PETER R. BITTERLI
RAFFAEL SCHWEITZER

IM DSCHUNGEL DER IT-NAHEN STANDARDS UND ZERTIFIKATE

Ein praktischer Leitfaden

Die Unternehmen und auch deren Wirtschaftsprüfer können heute im IT-Umfeld eine Vielzahl von Standards und Zertifikaten einsetzen – laufend kommen nationale und internationale hinzu. Es ist schwierig, den Überblick zu behalten und deren Bedeutung als Prüfer richtig einzuschätzen.

1. EINLEITUNG

Im heutigen Dschungel der Standards und Zertifikate wie *International Standard on Assurance Engagements (ISAE)* 3402, ISAE 3000, *Statement on Standards for Attestation Engagements (SSAE)* 16, *Service Organization Control (SOC)*1, SOC2, SOC3, *Schweizer Prüfungsstandard (PS)* 402, PS 870, PS 950, ISO 27001, ISO 27002, Datenschutz-Zertifizierungen, PCI DSS usw. hat kaum mehr jemand den Überblick, welche Bereiche diese Standards und Zertifizierungen abdecken und worin genau sie sich unterscheiden. Sogar die Anbieter von Dienstleistungen scheinen bisweilen Standards mit Zertifikaten zu vermischen oder erfinden Zertifizierungen für ihre Dienstleistungen und Produkte, die es in dieser Form gar nicht gibt. Das reicht von Aussagen wie «ISAE-3402-zugelassen» bis hin zu «Finma-zertifiziert» – obschon es weder das eine noch das andere in der Praxis gibt.

Das Ziel dieses Artikels ist es, den Wirtschaftsprüfern und anderen interessierten Lesern einen Überblick über die wichtigsten Standards und Zertifizierungen mit IT-Bezug zu geben. Ihre Charakteristiken, die Unterschiede, aber auch die Gemeinsamkeiten sollen aufgezeigt und übersichtlich dargestellt werden. Ausserdem gehen wir im Zusammenhang mit diesen Standards und Zertifizierungen auf typische Fallstricke in der Praxis ein.

2. OUTSOURCING UND PS 402

Immer mehr Unternehmen lagern einen Teil ihrer Leistungserbringung an Dienstleister (Service-Provider) aus – unter anderem, um sich auf ihre Kernkompetenzen zu konzentrieren und/oder um Kosten in unterstützenden Bereichen zu sparen. Aus Sicht der Revision stellt sich dabei die Frage, wie ein Unternehmen ausreichende Sicherheit über die ausgelagerte Leistungserbringung gewinnt und wie letztere sinnvoll überprüft werden kann.

Der PS 402 «Unternehmen, die Dienstleistungsorganisationen in Anspruch nehmen – Auswirkung auf die Abschlussprüfung» gibt eine Anleitung für den Abschlussprüfer, dessen Kunde eine Dienstleistungsorganisation in Anspruch nimmt. Der Prüfer muss feststellen, wie wesentlich die Aktivitäten des Providers für den Kunden und wie relevant sie für die Abschlussprüfung sind.

Kommt der Prüfer bei dieser Beurteilung zum Schluss, dass die für die Abschlussprüfung relevanten Schlüsselkontrollen nicht von der Dienstleistungsorganisation abhängen, erübrigt sich die Anwendung des PS 402. Kommt der Prüfer hingegen zum Schluss, dass die Aktivitäten des Dienstleisters für den Kunden wesentlich und für die Abschlussprüfung relevant sind, so muss er hinreichende Informationen erlangen, um das Rechnungswesen-System und die internen Kontrollen zu verstehen.

Die Erlangung hinreichender Informationen ist auf folgenden Wegen möglich:
→ Der Dienstleister verfügt über einen sogenannten «Service Auditor Report», und dieser Prüfbericht gibt hinreichende Informationen; → der Prüfer des Dienstleisters wird mit bestimmten Prüfungshandlungen beauftragt; → der Prüfer des auslagernden Unternehmens beschafft sich die Informationen beim Dienstleister selbst.

PETER R. BITTERLI, DIPL. MATH. ETH, CISA, CISM, CGEIT, MITGLIED FACHSTAB INFORMATIK VON EXPERTSUISSE, PARTNER, LEITER IT-REVISION & IT-SICHERHEITSBERATUNG, BDO AG, ZÜRICH

RAFFAEL SCHWEITZER, MSC UZH INFORMATION SCIENCE, CISA, MITGLIED FACHSTAB INFORMATIK VON EXPERTSUISSE, LEITER IT ASSURANCE FINANCIAL SERVICES, KPMG AG, ZÜRICH

3. OUTSOURCING UND INTERNATIONALE STANDARDS

Damit Dienstleister nicht von Anfragen der Abschlussprüfer ihrer Kunden überflutet werden (siehe obige Anmerkung zu PS 402), organisieren sie in der Regel die Erstellung eigener Service-Auditor-Berichte, welche sie dann an ihre Kunden abgeben können.

Hierfür wird heute vor allem der ISAE-3402-Standard (Assurance Reports on Controls at a Service Organization) eingesetzt, der 2011 den bekannten SAS 70 abgelöst hat. Entscheidend ist dabei, dass der ISAE 3402 in aller Regel für die Prüfung von Kontrollen über ausgelagerte finanzrelevante Prozesse eingesetzt wird – also die Prüfung von IT-Anwendungskontrollen und den sie unterstützenden generellen IT-Kontrollen (wie z. B. Änderungswesen, Zugriffschutz sowie IT-Betrieb).

In den USA wird hierfür vorwiegend die nationale Variante SSAE 16 (Reporting on Controls at a Service Organization) verwendet – inhaltlich und formal stimmen ISAE 3402 und SSAE 16 weitgehend überein: Der SSAE 16 verlangt eine umfassende Beschreibung des «Systems insgesamt» sowie der diesbezüglichen Kontrollziele und Kontrollen, wohingegen der ISAE 3402 eher auf die Kontrollziele und Kontrollen fokussiert.

Im Prüfbericht beschreibt der externe Dienstleister (Service Organisation) die von ihm angebotenen Dienstleistungen und die diesbezüglichen, von ihm implementierten internen Kontrollen. Zudem gibt er eine Zusicherung (Management Assertion) ab. Der Prüfer übernimmt in Berichten nach ISAE 3402/SSAE 16 diese Beschreibung im Wesentlichen unkommentiert und gibt dann je nach Prüfungstyp eine von zwei möglichen Aussagen ab:

→ In Prüfberichten vom Typ 1 wird vom Prüfer bestätigt, dass zu einem bestimmten Zeitpunkt angemessene interne Kontrollen implementiert und dokumentiert sind (entspricht in etwa einer Bestätigung der Existenz des *internen Kontrollsystems, IKS);* → in Berichten vom Typ 2 wird vom Prüfer bestätigt, dass angemessene interne Kontrollen implementiert und dokumentiert sind, sowie dass diese Kontrollen in einem definierten Zeitraum (in der Regel zwischen sechs und zwölf Monaten) wirksam waren.

«Bei Auslagerungen im IT-Umfeld interessieren ein Unternehmen nicht nur finanzrelevante Aspekte, sondern auch Fragen der Verfügbarkeit oder der Einhaltung von regulatorischen Vorgaben.»

Prüfberichte nach ISAE 3402 und SSAE 16 dienen primär dem Abschlussprüfer des auslagernden Unternehmens dazu: → das IKS des auslagernden Unternehmens vor allem in Bezug auf die ausgelagerten Bereiche zu verstehen; → zu verstehen, ob (und wie) der Dienstleister seiner Verpflichtung bezüglich der Kontrolldurchführung und -einhaltung nachkommt; → die Risiken wesentlicher falscher Darstellungen festzustellen und zu beurteilen; → weitere Prüfungshandlungen zu planen und durchzuführen, um diesen Risiken zu begegnen (beispielsweise, um komplementäre Kontrollen seitens des auslagernden Unternehmens aufzuspüren und diese zu prüfen).

Hinweise für weiterführendes Studium

- → Outsourcing-Berichte: Welcher Standard passt? ISACA-Newsletter im Swiss IT Magazin, Dezember 2014, Raffael Schweitzer;
- → Information security in banking, Banque & Finance, Dezember 2013, Tom Schmidt;
- → Datenschutz: Neue Anforderungen an die Banken-IT, Computerworld, Mai 2013, Tom Schmidt;
- → Zertifizierte Sicherheit – Illusion oder Wirklichkeit?, ISACA-Newsletter im Swiss IT Magazin, September 2011, Peter R. Bitterli;
- → Finma-Rundschreiben 2008/07 und 2013/3.

4. OUTSOURCING UND STANDARDS ISAE 3000/PS 950

Gerade bei Auslagerungen im IT-Umfeld interessieren ein Unternehmen vielfach nicht nur finanzrelevante Aspekte, sondern insbesondere auch Fragen der Verfügbarkeit oder der Einhaltung von regulatorischen Vorgaben.

Insbesondere Letztere sollten aufgrund ihrer Natur normalerweise nicht durch den ISAE-3402-Standard abgedeckt werden – hierfür existiert der sehr vielseitig einsetzbare ISAE-3000-Standard (Assurance Engagement Other Than Audits or Reviews of Historical Financial Information), der auf Organisation, Prozesse, IT-Anwendungen und Systeme sowie interne Kontrollen beim Dienstleister fokussiert ist, die keinen Bezug zur finanziellen Berichterstattung seiner Kunden haben. Beispiele dafür sind die Prüfung der Einhaltung von regulatorischen Vorgaben oder von Vertragsbestimmungen. In der Schweiz wird der ISAE 3000 durch den PS 950 der Treuhand-Kammer umgesetzt (veröffentlicht im Dezember 2013) [1].

Grundlage einer Prüfung nach ISAE 3000 ist in der Regel ein zu beurteilender Sachverhalt bzw. eine Liste von Kriterien, gegen welche geprüft werden kann. ISAE 3000 erlaubt nicht nur die Bestätigung eines Sachverhalts mit hinreichender Gewissheit (reasonable assurance engagement), sondern auch mit eingeschränkter Gewissheit (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 ist in der Schweiz insbesondere im Bereich von regulatorischen Prüfungen im Finma-Umfeld sinnvoll, da deren Rundschreiben [2] ebenfalls zwischen den Prüftiefen «Prüfung» und «kritische Beurteilung» unterscheiden, welche ein positives bzw. ein negatives Prüfurteil beinhalten (siehe nachstehend).

Tabelle: **ZERTIFIZIERUNGEN UND ATTESTIERUNGEN**
Übersicht

Bezeichnung	ISAE 3402	ISAE 3000	SSAE 16	SOC1	SOC2	SOC3	PS 870
Titel	International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization	International Standard on Assurance Engagements (ISAE) No. 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information	Statement on Standards for Attestation Engagements (SSAE) No. 16	Service Organization Controls Report 1	Service Organization Controls Report 2	Service Organization Controls Report 3	Schweizer Prüfungsstandard, Prüfung von Softwareprodukten
Typ	Prüfungsstandard	Prüfungsstandard	Prüfungsstandard	Berichterstattungsoption	Berichterstattungsoption	Berichterstattungsoption	Prüfungsstandard
Primäre Verbreitung	Weltweit	Weltweit	Vereinigte Staaten von Amerika	Weltweit	Weltweit	Weltweit	Schweiz
Abdeckung Bericht	Beliebige Kriterien mit Relevanz für die finanzielle Berichterstattung: → Transaktionen → Prozesse für Transaktionsabwicklung → Berichterstattung → Umgang mit wichtigen Geschäftsereignissen	Beliebige Kriterien einer betriebswirtschaftlichen Prüfung, die weder eine Prüfung noch ein Review von vergangenheitsorientierten Finanzinformationen darstellt	Beliebige Kriterien mit Relevanz für die finanzielle Berichterstattung: → Transaktionen → Prozesse für Transaktionsabwicklung → Berichterstattung → Umgang mit wichtigen Geschäftsereignissen	Beliebige Kriterien	Primär Themen wie: → Infrastruktur → Software → Prozesse → Personen → Daten	Primär Themen wie: → Infrastruktur → Software → Prozesse → Personen → Daten	Software-Produkt
Typische Inhalte	Kontrollen über die Transaktionsverarbeitung mit Relevanz für finanzielle Berichterstattung sowie Kontrollen über die unterstützenden IT-Prozesse	Beliebige Kontrollen oder zu bestätigende Sachverhalte	Kontrollen über die Transaktionsverarbeitung mit Relevanz für finanzielle Berichterstattung sowie Kontrollen über die unterstützenden IT-Prozesse	Beliebige Kontrollen oder zu bestätigende Sachverhalte	Eines oder mehrere der Trust Service Principles, wie z. B.: → Vertraulichkeit → Verfügbarkeit	Eines oder mehrere der Trust Service Principles, wie z. B. → Vertraulichkeit → Verfügbarkeit	Funktionalität der Software, wie z. B.: → Mandantenfähigkeit → Revisionsfähigkeit → Ordnungsmässigkeit
Empfängerkreis	Der Empfängerkreis eines Berichts nach ISAE 3402 ist eingeschränkt (Kunden und deren Prüfer).	Der Empfängerkreis eines Berichts nach ISAE 3000 kann, je nach Berichterstattungsoption, eingeschränkt (bspw. SOC2) oder nicht eingeschränkt (bspw. SOC3) sein.	Der Empfängerkreis eines Berichts nach SSAE 16 ist eingeschränkt.	Der Empfängerkreis eines SOC1-Berichts ist eingeschränkt (Kunden und deren Stakeholder).	Der Empfängerkreis eines SOC2-Berichts ist eingeschränkt (Kunden und deren Stakeholder).	Der Empfängerkreis eines SOC3-Berichts ist nicht eingeschränkt; kann als «Siegel» platziert werden (Marketing).	Der Empfängerkreis eines PS-870-Berichts kann eingeschränkt werden.

Tabelle: **ZERTIFIZIERUNGEN UND ATTESTIERUNGEN** (FORTSETZUNG)
Übersicht

Bezeichnung	ISAE 3402	ISAE 3000	SSAE 16	SOC1	SOC2	SOC3	PS 870
Zertifizierung möglich	Nein	Nein	Nein	Nein	Nein	Nein	Ja
Ausprägung von Berichten/Zertifikaten	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt
Prüfungsstandard weitgehend entsprechend mit	SSAE 16	AT 101 (US)	ISAE 3402	ISAE 3402/SSAE 16	ISAE 3000	ISAE 3000	n/a
Kommentar	Berichte nach ISAE-3402-Standard werden auch für Kontrollen von Dienstleistungserbringern erstellt, die keine direkte Relevanz für die Finanzberichterstattung des Dienstleistungsbezügers haben.	ISAE 3000 hat übergreifende Gültigkeit. Deswegen halten Berichte nach ISAE-3402-Standard implizit auch den ISAE-3000-Standard ein. Umgekehrt ist dies nicht der Fall.	SSAE-16-Berichte werden auch SOC1-Berichte genannt.	SOC1 ist eine Berichterstattungsoption. Als zugrundeliegender Standard wird ISAE 3402 oder SSAE 16 angewendet.	SOC2 ist eine Berichterstattungsoption. Als zugrundeliegender Standard wird ISAE 3000 oder AT 101 angewendet.	SOC3 ist eine Berichterstattungsoption. Als zugrundeliegender Standard wird ISAE 3000 oder AT 101 angewendet.	Das Zertifikat bezieht sich nur auf die geprüfte Version der Software und ist auch nur für diese vollumfänglich gültig.

Tabelle: **ZERTIFIZIERUNGEN UND ATTESTIERUNGEN** (FORTSETZUNG)
Übersicht

Bezeichnung	PS 920	PS 950	RS 2008/07	RS 2008/21	ISO/IEC 27001	ISO/IEC 27002
Titel	Schweizer Prüfungsstandard, Vereinbarte Prüfungshandlungen bezüglich Finanzinformationen	Schweizer Prüfungsstandard, Betriebswirtschaftliche Prüfungen, die weder Prüfungen noch Reviews von vergangenheitsorientierten Finanzinformationen darstellen	FINMA-Rundschreiben «Outsourcing Banken»	FINMA-Rundschreiben «Operationelle Risiken bei Banken»	Information technology – Security techniques – Information security management systems – Requirements	Information technology – Security techniques – Code of practice for information security management
Typ	Prüfungsstandard	Prüfungsstandard	Rundschreiben	Rundschreiben	Kontrollstandard	Leitfaden
Primäre Verbreitung	Schweiz	Schweiz	Schweiz	Schweiz	Weltweit	Weltweit
Abdeckung Bericht	Zwischen Prüfer und Unternehmen definierte Prüfungshandlungen bezüglich Finanzinformationen	Beliebige Kriterien einer betriebswirtschaftlichen Prüfung, die weder eine Prüfung noch ein Review von vergangenheitsorientierten Finanzinformationen darstellt	Von Banken an Dienstleister ausgelagerte Tätigkeiten	Von Banken an Dienstleister ausgelagerte Tätigkeiten mit Fokus auf Umgang mit kundenidentifizierenden Daten	Scope des definierten Informations-Sicherheits-Management-Systems in Kombination mit nicht ausgeschlossenen Kontrollen aus Anhang resp. ISO 27002; d. h. klar gekennzeichneter Teil der Organisation resp. Prozesse oder Produkte	n/a
Typische Inhalte	Aussage zu den vereinbarungsgemäss vorgenommen Prüfungshandlungen	Beliebige Kontrollen oder zu bestätigende Sachverhalte	9 spezifische Grundsätze wie z. B.: → Sicherheit → Geschäfts- und Bankgeheimnis, Datenschutz	9 spezifische Grundsätze mit Bezug auf kundenidentifizierende Daten (CID), wie z. B.: → Datenspeicherort → Mitarbeitende mit Zugriff auf CID	Vorhandensein eines Informations-Sicherheits-Management-Systems (ISMS)	n/a
Empfängerkreis	Der Bericht ist nur für die Parteien bestimmt, welche die Auftragsbedingungen kennen.	Der Empfängerkreis eines PS-950-Berichts kann – je nach den zugrunde liegenden Kriterien (öffentlich bekannt oder nicht) – eingeschränkt oder nicht eingeschränkt sein.	Der Empfängerkreis eines Finma-Berichts ist eingeschränkt.	Der Empfängerkreis eines FINMA-Berichts ist eingeschränkt.	Der Empfängerkreis eines ISO-27001-Zertifikats ist nicht eingeschränkt.	n/a
Zertifizierung möglich	Nein	Nein	Nein	Nein	Ja	Nein

Tabelle: **ZERTIFIZIERUNGEN UND ATTESTIERUNGEN** (FORTSETZUNG)
Übersicht

Bezeichnung	PS 920	PS 950	RS 2008/07	RS 2008/21	ISO/IEC 27001	ISO/IEC 27002
Ausprägung von Berichten/ Zertifikaten	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Periode (3 Jahre)	n/a
Prüfungsstandard weitgehend entsprechend mit	AT 201 (US)	ISAE 3000	n/a	n/a	n/a	n/a
Kommentar	Der Standard kann, soweit sinnvoll, auch für nicht finanzrelevante Aufträge verwendet werden.	Umsetzung von ISAE 3000 in der Schweiz			Ein ISO-27001-Zertifikat ist gültig für einen klar beschriebenen Geltungsbereich. Der Geltungsbereich kann bspw. eine Abteilung oder die gesamte Unternehmung sein.	Entgegen der allgemeinen Auffassung ist eine Zertifizierung nach ISO/IEC 27002 nicht möglich.

Prüfberichte nach ISAE 3000 und PS 950 dienen den Kunden eines Dienstleisters dazu:
→ die Organisation, Prozesse, IT-Anwendungen und -Systeme des Dienstleisters zu verstehen; → das IKS des Dienstleisters (oder ausgewählte Teile davon) zu verstehen; → die Risiken aus der Nutzung der Dienstleistungen festzustellen und zu beurteilen; → Rückschlüsse zu ziehen und komplementäre Kontrollen zu implementieren, um diesen Risiken zu begegnen.

5. OUTSOURCING UND SOC REPORTING: TRUST SERVICES PRINCIPLES

Nach der Ablösung von SAS 70 durch ISAE 3402 bzw. SSAE 16 wurde 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: sogenannte SOC-Reports [3]. Man unterscheidet dabei zwischen SOC1-, SOC2- sowie SOC3-Berichten.

SOC1-Berichte entsprechen inhaltlich vollumfänglich ISAE 3402 bzw. SSAE 16 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.

SOC2-Berichte fokussieren auf die Bestätigung von Sachverhalten ausserhalb der finanziellen Berichterstattung. Dies geschieht in der Schweiz in der Regel 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 sogenannten Trust Services Principles (Grundsätze) gegliedert: → Sicherheit (security); → Verfügbarkeit (availability); → Vertraulichkeit (confidentiality/privacy); → Verlässlichkeit der Verarbeitung (reliability).

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

Die Kurzform eines SOC2-Berichts wird als SOC3 bezeichnet. Dieser Bericht geht nicht mehr auf die tatsächlich durchgeführten Prüfungshandlungen ein, sondern bestätigt nur die Einhaltung der vorgegebenen Kriterien.

6. OUTSOURCING UND BERICHT GEMÄSS FINMA-RUNDSCHREIBEN 2008/07

Das Finma-Rundschreiben 2008/07 «Outsourcing Banken» der *Eidgenössischen Finanzmarktaufsicht (Finma)* beschreibt für die bei ihr unterstellten Banken und Effektenhändler die Voraussetzungen, unter welchen Outsourcing-Lösungen zulässig sind (für Dienstleistungen, welche die Finma überhaupt als «outsourcing-relevant» ansieht). Das Rundschreiben wurde am 1. Januar 2009 in Kraft gesetzt und im Dezember 2012 ergänzt. Es löst das vorher gültige EBK-Rundschreiben 99/2 (Outsourcing) ab.

Die Finma hat die bankengesetzlichen Revisionsstellen beauftragt, die Umsetzung der im Rundschreiben festgeleg-

ten Anforderungen bei existierenden und geplanten Outsourcing-Lösungen zu beschreiben und ihre Einhaltung zu prüfen. Dabei ist bei den Dienstleistern die Anwendung der nachfolgenden Voraussetzungen/Grundsätze für ein sicheres Outsourcing zu erheben und zu beurteilen:

- Grundsatz 1 – Bestimmung des auszulagernden Geschäftsbereichs;
- Grundsatz 2 – Auswahl, Instruktion und Kontrolle des Dienstleisters;
- Grundsatz 3 – Verantwortung;
- Grundsatz 4 – Sicherheit;
- Grundsatz 5 – Geschäfts- und Bankgeheimnis, Datenschutz;
- Grundsatz 6 – Kundenorientierung;
- Grundsatz 7 – Prüfung und Aufsicht;
- Grundsatz 8 – Auslagerung ins Ausland;
- Grundsatz 9 – Vertrag.

Im Vordergrund der Prüfung und Berichterstattung stehen diejenigen Grundsätze des Finma-Rundschreibens 2008/07, die vollständig oder teilweise in den Aufgaben- bzw. Verantwortungsbereich des Dienstleisters fallen. Man muss sich jedoch bewusst sein, dass die Ausführungsverantwortung für den Grossteil der Grundsätze vollständig oder primär bei der Bank resp. dem Effektenhändler liegt. Beim Dienstleister ist vor allem der Grundsatz 4 von Bedeutung, d. h. die organisatorische, logische und physische Sicherheit sowie die Geschäftskontinuität/Katastrophenvorsorge.

«Der Abschlussprüfer kann die Ergebnisse der Software-Prüfung im Rahmen seiner Risikobeurteilung verwerten.»

Die Berichte nach Finma-Rundschreiben 2008/07 dienen der Revisionsstelle der auslagernden Bank (und der auslagernden Institution selber) primär dazu:
→ den Beitrag des Dienstleisters zur Einhaltung der Grundsätze 1–9 zu verstehen; → die Risiken aus der Nutzung der Dienstleistungen festzustellen und zu beurteilen; → weitere Prüfungshandlungen zu planen und durchzuführen, um diesen Risiken zu begegnen (beispielsweise, um komplementäre Kontrollen seitens des auslagernden Unternehmens aufzuspüren und diese zu prüfen).

Das Abstellen der Revisionsstellen der betroffenen Banken und Effektenhändler auf die Ergebnisse der Revisionsstelle des Dienstleisters ist im Rundschreiben explizit vorgesehen, sofern letztere nach schweizerischem Recht organisiert ist und die Voraussetzungen des Rundschreibens erfüllt.

7. OUTSOURCING UND BERICHT GEMÄSS FINMA RUNDSCHREIBEN 2008/21

Das Finma-Rundschreiben 2008/21 «Operationelle Risiken bei Banken» enthält im Anhang 3 «Umgang mit elektronischen Kundendaten» die Grundsätze und die dazugehörigen Ausführungen für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen (Privatkunden), deren Geschäftsbeziehungen in oder von der Schweiz aus betreut oder geführt werden (Kundendaten). Das aktualisierte Rundschreiben inklusive dem neuen Anhang 3 trat am 1. Januar 2015 in Kraft.

In Prüfungen bei Dienstleistern von Banken ist die Anwendung der nachfolgenden Voraussetzungen/Grundsätze bezüglich Umgang mit elektronischen Kundendaten zu erheben und zu beurteilen:

- Grundsatz 1 – Governance;
- Grundsatz 2 – Kundenidentifikationsdaten *(Client Identifying Data, CID);*
- Grundsatz 3 – Datenspeicherort und -zugriff;
- Grundsatz 4 – Sicherheitsstandards für die Infrastruktur und die Technologie;
- Grundsatz 5 – Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben;
- Grundsatz 6 – Risikoidentifizierung und -kontrolle in Bezug auf die CID-Vertraulichkeit;
- Grundsatz 7 – Risikominderung in Bezug auf die CID-Vertraulichkeit;
- Grundsatz 8 – Vorfälle im Zusammenhang mit der CID-Vertraulichkeit, interne und externe Kommunikation;
- Grundsatz 9 – Outsourcing-Dienstleistungen und Grossaufträge in Verbindung mit CID.

Die Grundsätze sind hauptsächlich auf das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von Kunden-Massendaten durch Verwendung elektronischer Systeme zugeschnitten. Die einschlägigen rechtlichen Bestimmungen finden sich nicht nur im Aufsichtsrecht, sondern auch im Datenschutzrecht und Zivilrecht.

Im Bericht an den Dienstleister sind die Ergebnisse aus den Prüfungshandlungen bezogen auf die Grundsätze 1–9 zu dokumentieren und zu beurteilen. Gerade der letzte Grundsatz 9 (in der Randziffer 51) verlangt von der Bank, dass sie wissen und verstehen muss, welche Schlüsselkontrollen der Outsourcing-Dienstleister in Verbindung mit der Vertraulichkeit von CID durchzuführen hat.

Die Berichte «Umgang mit elektronischen Kundendaten» nach Anhang 3 des Finma-Rundschreibens 2008/21 dienen der Revisionsstelle der auslagernden Bank (und der auslagernden Bank selber) dazu:
→ Den Beitrag des Dienstleisters zur Erfüllung der Grundsätze 1–9 zu verstehen (also die Einhaltung interner Anforderungen sowie die Wirksamkeit der Schlüsselkontrollen zu prüfen und zu beurteilen); → die Risiken aus der Nutzung der Dienstleistungen festzustellen und zu beurteilen; → weitere Prüfungshandlungen zu planen und durchzuführen, um diesen Risiken zu begegnen.

8. ZERTIFIZIERUNG VON SOFTWARE MITTELS PS 870

Gegenstand von Software-Prüfungen resp. -Zertifikaten sind Software-Produkte, unabhängig von deren Implementierung und Produktivsetzung beim Anwender. Relevante Standards sind der PS 870 in der Schweiz (per Mitte Dezem-

ber 2013 in Kraft gesetzt) sowie der IDW PS 880 in Deutschland, der als Grundlage für den PS 870 diente.

Die Prüfung von Software-Produkten umfasst:
→ Aufnahme und Beurteilung der Software-Entwicklungsumgebung mit den entsprechenden Entwicklungs-, Wartungs-, Test- und Freigabeverfahren einschliesslich der Vollständigkeit und Aktualität der Verfahrensdokumentation;
→ Aufnahme des zu prüfenden Software-Produkts und Prüfung der Angemessenheit der für das Aufgabengebiet des Softwareprodukts notwendigen Programmfunktionen (Aufbauprüfung) einschliesslich der Aussagefähigkeit der diesbezüglichen Verfahrensdokumentation; → Prüfung der sachgerechten programmtechnischen Umsetzung der als angemessen beurteilten Programmfunktionen (Funktionsprüfung).

Einer Beurteilung von Software-Produkten mit Bezug zum Rechnungswesen werden zudem folgende Kriterien zugrunde gelegt:
→ die in Art. 957a Abs. 2 OR definierten Grundsätze ordnungsmässiger Buchführung; → die in Art. 958c OR definierten Grundsätze ordnungsmässiger Rechnungslegung; die in der Stellungnahme zur Rechnungslegung (RS) 10 der Treuhand-Kammer formulierten Grundsätze ordnungsmässiger Buchführung beim Einsatz von Informationstechnologie.

Zuhanden der Anwender der geprüften Software wird beurteilt, ob das geprüfte Softwareprodukt bei sachgerechter Implementierung und Anwendung eine den Grundsätzen ordnungsmässiger Buchführung entsprechende Rechnungslegung ermöglicht und den im Prüfbericht aufgeführten Kriterien entspricht.

Über die Software-Prüfung wird ein Prüfungsbericht angefertigt. Sofern aufgrund der Prüfungsergebnisse möglich, wird als Bestandteil des Prüfungsberichts auch ein Software-Zertifikat erteilt.

Der Abschlussprüfer kann die Ergebnisse der Software-Prüfung im Rahmen seiner Risikobeurteilung verwerten. Er wird den Prüfungsgegenstand, die Prüfungskriterien und die geprüften Funktionen im Hinblick auf deren Relevanz für seine Prüfungsstrategie und die von ihm identifizierten Risiken beurteilen und seine Beurteilung dokumentieren. Voraussetzung ist, dass ihm neben dem Software-Zertifikat auch der vollständige Prüfungsbericht über die Software-Prüfung vorliegt. Wichtig ist zudem, dass das Zertifikat nur für die geprüfte Version der Software anwendbar ist.

9. ZERTIFIZIERUNGEN (Z. B. ISO 27001)

In der Praxis wird oft versucht, andere, bereits bestehende Zertifizierungen zur Bestätigung von Outsourcing-Dienstleistungen zu verwenden, z. B. eine Zertifizierung des Informations-Sicherheits-Management-Systems (ISMS) nach ISO 27001 (mit dem «normativen» Anhang ISO 27002). Grundsätzlich deckt z. B. ISO 27001 einen Grossteil der Kriterien ab, welche für den Grundsatz Sicherheit in einem SOC2-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. Es besteht jedoch ein grosser Unterschied bezüglich der Art und Weise, wie die Effektivität der Kontrollen beurteilt wird.

Gerade bei Zertifikaten besteht leider ein grosser Wildwuchs – wichtig ist daher auf jeden Fall, durch wen und in welchem Kontext ein Zertifikat ausgestellt wurde. Neben beschränkt aussagekräftigen Zertifikaten von nicht-akkreditierten Unternehmen gibt es auch akkreditierte Zertifizierer, welche zusätzlich zu den offiziellen Zertifikaten teilweise abgespeckte Zertifikats-Versionen ausstellen, welche oft nur noch einen eingeschränkten Stellenwert haben. Es ist auch wichtig, genau hinzuschauen, welche Breite und Tiefe eines Kontrollumfelds eine entsprechende Zertifizierung oder Drittparteien-Bestätigung in Form eines Berichts abdeckt.

«Für Prüfer haben Zertifizierungen grundsätzlich keine grosse Bedeutung für das Vorgehen im Rahmen einer Abschlussprüfung.»

Für den Prüfer ist eine Zertifizierung in den meisten Fällen nicht ausreichend, da sie oft nicht alle relevanten Aspekte abdeckt, nur periodisch (z. B. alle drei Jahre) erneuert wird und nicht zwingend eine Abschlussperiode abdeckt. In jedem Fall sollte der Umfang, die Häufigkeit der Prüfung resp. Rezertifizierung sowie die abgedeckte Periode genau analysiert werden, bevor auf einen solchen Bericht abgestützt wird. Die Prüfer sind angehalten, ergänzende Prüfungen durchzuführen, um dadurch das gesamte Kontrollumfeld abzudecken und eine entsprechende Würdigung der vorhandenen Kontroll- und Rest-Risiken vornehmen zu können.

10. ANDERE BERICHTE

Neben den im Text des Artikels behandelten Attestierungen und Zertifikaten gibt es unzählige weitere Beispiele (wie PCI-DSS, PA-DSS, VDSZ usw.), welche teilweise in die *Tabelle* aufgenommen wurden, aber mangels Relevanz für die Abschlussprüfung nicht weiter erläutert werden.

Für Prüfer haben Zertifizierungen oder andere der im Artikel nicht behandelten Attestierungen grundsätzlich keine grosse Bedeutung und kaum Auswirkungen auf das Vorgehen im Rahmen einer Abschlussprüfung.

11. FAZIT

Neben dem bewährten und etablierten ISAE-3402-Bericht existieren heute verschiedene Berichtsformen, welche insbesondere zur Abdeckung von nicht auf die Finanzberichterstattung fokussierte Themenbereiche geeignet sind. Vor allem der «alte» ISAE-3000-Standard erlaubt mit seiner grossen Flexibilität eine sehr breite Anwendung und birgt ein grosses Potenzial für die Abdeckung von Themen wie Business Continuity Management, Vertraulichkeit oder

auch Kundendatenschutz. Der Standard ist zudem als PS 950 in die Schweizer Prüfungsstandards eingebettet. Die Standardisierung von Berichtsinhalten über die Trust Services Principles von SOC2- und SOC3-Berichten schränkt zwar die Flexibilität ein, erlaubt aber eine höhere Vergleichbarkeit von verschiedenen Berichtsformen. Zudem befriedigt SOC3 das Verlangen nach einem einfach zu verwendenden «Zertifikat» für Outsourcing-Provider und kann als Siegel auch zu Werbezwecken, z. B. auf der Homepage, gezeigt werden. Es bleibt abzuwarten, inwiefern diese Variante in Zukunft von Dienstleistern auch für regulatorische (Finma-)Berichte verwendet werden.

«Bei Aussagen wie ‹ISAE-zugelassen› oder ‹Finma-zertifiziert› sollte der Wirtschaftsprüfer hellhörig werden.»

Bei Aussagen wie «ISAE-zugelassen» oder «Finma-zertifiziert» sollte der Wirtschaftsprüfer hellhörig werden. In jedem Fall verlangt ein entsprechendes Zertifikat oder ein entsprechender Bericht nach einer kritischen Würdigung, bevor der Wirtschaftsprüfer sich darauf abstützt. Mithilfe der in diesem Artikel dargelegten Ausführungen und Beispiele wird das in Zukunft hoffentlich etwas leichter fallen. ■

Anmerkungen: 1) Für Berichte, die nach dem 15. Dezember 2015 datiert sind, kommt eine neue Version des ISAE 3000 zum Tragen, welche noch nicht in die Schweizer PS überführt wurde. Es ist ausdrücklich erlaubt, als «early application» bereits die neue Version des ISAE 3000 zu verwenden. **2)** Vgl. Finma-Rundschreiben 2013/3, Prüfwesen, Rz 32 ff. **3)** Siehe AICPA-Homepage zu Service Organization Control Reporting http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx.