Einhaltung der Anforderungen aus dem Sarbanes-Oxley Act mit Hilfe der Standards ISO/IEC 27001 & 27002

Daniel Russberger

Daniel Russenberger arbeitet seit über 15 Jahren als IT Revisor in der Finanzindustrie und leitet seit 2017 die interne IT Revision bei der St.Galler Kantonalbank. Daniel hat Wirtschaftsinformatik an der Universität Zürich studiert (lic.oec.publ.), hat ein Nachdiplomstudium «Economic Crime Investigation» an der Fachhochschule Luzern abgeschlossen und ist CISA, CRISC und CISSP.

Diverse Bilanzskandale mit wirtschaftsdeliktischem Hintergrund sorgten insbesondere in den USA in den Jahren 2001 und 2002 für Verunsicherung an den Kapitalmärkten. Bei den Anlegern entstand ein Misstrauen gegenüber der finanziellen Berichterstattung und der Unternehmensführung generell. Die US-Regierung reagierte innert kürzester Zeit mit einer entsprechenden Gesetzgebung, dem sogenannten Sarbanes-Oxley Act (SOX). Das Gesetz wurde im Juli 2002 in Kraft gesetzt und verlangt eine erhöhte Transparenz bei den internen Abläufen zur finanziellen Berichterstattung. Wirksame Kontrollen sind dabei zu implementieren und von der Unternehmensleitung formell zu bestätigen.

Aus der Praxis liegen in der Zwischenzeit Erfahrungen über die Auswirkungen von SOX vor. Generell wird von Investoren und Unternehmen festgehalten, dass die Finanzausweise nun transparenter und aussagekräftiger seien, dass die Kosten für die Umsetzung von SOX jedoch unverhältnismässig hoch sein würden. Basierend auf dieser Kritik wurden im Juni 2007 die Gesetzestexte nochmals angepasst und Empfehlungen abgegeben.

Heutige Prozesse zur Erstellung des Finanzausweises werden in der Regel entscheidend von IT-Systemen unterstützt, wodurch die IT selbst in den Fokus der SOX-Anforderungen rückt. Während die wichtige Rolle der IT im Zusammenhang mit SOX unbestritten ist, existieren auch nach den Änderungen vom Juni 2007 weiterhin nur sehr wenige und oft unpräzise Anforderungen an die IT. Namentlich wird bestätigt, dass Kontrollen im IT-Umfeld aus den Bereichen „Programm-Entwicklung & Änderung“, „Zugriffe auf Programme und Daten“ und „Computer Betrieb“ stammen sollen. Zudem wird betont, dass die IT nicht separat behandelt, sondern stets im Kontext der jeweiligen Geschäftsprozesse zu beurteilen ist.

Generell fordert SOX, dass sich Unternehmen bei der Gestaltung des internen Kontrollsystems an einem anerkannten Rahmenwerk (Framework) orientieren. Namentlich erwähnt der Gesetzgeber das COSO-Framework, das allerdings nicht speziell auf IT-Umgebungen ausgerichtet ist. Somit drängen sich bei Spezialthemen ergänzende Frameworks auf, wie beispielsweise die ISO/IEC Standards im IT-Umfeld: Die Standards ISO/IEC 27001 & 27002 (2005) sind international anerkannt und nennen umfassende Kontrollen zur Sicherstellung der Informationssicherheit.

ISO/IEC 27001 beschreibt das Vorgehen, wie Kontrollen auszuwählen, umzusetzen, zu überwachen und zu verbessern sind. Dieses Vorgehensmodell wird ergänzt durch ISO/IEC 27002, wo konkrete Kontrollziele, Massnahmen und Hilfstexte aufgezählt werden.

Im Rahmen dieser Arbeit sind nun Anforderungen, Erfahrungen und Publikationen zu den Themen SOX und IT als Ausgangslage genommen und mit den ISO/IEC 27001 & 27002 Standards verglichen worden. Ziel ist dabei, die Gemeinsamkeiten von SOX und ISO/IEC bezogen auf das IT-Umfeld zu erkennen. Ebenso soll gezeigt werden, welche ISO/IEC 27002 Kontrollen bei SOX eine besonders wichtige Rolle spielen und was bei der Umsetzung von SOX im Vergleich zu den ISO/IEC Standards speziell zu beachten ist.

Neben den Original-Gesetzestexten (US Congress, SEC, PCAOB) dient insbesondere die Publikation „IT Control Objectives for Sarbanes-Oxley“ des IT Governance Institutes als eine wesentliche Grundlage. In Ergänzung und als Praxisbeispiel wird zudem das SOX-Framework der Credit Suisse untersucht.

Der Vergleich von SOX und ISO/IEC 27001 zeigt, dass die Vorgehensweise zur Umsetzung der geforderten Massnahmen im Wesentlichen übereinstimmt. In beiden Fällen spielen Risikomanagement, regelmässige Überprüfung der Kontrollen und Nachvollziehbarkeit eine erhebliche Rolle. Die Zielsetzung „Informationssicherheit“ aus den ISO/IEC Standards ist ebenfalls ganz im Sinne von SOX. Zudem können praktisch alle Kontrollen aus ISO/IEC 27002 einen Beitrag zur Erfüllung der SOX-Anforderungen leisten.

Es zeigt sich weiter, dass insbesondere spezifische IT-Applikationskontrollen und logische Zugriffskontrollen eine sehr grosse Bedeutung bei SOX haben. In ISO/IEC 27002 sind dies namentlich die Kapitel „Korrekte Verarbeitung in Applikationen“, „Benutzer-Registrierung“, „Umgang mit privilegierten Zugriffsrechten“ und „regelmässige Überprüfung der Zugriffsrechte“. Die Kontrollen zum Change Management und zur physischen Sicherheit werden im Zusammenhang mit SOX ebenfalls konsequent erwähnt und lassen sich problemlos auf ISO/IEC 27002 abbilden. Neben eindeutigen Hinweisen zeigen sich aber auch Widersprüche zur SOX-Relevanz von einigen konkreten Kontrollen in ISO/IEC 27002.

So ist keine klare Tendenz bei übergeordneten Kontrollen, im Umgang mit Benutzerverantwortung und bei Spezialthemen zu erkennen. Gründe für die Widersprüche können sein, dass die jeweiligen Geschäftsprozesse je nach Unternehmen unterschiedlich sein können, die Gesetzgebung kürzlich geändert worden ist, kompensierende Kontrollen existieren können und dass generell ein grosser Interpretationsspielraum bei SOX besteht.

Spezielle Aspekte sind bei SOX zu beachten, die in den ISO/IEC Standards nicht oder nur indirekt adressiert werden. So liegt der Schwerpunkt von SOX auf den Prozessen zur Erstellung des Finanzausweises, wobei sich dieser spezielle Fokus an mehreren Stellen deutlich bemerkbar macht. Die Risikobeurteilung, die Definition der Zuständigkeiten, die Gestaltung der spezifischen IT-Applikationskontrollen und die Beurteilung der gefundenen Schwachstellen werden bei SOX viel stärker in Bezug zu den betroffenen Geschäftsprozessen gesetzt. Dabei wird deutlich, dass die individuellen Charakteristiken der Geschäftsprozesse bei SOX speziell zu beachten sind. Aus ähnlichen Überlegungen gilt bei SOX denjenigen Applikationen ein spezielles Augenmerk, die vom Fachbereich selbst erstellt werden. Zudem sind einige übergeordnete Kontrollen, deren Berücksichtigung vom Gesetzgeber in der aktuellen SOX-Diskussion generell erwähnt wird, bei ISO/IEC 27002 nicht umfassend abgedeckt. Beispiele sind die Kommunikation der generellen Aufbau- und Ablauforganisation oder Methoden zur Applikationsentwicklung.

Die ISO/IEC 27001 & 27002 Standards gehen in Bezug auf den Abdeckungsgrad bei Geschäftsprozessen weiter als SOX, da ISO/IEC nicht nur auf die finanzielle Berichterstattung fokussiert. Zudem sind die Standards systematischer aufgebaut und die Anforderungen präziser formuliert.

Der Trend zur Reduktion des SOX Aufwands ist in den geänderten, gesetzlichen Vorgaben bestätigt und unterstützt worden. Durch diese Änderungen erhalten die Unternehmen unter anderem eine höhere Flexibilität in der Dokumentation ihrer Geschäftsprozesse und Kontrollen sowie im Nachweis der Effektivität dieser Kontrollen. Dadurch wird eine ursprünglich strenge SOX-Forderung abgeschwächt, was zu einer Annäherung von SOX und ISO/IEC 27001 hinsichtlich Dokumentationspflicht führt. Es wird künftig wohl auch zu erwarten sein, dass die Anforderungen aus SOX weniger streng interpretiert werden und dass Unternehmen ihre Kontrollen mit Blick auf das Wesentliche nochmals überprüfen und gegebenenfalls anpassen werden. In diesem Fall ist es wichtig zu wissen, wo Schwerpunkte liegen und wo nochmals gekürzt werden kann, wobei die hier vorliegende Arbeit bei der Auswahl von generellen IT-Kontrollen helfen kann..

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Grafenauweg 10
Postfach 7344
CH-6302 Zug
+41 41 757 67 67
ifz@hslu.ch