[BSA+09] Marc Billeb, Achim Schäfer, Mourad Abbou, Michael Niemann, Julian Eckert, Nicolas Repp, Ralf Steinmetz: **Einfluss regulatorischer Anforderungen im Internet of Services.** In: IT-Governance, Zeitschrift des ISACA Germany Chapter e.V., no. 6, October 2009. ISSN 1864-6557. Seite 8–13

Einfluss regulatorischer Anforderungen im Internet of Services

Marc Billeb, Achim Schäfer, Mourad Abbou, Michael Niemann, Julian Eckert, Nicolas Repp, Ralf Steinmetz

Das Paradigma der serviceorientierten Architekturen (SOA) hat sich in den letzten Jahren zu einem der am meisten beachteten Themen im Bereich des Software- und Enterprise-Engineerings entwickelt. Kernideen von SOA sind die mit der Architektur verbundene Flexibilität und die Wiederverwendbarkeit von Services als Bausteine servicebasierter Systeme. Die Fortführung dieses Gedankens ist das Internet of Services, in dem standardisierte Services durch verschiedene Parteien je nach Bedarf angeboten, gehandelt und genutzt werden können.

Hierbei stellt sich jedoch die Frage, ob und wie in diesem Umfeld die Erfüllung regulatorischer Anforderungen in Bezug auf die Ordnungsmäßigkeit und Sicherheit des Betriebs dieser IT gewährleistet werden kann. Aus dieser Fragestellung abgeleitet wird in diesem Beitrag untersucht, wie sich die Anforderungen an den ordnungsgemäßen Betrieb von Anwendungen gemäß IDW RS FAIT 1 in einem solchen Umfeld darstellen und welche Relevanz sie jeweils im Vergleich zu einer herkömmlichen IT-Architektur besitzen. Dabei werden die Besonderheiten einer SOA mit den Auswirkungen von regulatorischen Anforderungen verknüpft und anhand praktischer Erfahrungen analysiert.

1 Einleitung

In den letzten Jahren hat sich das Paradigma der serviceorientierten Architekturen zu einem der am meisten beachteten Themen im Bereich des Software- und Enterprise-Engineerings entwickelt. Hauptbetrachtungsgegenstand von SOA sind Services, d.h. Kapselungen von Funktionalitäten einer fachlichen Domäne, die innerhalb eines Unternehmens Anwendung finden. Services können im Sinne von Bausteinen zu komplexeren Funktionseinheiten, wie z.B. zu Geschäftsprozessen und diese unterstützende Applikationen, zusammengesetzt werden.

Unter einem Service wird eine abgeschlossene, unabhängige Komponente verstanden, die eine klar definierte Funktionalität über eine Schnittstelle anbietet [Papazoglou 2003]. Ein Service abstrahiert von zugrunde liegenden Entitäten, Objekten und Klassen. In klassischen Softwarearchitekturen wird zumeist eine komplette Systemstruktur beschrieben. Eine SOA konzentriert sich in diesem Zusammenhang, zum Zwecke der Anwendungsintegration, auf die Bereitstellung fachlicher Dienste und Funktionalitäten in Form von Services, die sich durch lose Kopplung sowie Ortsunabhängigkeit der beteiligten Services auszeichnet. Eine SOA beschreibt die Modularisierung einer meist heterogenen, komplexen Anwendungslandschaft in Form von Services.

Betrachtungsgegenstand im Sinne eines Szenarios ist im Folgenden das *Internet of Services* [Janiesch et al. 2008]. Hierbei wird davon ausgegangen, dass eine Vielzahl von Services (im Verständnis des SOA-Paradigmas) einer bestimmten Funktionalität zur Verfügung steht, die sowohl in einem zentralen als auch einem verteilten Repository verwaltet und gelistet werden. Über das Repository erfolgt die Serviceregistrierung sowie das Suchen und Auffinden von Services. Darüber hinaus umfasst das Internet of Services die Verhandlung von Service Level Agreements (SLA), das Service-Monitoring, das Service-Pricing sowie -Billing.

Die involvierten Rollen in diesem Szenario sind: *Service Provider*, *Service Consumer*, *Service Intermediary*, *Service Executor* und *Platform Host* sowie *Service Marketplace*. Die ersten beiden Rollen bieten Services an bzw. fragen diese nach. Der Service Intermediary stellt sogenannte Composite Services aus mehreren einzelnen Services zusammen und verkauft dies wiederum als Service mit angereicherter Funktionalität und kann somit als Bindeglied zwischen Service Consumer und Service Provider fungieren. Die serviceausführende Rolle muss nicht notwendigerweise vom Service Provider oder dem Platform Host ausgefüllt werden, sondern kann auch von einer dritten Partei übernommen werden, dem sogenannten Service Executor. Der Platform Host ist primär für die Bereitstellung der Plattform zuständig (Suchen, Finden, Service Registry). Er kann jedoch zusätzlich auch andere Rollen übernehmen. In größerem Umfang werden die Services für die Service Consumer auf einem sogenannten Service Marketplace angeboten. Darüber hinaus wird angenommen, dass das Internet of Services einen hohen SOA-Reifegrad aufweist. Dies impliziert einen hohen Grad der Umsetzung des SOA-Paradigmas über alle involvierten Rollen hinweg [Johannsen & Goeken 2007].

Vorhandene Services gleicher Funktionalität unterscheiden sich lediglich hinsichtlich ihrer nicht funktionalen Parameter. Besonderer Wettbewerb entsteht dadurch, dass Service Provider, Service Consumer und Service Intermediary das Internet of Services nutzen, um dadurch IT-Funktionalitäten (Services) von extern einzubinden bzw. um Funktionalitäten Dritten bereitzustellen.

Durch die gewachsene Anzahl an involvierten Stakeholdern steigt auch der Bedarf an Absicherung zwischen den einzelnen Parteien, da diese mit zunehmender Zahl an Interdependenzen zwischen den Marktteilnehmern vermehrt aufeinander angewiesen sind. Für z. B. das Service Monitoring muss u.a. geklärt werden, wo ein Service ausgeführt und damit auch überwacht wird (Rolle des Service Executor). Im nächsten Schritt muss die ordnungsgemäße Durchführung des Service-Monitorings durch eine dieser Parteien sichergestellt werden.

Im Folgenden wird auf Themenbereiche regulatorischer Anforderungen eingegangen, die im Internet of Services besondere Relevanz haben. Grundlage der Darstellung werden dabei die Themenfelder im IDW RS FAIT 1 (»Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie« [IDW RS FAIT 1]) sein.

2 Untersuchung der Einflüsse regulatorischer Anforderungen auf das Internet of Services

2.1 IT-Umfeld und IT-Organisation

Aus dem IDW RS FAIT 1 ergeben sich Anforderungen an das IT-Umfeld und an die IT-Organisation, die zum einen auf eine angemessene Grundeinstellung und ein Problembewusstsein für IT-Risiken und zum anderen auf eine klar definierte Aufbau- und Ablauforganisation abzielen.

In einem SOA-Umfeld bedeutet dies ein Umdenken für die IT-Abteilungen. Das in vielen IT-Abteilungen weitverbreitete »Plattformdenken« sowie die Skepsis gegenüber fremdbezogenen Anwendungen müssen einem serviceorientierten Denken in Geschäftsprozessen weichen. Dieses Umdenken beginnt allerdings nicht erst in der IT-Abteilung selbst, sondern muss durch das Topmanagement getragen werden [Repp et al. 2009]. Es gilt, nach dem Top-down-Prinzip eine SOA-gerechte IT-Strategie zu definieren, in der der Internet-of-Service-Gedanke sowohl als Vision als auch in der Infrastruktur-, Applikations- und Sourcing-Strategie verankert ist.

Das IT-Projektmanagement ist dahingehend anzupassen, dass eine zentrale SOA-Instanz im Unternehmen alle IT-Projekte von der Designphase bis zum Übergang in die Produktion begleitet und dabei das Ziel »unternehmensweit einheitliches SOA-Verfahren« auf gleiche Ebene mit dem Ziel »schnelle und einfache Erreichung des Projektziels« gestellt wird. Innerhalb der IT-Organisation muss der Prozessgedanke abgebildet werden, indem sich die IT-Aufbauorganisation an den fachlichen Geschäftsprozessen ausrichtet. Die SLAs zwischen der IT-Abteilung und den Fachbereichen müssen umgestaltet werden, um von der Bereitstellung von Anwendungen und Verfügbarkeiten zu modularen, kombinierbaren und wiederverwendbaren Services zu gelangen.

Die IT-Ablauforganisation, die nach IDW RS FAIT 1 die Themen Entwicklung, Einführung, Steuerung und Betrieb von IT beinhaltet, bleibt in einem SOA-Umfeld in ihren Grundzügen unverändert, da diese operativen Tätigkeiten in der IT-Abteilung gleichermaßen für monolithische Systeme und eine SOA durchgeführt werden müssen.

2.2 IT-Infrastruktur

Die IT-Infrastruktur spielt im IDW RS FAIT 1 eine tragende Rolle, da in ihr wesentliche Kontrollen eines internen Kontrollsystems umgesetzt werden. Die wichtigsten Kontrollen umfassen das IT-Sicherheitskonzept, physische Sicherungsmaßnahmen, logische Zugriffskontrollen, Datensicherungs- und Auslagerungsverfahren, den geordneten Regelbetrieb und die Notfallplanung. In den folgenden Abschnitten werden die Besonderheiten dieser Kontrollen unter SOA-Gesichtspunkten näher erläutert.

Die mit den Grundsätzen ordnungsmäßiger Buchführung (GoB) verbundenen Anforderungen an die Sicherheit IT-gestützter Rechnungslegung werden üblicherweise in Form von Verfahrensanweisungen in einer unternehmensinternen IT-Sicherheitsrichtlinie zusammengefasst. Dieses Instrument ist in einer SOA-Umgebung von hoher Relevanz, da wegen der kleinteiligeren Gestaltung und die ggf. über mehrere Unternehmen hinaus verstreuten Services erhöhter Bedarf einer differenzierten Sicherheitsstrategie bzw. eines Sicherheitskonzepts besteht. So ist beispielsweise die örtliche Verteilung der physischen Server, auf denen die Services betrieben werden, in der Notfallplanung und im Sicherheitskonzept zu berücksichtigen.

Die physischen Sicherungsmaßnahmen beziehen sich im Wesentlichen auf die Rechenzentren und Datenräume und umfassen neben baulichen Maßnahmen und Zugangskontrollen auch Maßnahmen zum Schutz vor Umwelteinflüssen. Diese sind im SOA-Umfeld ebenso relevant wie bei traditionellen IT-Architekturen. Die Kontrolle hinsichtlich der Einhaltung physischer Sicherungsmaßnahmen weitet sich jedoch auf die unternehmensexternen Rechenzentren der Service Provider aus, die die vom Service Consumer bezogenen Services bereitstellen.

Die Kontrollen im Bereich des logischen Zugriffsschutzes müssen bei einer SOA-Architektur grundlegend überarbeitet werden, da der klassische Zugriffsschutz in abgeschlossenen Anwendungen (»Silos«) und nicht in verteilten Anwendungskomponenten im Sinne von Services umgesetzt ist. In einer servicebasierten IT-Umgebung empfiehlt es sich, ein ausgereiftes »Single-Sign-on«-Konzept für alle Services zu entwickeln, damit man sich nicht gegenüber jedem Service einzeln authentifizieren muss. Außerdem müssen die Verantwortlichkeiten im Sinne der Überwachung von Zugriffskontrollen ebenso neu festgelegt werden, da sich durch die lose, komponentenweise Verteilung der genutzten Anwendungen die zuvor klare Zuordnung zu Prozesseigentümern überlappt.

Datensicherungs- und Auslagerungsverfahren haben in einer serviceorientierten Architektur eine unveränderte Relevanz, da in den Unternehmen bereits eine Vielzahl unterschiedlicher Lösungen im Einsatz ist, die Daten auf heterogen organisierten Systemen sichern.

Während die Bedeutung des Regelbetriebs von IT-Anwendungen in einer SOA weitgehend gleich bleibt, spielt die Notfallvorsorge im Sinne von Maßnahmen zur Sicherstellung der Betriebsbereitschaft eine noch wichtigere Rolle. Aus Sicht des Service Provider kann aufgrund der Wiederverwendbarkeit von Services die Tragweite eines Ausfalls signifikant steigen (siehe Abb. 1). Darüber hinaus müssen die bereits definierten Notfallszenarien um die teilweise an andere Unternehmen ausgelagerten Services ausgeweitet werden. Dieser erhöhten Komplexität steht jedoch aus Sicht des Service Consumer bei einer Umsetzung des Internet-of-Service-Gedankens mit einem hohen SOA-Reifegrad wegen der vielfältigen Alternativen zum Bezug von Services ein besserer Notfallschutz gegenüber (siehe Abb. 2).

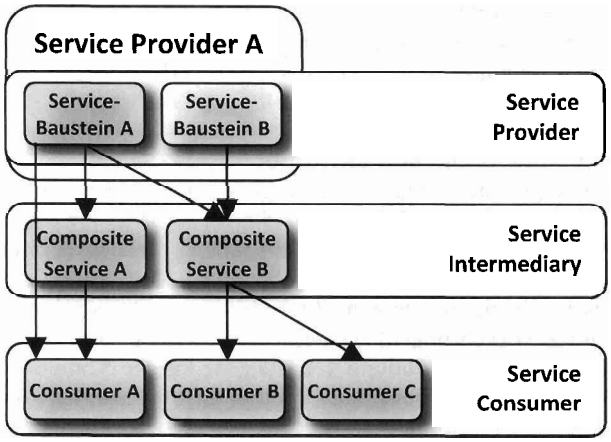


Abb. 1: Ausfall eines Service-Bausteins aus Sicht des Service Provider mit hoher Tragweite

Abbildung 1 zeigt die Auswirkung des Ausfalls eines Service-Bausteins (Service-Baustein A) auf die nachgelagerten Services, die diesen Service-Baustein nutzen.

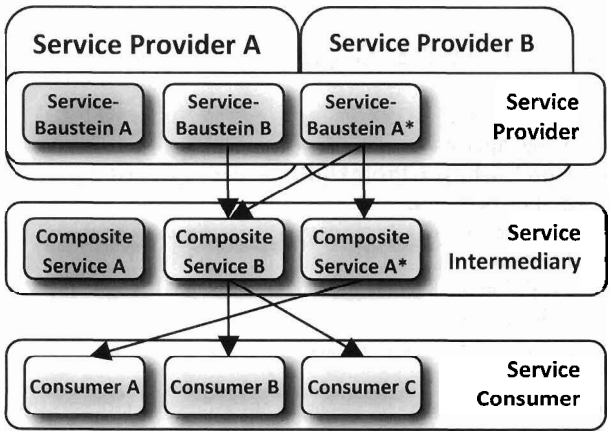


Abb. 2: Alternativer Bezug des ausgefallenen Service aus Sicht des Service Consumer

Abbildung 2 zeigt, wie der Ausfall eines Service-Bausteins (Service-Baustein A) durch die Nutzung des alternativen Service-Bausteins A* mit der gleichen Funktionalität – jedoch von einem anderen Service Provider innerhalb des Internet of Services – kompensiert werden kann.

2.3 IT-Anwendungen

Im Bereich der IT-Anwendungen werden Anforderungen an die Ordnungsmäßigkeit von IT-Anwendungen festgelegt. Neben den Anforderungen, die sich aus den GoB ergeben, sind Softwaresicherheit und die Einhaltung der durch die IT-Strategie bestimmten Funktionalität zentrale Aspekte.

Es ist zunächst zu berücksichtigen, dass in einem SOA-Umfeld eine klassische IT-Anwendung (monolithisches System) nicht mehr besteht, sondern sich die funktionalen Bestandteile aus einer Vielzahl von Services zusammensetzen. Die Services werden flexibel von verschiedenen Partnern bereitgestellt. Daraus ergibt sich, dass bislang etablierte Maßnahmen zur Umsetzung der Sicherheitsanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit) zu überdenken und fortzuentwickeln sind.

Beim Betrieb einer SOA kommt der Umsetzung von aufeinander abgestimmten Ein- und Ausgabekontrollen sowie Verarbeitungskontrollen besondere Bedeutung zu. Die Umsetzung einzelner Kontrollen ist Aufgabe der einzelnen Service Provider; darüber hinaus ist eine Kontrolle über den gesamten Prozess an zentraler Stelle erforderlich. Erreicht werden kann dies durch die Implementierung wirksamer technischer Abstimmungskontrollen an den Schnittstellen (z. B. durch Hashsignaturen oder Checksummen) sowie einer intensiven, spezialisierten Testphase im Softwareentwicklungsprozess (z. B. Integrations- und Kommunikationstests). Darüber hinaus sollte die Verarbeitungsqualität im laufenden Betrieb durch Überprüfung geeignet modellierter Vor- und Nachbedingungen permanent überwacht werden.

Durch eine Vielzahl von potenziell nutzbaren Services müssen die Daten über eine vermehrte Anzahl von Schnittstellen und Datenformaten übergeben werden. Der Grundgedanke einer SOA, standardisierte Schnittstellen und Nachrichtenformate einzuführen, ist eine notwendige, jedoch nicht hinreichende Bedingung für ein nachhaltiges Servicemanagement. Durch die Anpassung der Services an ein sich veränderndes Umfeld ergeben sich zwangsläufig Änderungen an den Schnittstellen und Datenformaten. Ein konsistentes Schnittstellenrichtlinienmanagement kann diesen Herausforderungen begegnen und beispielsweise das Risiko von »Schnittstellenfehlern« aufgrund der Vielzahl der Schnittstellen reduzieren. Insbesondere muss auch der Service-Lifecycle betrachtet werden. Da ein Service in verschiedenen Szenarien systemübergreifend und unternehmensübergreifend Verwendung finden kann und durch mehrere Consumer genutzt wird, wirkt sich ein Ausfall sehr viel stärker aus als eine fehlerhafte Ausführung einer Methode in einem monolithischen

System. Daher müssen spezifischere Test- und Freigabeverfahren sowie Funktions- und Integrationstests in den Service-Lifecycle integriert werden.

Zusätzlich sind neben dem Schnittstellenmanagement die anderen Phasen eines Service-Lifecycles zu berücksichtigen: Entwurf, Entwicklung, Test, Inbetriebnahme, Betrieb und Außerbetriebnahme. Im Unterschied zur klassischen Softwareentwicklung gilt es im Umfeld von SOA zu beachten, dass die Verantwortlichkeiten für die einzelnen Phasen nicht unbedingt beim Service Provider liegen müssen (z. B. initiale Tests und laufende Überwachung des Betriebs). Wesentlich ist somit, dass die Rollen und Verantwortlichkeiten für die Phasen eindeutig definiert sind.

2.4 IT-Geschäftsprozesse

Die Gestaltung von IT-gestützten Geschäftsprozessen folgt in einer klassischen Anwendungslandschaft vielfach den funktionalen Möglichkeiten, die ein vorhandenes Anwendungssystem (z. B. ein SAP-ERP-System) bietet. Bei Bestehen eines Internet of Services werden zunächst Geschäftsprozesse definiert. Die Anschaffung von Services bzw. der notwendigen IT-Funktionen erfolgt nachgeordnet.

Der IDW RS FAIT 1 fordert insbesondere eine Integration und ganzheitliche Betrachtung von IT-Anwendung und Kontrollen aus Sicht komplexer IT-gestützter Geschäftsprozesse. Dies steht nicht im Gegensatz zu den Notwendigkeiten in einem Internet of Services. Vielmehr ergibt sich aufgrund der viel höheren Anzahl von IT-Komponenten bezüglich deren Integration und Zusammenspiel eine deutlich gestiegene Relevanz (siehe auch Abschnitt 2.3).

2.5 Überwachung des IT-Kontrollsystems

Wesentliche Elemente der im IDW RS FAIT 1 geforderten Überwachung des IT-Kontrollsystems sind Aktivitäten, die eine Beurteilung dessen erlauben, ob die Strategien und die daraus abgeleiteten Richtlinien und Regelungen in Übereinstimmung mit den Unternehmenszielen umgesetzt wurden, das eingerichtete Kontrollsystem angemessen und wirksam ist sowie ob die eingerichteten Maßnahmen die Erreichung der Unternehmensziele sicherstellen. Typische Beispiele hierfür sind die Durchsicht von Fehler- und Ausnahmeberichten im Hinblick auf die Beeinträchtigung kritischer Erfolgsfaktoren, die Durchführung von Benchmarks oder die regelmäßige Analyse der internen Dienstleistungsqualität.

Diese Zielsetzungen und Vorgaben sind unabhängig von einer architektonischen Plattform bzw. IT-Architektur formuliert. Somit ist die Überwachung des IT-Kontrollsystems in einer SOA-Umgebung grundsätzlich in ähnlicher Weise wie in einer herkömmlichen Umgebung zu strukturieren. Durch die feingranulare Struktur und die damit verbundene erhöhte Anzahl an Schnittstellen ist jedoch mit einem Mehraufwand in Bezug auf die Implementierung von Kontrollen zur Sicherstellung der vollständigen und richtigen Datenübertragung (siehe Abschnitt 2.3) zu rechnen. Darüber hinaus sind ggf. ausgelagerte Bereiche in das IT-Kontrollsystem mit einzubeziehen (siehe auch im folgenden Abschnitt).

2.6 IT-Outsourcing

Kernaussage des IDW RS FAIT 1 zum IT-Outsourcing ist, dass die Auswirkungen der Auslagerung auf das interne Kontrollsystem zu beachten sind. Je nach Grad der Auslagerung muss sich der Service Consumer als das auslagernde Unternehmen die Ordnungsmäßigkeit des internen Kontrollsystems des Service Provider nachweisen lassen und sich Einsichtrechte vertraglich einräumen lassen. Wichtig ist festzuhalten, dass die Verantwortung für die Einhaltung der Ordnungsmäßigkeits- und Sicherheitsanforderungen weiterhin bei den gesetzlichen Vertretern des auslagernden Unternehmens verbleibt. Neben den Vorgaben des IDW RS FAIT 1 sind bei Auslagerungen im Finanzsektor insbesondere auch die Regelungen des § 25a, Abs. 2 KWG (Kreditwesengesetz) und der MaRisk AT 9 [BaFin 2007] zu beachten.

Die Umsetzung des Internet-of-Service-Gedankens bringt umfangreiche und ggf. kleinteilige Auslagerungen von Diensten mit sich. Bei dieser kleinteiligen Auslagerung sind die Vorgaben bezüglich der Überwachung der ausgelagerten Bestandteile (u.a. auch solch allgemeine Vorgaben wie physische Zutrittsrechte zum Rechenzentrum, Brandschutz und Notfallvorkehrungen) weiterhin einzuhalten. Dies erfordert zunächst die Einbindung in das eigene interne Kontroll- und Überwachungssystem, z. B. durch eine zentrale Koordination der Auslagerung in Form eines SLA-Managements gemäß ITIL [Johannsen & Goeken 2007] beim Service Consumer. Auch in der jetzigen Situation stoßen Unternehmen hierbei an ihre Grenzen, wie z. B. bei der Überwachung von Auslagerungen des IT-Betriebs, der Anwendungsentwicklung oder des IT-Supports in Drittländer wie z. B. Indien. Neben der ausreichenden Gestaltung der Verträge, die entsprechende Prüfungs- und Kontrollrechte einräumen müssen, sind dedizierte Reports und Überwachungsvorgänge in SLAs zu vereinbaren.

Typische Kontrollhandlungen könnten hierbei sein:

- Regelmäßige Überprüfung von Berechtigungen auf ausgelagerte Dienste,
- Durchsicht von Protokollen, in denen Zugriffe auf Dienste gespeichert sind,
- Auswertung der Meldung von Verfügbarkeiten,
- Lieferung von Nachweisen der Durchführung spezifisch vereinbarter Leistungen (z. B. Durchführung von Datensicherungen) und
- Durchsicht von Revisionsberichten und Controls-Reports.

Insgesamt sind also ähnliche Kontroll- und Überwachungshandlungen wie bei herkömmlicher Auslagerung durchzuführen. Jedoch erhöht sich der Aufwand für deren Durchführung aufgrund einer ggf. erhöhten Anzahl von Service

Provider als Outsourcing-Dienstleister sowie dem Sichtbarwerden vormals anwendungsinterner (Schnittstellen-)Kontrollen durch die feingranulare Gestaltung von Services in einer SOA. Wirksame Maßnahmen zur Reduzierung eines entsprechenden Aufwands sind die Durchführung und Nutzung externer Zertifizierungen des internen Kontrollsystems der Outsourcing-Dienstleister (sog. Controls-Reports), z. B. auf Basis von SAS 70 [AICPA 1993] oder IDW PS 951 [IDW 2007], sowie die Definition und Abstimmung standardisierter Outsourcing-Verträge. Verträge könnten dabei mit den jeweiligen Gesetzen der Länder der Service Provider abgestimmt sein. Danach sollte bei Inanspruchnahme eines Service durch den Service Consumer gleichzeitig eine Vereinbarung auf Basis des Standardvertrags geschlossen werden. Im Gegenzug würde der Service Consumer regelmäßig Reports gemäß SAS 70 bzw. IDW PS 951 erhalten. Die Kosten für die ggf. aufwendige internationale Abstimmung der Verträge sowie der Überwachung des ausgelagerten Bereichs gemäß IDW RS FAIT 1 z. B. durch Zertifizierungen sind somit in die Kosten/Nutzen-Überlegungen mit einzubeziehen.

3 Zusammenfassung und Ausblick

Zusammenfassend ist festzuhalten, dass etablierte Maßnahmen zur Umsetzung regulatorischer Anforderungen in einem SOA-Umfeld zu überdenken und fortzuentwickeln sind. So werden beispielsweise Maßnahmen zur Sicherstellung der Datenintegrität und Vertraulichkeit wichtiger, da kleinteiligere Services mit deutlich höherem Aufkommen an Datenaustausch-Schnittstellen außerhalb von Anwendungen und teilweise sogar außerhalb des Unternehmens zum Einsatz kommen.

Die wesentlichen Maßnahmen zur Umsetzung der Anforderungen zur Ordnungsmäßigkeit in einem SOA-Umfeld betreffen u. a. die

1. Anpassung der IT-Strategie von einer »Silo-Architektur« zur prozessgetriebenen SOA,
2. Erweiterung des Gültigkeitsraumes der IT-Sicherheitsvorgaben auf alle Service Provider,
3. Vereinheitlichung und Zentralisierung des logischen Zugriffsschutzes z. B. durch Single-Sign-on,
4. Implementierung technischer Abstimmungskontrollen an den Schnittstellen sowie einer intensiven, spezialisierten Testphase im Softwareentwicklungsprozess,
5. Einbindung der ausgelagerten Services in das eigene Kontroll- und Überwachungssystem z. B. durch ein SLA-Management nach ITIL und
6. regelmäßige Überwachung der Auslagerungen z. B. mithilfe von Controls-Reports.

Im Hinblick auf eine effiziente Ausgestaltung besteht die Herausforderung hierbei darin, Kontrollen dort (und nur dort) zu implementieren, wo sie wesentliche Risiken adressieren und reduzieren. Die Voraussetzung hierfür ist die transparente Darstellung der Risiken sowie der bereits vorhandenen Kontrollmechanismen. Weiterhin sind zusätzliche Kosten durch erhöhte Kontrollaktivitäten in der Planung und Strategie zu berücksichtigen.

Abschließend ist festzuhalten, dass die bestehenden Anforderungen des IDW RS FAIT 1 auch in einem SOA-Umfeld anwendbar und von Bedeutung sind. Einzelne Aspekte sind von besonderer Relevanz (z. B. Sicherheitsanforderungen), andere (z. B. zu IT-Anwendungen und IT-gestützten Geschäftsprozessen) gehen von einer monolithischen IT-Architektur aus und sind in eine SOA-Welt zu übertragen und neu zu interpretieren. ◗

Danksagung

Teile dieses Beitrags entstanden im Rahmen der Forschung des E-Finance Lab Frankfurt am Main e.V. sowie des aus Mitteln des Bundesministeriums für Wirtschaft und Technologie unter dem Förderkennzeichen »01MQ07012« geförderten Forschungsvorhabens Theseus/TEXO. Die Verantwortung für den Inhalt liegt bei den Autoren.

4 Literatur

[AICPA 1993] *American Institute of Certified Public Accountants (AICPA):* Statement on Auditing Standards (SAS) No. 70: Service Organizations, Stand 31.03.1993.

[BaFin 2007] *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin):* Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 5/2007 der BaFin, 30.10.2007.

[IDW 2007] *Institut der Wirtschaftsprüfer (IDW):* IDW Prüfungsstandard 951 – Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen (IDW PS 951), Stand 19.09.2007.

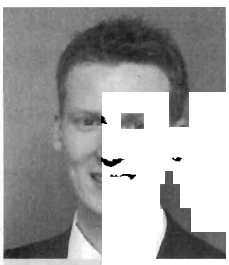
[IDW RS FAIT 1] *Institut der Wirtschaftsprüfer (IDW):* IDW Stellungnahme zur Rechnungslegung – Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1). In: WPg, Heft 21, S. 1157 ff., 2002.

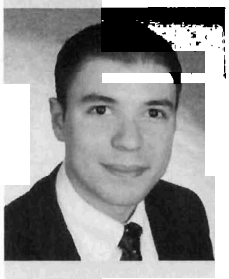
[Janiesch et al. 2008] *Janiesch, C.; Ruggaber, R.; Sure, Y.:* Eine Infrastruktur für das Internet der Dienste. In: HMD – Praxis der Wirtschaftsinformatik, 45. Jg., Heft 261, S. 71-79, dpunkt.verlag, 2008.

[Johannsen & Goeken 2007] *Johannsen, W.; Goeken, M.:* Referenzmodelle für IT-Governance – Strategische Effektivität und Effizienz mit COBIT, ITIL & Co. dpunkt.verlag, Heidelberg, 2007.

[Papazoglou 2003] *Papazoglou, M. P.:* Service-Oriented Computing: Concepts, Characteristics and Directions. In: 4th International Conference on Web Information Systems Engineering, 2003.

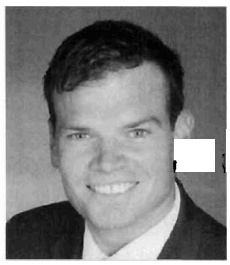
[Repp et al. 2009] *Repp, N.; Eckert, J.; Martin, W.:* SOA Check 2009: Status Quo und Trends im Vergleich zum SOA Check 2008 und 2007. IT-Verlag, 2009.





Marc Billeb
Achim Schäfer
Mourad Abbou
sind bei der PricewaterhouseCoopers AG WPG im Bereich Financial Services IT & Process Assurance tätig und beschäftigen sich im Rahmen von IT-System- und Prozessprüfungen sowie Beratungsprojekten mit modernen IT-Architekturen und deren Umsetzung. Ein Schwerpunkt der Tätigkeit ist zudem die Umsetzung regulatorischer Anforderungen in der IT und Geschäftsprozessen von Finanzdienstleistern.

WP Dipl.-Kfm. Marc Billeb
CISA
Dipl.-Inf. Achim Schäfer
CISA
Dipl.-Inf. (FH) Mourad Abbou
CISA
PricewaterhouseCoopers AG WPG
Olof-Palme-Str. 35
60439 Frankfurt am Main
{marc.billeb, achim.schaefer,
mourad.abbou}@de.pwc.com
www.pwc.com



Michael Niemann
Julian Eckert
Nicolas Repp
Ralf Steinmetz
sind am Fachgebiet Multimedia Kommunikation der Technischen Universität Darmstadt tätig. Im Rahmen der Forschungsarbeiten der Forschungsgruppe IT-Architekturen untersuchen sie u.a. Governance in heterogenen Systemen sowie das Management von Dienstgüte und Sicherheit in IT-Architekturen

Dipl.-Wirtsch.-Ing. Michael Niemann
Dipl.-Wirtsch.-Ing. Julian Eckert
Dr.-Ing. Nicolas Repp
Prof. Dr.-Ing. Ralf Steinmetz
Technische Universität Darmstadt
Fachgebiet Multimedia Kommunikation
Rundeturmstr. 10
64283 Darmstadt
{Michael.Niemann, Julian.Eckert,
Nicolas.Repp, Ralf.Steinmetz}
@kom.tu-darmstadt.de
www.kom.tu-darmstadt.de