

SOX-Compliance wirbelt IT durcheinander

Lästige Notwendigkeit oder

Wer glaubt, eine fehlerfrei arbeitende IT sei bereits die halbe „SOX“- (Sarbanes-Oxley Act-) Compliance, hat weit gefehlt. IT-Prozesse auf Best-Practices Niveau sind bestenfalls eine solide Ausgangsposition, da die SOX Anforderungen an Risikominimierung weit darüber hinausgehen. SOX-Compliance ist aber nicht nur notwendige Bürokratie – richtig angefasst steckt darin vielmehr die Chance für eine umfassende IT-Optimierung.



Sind Unternehmen selbst oder deren Konzernmütter an der US-Börse notiert, unterliegen sie dem Sarbanes-Oxley Act. Daraus ergibt sich auch für viele deutsche Unternehmen die Notwendigkeit für die Erlangung der SOX Compliance, die Firmen und Aktionäre vor betrügerischen Machenschaften schützen soll, wie sie nach den großen Pleitefällen bei Enron oder Worldcom aufgedeckt wurden. SOX Compliance bedeutet dabei auf den

Punkt gebracht die Sicherstellung der Richtigkeit der erstellten Finanzberichte.

Der Begriff Compliance wird dabei verstanden als „Einhaltung rechtlicher Regelungen“. Direkt übersetzt heisst Compliance „Fügsamkeit“ oder auch „Folgsamkeit“, was angesichts der Marktdynamik rund um die SOX Compliance die Situation durchaus treffend beschreibt:

Es geht für die betroffenen Unternehmen längst nicht mehr nur darum,

gesetzliche Regulierungsvorschriften zu erfüllen, sondern weit darüber hinaus um die Sicherung von bestehenden Marktpositionen sowie um die Wahrung von Optionen auf die Ausweitung des Geschäfts auf neue Marktfelder. Während viele nicht-US-amerikanische Unternehmen auf Grund der nötigen Anstrengungen zur Erlangung der SOX Compliance den Rückzug aus diesem Kapitalmarkt erwägen, sehen viele Wettbewerber gerade darin ihre Chance

Chance?



re Chancen gerade in der zurückhaltenden Wartestellung. Während sich zahlreiche Wettbewerber Hals über Kopf in SOX Compliance-Projekte stürzen, die ein Investment oft in relevanter Größenordnung bezogen auf die bestehenden Gewinnmargen erfordern, wännen sie ihren Vorteil aus der Ersparnis dieses Investments. Deren Argumentation basiert allerdings mehrheitlich auf der Auffassung, dass der Nutzen der SOX Compliance lediglich in der Erfüllung von Regulierungsvorschriften besteht und es keinen darüber hinausgehenden Einfluss auf das Marktgeschehen hat.

Was bei dieser Diskussionen oft in den Hintergrund gerät: Unabhängig von der Einschätzung rein marktrelevanter Nutzenfaktoren bietet die SOX Compliance auch die Basis für eine vollumfängliche „Renovierung“ der IT. Schließlich sorgt die tief greifende Überprüfung aller finanzrelevanten Prozesse vor allem in Bezug auf die Sicherheit und Stabilität der darunter liegenden IT-Prozesse sowie IT-Systeme automatisch für einen aktuellen Fitness-Check der IT. Hierin liegt die Chance für die IT, sich als erfolgsrelevanter Faktor im Unternehmen völlig neu zu positionieren.

Wieviel Geld muss für die SOX Compliance in die Hand genommen werden?

Betrachtet man die aktuellen Erfahrungswerte für die Kosten der SOX Compliance, so wird auch schnell deutlich, vor welcher Dimension eines Investments sich viele Unternehmen scheuen: Allein die Kosten für die Implementierung der für die IT-Organisation relevanten „SOX Section 404“ beziffert der Unternehmerverband FEI (Financial Executives International) in den USA auf durchschnittlich

4,36 Millionen US-Dollar. In Europa sind die Nennungen weitaus höherer Beträge im zweistelligen Millionenbereich kein Einzelfall.

Diese Summen zeigen, dass es sich hierbei um sehr umfangreiche Projekte handelt und nicht einfach nur um die Dokumentation und Einhaltung bestehender Abläufe sowie deren Zertifizierung durch einen Wirtschaftsprüfer. Die Herstellung der SOX Compliance fordert einem Unternehmen eine ungleich größere Investition ab als es zum Beispiel für die Erlangung eines ISO

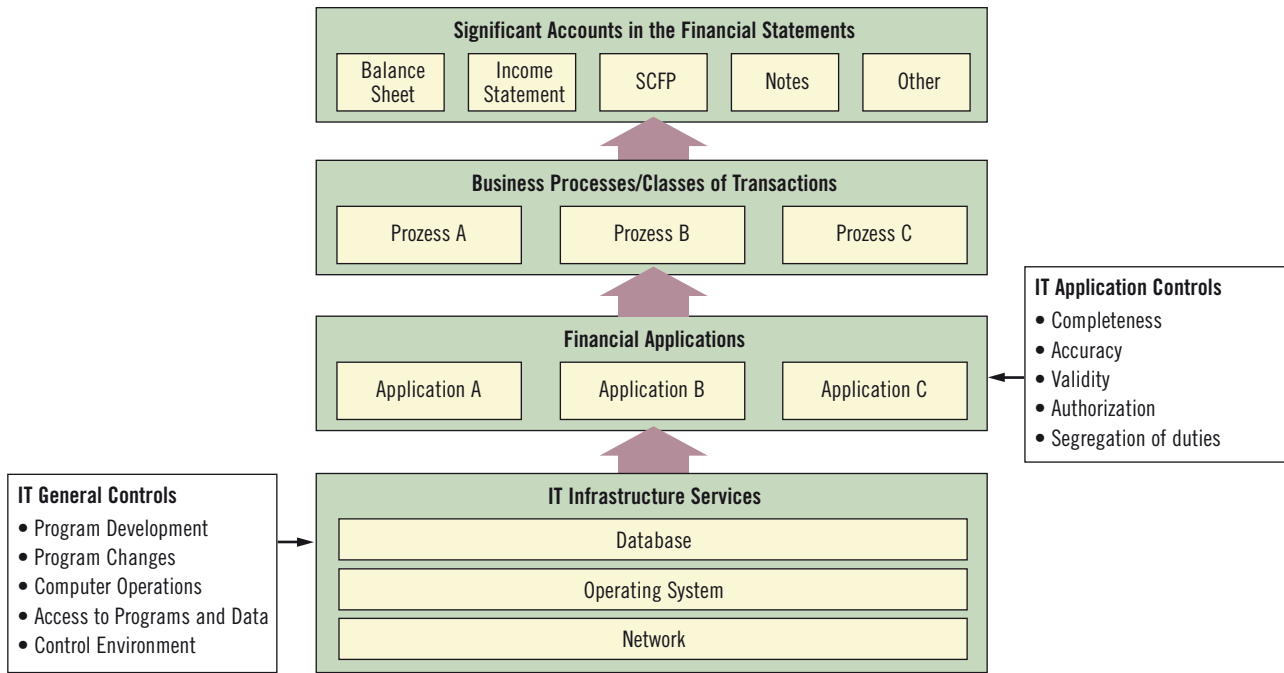
zu einer Verbesserung ihrer Wettbewerbssituation gegenüber den Rückzügler, die sich nicht „fügen“ wollen. Hierbei spielen sowohl öffentlichkeitswirksame PR-Effekte eine Rolle als auch die schlichte Überlegung, im Wettlauf um die Anlegergunst und den damit verbundenen Zugang zu weiteren Finanzmitteln Plätze gut zu machen.

Vor diesem Hintergrund haben viele Unternehmen auch außerhalb der USA die SOX Compliance als ein neues viel

versprechendes Schlachtfeld im Wettbewerb ausgemacht und sehen darin große Chancen für ihre Zukunft. Laut der Aberdeen-Studie „SOX Compliance and Automation“ verfügen 68 Prozent der betroffenen Firmen bereits über eine entsprechende SOX Roadmap. Sogar 74 Prozent wollen noch in diesem Jahr die SOX Compliance für ihre IT erlangen.

Viele zögernde und nicht „folgsame“ Unternehmen sehen wiederum ih-

IT Controls



Quelle: IT Governance Institute

Bild 1: Der Fokus der „IT Application Controls“ liegt auf den Business-Anwendungen. Dagegen beschreiben die „IT General Controls“ die Kontrollprozesse der IT Infrastruktur.

9000 Zertifikats erforderlich war. Der Löwenanteil entfällt dabei auf die IT als Basis des gesamten operativen Wirkens im Unternehmen.

Wieviel IT verlangt die SOX Compliance?

Die Finanzberichterstattung resultiert aus den Geschäftsprozessen, und zwar nicht nur aus denen im Finanzwesen, sondern aus allen Abläufen, die einen Einfluss auf das Finanzergebnis haben. Bis auf Randthemen, die sich komplett außerhalb des Kerngeschäfts bewegen wie zum Beispiel die Reservierung von Besucherparkplätzen gilt das erst einmal grundsätzlich für alle Geschäftsprozesse im Unternehmen.

Da die Geschäftsprozesse nahezu vollständig in Business Applikationen implementiert sind, ist die gesamte Anwendungslandschaft mit Relevanz für die Finanzberichte in die SOX Compliance einzubeziehen. Die Business-Applikationen basieren wiederum auf der installierten IT Infrastruktur, die dadurch ebenfalls im Fokus der SOX Compliance liegt. Dazu gehören alle Ebenen der IT Infrastruktur (Bild 1):

- Datenbanken
- Betriebssysteme
- Netzwerke

Eine SOX Compliance ist also eine Herausforderung für die gesamte IT. Aber muss 100% SOX-Compliance von Anfang an angestrebt werden? Ist 50% nicht besser als nichts? Best-Practices IT-Ansätze erlauben eine Diskussion über halbe Kosten, insbesondere im Verhältnis zu nicht 100%igen Leistungen. Bei der SOX Compliance hingegen geht es nicht um die Bewertung von Leistungsstufen im Sinne einer Wirtschaftlichkeitsbetrachtung, sondern um die Herstellung von größtmöglicher Sicherheit auf Basis eliminiertes und nicht nur reduzierter Risiken. Daraus ergibt sich eine weitestgehende Kompromisslosigkeit vor allem in Bezug auf die IT. Eine halbe SOX Compliance der IT ist gleich bedeutend mit keiner SOX Compliance. Viel schlimmer noch: Ein Unternehmen, bei dem sich eine „halbe SOX Compliance“ explizit in einer Abschlussprüfung herausstellen würde, hätte einen immensen Image-Schaden zu tragen, da in diesem Fall den Spekulationen über die

Ordnungsmäßigkeit der Finanzberichte Tür und Tor offen stehen würden.

Sellt die SOX Compliance die komplette IT auf den Kopf?

Manager sind zunächst vom SOX Abschnitt 404 („Section 404“) betroffen, der die Dokumentationspflicht von Kontrollprozessen umfasst. Das Management steht hier in der Verpflichtung, die Einführung angemessener interner Kontrollabläufe zur Finanzberichterstattung nachzuweisen. Da die Prozesse und Kontrollabläufe weitestgehend in IT-Systemen implementiert sind, müssen diese umfangreich bewertet werden hinsichtlich der Sicherstellung einwandfrei erstellter Finanzberichte.

Wer diese Forderung allerdings nur als erweiterte Plausibilität- und Konsistenzprüfung der IT-Systeme in der Fi-



nanzbuchhaltung versteht, hat weit gefehlt. Der SOX Abschnitt 404 umfasst alle Applikationen, die mit den Finanzapplikationen in Zusammenhang stehen im Sinne der Geschäftsprozesse oder mehr noch: die irgendeine Form von Schnittstellen zu den Finanzapplikationen aufweisen.

Dazu gehören meistens schlichtweg alle Business-Applikationen bis hin zum Beispiel zu Workflow- und Dokumentenmanagement-Systemen, die Vertragsdokumente verwalten, in denen für die Finanzberichte relevante Informationen stehen. Und welcher Vertrag in einem Unternehmen hat nicht irgendeine finanzielle Relevanz? In der SOX-Sprache sind diese die Applikationen betreffenden Kontrollabläufe als „IT Application Controls“ definiert (Bild 1).

In den „IT Application Controls“ werden die Kontrollabläufe in den anwendungsbezogenen Prozessen überprüft hinsichtlich:

- Vollständigkeit
- Genauigkeit
- Richtigkeit
- Berechtigung
- Verteilung der Verantwortung

Der Fokus der „IT Application Controls“ liegt allerdings nicht nur auf den dedizierten Business-Anwendungen. Soweit zum Beispiel in E-Mail-Systemen Vorgänge abgebildet sind, aus denen letztendlich eine Relevanz für die Finanzberichte abgeleitet werden kann, sind diese ebenfalls in die SOX Compliance einzubeziehen. Also müssen auch diese unterstützenden Systeme, die nicht direkt zur Abbildung wiederkehrender vorgegebener Geschäftsprozesse genutzt werden, entsprechend berücksichtigt werden, denn es wird kaum ein Unternehmen geben, das sein E-Mail-System nur für nicht-finanzrelevante Korrespondenz wie zum Beispiel die Ankündigung eines Betriebsfestes nutzt.

Die „IT Application Controls“ sind jedoch nur die halbe Miete. Die andere

Hälfte besteht in den „IT General Controls“, die die Kontrollprozesse der IT Infrastruktur beschreiben (s. Abb.1). Die Überprüfung der Kontrollabläufe in den „IT General Controls“ erfolgt unter folgenden Kernaspekten:

- Entwicklungsprozesse
- Änderungs-Management
- Systembetrieb
- Zugriff auf Daten und Anwendungen
- Kontrollmechanismen

Es reicht hierbei jedoch nicht aus, ordnungsgemäße Prozesse sicherzustellen. SOX Compliance bedeutet auch entsprechende Kontrollabläufe zu installieren, die jegliche Umgehung der sicheren Prozesse ausschließen und darüber hinaus belegen, dass keine Umgehungen stattgefunden haben.

Ein Beispiel hierzu: Der Nachweis, dass der Antrag auf Änderung von Benutzerberechtigungen wie von der Abteilungsleitung und der IT-Leitung abgezeichnet zeitnah, richtig und vollständig durchgeführt wurde, reicht nicht aus. Erst der Nachweis, dass Kontrollprozesse installiert sind, die ausgehend von den im System erfolgten Änderungen der Berechtigungen per Rückverfolgung von Stichproben dieser Änderungen garantieren, dass diese den beschriebenen sicheren Prozess durchlaufen haben, genügt den SOX Compliance Anforderungen.

Was dieser Vorgang mit der Richtigkeit von Finanzberichten zu tun hat? Ganz einfach: Scheidet zum Beispiel ein Mitarbeiter aus einem Unternehmen aus und wird seine Zugangsberechtigung nicht zeitnah gelöscht, so könnte er dann als ein Externer auf die Applikationen des Unternehmens zugreifen und unerlaubte Transaktionen durchführen.

Der IT-Verantwortliche in einem Unternehmen spielt somit eine Schlüsselrolle in SOX Compliance-Projekten, da zunächst die gesamte IT-Landschaft im Fokus von Kontrollprozessen steht.

Soweit der IT-Manager über seine

Verantwortung für den IT-Bereich hinaus eine Funktion auf der Ebene der Unternehmensführung ausübt, muss er des Weiteren dem SOX Abschnitt 302 („Section 302“) ein besonderes Augenmerk widmen. Der SOX Abschnitt 302 schreibt Strafen vor für den Fall, dass CEO und CFO wissentlich oder fahrlässig falsche Angaben gemacht haben. CIOs stehen in diesem Zusammenhang in der Pflicht, die Zuverlässigkeit und Sicherheit der IT-Systeme zu garantieren.

Erst die IT reorganisieren und dann SOX Compliance anstreben – oder umgekehrt?

Welch eine Unternehmensführung würde nicht unterstellen und sogar bekräftigen, dass ihre IT bezogen auf die Prozesse und die eingesetzten Systeme professionell betrieben wird und selbstverständlich auch der Kontrolle des Führungsgremiums unterliegt? Defizite werden zumeist auf zu hohe Kosten der IT insgesamt oder zu niedrige Leistungen im Sinne eines Wertschöpfungsbeitrags für das Unternehmen bezogen, nicht aber auf die Risikobetrachtung der IT. Es wird statt dessen meistens unterstellt, dass die Verantwortungshierarchie in Bezug auf Kosten sowie in Bezug auf die Sicherstellung des laufenden Betriebs eine bewährte und somit ausreichende Absicherung gegen unternehmerische Risiken darstellt.

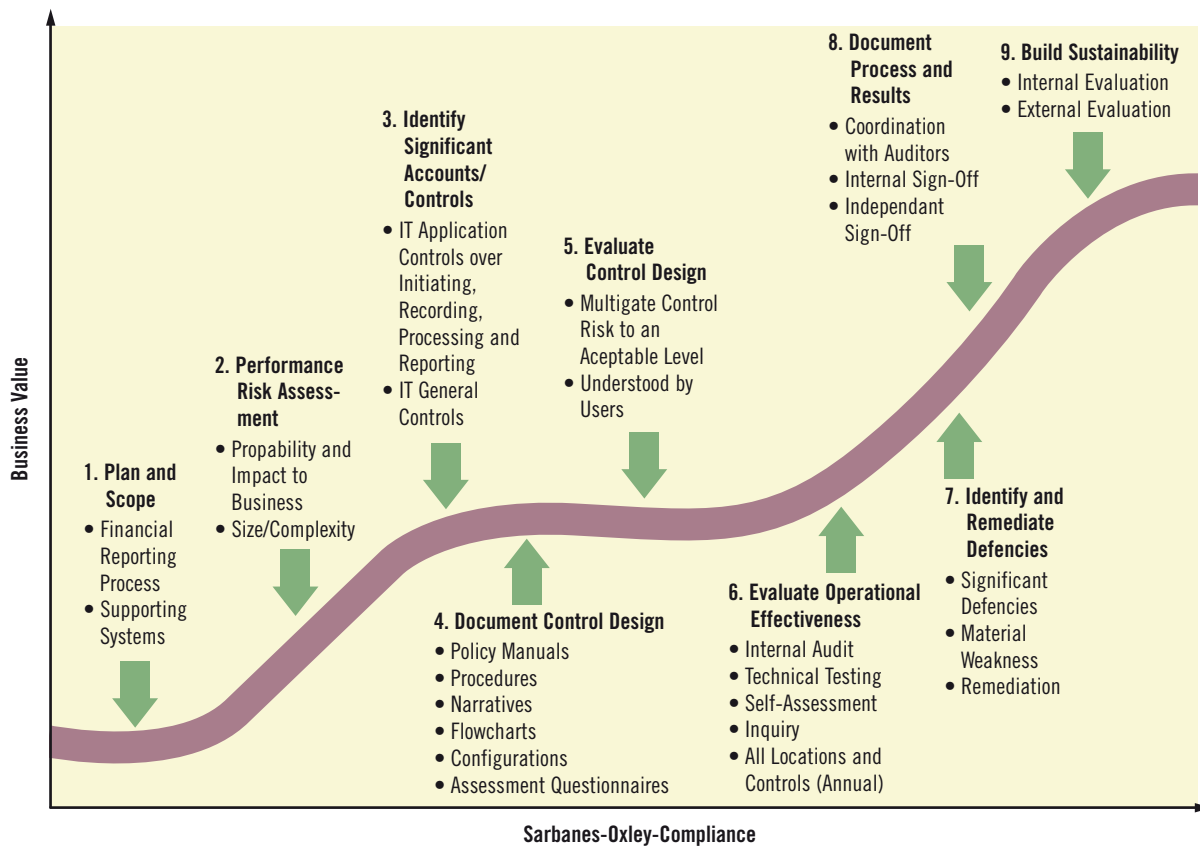
Daher neigen viele Unternehmen zu der Annahme, sie erfüllten bereits die SOX Compliance und es bestünde nur die Aufgabe, die bestehenden Abläufe zu dokumentieren sowie deren Einhaltung etwas öfter zu kontrollieren. Dies ist ein Trugschluss.

Es sind nicht alle Anwendungen und Systeme der IT sowie deren dahinter liegenden Prozesse für die Geschäftsabwicklung sowie auch in Bezug auf die IT-Organisation gleichermaßen SOX-relevant für ein Unternehmen, auch wenn sie zunächst allesamt im Fokus der SOX Compliance Betrachtung stehen.

Erst eine gründliche Risikoabschätzung auf Basis einer umfangreichen Ist-Aufnahme liefert die Grundlage für individuelle Festlegung der Eingrenzung der IT-Systeme und IT-Prozesse auf die SOX Compliance. Diese hängt ab von der Auswirkung der möglichen Schade-

Unabhängig von der Einschätzung rein marktrelevanter Nutzenfaktoren bietet die SOX Compliance auch die Basis für eine vollumfängliche „Renovierung“ der IT.

SOX Compliance Roadmap



Quelle: IT Governance Institute

Bild 2: Für die Erreichung der SOX Compliance im angestrebten Budget- und Zeitrahmen ist es unabdingbar, zu Beginn des gesamten Vorhabens eine Roadmap zu erstellen, wie zum Beispiel die SOX Compliance Roadmap vom IT Governance Institute.

ereignisse sowie von deren realistisch einzuschätzenden Wahrscheinlichkeit. Das Ergebnis hieraus ist der Katalog der für die SOX Compliance relevanten „IT Application Controls“ sowie „IT General Controls“ eines Unternehmens.

Werden die Ist-Aufnahme der IT sowie die Risikoabschätzung unter SOX Gesichtspunkten leichtfertig übergangen, weil man glaubt, die IT sowie deren Risikopotenziale aus der Praxis zu kennen, so besteht die Gefahr, dass erst die Abschlussprüfung durch den Auditor aufzeigt, welche Anwendungen und Systeme zu wenig oder manchmal auch zu stark in die SOX Compliance einbezogen wurden. Das hieße einerseits ganze Teilprojekte umsonst durchgeführt zu haben und andererseits erhebliche Nacharbeiten durchführen zu müssen anstatt die SOX Compliance bestätigt zu bekommen.

Ist-Aufnahme und Risikobewertung müssen aber nicht zwangsläufig eine nachfolgende Reorganisation der IT als Bedingung für die SOX Compliance be-

deuten. In der Praxis sieht es jedoch so aus, dass die meisten Unternehmen auf Basis der bestehenden IT-Prozesse keine SOX Compliance belegen konnten.

Werden die erfolgsentscheidenden Phasen der Ist-Aufnahme und Risikobewertung der IT übergangen, so wird nicht Zeit und Geld gespart, sondern eher umgekehrt der Grundstein für Budget- und Zeitplanüberschreitung des gesamt SOX Compliance-Projekts gelegt, da sich diese Schritte in späteren Phasen nicht einfach nachholen lassen auf Grund der Komplexität der fortgeschrittenen Dokumentation der Prozesse und Kontrollabläufe.

Ein Unternehmen mit zum Beispiel mehr als 20 Applikationen im Konzernverbund, die in mehr als 15 Standorten in nicht identischer Weise eingesetzt werden, kommt erfahrungsgemäß sehr schnell auf eine Anzahl von über 500 Kontrollprozessen (IT Application Controls und IT General Controls), die dokumentiert und als regelmäßige interne Prüfung nachgewiesen werden müssen.

Eine Infragestellung der Richtigkeit all dieser Kontrollprozesse in Bezug auf deren Umfang und Ausprägung in einem späteren Projektstadium wie etwa der internen Erstprüfung der Einhaltung dieser Kontrollprozesse kommt einem Neubeginn des gesamten Projekts gleich. Die Konsequenzen reichen dann weit über die Verschiebung von Zeitplänen und die Erhöhung von Projektbudgets hinaus: Das Top-Management muss dann anerkennen, ein für sich gesetztes Ziel nicht erreicht zu haben und die im Rahmen des SOX Compliance-Projekts weit über das Tagesgeschäfts hinaus beanspruchten Mitarbeiter müssen erkennen, dass die in aufwendigen Prozessen gelieferten Ergebnisse in



Form von SOX-relevanten Testplänen für jeden einzelnen Kontrollablauf in der IT eine weitgehende Überarbeitung erfordern.

Für die Erreichung der SOX Compliance im angestrebten Budget- und Zeitrahmen ist es unabdingbar, zu Beginn des gesamten Vorhabens eine Roadmap zu erstellen, die dem Rechnungsträger und die notwendigen Vorbereitungsschritte und Phasen enthält wie zum Beispiel die empfohlene SOX Compliance Roadmap des amerikanischen IT Governance Institute (Bild 2).

Welchen Payback aus einem SOX Compliance-Projekt kann die IT liefern?

Die Erlangung der erstmaligen SOX Compliance ist ein Projekt, das mit der SOX Compliance Bestätigung des externen Auditors noch nicht abgeschlossen ist. Über das Projekt der erstmaligen Zertifizierung hinaus ist ein Prozess zu installieren, der die dauerhafte SOX Compliance, also die Einhaltung aller in der externen Abschlussprüfung enthaltenen Kontrollprozesse, sicherstellt. Das bedeutet die Einrichtung von Prozessen, die es in diesem Ausmaß vorher nicht gab, zumindest nicht in dem von SOX geforderten Tiefgang und Umfang. Mit anderen Worten: Ohne dass neue IT-Systeme zum Einsatz kommen oder der Servicegrad der IT gesteigert wird, entstehen zunächst dauerhafte zusätzliche Folgekosten in der IT. Daraus resultiert zwangsläufig ein neuer Druck zur Effizienzsteigerung der IT, der als große Chance aufgegriffen werden sollte, indem die ermittelten Maßnahmen zur Mangelbehebung für die Herstellung der SOX Compliance erneut auf den Prüfstand kommen mit dem Ziel einer kostensenkenden Reorganisation.

Hierzu ein einfaches Beispiel: Werden die Tools und Prozesse zur Abwicklung vom Incident Management über alle Standorte, Organisationseinheiten und Tochtergesellschaften stan-

dardisiert, so ist hierfür nach der erreichten Standardisierung nur noch ein einheitlicher Kontrollprozess einzurichten, zu dokumentieren und für die SOX Compliance regelmäßig zu prüfen anstatt der vorher vielfach unterschiedlichen Kontrollprozesse.

Auf diese Weise lässt sich die Anzahl der SOX relevanten Kontrollprozesse und der damit verbundenen Aufwendungen oft um mehr als 50% reduzieren. Das Ergebnis derartiger Optimierungsprozesse geht allerdings weit über diesen Aspekt hinaus. Insgesamt sind folgende Effekte erreichbar:

- Deutlich reduzierter Aufwand der regelmäßig durchzuführenden Kontrollprozesse sowie deren Dokumentation und Nachweis
- Reduzierung der Anzahl eingesetzter Tools und Anwendungen und damit verbundene Kostensenkungen für Lizenzen oder Individualentwicklungen
- Senkung der Personalkosten im IT-Bereich durch Wegfall von Aufgaben, die vorher nur spezifisch für bestimmte Einheiten im Unternehmen und nicht im Konzernverbund vereinheitlicht bestanden
- Erstmalige Chance eines gruppenweiten IT-Benchmarks bezogen auf die eingesetzten IT-Systeme und die IT-Organisation auf Grund der erfolgten Standardisierung

Es ist darüber hinaus zu empfehlen, dass die SOX Compliance getriebene IT-Optimierung nicht nur mit Fokus auf Kostensenkung betrieben wird, sondern hierbei gleichermaßen die Chance ergriffen wird zu einer Steigerung des Wertschöpfungsbeitrags der IT für das Unternehmen. Ein guter Ansatz hierzu ist ein Initialschritt der IT-

Optimierung, der mittels eines umfangreichen Assessments, also letztendlich eines IT-Fitness-Checks, jeden SOX-relevanten Kontrollprozess einem Aufwand-/Nutzen-Benchmark unterzieht, der neben den Kostensenkungspotenzialen gleichzeitig auch die Potenziale für eine Leistungssteigerung offen legt.

Gernot Schäfer,
gernot.schaefer@helbling.de

Bitte kürzen

Links

www.itgi.org
www.isaca.org
www.coso.org

CIOs stehen in der Pflicht, die Zuverlässigkeit und Sicherheit der IT-Systeme zu garantieren: Eine „halbe SOX Compliance“ der IT ist gleich bedeutend mit keiner SOX Compliance.