Den Stein ins Rollen bringen

Sarbanes-Oxley bei der Xerox GmbH Deutschland

Autorin
Dr. Jutta Jessenberger

studierte Statistik an der Universität Dortmund und der University of Sheffield (UK). Nach einer Tätigkeit bei der Mars GmbH promovierte sie an der Universität Dortmund und durchlief danach verschiedene Management-Positionen bei AC Nielsen, Hamburg und bei der OnVista AG, Köln, wo sie zuletzt als Director Content Services tätig war. Derzeit ist sie Prokuristin bei der Xerox GmbH und Black Belt im Xerox Lean Six Sigma Programm sowie verantwortlich für das Deployment dieser Strategie in Deutschland.

Autor
Gundolf Zimmermann

studierte Wirtschaftswissenschaften an der Ruhr-Universität Bochum. Nach Tätigkeiten bei der Arthur Andersen GmbH und der Merckle/ratiopharm GmbH war er zuletzt Tax Manager bei der Wal-Mart Germany GmbH & Co KG. Derzeit ist er als Prokurist und Chief Accountant der Xerox GmbH verantwortlich für die Bereiche Rechnungswesen und Steuern.

Die beiden Ziele des im Juli 2002 vom amerikanischen Kongress verabschiedeten Sarbanes-Oxley-Acts (SOA) – Sicherstellung korrekter Veröffentlichungen (Section 302) sowie Vorhandensein und Testat eines internen Kontrollsystems (Section 404) – haben auf die Xerox GmbH als (mittelbare) Tochter eines US-amerikanischen Unternehmens beträchtliche Auswirkungen. Der vorliegende Beitrag stellt das bei der Xerox GmbH durchgeführte Projekt zur Einführung des internen Kontrollsystems nach Section 404 vor. Dabei werden die Herausforderungen beschrieben, die sich durch die anfängliche Unsicherheit in Bezug auf den notwendigen Dokumentationsumfang, die Xerox-Konzernstruktur sowie die knappen Zeitvorgaben ergaben sowie die gefundenen Lösungswege dargestellt. Den Abschluss bildet ein Ausblick auf den in der Zukunft notwendigen Prozess zur Erfüllung der SOA-Kriterien, seine Auswirkung auf das operative Geschäft und seine Wirksamkeit in Bezug auf das Risikomanagement.

Ausgangslage

Die Xerox Corporation unterliegt als US-amerikanisches Unternehmen mit Stammsitz in Stamford, Connecticut, und Notierung an der New York Stock Exchange (NYSE) sowie der Chicago Stock Exchange (CHX) strengeren Kontrollvorschriften als Unternehmen mit Stammsitz im außer-amerikanischen Ausland. Insbesondere muss die Xerox Corporation für die Erfüllung des Sarbanes-Oxley-Acts schon zum 31.12.2004 ein erfolgreiches Testat nachweisen. Damit waren für die Xerox Corporation mit der Verabschiedung des SOA eine Reihe von Aufgaben klar, die zur Erfüllung der Anforderungen durchgeführt werden mussten: die Bestandsaufnahme der Unternehmensprozesse, die Identifikation der notwendigen Schritte zur Erlangung des SOA-Testats sowie die Umsetzung der identifizierten Aktionen und Maßnahmen.

Gleichzeitig müssen die Anforderungen des SOA konzernweit erfüllt sein – dies erfordert auch eine entsprechende Transparenz der Finanzberichterstattung bei direkten und mittelbaren Tochterunternehmen. Aus diesem Grund war und ist von vornherein der weltweite Umfang des Projekts gegeben. Die Projektstruktur erstreckt sich über drei Projektebenen – weltweit, regional (Asien, Amerika und Europa) und lokal (Ländergesellschaften). Als oberstes Aufsichtsgremium fungiert das Steering Committee, dem Mitglieder der Unternehmensleitung sowie Vertreter der testierenden Wirtschaftsprüfungsgesellschaft (eine der „Big Four“) angehören. Das Audit Committee fungiert als Überwachungsgremium des Steering Committees und ist in seiner Funktion durch den SOA vorgeschrieben.

Wichtig zum Verständnis der hier beschriebenen Vorgehensweise ist die Unterscheidung der zwei mit dem Sarbanes-Oxley Act verbundenen Aspekte: SOA-Projekt und SOA-Prozess. Das SOA-Projekt beschreibt den einmaligen Anfangsaufwand zur Einführung des internen Kontrollsystems mit dem initialen Aufsetzen der Dokumentation und Vorgaben. Das dort erarbeitete Regelwerk bildet dann die Grundlage zur regelmäßigen nachfolgenden Durchführung des SOA-Prozesses mit seinem wiederkehrenden Zyklus Prozesses von Dokumentation, Überprüfung und Audit.

Die einzelnen Teilprojekte werden zentral überwacht von der amerikanischen Projektleitung mit direkter Berichtslinie an das Steering Committee, sowie einer europäischen und jeweils einer Projektleitung in den einzelnen Ländergesellschaften. Das SOA-Projekt wurde zusätzlich in der Anfangsphase durch Repräsentanten der Wirtschaftsprüfer auf diesen drei Ebenen begleitet. Die Einbeziehung der Wirtschaftsprüfer zum Start war unerlässlich, da der SOA keine konkrete Anweisung für die Unternehmen enthält, wie er zu erfüllen ist. Stattdessen ist eine Ableitung der Anforderungen nur aus den Vorgaben für die Wirtschaftsprüfungsgesellschaften möglich, die vom PCAOB (Public Company Accounting Oversight Board) in der Umsetzungsphase des SOA nach und nach erarbeitet wurden und werden. Auf diese Weise stellte Xerox sicher, dass die durchgeführten Aktionen jederzeit in Art und Umfang dem Projektziel entsprachen.

Weiterhin stehen – ebenfalls über alle drei Projektebenen – Mitarbeiter der ausgegliederten internen Firmenrevision in den Projektteams unterstützend zur Verfügung. Der Informationsaustausch und die Projektkoordination auf europäischer Ebene werden durch wöchentliche Telefonkonferenzen sowie ein web-basiertes, weltweit eingesetztes EDV-Programm zur Dokumentation des Projektfortschritts gesichert.

Die deutsche (lokale) Beteiligung am weltweit gesteuerten Sarbanes-Oxley-Projekt der Xerox Corporation wurde mit einer Tagung im März 2003 in der europäischen Konzernzentrale in London initiiert.

Phasen der Projektarbeit

Die Anforderung des SOA an eine funktionierende und zutreffende Finanzberichterstattung ist die Dokumentation und der Nachweis der Überwachung der Prozesse, die Einfluss auf die Konten der Bilanz und Gewinn-/Verlustrechnung haben.

Für den Projektplan und den nachfolgenden SOA-Prozess identifizierte das Projektteam fünf Schritte: Scoping, Mapping, Documenting, Testing und Auditing. Dabei ist zu beachten, dass die ersten vier Schritte (Scoping bis Testing) intern im Unternehmen, der fünfte hingegen von den externen Wirtschaftsprüfern durchgeführt wird.

Im SOA-Projekt erfordern Scoping, Mapping und Documenting vor allem Einmalaufwand und bilden die Grundlage für das erstmalige Testing und Auditing. Während des SOA-Prozesses werden dann alle diese Phasen zyklisch durchlaufen, wobei Scoping, Mapping und Documenting erwartungsgemäß weniger Umfang haben werden als in der Startphase und sich auf einen Review und eventuell notwendige Anpassungen beschränken können.

Scoping beinhaltet die Erfassung aller wesentlichen Konten, wobei in Abstimmung mit dem Konzern und den Wirtschaftsprüfern eine Wesentlichkeitsgrenze („materiality“) von 5 Millionen US-Dollar festgelegt wurde.

Im darauf folgenden **Mapping** werden alle Prozesse, die so genannten Zyklen, identifiziert, die Einfluss auf die im Scoping definierten Konten haben. Unter den elf identifizierten wichtigen Zyklen befinden sich unter anderem der Umsatz-Prozess (revenue cycle), Buchhaltungs-Prozess (accounting cycle), Unternehmensbesteuerungs-Prozess (tax cycle) und der Leasing-Prozess (leasing cycle).

Diese werden dann im **Documenting** zunächst mit Hilfe von Flussdiagrammen beschrieben. In fast klassischer Qualitätssicherungsmethodik einer Fehler-Möglichkeits- und Einfluss-Analyse (FMEA) werden dann die Risiken (so genannte WCGW's – „What can go wrong?“) und Kontrollen (Controls) bestimmt und die Wahrscheinlichkeit für die Entdeckung eines unerwünschten Zustandes festgestellt. Für jeden Prozessschritt werden bei dieser Vorgehensweise alle potenziellen Risiken und die dazu existierenden Überwachungsmaßnahmen eingehend beschrieben und detailliert bewertet (Risk/Control Ratings). Im Verlauf der Dokumentation wurden für die bestehenden elf Zyklen insgesamt über 200 Key Controls und zusätzliche Supporting Controls beschrieben.

Als Grundlage für die Risiko-Bewertung dienen die so genannten Assertions. Hiermit werden diejenigen Eigenschaften bezeichnet, die dem Anteilseigner mit der Unterschrift unter die Finanzberichterstattung bestätigt werden, wie beispielsweise Existence (Existenz der Vermögensgegenstände/Verbindlichkeiten), Completeness (Vollständigkeit der berichteten Transaktionen) etc. Für jeden Prozess-Schritt werden das Risiko einer Verletzung der Assertions und die Wahrscheinlichkeit des Auftretens dieses Risikos bestimmt.

Risk Ratings werden dabei aufgrund ihrer Bedeutung und der Wahrscheinlichkeit ihres Auftretens unterschieden. Ein Risiko mit „kritischer“ Einstufung ist beispielsweise als Risiko von über 20 Millionen US-Dollar definiert, die Wahrschein-

lichkeit seines Eintretens möglicherweise mit „remote“, das heißt mit weniger als 5 Prozent. Die Wahrscheinlichkeiten werden dabei sowohl ohne also auch unter Einbeziehung der bestehenden Überwachungsmethodik bestimmt (inherent beziehungsweise residual risk).

Die Controls werden hinsichtlich der Arten von Kontrollen beschrieben – vorbeugend, entdeckend, manuell, automatisch und computergestützt. Gleichzeitig wird für jede Kontrolle ihre Wichtigkeit („key control“, „supporting control“) und die Frequenz der durchzuführenden Tests angegeben.

Das Control Rating wird bezüglich der Effektivität vergeben – beispielsweise bedeutet der Wert „optimized“, dass diese Überwachungsmethode mit Echtzeit-Monitoring durch das Management in die interne Revision aufgenommen ist. Sie unterliegt ebenfalls dem Prozess der kontinuierlichen Verbesserung. Jede Kontrolle wird im Testing vor der externen Bewertung in der Control Conclusion als effektiv oder ineffektiv (oder nicht untersucht) bewertet. Eine zusätzliche Klasse von Überwachungsmaßnahmen sind die Monitoring Controls, die ihrerseits die Key oder Supporting Controls überwachen, etwa durch ein Management Review oder institutionalisierte interne Kontrollen.

Das „Final Risk Assessment“ schließlich gibt an, ob bezüglich der beschriebenen Risiken effektive Überwachungsmethodiken bestehen. Wie bei der Control Conclusion gibt es dort nur zwei mögliche Bewertungen: (Risk) Mitigated oder Unmitigated. Weiterhin existiert ein weiterer Abschnitt „Information & Communication“, in dem jede Art von Information bezüglich des Prozesses oder der Kontrollen festgehalten wird. Er umfasst beispielsweise Arbeitsanweisungen, interne Vorgaben, Schulungen oder Bekanntmachungen.

Im Schritt **Testing** werden zunächst die notwendigen Testpläne definiert beziehungsweise dokumentiert; dann werden die in der Dokumentationsphase beschriebenen Kontrollen in internen Tests auf Design und Effektivität überprüft und zuletzt beim **Auditing** extern von den Wirtschaftsprüfern abgenommen.

Umsetzung des SOA in Deutschland – Lessons Learned

Die Xerox GmbH in Deutschland ist ein Vertriebs- und Serviceunternehmen. Die wesentlichen Unternehmensprozesse sind der Vertriebsprozess mit der Pflege der Kundenkontakte, Erstellung und Versand des Angebots und Vertragsabschluss beziehungsweise der Serviceprozess zur Sicherstellung der gewünschten Kundenqualitat. Unmittelbar darauf folgen die administrativen Prozesse – Vertragsprüfung, Vertragseingabe, Maschinen- oder Servicelieferung, Rechnungserstellung und Verbuchung der eingehenden Beträge auf den Konten. Alle diese Prozesse sind – ebenso wie die in der Buchhaltung ablaufenden Aufgaben – wichtig im Sinne von Sarbanes-Oxley. Unterstützend wirken die Prozesse in der Finanzplanung, im Personalbereich sowie der Infrastruktur (Einkauf, Facility Management, IT), ebenfalls mit Auswirkungen auf SOA-relevante Konten.

Damit haben fast alle Prozesse innerhalb des Unternehmens Einfluss auf ein Berichtskonto – sei es die Angebotserstellung, Vertragsabschluss und -eingabe oder die Verbuchung einer Servicerechnung – und die Aufgabe der Erlangung des SOA-Testats ist gleichbedeutend mit einer Dokumentation aller Unternehmensprozesse und der sie betreffenden Überwachungs- und Kontrollmechanismen.

Bei der Umsetzung des SOA-Projekts in Deutschland konnten zwei große Vorteile genutzt werden: einerseits das Vorhandensein eines bereits existierenden, gut geführten und stringent gelebten internen Kontrollsystems durch den weltweit gesteuerten Internal Controls Management Process (ICMP) und andererseits das in Deutschland vorhandene vollständig integrierte Buchhaltungs-System.

Der ICMP-Prozess deckt alle relevanten Unternehmensprozesse ab im Hinblick auf deren Existenz und Effizienz mit dem Ziel einer Effizienzsteigerung. Im Gegensatz zum SOA fokussiert sich dieser Prozess damit nicht auf die Finanzberichterstattung. Dennoch ist er für das SOA-Projekt hilfreich zur Identifikation bestehender Prozesse mit möglichem Einfluss auf die Berichtskonten. Der zweite positive Aspekt lag und liegt in der mit ihm verbundenen Kultur eines internen Kontrollsystems. Durch den ICMP-Prozess und seine bekannte Wichtigkeit quer durch das Unternehmen war die Bedeutung und der Inhalt des SOA-Prozesses bei der Xerox GmbH deutlich leichter zu vermitteln als in einem Unternehmen ohne ein derartiges System.

Der zweite Vorteil war die Existenz eines vollständig integrierten Buchhaltungs-Systems, mit dessen Hilfe alle Vorgänge in der deutschen Xerox-Gesellschaft abgebildet und unterstützt werden. Insbesondere war bei den System-Be-

ratern (den so genannten „Business System Consultants“), die für die im System abgebildeten Prozesse verantwortlich sind, die notwendige Expertise und das Wissen über die internen Geschäftsabläufe im Detail vorhanden. Diese Business System Consultants waren demzufolge auch für einen großen Teil der Dokumentation – in Absprache mit den Fachverantwortlichen – zuständig. Auf diese Weise wurden die Fachverantwortlichen im Tagesgeschäft entlastet, wobei gleichzeitig der notwendige Detailgrad sichergestellt werden konnte.

Als ausgesprochen schwierig zum Projektstart erwies sich das Fehlen detaillierter Anleitungen zu Art und Tiefe der geforderten Dokumentation, so dass anfangs eine gewisse Unsicherheit über Inhalt und Umfang bestand. Die einzige Möglichkeit für die Bestimmung einer solchen Anleitung boten die Anweisungen für die Wirtschaftsprüfer, auf deren Grundlage das Vorgehen für die Erfüllung des SOA indirekt abgeleitet werden konnte.

Xerox entschied sich aufgrund des Zeitmangels gegen ein weiteres Abwarten der Klärung und für die Entwicklung eines eigenen Standards zur einheitlichen Dokumentation, verbunden mit Anleitungen zu Inhalt und Detailgrad. In dieser Anfangsphase war die Einbeziehung der Wirtschaftsprüfer von besonderer Bedeutung, um auch aus ihrer Sicht die Übereinstimmung mit den Anforderungen zu gewährleisten und nicht im Nachhinein nachbessern zu müssen. Trotzdem mussten selbstverständlich aufgrund der im Projekt gemachten Erfahrungen im weiteren Verlauf Anpassungen vorgenommen werden. Beispielsweise erwies sich die Bestimmung der Wesentlichkeitsgrenze als nicht einfach – hier wurde dann in Abstimmung mit der Wirtschaftsprüfung unter Berücksichtigung der Anzahl der Konten pragmatisch die Grenze von 5 Millionen US-Dollar definiert. Alle Prozesse (Zyklen), die Einfluss auf diese Konten nehmen/nahmen, wurden dann in der eigentlichen Dokumentation (wie oben bereits erwähnt) beschrieben.

Die beschriebene Vorgehensweise der Definition, Ergänzung und Änderung der Vorgaben führte dann letztendlich dazu, dass die Dokumentation der Xerox GmbH sogar als Benchmark auch für die anderen Ländergesellschaften herangezogen wurde.

Ausschlaggebend war vor allem die stringente Projektleitung mit regelmäßigen Meetings und Reviews zur Überprüfung des Fortschritts, aber auch der Qualität der Dokumentation, so dass man einen einheitlichen Standard für alle Prozesse vorweisen konnte und kann.

Um bei der Prüfung zur Erlangung des eigentlichen Testats vorbereitet zu sein, führte die Projektleitung im August/September außerdem einen so genannten „Dry Run“ durch, also eine Simulation des Testings mit (internen) Prüfern unter realistischen Bedingungen, um den Zwischenstand des Projektes zu bestimmen sowie die eventuell noch auftretenden Probleme und Herausforderungen priorisieren und in der Zeit bis zum Jahresende beheben zu können. Der aktuelle Status ist, dass es keine „ineffective“ getesteten Kontrollen mehr gibt.

Eines der wichtigen Ergebnisse dieses Dry Run war, dass eine Reihe von Key Controls gestrichen werden konnte und in Zukunft nicht mehr getestet werden muss. Alleine für dieses Ergebnis mit der verbundenen Kostenreduktion hat sich der zusätzliche Aufwand des Dry Runs bezahlt gemacht.

Aus Sicht der Projektleitung gab es für das SOA-Projekt drei Erfolgsfaktoren – zunächst die stringente Projektleitung, bei der zu jeder Zeit die Ausrichtung an denselben Zielen mit denselben Grundlagen gewährleistet war, sowie die Einbeziehung der notwendigen Ressourcen mit fachlichen und technischen Spezialisten (den Fachverantwortlichen und den Business Systems Consultants). Als besonders hilfreich in der Anfangsphase hat sich darüber hinaus die Einbeziehung der Wirtschaftsprüfer und der internen Revision erwiesen. Beide Partner konnten aufgrund ihrer Erfahrungen mit anderen Unternehmen andere Sichtweisen auf die Problematik bieten. Xerox gab die enge Zusammenarbeit mit den Prüfern größere Sicherheit, auf dem richtigen Weg zum Ziel, der Erlangung des SOA-Testats, zu sein.

Diskussion und Ausblick

Eine der wesentlichen Erkenntnisse aus dem SOA-Projekt war, dass entgegen der eigentlichen Zielsetzung dieses Gesetz für sich genommen nicht ausreicht, um die Risiken eines Unternehmens umfassend abzudecken. Bei einem Vergleich mit dem bereits existierenden internen Kontrollsystem ICMP ergab sich, dass ungefähr 50 Prozent der bereits durch ICMP abgedeckten Prozesse und Risiken nicht durch den SOA erfasst werden. Aus diesem Grund entschied Xerox, das bestehende interne Kontrollsystem beizubehalten und nur die relevanten Teile aus diesem System durch SOA-konforme

Vorgehensweisen zu ersetzen und zertifizieren zu lassen.

Ohne den Sarbanes-Oxley-Act hätte Xerox mit Sicherheit nicht den Aufwand betrieben, nur den die Finanzberichterstattung betreffenden Teil des bestehenden Systems in dem jetzt verwendeten Detailgrad zu dokumentieren und zu testen. Ein Unternehmen hat zuerst und allererst die Aufgabe, profitabel zu sein, den Aktienkurs zu maximieren und auf diese Weise positiv auf Anteilseigner, Mitarbeiter und Umwelt einzuwirken. Dass dazu ein korrektes Finanz-Reporting gehört, ist selbstverständlich und bereits vielfach durch lokale und internationale Gesetze geregelt. Die prominenten Beispiele, deren Zusammenbruch der Anlass für den Erlass des SOA war – Enron, WorldCom etc. – hätten jedoch schon mit den bestehenden gesetzlichen Grundlagen entdeckt werden können und müssen. Inwieweit der Sarbanes-Oxley-Act nun vorsätzlich falsche Berichterstattung verhindert, bleibt abzuwarten.

Aus Unternehmenssicht werden durch den SOA zunächst einmal Kosten durch Dokumentation und Berichterstattung verursacht. Kosten, die zusätzlich zu den bereits bestehenden Reporting-Pflichten aufzubringen sind.

Zur Unternehmenssteuerung sind die erhobenen Prozesse, Risiken und Kontrollen nur eingeschränkt zu verwenden, da sich der SOA vor allem auf das Vorhandensein eines internen Kontrollsystems konzentriert. Die eigentlichen Geschäftsergebnisse stehen in diesem Zusammenhang nicht im Fokus. In dieser Beziehung ist der SOA sogar fast vergleichbar mit der DIN ISO 9000ff., in der ganz ähnlich zwar das Vorhandensein eines Qualitätsmanagementsystems und der dazugehörigen kontinuierlichen Verbesserung und Anpassung bestätigt wird, die eigentlichen Resultate aber nicht zertifiziert werden. Bei beiden Systemen wird dann postuliert, dass das Vorhandensein der Systematik auch die Zuverlässigkeit der Resultate zwingend nach sich zieht. Nichtsdestoweniger kann der SOA einem Unternehmen bei der Verbesserung seiner Prozesse helfen und auch bei Xerox sind auf diese Weise in der Tat ein paar kleinere Prozesslücken geschlossen worden.

Der nächste große Schritt im Sinne des SOA für die Xerox GmbH und die Xerox Corporation ist nun die Erlangung des Testats zum Jahresende. Aus der Erkenntnis heraus, dass die Erlangung des SOA-Testats nicht für ein umfassendes Risikomanagement ausreicht, arbeitet das Projektteam außerdem gleichzeitig an der Entwicklung eines unternehmensübergreifenden Risikomanagement-Prozesses im Sinne des KonTraG. Dieser wird sowohl den SOA-Prozess als auch den überarbeiteten ICMP-Prozess beinhalten. Darüber hinaus wird das neue umfassende Risikomanagement-System andere Risiken überprüfen und steuern wie beispielsweise Budgetüberschreitungen, Rechtsfälle, Umstrukturierungen, Kunden-/Lieferantenrisiken oder IT-Risiken. Mit der Integration der nach US-amerikanischem und deutschem Recht geforderten Risikomanagement-Systeme hat die deutsche Geschäftsleitung eine sehr gute Ausgangslage geschaffen für eine optimale Steuerung etwa auftretender Risiken. ■