten Prüfungshandlungen eingeht, sondern nur noch die Einhaltung der vorgegebenen Kriterien bestätigt.

Banken: freie Bestätigung regulatorischer Vorgaben

Auch in der Schweiz existieren spezifische Vorgaben bezüglich Outsourcing. Im Bereich der FINMA Regulation von Banken und Effektenhändlern kommt bezüglich Outsourcing dem FINMA Rundschreiben 2008/7 eine zentrale Bedeutung zu. Es gibt neun Grundsätze für regulierte Unternehmen vor, welche diese für als relevant eingestufte Outsourcing Verhältnisse einhalten müssen. Die Grundsätze umfassen sowohl organisatorische, vertragliche als auch technische Vorgaben, welche weit über die finanzielle Berichterstattung hinausgehen. Hier werden in der Regel gesonderte Berichte erstellt, welche nicht einem der oben diskutierten Standards folgen, sondern sich nur an den Vorgaben der FINMA orientieren. Grundsätzlich wäre eine Erstellung von solchen Berichten nach PS 950 bzw. dem ISAE 3000 Standard aber durchaus möglich.

Andere Berichte und Zertifizierungen

In der Praxis wird oft versucht, andere, bereits bestehende Zertifizierungen zur Bestätigung von Outsourcing-Dienstleistungen zu verwenden, z.B. eine Zertifizierung des Informationssicherheitsmanagementsystems nach ISO 27001. Grundsätzlich deckt z.B. ISO 27001 einen Grossteil der Kriterien ab, welche ebenfalls für den Grundsatz Sicherheit in einem SOC 2 Bericht verwendet werden. Die für ISO 27001 identifizierten Massnahmen und Kontrollen im Unternehmen können deshalb für eine Outsourcing Berichterstattung nach einem der oben diskutierten Standards verwendet werden. Die Zertifizierung selbst ist aber in den meisten Fällen nicht ausreichend, da sie oft nicht alle relevanten Aspekte abdeckt, nur periodisch (z.B. alle 3 Jahre) geprüft wird und andere Zeitperioden abdeckt. In jedem Fall sollte der Umfang, Häufigkeit der Prüfung sowie abgedeckte Periode genau analysiert werden, bevor ein solcher Bericht wiederverwendet wird. Sie müssen geeignet sein, die von

Berichtsform Kriterium	ISAE 3402 (SOC 1)	ISAE 3000	SOC 2	SOC 3	FINMA Standard
Abdeckung Bericht	Beliebige Kriterien mit Relevanz für die finanzielle Berichterstattung: • Transaktionen • Prozesse für Transaktionsabwicklung • Berichterstattung • Umgang mit wichtigen Geschäftsereignissen	Beliebige Kriterien	Primär Bereiche wie: • Infrastruktur • Software • Prozesse • Personen • Daten	Primär Bereiche wie: • Infrastruktur • Software • Prozesse • Personen • Daten	Beliebige Kriterien
Typische Inhalte	Kontrollen über Transaktionsverarbeitung mit Relevanz für die finanzielle Berichterstattung Kontrollen über die unterstützenden IT Prozesse (Generelle IT Kontrollen)	Beliebige Kontrollen oder zu bestätigende Sachverhalte	Eines oder mehrere der Trust Service Principles: • Sicherheit • Verfügbarkeit • Vertraulichkeit • Integrität der • Verarbeitung • Datenschutz	Eines oder mehrere der Trust Service Principles: • Sicherheit • Verfügbarkeit • Vertraulichkeit • Integrität der • Verarbeitung • Datenschutz	Grundsätze eines Rundschreibens, z.B. • RS 2008/7 Outsourcing oder • RS 2008/21 Operationelle Risiken
Standardisierung Inhalt	Kontrollframework wird durch den Dienstleister definiert	Kontrollframework wird durch den Dienstleister definiert	Der Dienstleister kann die abzudeckenden Trust Service Principles wählen, deren Umfang ist aber festgelegt	Der Dienstleister kann die abzudeckenden Trust Service Principles wählen, deren Umfang ist aber festgelegt	Beliebiger Inhalt (nicht standardisiert)
Berichtsformat	• Bestätigung Prüfer • Bestätigung Management • Beschreibung Framework, Kontrollziele und Kontrollaktivitäten • Resultat der Effektivitätsprüfung • Zusatzinformationen	Beliebig, orientiert sich aber oft an ISAE 3402	• Bestätigung Prüfer • Bestätigung Management • Beschreibung Framework, Kriterien und Kontrollaktivitäten • Resultat der Effektivitätsprüfung • Zusatzinformationen	Bestätigung (Zertifikat) Keine Informationen zu durchgeführten Prüfungshandlungen Kann nur bei einem nicht qualifizierten Bericht verwendet werden	Beliebig, orientiert sich oft an FINMA Longform Reports
Umgang mit Unterakkordanten[5]	Carve-in oder carve-out möglich	Carve-in oder carve-out möglich	Carve-in oder carve-out möglich	Nur carve-in	Carve-in oder carve-out möglich
Empfänger	Kunden und deren Prüfer	Kunden und deren Prüfer	Kunden und deren Prüfer	Kunden und deren Prüfer, kann aber als Siegel auch publiziert werden	Der FINMA unterstellte Institute und deren Prüfer
Verbreitung	De-facto Standard	Geringe Verbreitung	Geringe Verbreitung	Sehr geringe Verbreitung	De-facto Standard

den Unternehmen an den Dienstleister gestellten Anforderungen zu erfüllen.

Vor- und Nachteile der verschiedenen Standards

Die obenstehende Tabelle versucht, die verschiedenen Standards einander gegenüberzustellen und aufzuzeigen, in welchen Fällen welche Standards am besten geeignet sind.

Fazit

Neben dem bewährten und etablierten ISAE 3402 Bericht existieren heute weitere Berichtsformen, welche insbesondere zur Abdeckung von nicht auf die Finanzberichterstattung fokussierten Themenbereichen geeignet sind. Vor allem der ISAE 3000 Standard erlaubt mit seiner grossen Flexibilität eine sehr breite Anwendung und birgt ein grosses Potential für die Abdeckung von Themen wie Business Continuity Management, Vertraulichkeit oder auch Kundendatenschutz. Der Standard ist zudem als PS 950 in die Schweizer Prüfstandards eingebettet. Die Standardisierung von Berichtsinhalten über die Trust Services Principles von SOC 2 und SOC 3 Berichten schränkt zwar die Flexibilität ein, erlaubt aber eine höhere Vergleichbarkeit von Berichten verschiedener Dienstleister und auch deren einfachere Verwendung. Zudem befriedigt SOC 3 das Verlangen nach einem einfach zu verwendenden Zertifikat für Outsourcing Dienstleister und kann als Siegel auch zu Werbezwecken z.B. auf der Homepage gezeigt werden. Es bleibt abzuwarten, inwiefern diese Möglichkeiten in Zukunft von Dienstleistern auch für regulatorische (FINMA-) Berichte verwendet werden.

1) Der Prüfstandard PS 402 der Treuhandkammer regelt die Verwendung von Outsourcing Berichten im Rahmen der Finanzprüfung. Es handelt sich dabei um keinen Berichtsstandard.

2) Eine umfassende Beschreibung des PS 950 und ISAE 3000 findet sich im Artikel ‚Betriebswirtschaftliche Prüfungen nach Schweizer Prüfungsstandard 950' von Hans Moser, Der Schweizer Treuhänder, Ausgabe 2014 1-2

3) Vgl. FINMA Rundschreiben 2013/3, Prüfwesen, Rz 32ff

4) Siehe AICPA Homepage zu Service Organization Control Reporting http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

5) Ein Bericht kann Aussagen zu Unterakkordanten (z.B. Hosting Provider) einschliessen (carve-in) oder von der Bestätigung ausnehmen (carve out)

DER AUTOR

Raffael Schweitzer ist diplomierter Wirtschaftsinformatiker und 34 Jahre alt. Er ist seit rund 10 Jahren bei KPMG als IT Prüfer tätig und leitet dort den Bereich IT Assurance Financial Services. In dieser Funktion ist er unter anderem für periodische Erstellung von Berichten nach den ISAE Standards sowie auch regulatorischen Berichten für verschiedenste Banken und Dienstleister im Finanzbereich verantwortlich. Zudem berät er Outsourcing Dienstleister ebenfalls bei der Erstellung von Kontrollframeworks für solche Berichte.

Informationen des Verbands

IT-Prüfer gesucht – sind Sie ein Sherlock Holmes oder lieber ein Dr. Watson?

Wie der Artikel von Raffael Schweitzer aufzeigt, bestehen unterschiedlichste Zertifikate und Attestierungen im IT-Umfeld, welche jeweils ihre spezifischen Eigenschaften haben und für einen bestimmten Anwendungszweck geschaffen wurden. Gemeinsam ist allen, dass es Spezialisten benötigt, welche die Unternehmen analysieren («auditieren»). Während die Vorgaben für die Prüfungen im Rahmen der meisten ISO-Zertifizierung (z.B. ISO27001, ISO20000) relativ schlank sind, umfassen die nationalen und internationalen Standards der Finanzprüfung (z.B. PS950, ISAE3402) unzählige Vorgaben, die bei einer Prüfung einzuhalten sind.

Es nützt jedoch wenig, die einschlägigen Standards auswendig zu lernen: Standards entsprechen eigentlich in den meisten Fällen der bewährten Praxis – um die Standards zu verstehen, muss man die bewährte Praxis im Detail kennen und verstehen. Hier hilft entweder eine lange und breite Berufserfahrung oder eine seriöse Ausbildung.

Seit über 20 Jahren bietet das ISACA Switzerland Chapter die CISA-Vertiefungskurse an, welche den Teilnehmern sowohl die notwendigen theoretischen Grundlagen (grösstenteils im Rahmen eines strukturierten Selbststudiums ab 1. Februar 2015) als auch die bewährte Berufspraxis (grösstenteils im Präsenzunterricht im Juni/Juli) vermitteln. Ausführliche und klar strukturierte Unterlagen mit Fachbüchern, Skript und Fallstudien dienen nicht nur zur Vorbereitung auf die internationale Zertifikatsprüfung sondern auch als Nachschlagewerk im Berufsalltag. Der kompakte CISA-Prüfungsvorbereitungkurs jeweils im Herbst kann in Kombination mit dem CISA-Vertiefungskurs oder auch separat gebucht werden.

Erkundigen Sie sich auf unserer Webseite www.isaca.ch.

Ein Dr. Watson oder Sherlock Holmes werden Sie zwar auch mit unseren Kursen nicht. Aber ein kompetenter IT-Prüfer auf jeden Fall.

CISA® Certified Information Systems Auditor®
An ISACA® Certification

WEITERE INFORMATIONEN

Weitere Details zum CISA-Zertifikat und zur entsprechenden Ausbildung finden Sie auf: www.isaca.ch

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
22.-23.01.2015		Network Analysis & Advanced (Jona)
05.-06.02.2015		iPhone & iPad Security (Jona)
www.isaca.ch		
05.-07.01.2015	P-SOGF3	Sourcing Governance Foundation
26.-28.01.2015	P-PCSM3	Professional Cloud Service Manager
www.glenfis.ch		

IMPRESSUM ISACA NEWS

ISACA

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Sekretariat ISACA c/o BDO AG, Biberiststrasse 16, 4501 Solothurn
Erscheinungsweise: 4x jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch