HSW LUZERN

COMPETENCE CENTER
FORENSIK UND
WIRTSCHAFTSKRIMINALISTIK

Master of Advanced Studies Economic Crime Investigation (MAS ECI)

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

Diplomarbeit

eingereicht am 24. September 2007 von

lic. oec. publ. Daniel Russenberger

MAS ECI, Klasse 6

betreut von

lic. jur. Peter Cosandey (Tutor)
Prof., dipl. El.-Ing. FH Carlos Rieder (Diplomarbeitsbetreuer)

HSW LUZERN
CCFW
Zentralstrasse 9
CH—6002 Luzern

T: 041—228—41—70
F: 041—228—41—71
E: ccfw@hsw.fhz.ch
W: www.ccfw.ch

Inhaltsverzeichnis

Inhaltsverzeichnis II
Literaturverzeichnis IV
Abkürzungsverzeichnis VIII
Management Summary IX
Kurzfassung XII

1. EINLEITUNG 1

2. DER SARBANES-OXLEY ACT 2

2.1. ÜBERBLICK 2
2.1.1. Entstehung des Sarbanes-Oxley Act 2
2.1.2. PCAOB und SEC 2
2.1.3. Örtlicher Geltungsbereich 2
2.1.4. Allgemeine Anforderungen 2
2.2. IT-ASPEKTE 4
2.2.1. Anforderungen an die IT 4
2.2.2. IT Governance Institute: "IT Control Objectives for Sarbanes-Oxley" 5
2.2.3. Kategorien von Kontrollen im IT-Umfeld 5
2.3. AKTUELLER STAND 8

3. ISO/IEC STANDARDS ZUR INFORMATIONSSICHERHEIT 9

3.1. ÜBERBLICK 9
3.1.1. ISO und IEC 9
3.1.2. ISO/IEC 2700x Familie 10
3.2. ISO/IEC 27001:2005 11
3.2.1. Inhalt 11
3.2.2. Zertifizierung 13
3.3. ISO/IEC 27002:2005 14
3.3.1. Entstehungsgeschichte 14
3.3.2. Inhalt 14
3.3.3. Gegenüberstellung mit anderen Standards 15

4. VERGLEICH VON SOX UND ISO/IEC 27001 & 27002 16

4.1. EINLEITUNG 16
4.2. BEISPIELE VON BISHERIGEN VERGLEICHEN 17
4.2.1. ISO/IEC 17799:2000 als Ausgangslage für SOX 17
4.2.2. Weitere Beispiele 18
4.3. SOX UND ISO/IEC 27001 19
4.3.1. Grundlage 19
4.3.2. Übereinstimmung 19
4.3.3. Zusätzliche Aspekte bei SOX 19
4.3.4. Zusätzliche Aspekte bei ISO/IEC 27001 20

4.4. SOX UND ISO/IEC 27002 21
4.4.1. Grundlage 21
4.4.2. Übereinstimmung 21
4.4.3. Zusätzliche Aspekte bei SOX 22
4.4.4. Gewichtung der ISO/IEC 27002 Kontrollen 24
4.5. ISO/IEC 27002 UND SOX-KONTROLLZIELE GEMÄSS CREDIT SUISSE 24
4.5.1. Einleitung und Grundlage 24
4.5.2. Schwerpunkte und Unterschiede im SOX-Framework der CS 25

5. ZUSAMMENFASSUNG DER ERGEBNISSE 26

5.1. GEMEINSAMKEITEN VON SOX UND ISO/IEC 2700X 26
5.2. SOX-RELEVANZ AUSGEWÄHLTER KONTROLLEN AUS ISO/IEC 27002 27
5.2.1. Spezifische IT-Applikationskontrollen und logische Zugriffskontrollen 27
5.2.2. Kontrollen bei Änderungen an IT-Systemen 27
5.2.3. Umgebungssicherheit und Business Continuity 27
5.2.4. Weitere ISO/IEC 27002 Kontrollen 27
5.3. UNTERSCHIEDE BEI SOX UND ISO/IEC 2700X 28
5.3.1. Wo geht SOX weiter als ISO/IEC 2700x? 28
5.3.2. Wo geht ISO/IEC 2700x weiter als SOX? 29

6. SCHLUSSBEMERKUNGEN UND AUSBLICK 29

Anhang A: Detailvergleich ISO/IEC 27001:2005 und SOX

Anhang B: Mapping SOX requirements to ISO/IEC 27002:2005 using a 2-step transition

Anhang C: Vergleich der illustrativen SOX-Kontrollen gemäss IT Governance Institute mit ISO/IEC 27002:2005

Anhang D: Liste der Kontrollen aus ISO/IEC 27002:2005 und Hinweise zu deren SOX-Relevanz

Anhang E: Abbildung der generellen IT-Kontrollen der Credit Suisse auf ISO/IEC 27002:2005

Anhang F: Liste der Kontrollen aus ISO/IEC 27002:2005, abgeleitet aus SOX-Kontrollen der Credit Suisse und Vergleich mit dem IT Governance Institute

Literaturverzeichnis

Asma Jörg (2006), BS 7799 and SOX; Artikel im ISMS Journal der ISMS IUG (International User Group), Issue 6; England, Januar 2006

BITKOM und DIN (2006), Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, Version 2; Berlin, Juni 2006

BSI (2006), IT-Grundschutz-Kataloge, Version 2006; Bonn 2006;
Internet: http://www.bsi.de, abgerufen: 16.04.2007

Butler Henry N. und Ribstein Larry E. (2006), The Sarbanes-Oxley Debacle – What We've Learned - How to Fix It; AEI Liability Studies; Washington D.C., 2006

COSO (1994), Internal Control – Integrated Framework; Juli 1994; USA;
Internet: http://www.coso.org, abgerufen: 29.08.2007

COSO (2004), Enterprise Risk Management – Integrated Framework; September 2004; USA;
Internet: http://www.coso.org, abgerufen: 29.08.2007

CSG (2007a), General Computer Controls (GCC) V3.0; internes Dokument zum SOX-Framework der Credit Suisse; Zürich, 10.04.2007

CSG (2007b), Credit Suisse – Facts & Figures; Online-Publikation; Zürich, 02.08.2007;
Internet: http://www.credit-suisse.com, abgerufen: 07.08.2007

CSG Audit Department (2005a), Einführung SOX; Präsentation von Thomas Kuhn an der Tagung "SVIR, ERFA Versicherungen"; Basel, 11.05.2005

CSG Audit Department (2005b), SOX IT Controls; Präsentation von Daniel Russenberger an der Tagung "SVIR, ERFA Versicherungen"; Basel, 11.05.2005

Datardina Malik (2005), Comparative Analysis of IT Control Frameworks in the Context of SOX; Studie; University of Waterloo Centre for Information Systems Assurance; Canada, August 2005;
Internet: http://accounting.uwaterloo.ca/uwcisa/symposium_2005/Datardina.pdf, abgerufen: 13.07.2007

Dummer Stefan (2006), Compliance durch Standards der Informationssicherheit - Untersuchung von gesetzlichen Anforderungen an das Management der Informationssicherheit und deren Erfüllung durch ISO27001/17799; Diplomarbeit an der Universität Regensburg; 06.09.2006

Haworth Dwight A. und Pietron Leah R. (2006), Sarbanes-Oxley: Achieving Compliance by starting with ISO 17799; in "Information Systems Management, Winter 2006", 2006;
Internet: http://www.ism-journal.com/ITToday/SOX.pdf, abgerufen: 04.05.2007

ISACA (2007a), Response to SEC's „Guidance for Management's Reports on Internal Control Over Financial Reporting"; Brief und Online-Dokument; Illinois, 26.02.2007;
Internet: http://www.isaca.org, abgerufen: 12.05.2007

ISACA (2007b), Response to PCAOB's proposed Auditing Standard "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements "; Brief und Online-Dokument; Illinois, 26.02.2007;
Internet: http://www.isaca.org, abgerufen: 12.05.2007

ISO/IEC (2005a), ISO/IEC 27001:2005; Internationaler Standard, First Edition; Genf, 15.10.2005

ISO/IEC (2005b), ISO/IEC 27002:2005; Internationaler Standard, Second Edition - renumbered 07/2007; Genf, 15.06.2005

ISO/IEC (2005c), ISO/IEC 17799:2005; Internationaler Standard, Second Edition; Genf, 15.06.2005

ISO (2006), ISO in brief – International Standards for a sustainable world; Broschüre; Genf 2006;
Internet: http://www.iso.org, abgerufen: 23.06.2007

ISO (2007), SC 27 Standing Document 7 (SD7) – Catalogue of ISO/IEC JTC1 – SC27 Projects and Standards (SC 27 N5717); Online-Dokument zum Projektstatus; Genf, 24.04.2007;
Internet: http://www.iso.org, abgerufen: 23.06.2007

IT Governance Institute (2005), COBIT 4.0; Online-Publikation; Illinois, 2005;
Internet: http://www.isaca.org, abgerufen: 04.05.2007

IT Governance Institute (2006a), IT Control Objectives for Sarbanes-Oxley; Online-Publikation, 2nd Edition; Illinois, September 2006;
Internet: http://www.isaca.org, abgerufen: 04.05.2007

IT Governance Institute (2006b), COBIT Mapping: Mapping of ISO/IEC 17799:2005 with COBIT 4.0; Online-Publikation; Illinois, 2006;
Internet: http://www.isaca.org, abgerufen: 01.07.2007

IT Governance Institute (2006c), COBIT Mapping: Overview of international IT guidance; Online-Publikation, 2nd Edition; Illinois, 2006;
Internet: http://www.isaca.org, abgerufen: 30.06.2007

IT Governance Institute (2007), COBIT 4.1; Online-Publikation; Illinois, 2007;
Internet: http://www.isaca.org, abgerufen: 17.05.2007

ITACS Training (2007), Informatik-Revision; Handout von Peter Bitterli / Bitterli-Consulting im Rahmen des Nachdiplomstudiums zur Bekämpfung der Wirtschaftskriminalität (MAS ECI 6); Luzern, 26.01.2007

Kaufmann Helmut (2007), Sarbanes-Oxley – A schematic approach; Präsentation und Handout im Rahmen des MAS Information Security an der HSW Luzern; März 2007

KPMG (2006), Defining Issues, Proposed SEC and PCAOB Guidance on Internal Control Over Financial Reporting; KPMG LLP, No. 06-34; Dezember 2006

Liegl Patrick (2005), Der Sarbanes-Oxley Act und seine Anforderungen an das Management – Eine Ausarbeitung von Umsetzungsmassnahmen zur Erfüllung der gesetzlichen Anforderungen für IT-Prozesse; Diplomarbeit an der FH Joanneum GmbH; Graz, 10.06.2005

PCAOB (2004), Auditing Standard No. 2 – An audit of internal control over financial reporting performed in conjunction with an audit of financial statements (as of May 12, 2006); PCAOB Standard, USA, 09.03.2004;
Internet: http://www.pcaob.org, abgerufen: 05.05.2007

PCAOB (2006a), Proposed Auditing Standard– An audit of internal control over financial reporting performed that is integrated with an audit of financial statements; PCAOB Release No. 2006-007, Docket Matter No. 021; Washington D.C., 19.12.2006;
Internet: http://www.pcaob.org, abgerufen: 12.05.2007

PCAOB (2006b), Auditing Standard No. 4 – Reporting on Whether a Previously Reported Material Weakness Continues to Exist (as of May 12, 2006); PCAOB Standard, File No. PCAOB-2005-01, USA, 06.02.2006;
Internet: http://www.pcaob.org, abgerufen: 05.05.2007

PCAOB (2007), Auditing Standard No. 5 – An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements (as of August 6, 2007); PCAOB Standard, USA, 12.06.2007;
Internet: http://www.pcaob.org, abgerufen: 09.08.2007

PricewaterhouseCoopers LLP (2004a), The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act; Online-Publikation und Broschüre, Connectedthinking, CI-CI-05-0076-A; USA, Juli 2004;
Internet: http://www.pwc.com, abgerufen: 19.05.2007

PricewaterhouseCoopers (2004b), Sarbanes-Oxley Act: Section 404 – Practical Guidance for Management; Online-Publikation und Broschüre; USA, Juli 2004;
Internet: http://www.pwc.com, abgerufen: 13.07.2007

PricewaterhouseCoopers LLP (2006), Private Companies – Are your internal controls supporting your business strategy?; Online-Publikation und Broschüre, Connectedthinking, BS-BS-06-0570-A.07/06.lmt; USA, 2006;
Internet: http://www.pwc.com, abgerufen: 19.05.2007

Schwaiger Martin A. und Urbina Hector A. (2006), IT-Governance Frameworks for Compliance – A comprehensive discussion and comparison of IT-Governance Frameworks to meet requirements derived from the Sarbanes Oxley Act; Master Thesis; Department of Computer and Systems Sciences and the Royal Institute of Technology (KTH) Stockholm; 09.06.2006

SEC (2003), SEC Final Rule 33-8238 – Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports; Washington D.C., 14.08.2003;
Internet: http://www.sec.gov (SEC Final Rules 2003), abgerufen: 05.05.2007

SEC (2006), SEC Proposed Rule 33-8762 – Management's Report on Internal Control Over Financial Reporting; SEC Release, File No.S7-24-06; Washington D.C., 20.12.2006; Internet: http://www.sec.gov, abgerufen: 12.05.2007

SEC (2007a), Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934; SEC Interpretive Release No. 33-8810, 34-55929, File No. S7-24-06; Washington D.C., 20.06.2007;
Internet: http://www.sec.gov, abgerufen: 09.08.2007

SEC (2007b), Amendments to Rules Regarding Management's Report on Internal Control Over Financial Reporting; SEC Final Rule Release No. 33-8809, 34-55928, File No. S7-24-06; Washington D.C., 20.06.2007;
Internet: http://www.sec.gov, abgerufen: 09.08.2007

Sigrist Beat (2004), Sarbanes-Oxley Act of 2002 – Anforderungen an das Interne Kontrollsystem für die Rechnungslegung; Diplomarbeit, 17. Lehrgang des Executive Programms, Swiss Banking School; Zürich, 06.05.2004

US Congress (2002), Sarbanes-Oxley Act of 2002; Public Law 107-204; USA, 30.07.2002; Internet: http://www.pcaob.org/About_the_PCAOB/Sarbanes_Oxley_Act_of_2002.pdf, abgerufen: 04.05.2007

Vaccaro Angelo (2005), IT Control im Rahmen des Sarbanes-Oxley Act, Sec. 404; Diplomarbeit, Institut für Informatik, Universität Zürich; 10.11.2005

Van der Crone Hans Caspar und Roth Katja (2003), Der Sarbanes-Oxley Act und seine extraterretoriale Bedeutung; Aufsatz in AJP/PJA, 2/2003

Weiss Peter (2007), ISO/IEC Information Security Standards; Präsentation bei der Konzernrevision der Credit Suisse; Zürich, 10.01.2007

Zihlmann Alex (2006), Weitere Standards/Normen/Methoden; Präsentation und Handout im Rahmen des MAS Information Security an der HSW Luzern; 04.11.2006

Abkürzungsverzeichnis

BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BS 7799	British Standard Nr. 7799
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
CAVR	Completeness, Accuracy, Validity, Restricted access
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CMMI	Capability Maturity Model Integration
COBIT	Control OBjectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CS	Credit Suisse
CSG	Credit Suisse Group
CSGN	Namenaktien der Credit Suisse Group
DIN	Deutsches Institut für Normung
EUC	End User Computing
FIPS	Federal Information Processing Standard
GCC	General Computer Control
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO 17799	ISO/IEC 27002:2005, ISO/IEC 17799:2005
ISO 27001	ISO/IEC 27001:2005
ISO 27002	ISO/IEC 27002:2005, ISO/IEC 17799:2005
ISO 2700x	ISO/IEC 27001:2005 & ISO/IEC 27002:2005
IT	Informationstechnologie
IT-BPM	IT-Baseline Protection Manual; IT-Grundschutz-Kataloge
ITGI	IT Governance Institute
ITIL	IT Infrastructure Library
ITU	International Telecommunication Union
KPMG	Klynveld, Peat, Marwick und Goerdeler
Mio.	Millionen
NIST	National Institute of Standards and Technology (hier: NIST 800-14)
No.	Number (Nummer/Anzahl)
PCAOB	Public Company Accounting Oversight Board
PDCA	Plan-Do-Check-Act
PRINCE2	Projects in controlled environments
PwC	PricewaterhouseCoopers
Ref.	Referenz
SAS 70	Statement on Auditing Standards No. 70
SDLC	Software Development Life Cycle
SEC	Securities and Exchange Commission
Sec.	Section (Kapitel)
Sig.	Signature (Unterschrift)
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act
TOGAF	The Open Group Architecture Framework
US	United States (of America)

Management Summary

A number of major corporate accounting scandals in 2001 and 2002 resulted in a decline of public trust in accounting and reporting practices. The US government quickly responded to this situation by issuing a United States federal law called the “Sarbanes-Oxley Act (SOX)”. This legislation requires companies to increase transparency in internal financial processes and to implement effective controls in their processes. Furthermore, management has to formally confirm the effectiveness of the company’s internal control system. SOX was signed to law in July 2002.

Experiences have been gained in the meantime with regard to SOX implementation and consequences thereof. In general, investors and companies agree on improvements in the quality and efficiency of important corporate processes and controls. However, these benefits have come with significant costs. Based on these conclusions, parts of SOX requirements were changed in July 2007 and further guidelines were issued for SOX implementation.

Today’s financial processes are highly dependent on IT systems and as a result, IT must be considered in SOX implementations as well. While the key role of IT is beyond dispute, legislation only gives little guidance with regard to IT. Often, precise requirements to IT environments are missing. Publications from legislators as of July 2007 solve this issue neither but emphasize that IT should be an integral part of management’s overall assessment. The identification of risks and controls within IT should not be a separate evaluation. Furthermore, SOX guidelines advise to implement general IT controls in the areas of program development, program changes, computer operations, and access to program and data.

SOX requires management to base its evaluation of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework. Legislation specifies characteristics of such a framework and refers to COSO as an example of a suitable framework. However, the COSO framework does not specifically address issues related to the IT environment and as a result, additional frameworks have to be considered. From an IT point of view, the ISO/IEC 27001 & 27002 (2005) standards may help and contribute to SOX compliance: These standards focus on information security and are commonly known and well accepted. The ISO/IEC 27001 standard defines how to proceed when selecting, implementing, monitoring and improving controls. In addition to such a management system, ISO/IEC 27002 provides a list of control objectives as well as detailed activities and guidelines.

As a part of this diploma thesis, SOX publications and requirements have been reviewed, analyzed and compared to ISO/IEC 27001 / 27002 having the following objectives in mind:

1. Identify common characteristics between SOX and ISO/IEC 27001 & 27002.
2. Identify important controls in the ISO/IEC 27002 standard with regard to SOX.
3. Highlight issues which have to be particularly considered from a SOX point of view due to less importance in ISO/IEC standards.

The scope of this thesis is limited to SOX in combination with IT systems; pure non-IT issues have not been followed-up during comparison. Beside of original legislation (see US Congress, SEC and PCAOB), the document “IT control Objectives for Sarbanes Oxley” of the IT Governance Institute has been used as an essential theoretical basis for analysis. Furthermore, experiences have been incorporated by examining the SOX framework of Credit Suisse.

The following main results and conclusions derive from the comparison of SOX and ISO/IEC 27001 & 27002 standards:

Common characteristics:

- SOX and ISO/IEC 27001 mainly require the same steps to implement and maintain their control system: In both cases, key elements are “risk management”, “regular assessment of control effectiveness” and “documentation”.
- Information security as defined in ISO/IEC is fully in line with SOX objectives. In addition, nearly all controls of ISO/IEC 27002 contribute to fulfill SOX requirements (at least to a certain degree).

Important controls in ISO/IEC 27002:

- Specific IT application controls and logical access controls are most relevant with regard to SOX. Such controls are defined in the following chapters of ISO/IEC 27002: Correct processing in applications, user registration, privilege management, review of user access rights.
- Change management controls and physical security are requirements which have consistently been mentioned in SOX publications. Such controls can also be clearly mapped to ISO/IEC 27002.
- The importance of some controls in ISO/IEC 27002 is unclear with regard to SOX due to inconsistent results deriving from mappings. In particular, entity level controls were not consistently mentioned in ISO/IEC 27002. Furthermore, different opinion exist with regard to the importance of user responsibilities in SOX implementations. Special topics in ISO/IEC 27002 are also not consistently referred to from a SOX point of view. Reasons for such inconsistencies might be: Individual character of business processes (including compensating controls), adaptation of SOX legislation and vague descriptions of SOX requirements in general.

Important SOX issues and other deviations

- ISO/IEC standards do not restrict their scope on predefined business processes, which is in contrast to the limited scope of SOX focusing on financial processes. This difference requires special attention and has a deep impact: Risk assessment, definition of responsibilities, design of specific IT application controls and assessment of identified weaknesses must always be done in the light of financial processes. By doing so, individual characteristics of business processes have to be taken into account.
- Attention should be paid to applications developed by end users as these applications are often used in financial processes and are prone to errors.
- Entity level controls have to be considered in the design and assessment of control effectiveness. These controls have particularly been highlighted during adaptation of SOX requirements in 2007. However, ISO/IEC 27002 does not fully cover certain entity level controls such as communication of procedures and responsibilities in general or standardized methods regarding software development.
- ISO/IEC 27001 & 27002 standards are more structured and precise than SOX.

Based on experiences with SOX implementation in the past years, tendencies exist to reduce costs. This trend was confirmed and supported by updated SOX legislation in July 2007. In particular, companies are now more flexible to document their processes, control designs and assessments of operating effectiveness. As a consequence, documentation requirements are not as strict as defined in former releases leading to fewer differences between SOX and ISO/IEC 27001. Going forward, SOX requirements might be interpreted more laxly and

companies may want to review and reduce controls again focusing on most important controls. Results from this diploma thesis may help in selecting general IT controls.

Kurzfassung

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 Risi-

komanagement, 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.

1. Einleitung

Diverse US-Bilanzskandale mit wirtschaftsdeliktischem Hintergrund trugen in den Jahren 2001 und 2002 massgeblich zur Verunsicherung an den Kapitalmärkten bei. 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. Bei Verstössen drohen hohe Bussen bis hin zu Freiheitsstrafen.

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. So wird von SOX ganz allgemein verlangt, dass sich Unternehmen bei der Gestaltung ihres internen Kontrollsystems (IKS) an bewährten Kontroll-Frameworks orientieren. Als mögliches Beispiel nennt der Gesetzgeber das COSO-Framework[1], das generelle Kontrollen in Unternehmungen abdeckt, jedoch nicht spezifisch auf die IT 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.

Im Rahmen dieser Arbeit werden nun Anforderungen, Erfahrungen und Publikationen zum Thema SOX als Ausgangslage genommen und mit den ISO/IEC 2700x Standards verglichen. Dabei werden zuerst die wesentlichen Anforderungen und Ansätze zur Implementierung von SOX kurz aufgezeigt. Ebenso werden die Standards ISO/IEC 27001 & 27002 vorgestellt, um anschliessend zu beurteilen, inwieweit SOX und ISO/IEC übereinstimmen. Ziel ist es, die Gemeinsamkeiten aufzuzeigen sowie diejenigen Kontrollen aus ISO/IEC 27002 zu ermitteln, welche bei SOX eine besonders wichtige Rolle spielen. Zudem soll dargestellt werden, welche Punkte bei der Umsetzung von SOX im Vergleich zu ISO/IEC 27001 & 27002 speziell zu beachten sind.

Anforderungen aus dem Sarbanes-Oxley Act ohne jeglichen Bezug zur IT werden bei den Vergleichen in dieser Arbeit ausgeklammert. So wird beispielsweise bei den Abweichungsanalysen nicht darauf eingegangen, dass SOX keine privaten Kredite an leitende Angestellte zulässt. Die Schnittstelle zwischen IT und Fachbereich wird hingegen berücksichtigt.

Während die gesetzlichen Vorgaben aus dem Sarbanes-Oxley Act in Bezug auf die IT vage sind, schliesst das IT Governance Institute diese Lücke weitgehend: In der Publikation „IT Control Objectives for Sarbanes-Oxley“[2] werden die notwendigen Kontrollen sehr ausführlich beschrieben, allerdings unverbindlich und ohne Pflicht zur Umsetzung. Da sowohl der Herausgeber als auch die Publikation in der Fachwelt sehr angesehen sind,[3] wird das Dokument des IT Governance Institutes im Folgenden als eine wesentliche, theoretische Grundlage angesehen und darauf abgestützt. In Ergänzung und als Praxisbeispiel wird zudem das SOX-Framework der Credit Suisse untersucht.

---

1 COSO (1994)

2 IT Governance Institute (2006a)

3 Das IT Governance Institute (2007) ist Herausgeber des weltweit anerkannten IT Governance Frameworks „COBIT“.

2. Der Sarbanes-Oxley Act

2.1. Überblick

2.1.1. Entstehung des Sarbanes-Oxley Act

Diverse Bilanzskandale wie beispielsweise Enron/Arthur Andersen oder Worldcom in den Jahren 2001 und 2002 sorgten insbesondere in den USA für Verunsicherung. Bei Aktionären und Investoren entstand ein Misstrauen gegenüber der finanziellen Berichterstattung sowie ganz generell gegenüber der Unternehmensführung.[4] Als Gegenmassnahme wurde deshalb in den USA von Paul Sarbanes (Senator) und Michael G. Oxley (Mitglied des Repräsentantenhauses) nach kurzer Zeit ein entsprechender Gesetzestext eingereicht. Am 30. Juli 2002 wurde der sogenannte „Sarbanes-Oxley Act of 2002" (SOX) offiziell vom US Präsidenten, George W. Bush, unterzeichnet.

Ziel des Gesetzes ist eine bessere Aussagekraft der finanziellen Berichterstattung sowie eine Stärkung der Corporate Governance, namentlich durch eine eidesstattliche Bestätigung der Korrektheit des Finanzausweises durch den CEO und den CFO (bzw. Personen mit ähnlichen Funktionen).[5] Um dies zu erreichen, wird von der Unternehmensleitung unter anderem die Errichtung und der Unterhalt eines internen Kontrollsystems gefordert. Bei falscher Bestätigung des Finanzausweises drohen persönliche Geldbussen bis USD 5 Mio., Berufsverbot und Freiheitsstrafen bis zu 20 Jahren.[6]

2.1.2. PCAOB und SEC

Der Sarbanes-Oxley Act ist als Rahmengesetz ausgestaltet und wird durch Vorschriften der amerikanischen Börsenaufsicht (SEC) konkretisiert.[7] Daneben wurde gestützt auf den Sarbanes-Oxley Act[8] das sogenannte Public Company Accounting Oversight Board (PCAOB) gegründet. Es handelt sich dabei um eine nicht gewinnorientierte Gesellschaft des privaten Sektors zur Überwachung von Revisoren. In dieser Funktion erstellt das PCAOB abgeleitete, konkretere Vorschriften, welche von den Revisionsgesellschaften zu beachten sind und dadurch indirekt Einfluss auf die zu prüfenden Unternehmen selbst haben.[9]

2.1.3. Örtlicher Geltungsbereich

Die Anforderungen aus dem Sarbanes-Oxley Act sowie abgeleitete Vorschriften gelten für Gesellschaften, welche an einer US-Börse kotiert sind. Dies beinhaltet neben amerikanischen Gesellschaften explizit auch nicht-amerikanische Unternehmen, welche in den USA zweit kotiert sind.[10]

2.1.4. Allgemeine Anforderungen

Es existieren zahlreiche Anforderungen, welche direkt oder indirekt aus dem Sarbanes-Oxley Act resultieren und sich auf die Prozesse zur Erstellung des Finanzausweises

---

4 CSG Audit Department (2005a), Seiten 4 bis 6
5 Van der Crone Hans Caspar und Roth Katja (2003), Seite 1
6 US Congress (2002), Sarbanes-Oxley Act, Sec. 302, 906 und 1105
7 SEC (2003); SEC (2007b)
8 US Congress (2002), Sarbanes-Oxley Act, Sec. 101; vgl. auch http://www.pcaob.org
9 vgl. insbesondere PCAOB (2004) und PCAOB (2007)
10 Van der Crone Hans Caspar und Roth Katja (2003), Seite 2

einer Unternehmung auswirken. Im Folgenden wird eine Auswahl von wichtigen Anforderungen aus SOX, SEC und PCAOB aufgeführt:[11]

1. Die Unternehmensführung muss jährlich einen schriftlichen Bericht über das interne Kontrollsystem (IKS) abgeben, das der finanziellen Berichterstattung zugrunde liegt. Dazu ist jeweils eine vorgängige, systematische Beurteilung des IKS durch die Unternehmensführung erforderlich.[12]
2. Bei jeder Abschlussrechnung (inkl. Quartalsabschluss) muss die Unternehmensführung bestätigen, dass die Zahlen im Bericht und die Angaben im Anhang korrekt sind, dass die Unternehmensführung für die Erstellung und den Unterhalt eines IKS verantwortlich ist, dass das IKS implementiert ist und dass wesentliche Kontroll-Schwachstellen sowie entdeckte kriminelle Handlungen gemeldet wurden.[13]
3. Es ist ein Audit Committee zu bilden, es sind mehrere Punkte zur Unabhängigkeit der Revisoren zu beachten und Revisoren müssen bei der eigenen Beurteilung des IKS zahlreiche Punkte berücksichtigen.[14]
4. Grundsätzlich sind keine privaten Kredite an leitende Angestellte zu geben. Zudem gelten strengere Offenlegungsvorschriften bei legalen Insider-Geschäften.[15]
5. Wesentliche Änderungen in der finanziellen „Verfassung“ und in Abläufen / Prozessen der Unternehmung müssen der Öffentlichkeit zeitnah gemeldet werden.[16]
6. Die Unternehmensführung hat bei der Beurteilung des IKS ein anerkanntes Framework zu verwenden. Als ein mögliches, ausreichendes Framework wird namentlich das sogenannte COSO-Framework erwähnt.[17]
7. Die Unternehmensführung muss bei der Beurteilung des IKS sowohl die Gestaltung als auch die Umsetzung der internen Kontrollen überprüfen (Design and Operating Effectiveness). Dabei ist zu dokumentieren, wie die Kontrollen ausgestaltet, wie die Kontrollen getestet wurden und was die Schlussfolgerungen des Managements sind.[18]
8. Revisoren dürfen sich bei der Beurteilung der Wirksamkeit der Kontrollen nicht ausschliesslich auf Befragungen abstützen. Es muss zusätzlich die erstellte Dokumentation berücksichtigt werden und die Prozesse sind üblicherweise mittels sogenannter „Walkthroughs“ systematisch durchzugehen. Dabei ist die gesamte Prozesskette von der Initiierung, Autorisierung, Dokumentierung, Verarbeitung und Berichterstattung unter Berücksichtigung der Wesentlichkeit zu beurteilen. Kontrollen betreffend wirtschaftskriminellen Handlungen sind dabei ebenfalls zu berücksichtigen.[19] (Analoge Aussagen dürften somit für die Beurteilung durch die Unternehmensführung selbst gelten.)

---

[11] Die Auswahl wurde erstellt aufgrund der Original-Gesetzestexte sowie diversen Zusammenfassungen: CSG Audit Department (2005a), Sigrist Beat (2004), Van der Crone Hans Caspar und Roth Katja (2003), Haworth Dwight A. und Pietron Leah R. (2006)

[12] US Congress (2002), Sarbanes-Oxely Act, Sec. 404

[13] US Congress (2002), Sarbanes-Oxely Act, Sec. 302

[14] US Congress (2002), Sarbanes-Oxely Act, Sec. 202ff. und Sec. 301 sowie Sec. 101ff. und PCAOB (2004, 2007) generell.

[15] US Congress (2002), Sarbanes-Oxely Act, Sec. 402 und Sec. 403

[16] US Congress (2002), Sarbanes-Oxely Act, Sec. 409

[17] SEC (2003); SEC (2007b), Seite 50; PCAOB (2004), Paragraph 14; PCAOB (2007), Paragraph 87

[18] SEC (2003), Sec. II.B.3; SEC (2007a), Sec. A.I-II; PCAOB (2004), Paragraph 42; PCAOB (2007), Paragraph 42-45

[19] PCAOB (2004), Paragraph 79-80; PCAOB (2007), Paragraph 34-38

2.2. IT-Aspekte

2.2.1. Anforderungen an die IT

Wie erwähnt, ist der Sarbanes-Oxley Act aufgrund von Bilanzskandalen entstanden und die abgeleiteten Anforderungen zielen primär auf Prozesse und Kontrollen der finanziellen Berichterstattung ab. Heutige Prozesse in diesem Bereich werden in der Regel massgeblich von IT-Systemen unterstützt, wodurch die IT selbst in den Fokus der SOX-Anforderungen rückt.[20]

Während die wichtige Rolle der IT im Zusammenhang mit SOX unbestritten ist, existieren aus den gesetzlichen Vorschriften nur sehr wenige und oft unpräzise Anforderungen an die IT. Die folgenden wichtigen Punkte sind bei einer Umsetzung der SOX Anforderungen aus IT-Sicht generell zu beachten, da diese Themen direkt oder indirekt in den Vorschriften des Sarbanes-Oxley Act erwähnt werden:[21]

- Es ist auf IT-Systeme zu fokussieren, welche Prozesse der finanziellen Berichterstattung unterstützen und beeinflussen.[22]
- Es ist eine Risikobeurteilung für die betroffenen IT-Systeme durchzuführen, wobei die Wahrscheinlichkeit von Fehlern sowie kriminellen Handlungen und deren Ausmass im Finanzabschluss zu berücksichtigen sind.[23]
- Wesentliche Kontrollen in der IT-Umgebung sind zu dokumentieren und hinsichtlich Ausgestaltung und Umsetzung zu beurteilen. Dabei sind die festgestellten Mängel zu gewichten, wesentliche Schwachstellen zu berichten und schliesslich zu beheben.[24]
- Namentlich sollten Kontrollen aus den folgenden Bereichen im IT-Umfeld durchgeführt werden: Programm-Entwicklung, Programm-Änderungen, Computer Betrieb und Zugriff auf Programme und Daten.[25]
- Das mehrmals referenzierte COSO-Framework aus dem Jahr 1994 erwähnt die Themengebiete „Control Environment“, „Risk Assessment“, „Control Activities“, „Information and Communication“ und „Monitoring“, wodurch sich Anforderungen an die IT ableiten lassen.[26] Zudem existiert eine Abbildung[27] vom COSO Framework zu COBIT.[28]

---

[20] PCAOB (2004), Paragraph 75: „The nature and characteristics of a company’s use of information technology in its information system affects the company’s internal control over financial reporting.”

[21] In Anlehnung an IT Governance Institute (2006a), Seite 12 und 27ff.

[22] US Congress (2002), Sarbanes-Oxley Act, Sec. 302 und 404; SEC (2007a), Sec. A.1.d

[23] PCAOB (2004), Paragraph 40 und 49; SEC (2007a) generell

[24] PCAOB (2004), Paragraph 42; PCAOB (2006b); SEC (2003), Sec. II.B.3; US Congress (2002), Sarbanes-Oxley Act, Sec. 404; SEC (2007a) generell

[25] PCAOB (2004), Paragraph 50; SEC (2007a), Sec. A.1.d

[26] Das ursprüngliche COSO-Framework wurde 2004 ergänzt (vgl. COSO (2004)). Im Zusammenhang mit SOX wird aber oft auf das Framework aus dem Jahre 1994 verwiesen, weshalb im Rahmen dieser Arbeit ebenfalls auf COSO (1994) fokussiert wird.

[27] vgl. Anhang 2 in IT Governance Institute (2007)

[28] COBIT ist ein international anerkanntes Modell für IT-Security, IT-Audit und IT Governance; vgl. z.B. Zihlmann Alex (2006), Seite 25

2.2.2. IT Governance Institute: "IT Control Objectives for Sarbanes-Oxley"

Während das COSO Framework ein anerkannter Standard im Fachbereich ist, macht es kaum Aussagen bezüglich IT spezifischen Aspekten. Hier können anerkannte Informationssicherheitsstandards wie beispielsweise COBIT, ISO/IEC 27001 & 27002 oder die IT-Grundschutz-Kataloge weiterhelfen.[29] Diese Standards sind allerdings nicht speziell auf SOX ausgerichtet.

In der Literatur und Praxis wird bei der Verbindung von SOX und IT häufig das Werk „IT Control Objectives for Sarbanes-Oxley" des IT Governance Institutes (ITGI) erwähnt.[30] Zwar handelt es sich hierbei nicht um einen explizit vom Gesetzgeber genannten Standard, trotzdem nimmt das Werk eine bedeutende Rolle im Bereich SOX und IT ein, insbesondere aus folgenden Gründen:

- Das Dokument „IT Control Objectives for Sarbanes-Oxley" besitzt einen engen Bezug zum weltweit anerkannten und umfassenden IT-Framework COBIT: Der Herausgeber ist in beiden Fällen die ISACA[31] beziehungsweise die daraus abgeleitete Stiftung für internationale Standards, das IT Governance Institute. Zudem ist „IT Control Objectives for Sarbanes-Oxley" aus COBIT entstanden und besitzt detaillierte Querverweise.
- Es werden aus dem Blickwinkel von SOX konkrete IT-Kontrollziele aufgeführt: Eingangs ist zwar ein „Disclaimer" angebracht und es wird stets darauf hingewiesen, dass bei einer Umsetzung der SOX Anforderungen die jeweiligen Eigenheiten der Unternehmung zu berücksichtigen sind, dennoch geht das Dokument detailliert auf Kontrollziele ein und gibt ausführliche Beispiele von Kontrollaktivitäten und Hilfestellungen.
- Der Bezug zum COSO Framework ist mit der Abbildung über COBIT gegeben.
- Es werden anhand einer sogenannten „Road Map" Empfehlungen zum Projektvorgehen bei der Einführung von SOX in einer Unternehmung gegeben.
- Das Dokument wurde seit seiner Einführung im Jahre 2004 aktualisiert, wodurch diverse praktische Erfahrungen im Umgang mit SOX eingeflossen sind.

Das IT Governance Institute (2006a) stützt sich direkt auf den Sarbanes-Oxley Act gemäss US Congress (2002), PCAOB (2004) und SEC (2003) ab und verbindet diese gesetzlichen Vorgaben mit COSO und COBIT. Daneben werden zahlreiche Hilfsmittel für die Praxis angegeben.[32]

2.2.3. Kategorien von Kontrollen im IT-Umfeld

Durch eine starke Integration der IT in die Geschäftsprozesse sowie die diversen Schichten und Module innerhalb der IT selbst ergeben sich zahlreiche Möglichkeiten für „Kontrollen im IT-Umfeld". Eine Unterteilung in verschiedene Kategorien ist wich-

---

[29] IT Governance Institute (2007), ISO/IEC (2005a) ISO/IEC (2005b) und BSI (2006)

[30] IT Governance Institute (2006a); diese Publikation wird beispielsweise erwähnt in Dummer Stefan (2006), Liegl Patrick (2005), Vaccaro Angelo (2005), Zihlmann Alex (2006)

[31] ISACA (2007a), Seite 5: „With more than 50'000 members in more than 140 countries, ISACA is a recognized worldwide leader in IT governance, control, security and assurance. … The IT Governance Institute (ITGI) was established by ISACA in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology."

[32] Vgl. beispielsweise "Project Estimating Tools" oder "Issues in Using SAS 70 Examination Reports" im Anhang des IT Governance Institutes (2006a)

tig, weil die Zuständigkeiten für die jeweiligen Kontrollen nicht immer gleich sind und die Nähe zum Geschäftsprozess beziehungsweise Finanzausweis variiert. Zudem haben die Kontrollen selbst teilweise unterschiedliche Charakteristiken. Eine mögliche Aufteilung von IT-Kontrollen ist in der nachfolgenden Abbildung dargestellt:[33]

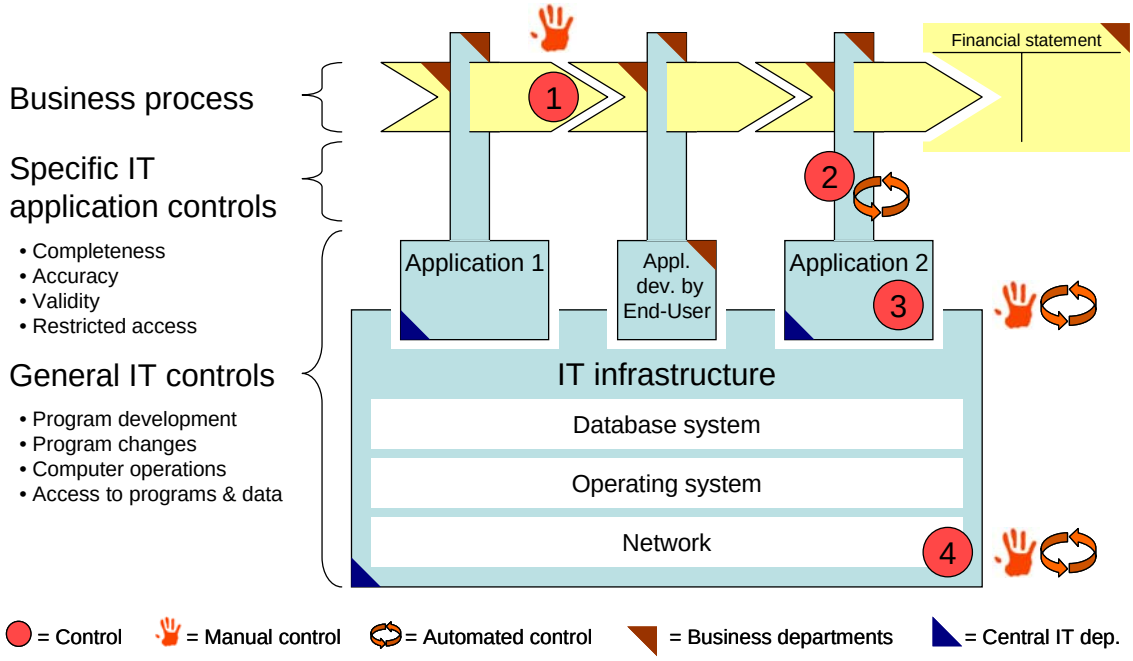

Abbildung 1 – Kontrollen im IT-Umfeld

Der Begriff „Kontrolle“

Der Begriff „Kontrolle“ wird auf zwei miteinander verwandte, aber doch recht unterschiedliche Arten verwendet: Unter “kontrollieren“ im engeren Sinn verstehen die meisten den klassischen Soll/Ist-Vergleich (z.B. Geschwindigkeitskontrolle). Vor allem Revisoren und immer häufiger auch Sicherheitsfachleute fassen den Begriff „kontrollieren“ viel breiter und meinen damit „definieren“, „steuern“, „regeln“ oder „überprüfen.[34] Diese zweite Interpretation dürfte auch den Vorschriften von SOX sowie ISO/IEC 2700x zugrunde liegen und wird in dieser Arbeit in diesem Sinne verstanden.

Manuelle Kontrollen im „traditionellen“ Geschäftsprozess

Zahlreiche Geschäftsprozesse einer Unternehmung beeinflussen die finanzielle Berichterstattung massgeblich und führen über eine Kette von Schritten schliesslich in die Buchhaltungsabteilung. Dabei werden entlang des Prozesses klassische, manuelle Kontrollen durchgeführt wie beispielsweise ein Vergleich der Zahlen in der Lagerbuchhaltung mit dem nachgezählten Lagerbestand. In dieser „traditionellen“ Form führt ausschliesslich der Fachbereich die Kontrolle durch und ist für deren Effektivität verantwortlich.

---

[33] Eigene Darstellung, in Anlehnung an IT Governance Institute (2006a), PricewaterhouseCoopers LLP (2006), Kaufmann Helmut (2007), CSG Audit Department (2005b)

[34] ITACS Training (2007), Seite 9

Spezifische IT-Applikationskontrollen

Ein Teil der manuellen Kontrollen des „traditionellen“ Geschäftsprozesses wurde mit zunehmender Integration der IT ersetzt und wird heute automatisch durch IT-Applikationen durchgeführt. Beispiele solcher spezifischen IT-Applikationskontrollen sind beispielsweise „Wertebereich-Checks bei der Dateneingabe“ oder „Summenvergleiche zwischen zwei Beständen“. Es handelt sich bei den spezifischen IT-Applikationskontrollen um massgeschneiderte Kontrollen für die jeweiligen Geschäftsprozesse mit dem Ziel, dass die betroffenen Daten vollständig, korrekt, genehmigt und vor unberechtigtem Zugriff geschützt[35] sind. Spezifische IT-Applikationskontrollen befinden sich an der Schnittstelle zwischen den Tätigkeiten des Fachbereichs und der IT-Abteilung. Häufig wird die abschliessende Verantwortung über diese Kontrollen dem Fachbereich zugeordnet.[36] In einigen Fällen ist eine manuelle Intervention erforderlich, wenn die automatische Kontrolle eine Abweichung feststellt. Deshalb verwenden einige Autoren zusätzlich noch den Begriff „halb-automatische Kontrolle“.

Generelle IT-Kontrollen

Die Effektivität spezifischer IT-Applikationskontrollen ist untrennbar mit der allgemeinen Sicherheit der IT-Applikation sowie der IT-Infrastruktur ganz generell verbunden. Wenn beispielsweise Programm-Teile einer IT-Applikation uneingeschränkt und von jedermann abgeändert werden könnten, so wäre die Effektivität der Kontrollen in dieser Applikation nicht mehr gegeben: bei kriminellen Absichten könnte ja problemlos der Summenvergleich zwischen zwei Beständen ausgeschaltet werden, die Genehmigungs-Limiten könnten umgangen werden usw.

Aus diesem Grund sollen „generelle IT-Kontrollen“ die Sicherheit im IT-Umfeld ganz allgemein sicherstellen. Die betreffenden Kontrollen stehen somit nur indirekt in Verbindung zum übergeordneten Geschäftsprozess und zur finanziellen Berichterstattung. Einige Autoren unterscheiden dabei noch zwischen „generellen IT-Applikationskontrollen“ und „generellen IT-Infrastrukturkontrollen“, indem sie den Fokus auf das jeweilige Teilgebiet einschränken.

Die generellen IT-Kontrollen können weiter unterteilt werden, wie dies beispielsweise im Rahmen von SOX wie folgt vorgeschlagen wird: Programm-Entwicklung, Programm-Änderungen, Computer Betrieb und Zugriff auf Programme und Daten. IT-Standards wie COBIT, ISO/IEC 27002 oder die IT-Grundschutz-Kataloge beziehen sich hauptsächlich auf solche „generellen IT-Kontrollen“, da diese Kontrollen grundlegender Natur sind und nach kleineren Anpassungen häufig direkt von den Unternehmungen übernommen werden können, im Gegensatz zu den „spezifischen IT-Applikationskontrollen“ mit Abhängigkeiten zu den sehr individuellen Geschäftsprozessen.

Die Hauptverantwortung für die generellen IT-Kontrollen liegt bei der IT. Es kann sich dabei um automatische Kontrollen handeln, wie beispielsweise ein Deaktivieren von inaktiven Benutzerkonten. Ebenso sind manuelle Kontrollen denkbar, wie beispielsweise das Überprüfen, ob ein Programm getestet wurde, bevor es in die Produktion verschoben wird.

---

[35] CAVR ist ein Ansatz von PwC zur Einteilung von Kontrollen; vgl. z.B. PricewaterhouseCoopers LLP (2006), Seite 11

[36] vgl. z.B. IT Governance Institute (2007), Seite 15 und 16

Applikationen von End-Anwendern

Spezielle Beachtung ist IT-Applikationen zu schenken, welche vom Fachbereich, sprich Endanwendern, und nicht von der zentralen IT-Abteilung entwickelt wurden. Beispielsweise werden in Finanzabteilungen oft komplizierte Berechnungen mit eigenentwickelten Anwendungen in Tabellenkalkulationsprogrammen durchgeführt. Prinzipiell gelten analoge SOX-Anforderungen für solche IT-Applikationen. Es sind also auch hier Kontrollen bei der Entwicklung und Änderung von Programmen durchzuführen, und der Betrieb sowie Zugriff ist geordnet zu regeln. Im Umfeld des Fachbereichs besteht jedoch das inhärente Risiko, dass Endanwender nicht so gut mit den gängigen generellen IT-Kontrollen vertraut sind und entsprechende Massnahmen nicht ergreifen. Die abschliessende Verantwortung über IT-Kontrollen bei Applikationen von End-Anwendern liegt im Fachbereich. Es ist jedoch ratsam, dass der Fachbereich bei der Entwicklung entsprechender IT-Applikationen von Spezialisten aus der IT-Abteilung unterstützt wird.[37]

2.3. Aktueller Stand

Die Vorschriften aus dem Sarbanes-Oxley Act wurden sehr generell formuliert und sind für Unternehmen aus unterschiedlichen Brachen und mit unterschiedlichen Grössen verbindlich. Dementsprechend sind Erfahrungsaustausche und Meinungen von Experten in einem solchen Umfeld von zentraler Bedeutung. In diesem Zusammenhang ist insbesondere ein Treffen von Wirtschaftsvertretern zu erwähnen, wo unter der Leitung von SEC und PCAOB an einem sogenannten „Roundtable“ die Erfahrungen seit in Kraft treten von SOX diskutiert wurden. Generell wurde festgestellt, dass sich die Corporate Governance und die Qualität der Kontrollen stark verbessert habe und die Finanzausweise nun viel transparenter und aussagekräftiger seien. Massiv wurde jedoch kritisiert, dass die Kosten für die Umsetzung von SOX unverhältnismässig hoch seien.[38] Ebenso wurde bemängelt, dass die Vorschriften und Anforderungen unpräzise und zu wenig konkret seien. Basierend auf dieser Kritik erarbeiteten SEC und PCAOB im Rahmen eines zweiten „Roundtables“ im Mai 2006 Anleitungen und Änderungsvorschläge für die Umsetzung von SOX. Die entsprechenden Entwürfe[39] wurden im Dezember 2006 zur Stellungnahme veröffentlicht, und bis zum Einsendeschluss im Februar 2007 gingen insgesamt über 300 Schreiben ein. Mit Blick auf die IT sind vor allem die Kommentare der ISACA und des IT Governance Institutes erwähnenswert: Es wird bemängelt, dass die Entwürfe immer noch sehr abstrakt formuliert seien und auf generelle IT-Kontrollen sehr knapp eingegangen würde.[40]

Auf dieser Grundlage überarbeiten SEC und PCAOB die entsprechenden Vorgaben und Richtlinien nochmals. Im Juli 2007 wurde schliesslich der PCAOB Standard Nummer 2 offiziell durch den Standard Nummer 5 ersetzt.[41] Ebenso setzte die SEC ihre Änderungen zu den SOX-Vorgaben in Kraft und veröffentlichte eine Richtlinie mit Empfehlung-

---

[37] Beispielsweise erfolgt die Unterstützung, indem ein Vorschlag über durchzuführende generelle IT Kontrollen gemacht wird. Vgl. dazu auch PricewaterhouseCoopers LLP (2004a)

[38] SEC (2006); PCAOB (2006a), Seite 2 und 3; Butler Henry N. und Ribstein Larry E. (2006) sprechen bei SOX gar von einem Debakel.

[39] SEC (2006); PCAOB (2006a)

[40] ISACA (2007a) und ISACA (2007b)

[41] Die PCAOB Standards No. 2 und 5 sind insbesondere für Revisoren im Zusammenhang mit SOX von zentralster Bedeutung. (vgl. PCAOB (2004) und PCAOB (2007))

en zur Umsetzung.[42] Zusammengefasst ergeben sich die folgenden wichtigen Änderungen und Aussagen: [43]

- Die Unternehmensführung besitzt höhere Flexibilität in ihrer Beurteilung der internen Kontrollen. Bei der Beurteilung soll das zugrunde liegende Risiko noch stärker berücksichtigt und unwesentliche Bereiche ausgeklammert werden. Dabei soll die Analyse von oben nach unten (Top-Down) und mit starkem Fokus auf unmittelbare Prozesse der finanziellen Berichterstattung erfolgen.
- Übergeordnete Kontrollen[44] sind im IKS speziell zu beachten. Diese Kontrollen können sich nämlich auf andere Kontrollen auswirken und dafür sorgen, dass bei der Beurteilung der Effektivität von Detail-Kontrollen weniger Zeit aufgewendet werden muss.
- Die Dokumentationspflicht der Unternehmensführung wird vereinfacht (aber nicht aufgehoben): So kann die Unternehmensführung den Dokumentationsaufwand bei der Beurteilung des IKS reduzieren, wenn die Unternehmensführung selbst direkt im Prozess involviert ist, indem vor allem die Interaktion dokumentiert wird. Ebenso soll der zuvor genannte risikobasierte Ansatz ebenfalls zu einer Vereinfachung führen, indem bei kleinen Risiken weniger Dokumente als Nachweis aufbewahrt werden müssen. Eine Dokumentation des gesamten Geschäftsprozesses mit sämtlichen Kontrollen ist aufgrund ähnlicher Überlegungen ebenfalls nicht zwingend erforderlich.
- Revisoren müssen keine Meinung mehr abgeben über die Beurteilung, welche die Unternehmensführung zum IKS gemacht hat. Es ist ausreichend, wenn die Revisoren die Effektivität des IKS selbst beurteilen.
- Revisoren können sich bei der Beurteilung des IKS nun einfacher auf bereits durchgeführte Arbeiten abstützen.

In Bezug auf die IT werden keine neuen konkreten Angaben gemacht. Bestätigt wird jedoch die bis anhin konkrete Unterteilung der generellen IT-Kontrollen in „Programm-Entwicklung“, „Programm-Änderungen“, „Computer Betrieb“ und „Zugriff auf Programme und Daten“. Zudem heben SEC und PCAOB ausdrücklich hervor, dass die IT nicht separat behandelt werden sollte und dass bei der Beurteilung stets auf die damit verbundenen Geschäftsprozesse beziehungsweise Risiken zu achten ist.[45]

3. ISO/IEC Standards zur Informationssicherheit

3.1. Überblick

3.1.1. ISO und IEC

Die Internationale Organisation für Standards (ISO) ist eine Vereinigung von Vertretern aus über 150 Ländern zur Entwicklung von weltweiten Standards. Zurzeit sind über 16'000 Standards veröffentlicht, wobei Unternehmen sich nach einigen dieser Standards

---

42 SEC (2007b); SEC (2007a)

43 in Anlehnung an KPMG (2006) sowie SEC (2007a, 2007b) und PCAOB (2007)

44 PCAOB und SEC sprechen von sogenannten „Entity-Level Controls“; diese Kontrollen beziehen sich auf verschiedene Bereiche einer Unternehmung und können beispielsweise sein: Management Philosophie, ethische Werte, Zuordnung von Kompetenzen und Verantwortung etc.; vgl. SEC (2007a), Sec. II.A

45 SEC (2007a), Sec. II.A.1d; PCAOB (2007), Paragraph 36

zertifizieren lassen können.[46] Bekannteste Werke sind insbesondere die ISO 9000 Familie mit Fokus auf Qualitätsmanagement und die ISO 14000 Familie zum Umgang mit der Umwelt.

Die ISO arbeitet eng mit diversen Partnern zusammen. Im Bereich der Informations- und Telekommunikationstechnologie ist dies insbesondere die Internationale Elektrotechnische Kommission (IEC[47]), ein internationales Normierungsgremium für Elektrotechnik mit Sitz in Genf und über 50 Länder-Mitgliedern in Form von Nationalen Komitees, sowie der Internationalen Fernmelde-Union (ITU[48]), einer Unterorganisation der Vereinten Nationen mit über 190 Mitgliedstaaten zur Standardisierung und Entwicklung der Telekommunikation.

3.1.2. ISO/IEC 2700x Familie

Die ISO und IEC konzentriert sich im Rahmen einer gemeinsamen Gruppe, dem sogenannten „Joint Technical Committee 1 – Subcommittee 27“, auf Aspekte der IT-Sicherheitstechnik. Diese Gruppe umfasst über 30 Mitgliedstaaten[49] und entwickelt unter dem Namen ISO/IEC 2700x eine Reihe von Standards zum Thema Informationssicherheit:

ISO-Nr.	**Inhalt**	**Status** (Aktuelle Version)
ISO/IEC 27000	Grundlagen und Begriffe (baut auf Teilen des ISO 13335 und 17799 auf)	in Entwicklung
ISO/IEC 27001	Anforderungen an ein Informations-Sicherheits-Management-System (ISMS) (überarbeite Version des BS 7799, Teil 2)	veröffentlicht am 15.10.2005
ISO/IEC 27002	Anleitung zum Management der Informationssicherheit (Synonym für ISO/IEC 17799:2005; abgeleitet vom BS 7799, Teil 1)	veröffentlicht am 15.06.2005; Namensänderung im Juli 2007
ISO/IEC 27003	ISMS Implementierungsanleitung (Ergänzungen und Hilfestellungen zu ISO/IEC 27001 werden hier behandelt.)	in Entwicklung
ISO/IEC 27004	Metriken zur Messung der Effektivität von Kontrollen	in Entwicklung
ISO/IEC 27005	Risikomanagement für Informationssicherheit (teilweise basierend auf ISO/IEC 13335)	in Entwicklung
ISO/IEC 27006	Anforderungen für die Akkreditierung von Zertifizierungsstellen, welche ISMS prüfen und Zertifikate vergeben	veröffentlicht am 01.03.2007

[46] ISO (2006). Die ISO führt selbst keine Zertifizierungen durch.
[47] Internet: http://www.iec.ch
[48] Internet: http://www.itu.int
[49] 35 sogenannte Participating Members und 13 Observing Members; Stand Juni 2007

ISO-Nr.	Inhalt	Status (Aktuelle Version)
ISO/IEC 27007	ISMS Audit Anleitung	in Entwicklung

Tabelle 1 – ISO/IEC 2700x Familie im Überblick[50]

Während mit ISO/IEC 27000 die grundlegenden Begriffe erklärt werden, bildet der Standard ISO/IEC 27001 den eigentlichen Kern dieser „Familie“ und dient als Grundlage für Zertifizierungen. Dieser Kern ist relativ kurz gefasst[51] und wird durch die weiteren Standards ergänzt, welche Anleitungen und Hilfestellungen zu Teilaspekten und Spezialthemen beinhalten. Dabei ist insbesondere der Standard ISO/IEC 27002 hervorzuheben, welcher ausführlich auf Kontrollziele und Massnahmen eingeht.

3.2. ISO/IEC 27001:2005

3.2.1. Inhalt

Ausgangslage für den ISO/IEC Standard 27001 bilden die Ziele zur Informationssicherheit, namentlich Vertraulichkeit, Verfügbarkeit und Integrität.[52] Der Standard beschreibt ein sogenanntes „Informations-Sicherheits-Management-System (ISMS)“. Darunter wird derjenige Teil eines Managementsystems verstanden, welcher die Informationssicherheit auf der Basis einer Risikobeurteilung sicherstellt, und zwar mittels systematischer Erstellung, Umsetzung, Ausführung, Überwachung und Weiterentwicklung. Der Standard richtet sich vor allem ans Management und an IT-Sicherheitsbeauftragte. Aufgrund der engen methodischen Anlehnung an die ISO 9000 / 14000 Standards kann der ISO/IEC 27001 als Qualitätsstandard für Managementsysteme bezüglich Informationssicherheit angesehen und mit bestehenden Managementsystemen kombiniert werden.[53]

Der Kernpunkt des ISO/IEC 27001 ist das Verständnis von Informationssicherheit als geplanter, gelebter, überwachter und sich kontinuierlich verbessernder Prozess.[54] Dazu verwendet der Standard das „Plan-Do-Check-Act“ Modell, auch bekannt unter den Namen PDCA-Modell oder Deming-Cycle[55]. Das adaptierte ISO/IEC 27001 Modell stellt sich schematisch wie folgt dar:

---

[50] in Anlehnung an Weiss Peter (2007), Dummer Stefan (2006) und ISO (2007)
[51] Die wesentlichen Anforderungen von ISO/IEC 27001 sind auf 9 Seiten beschrieben.
[52] Es werden im Standard weiter erwähnt: Authenticity, Accountability, Non-Repudiation und Reliability.
[53] BITKOM und DIN (2006), Seite 25
[54] Dummer Stefan (2006), Seite 77
[55] in Anlehnung an den ursprünglichen Erfinder, Dr. William Edwards Deming

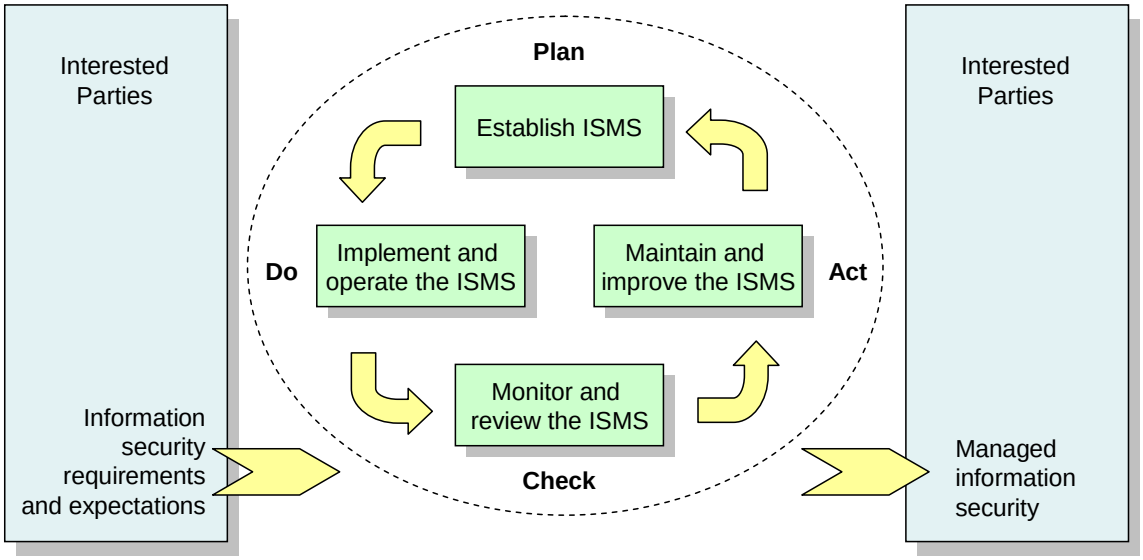

Abbildung 2 – PDCA-Modell gemäss ISO/IEC 27001 (2005a)

Im Standard werden für jede der vier Phasen die Anforderungen beziehungsweise die zu ergreifenden Massnahmen beschrieben. Es sind dies im Wesentlichen:

Plan: In Abstimmung mit den Unternehmenszielen ist der Umfang des ISMS zu bestimmen und in einer Richtlinie festzuhalten. Danach ist eine Risikobeurteilung durchzuführen. Schliesslich sind auf der Grundlage des ISO/IEC 27002 (!) geeignete Kontrollziele und konkrete Massnahmen auszuwählen.

Do: Der Plan zum Umgang mit Risiken ist zu dokumentieren und umzusetzen. Insbesondere sind nun die ausgewählten Kontrollen zu implementieren, die Mitarbeiter zu sensibilisieren und zu schulen sowie den Betrieb des ISMS generell sicherzustellen. Dazu sind auch Metriken zur Messung der Effektivität der Kontrollen zu definieren.

Check: Die umgesetzten Massnahmen sind nun zu überwachen. Dazu sollen die direkt involvierten Personen wie auch unabhängige Instanzen (wie beispielsweise mittels intern unabhängigen Qualitäts-Auditoren) beitragen. Die zuvor definierten Metriken sind zu berücksichtigen. Zudem sind in regelmässigen Abständen die eingangs festgelegten Rahmenbedingungen (wie Umfang des ISMS, Ergebnisse der Risikobeurteilung etc.) erneut zu hinterfragen und nötigenfalls anzupassen. Ergebnisse sind dem Management zu kommunizieren.

Act: Die identifizierten Verbesserungsmöglichkeiten sind umzusetzen. Die involvierten Personen und Interessengruppen sind stufengerecht über die Ergebnisse sowie das weitere Vorgehen zu informieren.

Zusätzlich fordert der Standard eine umfassende Dokumentation der Ergebnisse aus diesen Phasen. Dabei sind insbesondere der Umfang des ISMS, das Vorgehen und die Ergebnisse des Risikomanagements sowie die daraus abgeleiteten Massnahmen und Kontrollen zu dokumentieren. Es ist darauf zu achten, dass die Dokumente geordnet abgelegt werden, Änderungen kontrolliert erfolgen und zeitgerecht den betroffenen Personen kommuniziert werden.

Eine weitere wichtige Anforderung aus dem ISO/IEC 27001 Standard ist die Einbindung der obersten Führungsstufe. So soll die Geschäftsleitung ihre Zustimmung zur konsequenten Umsetzung des Standards geben, in den PDCA-Ablauf involviert werden und entsprechende Ressourcen zur Verfügung stellen.

Ein wesentliches Element mit weitreichenden Konsequenzen ist die Referenz im ISO/IEC 27001 auf den ISO/IEC 27002 Standard.[56] Bei der Festlegung von Massnahmen im PDCA-Ablauf müssen sämtliche ISO/IEC 27002 Kontrollen zwingend in Betracht gezogen werden. Auf die Umsetzung der entsprechenden Massnahmen darf nur verzichtet werden, wenn Risikoüberlegungen dies rechtfertigen.

Bei einer Risikobeurteilung im PDCA-Ablauf sind sämtliche ISO/IEC 27002 Kontrollen zu berücksichtigen.

Bei der Festlegung von Massnahmen aufgrund einer Risikobeurteilung im PDCA-Ablauf müssen somit sämtliche ISO/IEC 27002 Kontrollen zwingend in Betracht gezogen werden.

3.2.2. Zertifizierung

Eine Zertifizierung gemäss ISO Standard zur Informationssicherheit kann ausschliesslich auf der Basis von ISO/IEC 27001 erfolgen. Da dieser Standard wie erwähnt auf ISO/IEC 27002 Standard verweist, muss dieser zweite Standard bei einer Zertifizierung jedoch zwingend berücksichtigt werden. Es ist aber nicht möglich, unter Vernachlässigung des ISO/IEC 27001 Standards eine ausschliesslich auf den ISO/IEC 27002 Standard ausgerichtete Zertifizierung zu erhalten.

Weltweit sind über 50 Zertifizierungsstellen zugelassen, die Prüfungen auf der Basis von ISO/IEC 27001 durchführen. Ein Zertifikat kann für eine Unternehmung als ganzes oder für eingeschränkte Unternehmensteile vergeben werden.

Weltweit besitzen über 3’000 Unternehmungen ein ISMS-Zertifikat. Grundlage für diese Zertifikate bildet der ISO/IEC 27001 Standard oder sein Vorgänger, der BS 7799-2 Standard. Seit Juni 2006 sind Zertifizierungen auf der Basis von BS 7799-2 nicht mehr möglich. Unternehmungen mit Zertifikaten zur Vorgängerversion besitzen jedoch die Möglichkeit, im Rahmen der Re-Zertifizierung auf den neuen ISO Standard zu wechseln. Tabelle 2 zeigt einen Überblick zu den herausgegebenen ISMS-Zertifikaten:

[56] vgl. „Establish the ISMS – Select control objectives and controls for the treatment of risks“ sowie Anhang A in ISO/IEC (2005a)

Anzahl herausgegebener ISMS-Zertifikate:	*3'781*
Anzahl herausgegebener ISO/IEC 27001 Zertifikate:	*2'026*
Anzahl herausgegebener ISO/IEC 27001 Zertifikate, abgeleitet von BS 7799-2 durch Erneuerung:	*1'104*
Anzahl ISMS-Zertifikate bei Schweizer Unternehmungen:	*12* (57)

Tabelle 2 – Statistik ISMS-Zertifikate; Stand Juli 2007 [58]

Die Informationssicherheit nimmt in der heutigen Welt eine immer wichtigere Rolle ein. Vermehrt fordern unterschiedlichste Anspruchsgruppen wie Kunden, Partner oder Regierungen, dass Massnahmen zur Sicherstellung der Informationssicherheit ergriffen werden. Eine offizielle Bestätigung in Form eines ISO/IEC 27001 Zertifikats kann einer Unternehmung helfen, ihre Anstrengungen in diesem Bereich zu untermauern und gegenüber Konkurrenten einen Wettbewerbsvorteil zu erhalten.

3.3. ISO/IEC 27002:2005

3.3.1. Entstehungsgeschichte

Der Britische Standard BS 7799-1 diente im Jahre 2000 als Grundlage für den damals neu geschaffenen ISO/IEC 17799 Standard. In der Zwischenzeit wurde dieser ISO Standard überarbeitet und im Juni 2005 veröffentlicht. Um eine einheitliche Namensgebung zu verwenden, wurde der Standard im Juli 2007 in ISO/IEC 27002:2005 umbenannt. Inhaltlich unterscheidet sich der ISO/IEC 17799:2005 keineswegs vom ISO/IEC 27002:2005 Standard. In dieser Arbeit werden diese Bezeichnungen deshalb synonym und abgekürzt (ISO/IEC 27002 oder ISO 27002) verwendet.

3.3.2. Inhalt

In der Einleitung des Standards wird der Fokus auf Informationssicherheit hervorgehoben. Es wird darauf hingewiesen, dass Informationen nicht nur in elektronisch gespeicherten Daten vorkommen, sondern ebenso aus handgeschriebenen Notizen oder Gesprächen hervorgehen. Zudem wird eingangs nochmals die Wichtigkeit einer Risikobeurteilung unterstrichen, die als Ausgangslage für die Auswahl von Kontrollen dienen soll.

Der Hauptteil des ISO/IEC 27002 Standards besteht aus 11 Bereichen, sogenannten „Clauses", mit insgesamt 39 Sicherheitskategorien. Abbildung 3 stellt den Aufbau des Standards schematisch dar:

---

[57] Schweizer Unternehmungen mit ISMS-Zertifikaten sind: AlpTransit Gotthard AG; Bedag Informatik AG; CPGMarket.com SA; innova Versicherungen AG / innova Krankenversicherung AG; Reuters SA; RTC Real-Time Center AG; Serono International S.A.; Serono International S.A. The Information Technology Function; SRG SSR idée Suisse; Swiss Post - Post Finance Information Technology; Swisscom IT Services AG; T-Systems Schweiz AG

[58] Zahlen gemäss internationalem Register für ISMS-Zertifikate; im Internet abrufbar unter http://www.iso27001certificates.com

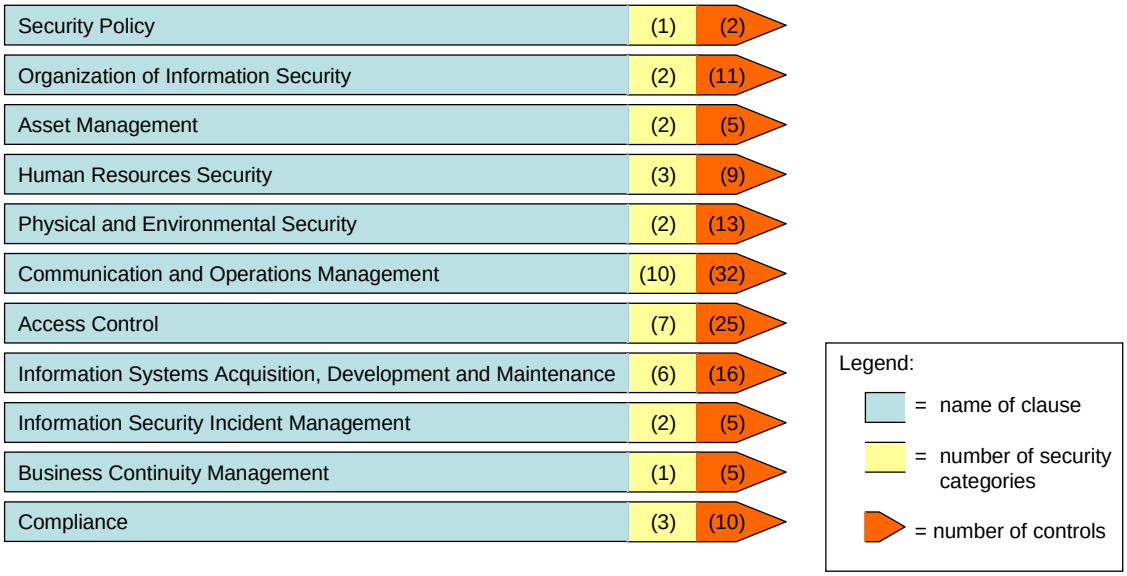

Abbildung 3 – ISO/IEC 27002 Bereiche, Sicherheitskategorien und Kontrollen

Zu jeder Sicherheitskategorie ist ein Kontrollziel angegeben, wo festgelegt wird, was eigentlich erreicht werden soll. Daneben sind jeweils eine oder mehrere Kontrollen (in Form von Massnahmen) definiert, die zur Erreichung des Kontrollziels beitragen. Gesamthaft umfasst der Standard 133 Kontrollen, und jede Kontrolle enthält weiterführende Anleitungen und Hilfstexte.[59]

Der ISO/IEC 27002 Standard stellt indirekt eine Verbindung zu SOX her, indem in der Einleitung und im Kapitel „Compliance“ unter anderem gefordert wird, dass die gesetzlichen Anforderungen identifiziert werden und diese als Ausgangslage für die zu ergreifenden Massnahmen dienen.

3.3.3. Gegenüberstellung mit anderen Standards

Die Kontrollen im ISO/IEC 27002 Standard sind relativ allgemein formuliert. Die hohe Anzahl an Kontrollen und die ausführlichen Zusatzangaben ermöglichen jedoch eine flexible Anpassung an die Grösse der jeweiligen Unternehmung unter gleichzeitiger Wahrung einer gewissen Tiefe. Die nachfolgende Abbildung zeigt die Einordnung des ISO/IEC 27002 Standards im Vergleich zu anderen international anerkannten IT-Frameworks:

[59] Der Standard spricht von sogenannter “Implementation Guidance” und “Other Information”.

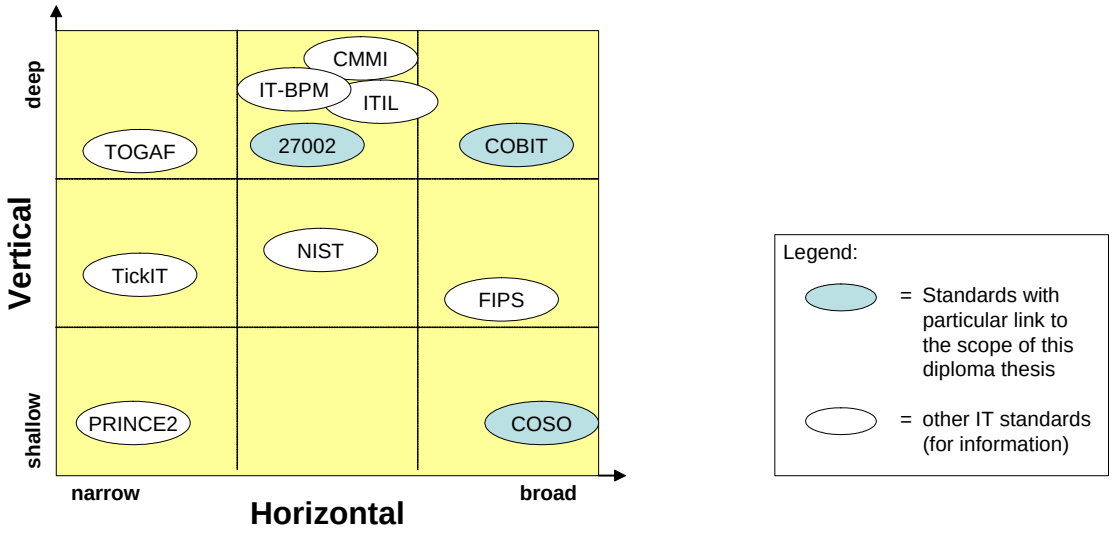

Abbildung 4 – ISO/IEC 27002 im Vergleich mit anderen IT-Standards[60]

Das im SOX-Umfeld häufig zitierte COSO Framework deckt sehr viele Aspekte in der Breite ab, geht aber insbesondere auf IT-Details kaum ein. Demgegenüber ist der COBIT Standard sowohl im Umfang als auch in der technischen Tiefe weitreichend und geht über die reinen Sicherheitsaspekte von ISO/IEC 27002 hinaus.

4. Vergleich von SOX und ISO/IEC 27001 & 27002

4.1. Einleitung

In den beiden vorangegangen Kapiteln wurden die Grundlagen und Anforderungen sowohl von SOX als auch von ISO/IEC 27001 und 27002 vorgestellt. Aus den Beschreibungen ist bereits erkennbar, dass zwischen den beiden Ansätzen Verbindungen und Gemeinsamkeiten existieren. Einerseits verweist SOX auf anerkannte Frameworks, was beispielsweise ISO/IEC 2700x im IT-Umfeld sein dürfte, und andererseits unterstreichen die ISO/IEC Standards die Bedeutung von gesetzlichen Anforderungen, worunter auch SOX fällt.

In diesem Kapitel wird nun vertieft auf die Gemeinsamkeiten, Schwerpunkte und Unterschiede eingegangen. Dazu wird anhand von Beispielen zuerst die Meinung von anderen Autoren beschrieben. Anschliessend werden SOX-Anforderungen systematisch den ISO/IEC 27001 und 27002 Vorgaben gegenübergestellt und analysiert. Die Analyse stützt sich mehrheitlich auf das weit verbreitete, theoretische Framework des IT Governance Institutes (2006a) und wird mit einem Praxisbeispiel (Credit Suisse) ergänzt.

[60] Abbildung aus IT Governance Institute (2006c), Seite 71

4.2. Beispiele von bisherigen Vergleichen

4.2.1. ISO/IEC 17799:2000 als Ausgangslage für SOX

Dwight A. Haworth und Leah R. Pietron beschreiben in einem Artikel[61] aus dem Jahr 2006, welche Kontrollen aus ISO/IEC 17799:2000 im Zusammenhang mit SOX relevant sind. Dazu gehen die Autoren schrittweise durch sämtliche Kontrollen des ISO/IEC Standards und prüfen, inwieweit die Kontrollen aus Sicht von SOX von Bedeutung sind. Die SOX-Anforderungen werden dabei mehrheitlich aus dem PCAOB (2004) Auditing Standard Nummer 2 abgeleitet. Zusammengefasst kommen die beiden Autoren zu folgenden Ergebnissen:

- Der Grossteil der Kontrollen gemäss ISO/IEC ist für SOX relevant und leistet einen Beitrag zur Erfüllung der SOX-Anforderungen.
- SOX verlangt eine umfassendere Dokumentation[62] als ISO/IEC 17799:2000 im Bezug auf Prozessabläufe, Kontrollen und Tests. Der Fokus liegt dabei auf den Prozessen zur Erstellung des Finanzausweises.
- Kontrollen müssen im Rahmen von SOX häufiger[62] beurteilt werden, als dies bei ISO/IEC 17799:2000 gefordert wird.

Bezüglich der 11 Bereiche (Clauses) aus ISO/IEC 27002 wird im betreffenden Artikel festgehalten:

- Security Policy: Massnahmen in diesem Bereich gehören zu den generellen IT-Kontrollen und sind als solche für SOX relevant.
- Organization of Information Security: Diese Massnahmen können indirekt in Form von generellen Kontrollen („tone at the top“) relevant für SOX sein.
- Asset Management: Ein Inventar ist Ausgangspunkt für weitere Massnahmen und für die von SOX geforderte Dokumentation. Die Klassifikation von Assets wird als wenig SOX relevant eingestuft.
- Human Resources Security: Diese Massnahmen werden als SOX relevant bezeichnet, weil sie auf übergeordneter Stufe wirken.
- Physical and Environmental Security: Physische Sicherheit wird als generelle IT-Kontrolle angesehen, da sie den Zugang zu Systemen und Daten einschränken. Die Umgebungssicherheit dient der Kontinuität der Prozesse zur finanziellen Berichterstattung. Die physische Sicherheit wird als direkt SOX relevant bezeichnet.
- Communications and Operations Management: In den SOX-Anforderungen sind Themen wie „Dokumentation der Abläufe im Betrieb“ und „Funktionstrennung“ direkt erwähnt. Change Management wird speziell als SOX relevant hervorgehoben.
- Access Control: Massnahmen zum logischen Zugriffsschutz werden von D. Haworth & Leah Pietron als wichtigste Kontrollen im Zusammenhang mit SOX beurteilt. Ohne diese Kontrollen können andere Kontrollen einfach umgangen werden. Es sind sämtliche Kontrollen zu diesem Kapitel aus ISO/IEC 17799:2000 als Ausgangspunkt zu berücksichtigen.

---

[61] Haworth Dwight A. und Pietron Leah R. (2006)

[62] Die Ergebnisse der Autoren basieren auf PCAOB (2004) und ISO/IEC 17799:2000. Beide Standards sind in der Zwischenzeit abgelöst worden. Die neuen SOX-Anforderungen von SEC (2007a, 2007b) und PCAOB (2007) sind weniger strikt und so dürften in der Zwischenzeit die Unterschiede betreffend Dokumentation und Häufigkeit der Beurteilung geringer sein. Zudem gehen D. Haworth und L. Pietron in ihrem Artikel nur vom ISO/IEC 17799:2000 Standard aus und berücksichtigen den ISO/IEC 27001 Standard nicht. Letzterer stellt ebenfalls erhöhte Anforderungen; so muss das Management mindestens jährlich die Kontrollen überprüfen.

- Information Systems Acquisition, Development & Maintenance: Kontrollen in diesen Bereichen haben nach Ansicht der Autoren zweithöchste SOX-Priorität. Von zentraler Bedeutung sind insbesondere: Validation von Ein- und Ausgabedaten sowie Verarbeitungskontrollen.
- Information Security Incident Management: Hier werden wichtige Kontrollen zur Aufdeckung von Fehlern und kriminellen Handlungen erwähnt, was im Zusammenhang mit SOX ebenfalls wichtig ist.
- Business Continuity Management: Es existiert ein indirekter Bezug zu SOX, da eine Unternehmung in der Lage sein muss, den Finanzausweis zu erstellen.
- Compliance: Diese Massnahmen sind generell zu beachten.

4.2.2. Weitere Beispiele

Stefan Dummer untersucht in seiner Diplomarbeit[63] die gesetzlichen Forderungen an das Management der Informationssicherheit und die Erfüllung dieser Anforderungen durch IT-Frameworks. Er kommt zum Schluss, dass die ISO/IEC 27001 & 27002 Standards sämtliche SOX-Anforderungen bezüglich Informationssicherheit erfüllen. Es wird zudem eine Kombination mit COBIT vorgeschlagen, um weitere Anforderungen[64] an die IT abdecken zu können.

Jörg Asma beschreibt in einem Artikel[65] die Ähnlichkeiten zwischen SOX (Section 404) und ISO/IEC 27001. Dabei werden die Gemeinsamkeiten in den Bereichen „Risikomanagement“, „Dokumentation“ und „regelmässige Überprüfung der Kontrollen“ hervorgehoben.

Patrick Liegl stellt in seiner Diplomarbeit[66] fest, dass der ISO/IEC 27002 Standard für die Erfüllung der SOX Anforderungen alleine nicht ausreicht. Zur gleichen Schlussfolgerung kommt Malik Datardina[67] in einer Studie. Er weist darauf hin, dass spezifische Applikationskontrollen und das Thema „zeitgerechte, aktuelle und richtige Informationen“ nur indirekt und knapp adressiert werden. Bei beiden Arbeiten wird der ISO/IEC 27001 Standard nicht berücksichtigt.

Martin A. Schwaiger und Hector A. Urbina untersuchen in ihrer gemeinsamen Diplomarbeit,[68] inwieweit verschiedene IT Governance Frameworks die SOX-Anforderungen erfüllen können. Grundlage für die Arbeit bilden PCAOB (2004), ein Ansatz von PwC (2004b) sowie ISO/IEC 27001 und 27002. Die Autoren kommen zum Schluss, dass sich COBIT am Besten zur Erfüllung der SOX-Anforderungen eignet und die ISO/IEC 2700x Standards bei Detailfragen zur Informationssicherheit hinzugezogen werden sollten. Nach ihrer Ansicht gehen die ISO/IEC Standards aber bei der Errichtung einer generellen IT Governance Struktur zuwenig weit und können dadurch die SOX-Anforderungen nicht vollständig erfüllen.

---

63 Dummer Stefan (2006); Grundlage für die Diplomarbeit bildet ISO/IEC 17799:2005

64 S. Dummer erwähnt namentlich Effizienz und Effektivität. Zudem weist er darauf hin, dass COBIT und andere IT-Frameworks bei gewissen Themen weitere hilfreiche Massnahmen nennen.

65 Asma Jörg (2006); Grundlage für den Artikel bildet BS 7799-2:2002.

66 Liegl Patrick (2005), Seite 53; Grundlage für die Diplomarbeit bildet ISO/IEC 17799:2000.

67 Malik Datardina (2005), Seite 18; Grundlage für die Studie bildet ISO/IEC 17799:2005.

68 Schwaiger Martin A. und Urbina Hector A. (2006); Seite 31 und 32

4.3. SOX und ISO/IEC 27001

4.3.1. Grundlage

Wie bereits festgehalten, existieren verschiedene Gremien und Organisationen, welche Anforderungen mit unterschiedlichem Detaillierungs- und Verbindlichkeitsgrad auf der Basis der SOX-Gesetzgebung stellen. Das IT Governance Institute (2006a) beschreibt in Form einer sogenannten „Road Map", wie Unternehmen vorgehen sollten, um die Anforderungen aus der Sarbanes-Oxley Gesetzgebung erfolgreich umzusetzen. Die Empfehlungen in der „Road Map" sind relativ detailliert und beschreiben das Vorgehen mit Blick auf IT-Systeme. Es handelt sich dabei aber um keine zwingenden Anforderungen. Trotzdem sollten die Empfehlungen genau angeschaut und nur bei guter Begründung nicht umgesetzt werden, da das IT Governance Institute eine bedeutende Stellung hat und in der Road Map zahlreiche Erfahrungswerte berücksichtigt worden sind.

ISO/IEC 27001 beschreibt im Zusammenhang mit der Informationssicherheit ebenfalls ein Vorgehensmodell für die Erstellung und den Betrieb eines „Kontrollsystems".

In den drei nachfolgenden Unterkapiteln werden nun die Ergebnisse eines Vergleichs dieser beiden Vorgehensmodelle präsentiert. Eine detaillierte Herleitung dieser Ergebnisse befindet sich im Anhang A.

4.3.2. Übereinstimmung

In den wesentlichen Vorgehensschritten stimmen ISO/IEC 27001 und die IT SOX Compliance Road Map des IT Governance Institutes überein: Es wird von einem kontinuierlichen Verbesserungsprozess ausgegangen. Dabei wird der Fokus zu Beginn festgelegt, es erfolgt eine Risikobeurteilung und daraus abgeleitet werden Kontrollen ausgewählt und umgesetzt. Bei beiden Modellen ist ein Kernelement, dass das System überprüft wird und Schwachstellen identifiziert beziehungsweise adressiert werden. Ebenso unterstreichen sowohl ISO/IEC 27001 als auch die Road Map die Bedeutung der Nachvollziehbarkeit (sprich Dokumentation), die Einbindung des Managements und die Schulung der Mitarbeiter.

4.3.3. Zusätzliche Aspekte bei SOX

Fokus auf Finanzabschluss und Dokumentation der Geschäftsprozesse: Die IT SOX Compliance Road Map des IT Governance Institutes empfiehlt, dass die Geschäftsprozesse und dazugehörende IT-Applikationen beim Festlegen des Fokus (Scope) systematisch dokumentiert werden.[69] Dies soll dazu dienen, die relevanten Systeme zu identifizieren. Zudem hilft eine solche Dokumentation bei der Gestaltung gegenseitig abhängiger Kontrollen. Dabei sind die Kontrollen im Gesamtzusammenhang und abgestimmt auf die Risiken bei der Erstellung des Finanzabschlusses zu gestalten.

Arten von Kontroll-Effektivität: Während beide Modelle verlangen, dass die Effektivität der Kontrollen regelmässig überprüft wird, enthalten die SOX-Anforderungen einen expliziten Hinweis, dass zwischen Gestaltung und Umsetzung zu unterscheiden ist. Es muss somit die sogenannte „Design Effectiveness" als auch die „Operating Effective-

[69] Die geänderten Vorgaben der SEC (2007a), Sec. I, fordern nicht mehr in jedem Fall eine Dokumentation der Geschäftsprozesse. Die spezielle Ausrichtung auf den Finanzabschluss bleibt jedoch bestehen.

ness“ beurteilt werden. Mit diesem Hinweis wird wiederum die Nähe zum Geschäftsprozess deutlich.

Beurteilung der Kontroll-Effektivität: Die Road Map macht detaillierte Empfehlungen, wie das Management bei der Beurteilung der Kontroll-Effektivität vorzugehen hat und was dabei dokumentiert werden sollte. Die Empfehlungen gehen über die Anforderungen von ISO/IEC 27001 hinaus.[70]

Beurteilung der Schwachstellen: Die SOX-Anforderungen zielen ausschliesslich auf Prozesse und Systeme im Zusammenhang mit der finanziellen Berichterstattung ab. Dementsprechend sind identifizierte Schwachstellen auch in diesem Zusammenhang zu beurteilen und mit entsprechender Priorität zu beseitigen. Es wird vorgeschlagen, die Schwachstellen stets mit den Fachbereichen und insbesondere Vertretern aus der Finanzabteilung zu besprechen.

Verantwortlichkeiten bei spezifischen IT-Applikationskontrollen: Spezifische IT-Applikationskontrollen sind Kontrollen, welche ursprünglich manuell im Geschäftsprozess durchgeführt wurden, nun aber in IT-Applikationen integriert sind. Somit liegen diese Kontrollen direkt an der Schnittstelle zwischen Fachbereich und IT. Unklarheiten an dieser Stelle sind kritisch für eine erfolgreiche SOX-Implementation. Dementsprechend wird in der Road Map hervorgehoben, dass die Verantwortlichkeiten bezüglich spezifischer IT-Applikationskontrollen klar zu regeln sind. ISO/IEC 27001 fordert zwar auch eine klare Zuordnung der Verantwortlichkeiten, geht aber nicht speziell auf diesen Teilaspekt ein.

Outsourcing: SOX Compliance Bestätigungen[71] sind von wichtigen externen Dienstleistungsanbietern einzufordern.

4.3.4. Zusätzliche Aspekte bei ISO/IEC 27001

Allgemeiner Fokus: Während die Anforderungen von SOX stets im Zusammenhang mit Prozessen zur finanziellen Berichterstattung stehen, grenzt ISO/IEC 27001 den Fokus prinzipiell nicht ein.

Systematik: Das Vorgehensmodell ist bei ISO/IEC 27001 mehrmals systematischer aufgebaut als bei der IT SOX Compliance Road Map. Beispielsweise stellt ISO/IEC den iterativen Charakter des Modells viel deutlicher in den Vordergrund, beschreibt das Risikomanagement strukturierter und fordert explizite Metriken zur Messung der Kontrolleffektivität. Weiter wird gefordert, dass das Dokumentenmanagement selbst dokumentiert wird.

Vorgegebene Kontrollen: Standardmässig sind sämtliche Kontrollen aus ISO/IEC 27002 zu übernehmen. In Ausnahmefällen dürfen Kontrollen weggelassen werden, wenn dies aufgrund von Risikoüberlegungen gerechtfertigt ist und genau begründet wird. Die IT SOX Compliance Road Map zählt in ihrem Anhang zwar auch konkrete Kontrollen auf, es handelt sich dabei aber stets um unverbindliche Vorschläge; dementsprechend sind diese Abweichungen nicht zu dokumentieren.

---

[70] Dieser Unterschied hat sich durch die geänderten Vorgaben der SEC (2007a) verkleinert oder besteht möglicherweise gar nicht mehr.

[71] SOX Compliance bei externen Dienstleistungsanbietern wird normalerweise in der Form von sogenannten „SAS 70-Type II“ Berichten bestätigt.

4.4. SOX und ISO/IEC 27002

4.4.1. Grundlage

Die illustrativen Kontrollen des IT Governance Institutes (ITGI, 2006a) beziehen sich auf IT-Aspekte. Es handelt sich dabei um eine Auswahl von Kontrollen aus COBIT 4.0, die im Hinblick auf SOX angepasst wurden. Unabhängig von der SOX Diskussion existiert zudem eine Abbildung zwischen COBIT 4.0 und ISO/IEC 27002.[72] Somit können die IT-SOX Kontrollen mechanisch via COBIT 4.0 auf die ISO/IEC 27002 Kontrollen abgebildet werden.

Abbildung 5 – Ansatz: IT-SOX Kontrollen via COBIT 4.0 mit ISO/IEC 27002 vergleichen

Die oben gezeigte, transitive Abbildung ist im Rahmen dieser Arbeit durchgeführt und als Ausgangslage für die folgenden beiden Analysen verwendet worden:

1. Sämtliche SOX Kontrollziele gemäss IT Governance Institute (2006a) werden mit den Kontrollzielen und Kontrollen von ISO/IEC 27002 verglichen. Das Hauptziel besteht darin, Themenbereiche zu finden, die im ISO-Standard nicht oder nur teilweise abgedeckt sind. Die transitive Abbildung dient in dieser Analyse als Unterstützungshilfe, wird aber um eigene Interpretationen und Schlussfolgerungen ergänzt.

2. Die SOX-Kontrollen gemäss IT Governance Institute (2006a) werden via COBIT 4.0 mechanisch mit den Kontrollen von ISO/IEC 27002 verknüpft, gewichtet und gezählt. Es entsteht eine Häufigkeitsverteilung, wodurch sich Hinweise bezüglich der SOX-Relevanz einzelner ISO/IEC 27002 Kontrollen ergeben.

Die Ergebnisse der beiden Analysen werden in den nachfolgenden Unterkapiteln beschrieben. Eine detaillierte Herleitung befindet sich in den Anhängen B, C und D.

4.4.2. Übereinstimmung

Zielsetzung: Die ISO/IEC 2700x Familie konzentriert sich auf das Thema „Informationssicherheit“. In den ISO/IEC Standards werden entsprechende Kontrollziele und Massnahmen genannt, welche zur Vertraulichkeit, Integrität und Verfügbarkeit von Informationen beitragen. Solche Zielsetzungen und Massnahmen widersprechen in keiner Weise den SOX-Anforderungen – im Gegenteil: Wenn nämlich eine vollständige, richtige, aktuelle und geprüfte finanzielle Berichterstattung erfolgen soll, so trägt die Informationssicherheit mit einem erheblichen Teil dazu bei. Insbesondere die Forderung nach der Integrität von Daten ist weitreichend und ganz im Sinne von SOX. Die Ziele „Authentizität“, „Nicht-Abstreitbarkeit“ und „Verlässlichkeit“ von Informationen sind ebenfalls sowohl im Sinne von SOX als auch von ISO/IEC 27002. Häufig wird von IT-

[72] IT Governance Institute (2006b)

Frameworks noch das Ziel „Effizienz“ gefordert, was nicht in ISO/IEC 27002 abgedeckt wird. Dieses Ziel spielt im Zusammenhang mit SOX aber eine untergeordnete Rolle, weshalb diese Abweichung hier kaum relevant ist.[73]

Beitrag zur Erfüllung der SOX-Kontrollziele: Alle genannten SOX-Kontrollziele des IT Governance Institutes (2006a) werden direkt oder indirekt zumindest bis zu einem gewissen Grad von den ISO/IEC 27002 Kontrollen abgedeckt.

Relevanz der ISO/IEC 27002 Kontrolle: Beinahe alle 133 Kontrollen aus ISO/IEC 27002 können einen Beitrag zur Erfüllung der SOX-Anforderungen leisten. Die transitive Abbildung über COBIT ergibt, dass 85% der ISO/IEC 27002 Kontrollen zur Erfüllung der SOX-Kontrollziele des IT Governance Institutes (2006a) beisteuern.[74] Die Prozentzahl dürfte sogar noch höher sein (vgl. Bemerkungen im Anhang D). Tatsächlich kann wohl bei jeder Kontrolle aus ISO/IEC 27002 ein Argument gefunden werden, weshalb sie für SOX relevant ist.

4.4.3. Zusätzliche Aspekte bei SOX

Wie bereits in Abbildung 4 dargestellt, deckt COBIT im Vergleich zu ISO/IEC 27002 einen breiteren Rahmen ab. Die SOX-Kontrollen gemäss IT Governance Institute (2006a) basieren auf COBIT, und so verwundert es nicht, dass gewisse Abweichungen auftreten.

Umfassendes IT-Framework: Das Ziel von ISO/IEC 27002 ist klar und eindeutig Informationssicherheit. Demgegenüber gehen die SOX Anforderungen des IT Governance Institutes und von COBIT über die direkten Kontrollen zur Informationssicherheit hinaus. Insbesondere:

- Die IT-Aufbau- und Ablauforganisation soll definiert und kommuniziert werden. Diese Massnahme hilft generell, Unstimmigkeiten und Fehler zu vermeiden und trägt dadurch am Ende auch zu einer höheren Datenqualität bei. ISO/IEC 27002 geht zwar auch auf die Organisation ein, konzentriert sich aber speziell auf Zuständigkeiten und Abläufe zur Informationssicherheit.
- Wenn Benutzer im Umgang mit Applikationen geschult werden, hilft dies zur Vermeidung von Fehlmanipulationen. ISO/IEC 27002 geht ebenfalls auf die Schulung ein, konzentriert sich dabei aber mehrheitlich auf die Sensibilisierung bei Informationssicherheit.
- Applikationsentwicklung (vgl. weiter unten).

Übergeordnete Kontrollen und Unterstützung durch ISO/IEC 27001: Einige Kontrollen in ISO/IEC 27002 können die SOX-Anforderungen des IT Governance Institutes nur teilweise erfüllen, werden aber von Massnahmen in ISO/IEC 27001 unterstützt. Insbesondere die Anforderungen an übergeordnete Kontrollen[75] gehen über ISO/IEC 27002 hinaus, wobei ISO/IEC 27001 einen zusätzlichen Beitrag leisten kann. So wird beispielsweise in ISO/IEC 27002 nur punktuell erwähnt, dass aktuelle Informationen über

---

[73] Es ist für SOX wichtig, dass das Unternehmen in der Lage ist, den finanziellen Bericht zeitgerecht zu erstellen, und dass der Bericht vollständig und korrekt ist. Über welche Stufen und mit welchen Mitteln dies erfolgt, ist für SOX weniger wichtig.

[74] 114 Kontrollen von 133 ISO/IEC 27002 Kontrollen werden mindestens einmal in einer SOX-Kontrolle des IT Governance Institutes genannt.

[75] vgl. sogenannte „Entity-Level Controls“ in IT Governance Institute (2006a), Seite 13 und 57

interne und externe Geschehnisse beschafft und kommuniziert werden sollten. Demgegenüber fordert ISO/IEC 27001, dass Informationen systematisch zu beschaffen und zu verarbeiten sind. Analoge Schlussfolgerungen ergeben sich bei der Abstimmung der Informatik-Strategie mit der Geschäftsstrategie sowie beim Risikomanagement.

Applikationsentwicklung: Ein geordneter Prozess bei der Applikationsentwicklung hilft, dass die IT-Applikationskontrollen wie gewünscht implementiert werden und verlässlich funktionieren. ISO/IEC 27002 enthält ein eigenes Kapitel zum Thema „Beschaffung und Entwicklung von Applikationssoftware". Darin wird beschrieben, dass zu Beginn die Sicherheitsanforderungen erfasst werden müssen und Kontrollen bei der Eingabe, Verarbeitung und Ausgabe vorhanden sein sollten. Da ISO/IEC 27002 hier sehr allgemeine Formulierungen verwendet, ist im Zusammenhang mit SOX speziell zu berücksichtigen und nicht zu vergessen, dass die Endbenutzer (insbesondere Vertreter aus der Finanzabteilung) eingebunden werden und deren Anforderungen systematisch und ausführlich erfasst werden. Dies sollte neben allgemeinen Sicherheitsanforderungen auch spezifische IT-Applikationskontrollen umfassen. Ebenso sollten diese Kontrollen vor und nach der Einführung getestet werden, was in ISO/IEC 27002 sehr knapp behandelt wird. Auf die Themen „Ablauforganisation" und „Methoden/Anleitungen" zur Software-Entwicklung wird in ISO/IEC 27002 nicht direkt eingegangen.

Eigenentwickelte IT-Applikationen (EUC): Im Zusammenhang mit SOX sind IT-Applikationen speziell zu beachten, die durch den Fachbereich entwickelt worden sind. Für diese Applikationen gelten prinzipiell die gleichen Anforderungen wie für alle anderen Applikationen, trotzdem ist diesem Aspekt erhöhte Aufmerksamkeit zu schenken und durch entsprechende Massnahmen geeignet zu kontrollieren. Es werden nämlich insbesondere in der Finanzabteilung häufig selbst erstellte Tabellenkalkulationsprogramme eingesetzt, bei denen die generellen IT-Kontrollen nicht konsequent befolgt werden.

Spezifische IT-Applikationskontrollen: Die spezifischen IT-Applikationskontrollen sind oftmals im Verantwortungsbereich der Fachabteilungen und sind ein Schlüssel-Element im Rahmen von SOX. Es handelt sich um massgeschneiderte Kontrollen für die jeweiligen Geschäftsprozesse. ISO/IEC 27002 geht prinzipiell auf diese Kontrollen ein.[76] Das IT Governance Institute hebt jedoch das Zustandekommen dieser spezifischen IT-Applikationskontrollen und deren Bezug zu den Geschäftsprozessen viel deutlicher hervor. Zudem wird hier die Bedeutung der Kontrollen mit zahlreichen Beispielen untermauert.

Interne Dienstleistungen: Wie bereits beim Vergleich von ISO/IEC 27001 mit SOX erwähnt, ist die Zusammenarbeit zwischen den verschiedenen Bereichen (und insbesondere mit der Finanzabteilung) wichtig. In den illustrativen SOX-Kontrollen des IT Governance Institutes wird dieser Aspekt unter anderem mit Service Level Agreements (SLA) berücksichtigt. Entsprechende Kontrollen können helfen, die SOX-Anforderungen betreffend „aktuellen Daten" und „fristgerechter Erstellung des Jahresabschlusses" zu erfüllen. ISO/IEC 27002 konzentriert sich bei den SLAs auf externe Dienstleistungserbringer.

Outsourcing: SOX Compliance Bestätigungen sind von wichtigen externen Dienstleistungsanbietern einzufordern (analoge Feststellung wie beim Vergleich mit ISO/IEC 27001).

---

[76] vgl. ISO/IEC 27002, Kapitel „12.2, Correct Processing in Applications"

4.4.4. Gewichtung der ISO/IEC 27002 Kontrollen

Einige Kontrollen aus ISO/IEC 27002 tragen mehr zur Erfüllung der SOX-Anforderungen bei als andere, und so ergeben sich Unterschiede bezüglich der SOX-Relevanz dieser Kontrollen. Sowohl das Studium der Kontrollziele des IT Governance Institutes (2006a) als auch die transitive Abbildung dieser Kontrollen auf ISO/IEC 27002 führen zu folgenden Ergebnissen:

Schwerpunkte

- *Spezifische IT-Applikationskontrollen* sind bei der Umsetzung der SOX Anforderungen von zentraler Bedeutung. Gemäss der transitiven Abbildung sind dies die wichtigsten Kontrollen im IT-SOX Umfeld. In ISO/IEC 27002 werden diese Kontrollen im Kapitel „Correct Processing in Applications“ erwähnt.
- *Logischer Zugriffsschutz* beinhaltet wichtige, generelle IT-Kontrollen, die dafür sorgen, dass spezifische IT-Applikationskontrollen nicht umgangen werden. In ISO/IEC 27002 sind entsprechende Massnahmen insbesondere im Kapitel „Access Control“ beschrieben.
- *Change Management* nimmt hinsichtlich SOX-Relevanz ebenfalls eine wichtige Stellung ein. Diese generellen IT-Kontrollen sind in ISO/IEC 27002 vor allem in den Kapiteln „Security in Development and Support Processes“ sowie „Operational Procedures and Responsibilities“ zu finden.

Untergewichtete Punkte

- *Umgebungssicherheit (Environmental Security)* wird im Zusammenhang mit den SOX-Kontrollen weniger häufig erwähnt. Diese generellen Kontrollen stellen primär sicher, dass die Systeme und Daten verfügbar sind. Im Zusammenhang mit SOX ist es zwar wichtig, dass ein Unternehmen in der Lage ist, den Finanzausweis zu erstellen, doch scheint der Bezug zur Umgebungssicherheit hier bereits sehr weit weg zu sein. Das Kapitel „Equipment Security“ in ISO/IEC 27002 geht auf die Umgebungssicherheit ein.
- *Business Continuity Management* hat ebenfalls das primäre Ziel, die System- und Datenverfügbarkeit zu gewährleisten. Ähnlich wie die Umgebungssicherheit hat dieses Thema im Zusammenhang mit SOX eine untergeordnete Bedeutung. Die entsprechenden Kontrollen werden in ISO/IEC 27002 unter „Business Continuity Management“ erwähnt.
- *Ausgewählte Spezialthemen* aus ISO/IEC 27002 sind bei den SOX-Kontrollen ebenfalls nicht erwähnt. Beispiele sind „Regulation of Cryptographic Controls“ und „Clock Synchronization“.

4.5. ISO/IEC 27002 und SOX-Kontrollziele gemäss Credit Suisse

4.5.1. Einleitung und Grundlage

Die Credit Suisse Group ist ein global tätiges Finanzdienstleistungsunternehmen mit Hauptsitz in Zürich. Als integrierte, globale Bank bietet die Credit Suisse (CS) weltweit Dienstleistungen in den Bereichen Investment Banking, Private Banking und Asset Management an. Die Bank wurde 1856 gegründet, ist in über 50 Ländern tätig und beschäftigt rund 45’000 Mitarbeitende. Im Jahr 2006 erzielte die Credit Suisse einen Reinge-

winn von CHF 11’327 Millionen und verwaltete Vermögen im Wert von CHF 1’485 Milliarden.[77] Die Namenaktien der Credit Suisse Group (CSGN) sind in der Schweiz sowie in New York kotiert, wodurch die Anforderungen aus dem Sarbanes-Oxley Act für die Bank verbindlich werden und zwingend einzuhalten sind.

Die Credit Suisse hat dementsprechend intern ein SOX-Framework ausgearbeitet, welches in den vergangenen Jahren umgesetzt und mit Erfahrungen aus der Praxis ergänzt worden ist. Zudem hat das Wirtschaftsprüfungsunternehmen KPMG im Rahmen ihres Mandats als externe Revisionsgesellschaft bei der Credit Suisse unter anderem auch das SOX-Framework überprüft. Im IT-Umfeld hat die Credit Suisse eine Liste mit Kontrollzielen und Massnahmen zu generellen IT-Kontrollen erstellt.[78] Interne Weisungen schreiben vor, dass diese vordefinierten Kontrollen bei sämtlichen SOX relevanten Applikationen und Systemen anzuwenden sind.

Die vordefinierten, generellen IT-Kontrollen aus dem SOX-Framework der Credit Suisse sind im Rahmen dieser Arbeit auf die ISO/IEC 27002 Kontrollen abgebildet worden. Analog zur Analyse der SOX-Kontrollen gemäss IT Governance Institute[79] sind die abgebildeten Kontrollen gewichtet und deren Auftretenshäufigkeit bestimmt worden. Es ergibt sich wiederum eine Liste von ISO/IEC 27002 Kontrollen mit Hinweisen zur SOX-Relevanz. Zudem sind nun die Schwerpunkte der beiden SOX-Frameworks[80] erkennbar und vergleichbar.

Eine Zusammenfassung der Ergebnisse wird im nachfolgenden Kapitel beschrieben. Die detaillierte Herleitung befindet sich in den Anhängen E und F.

4.5.2. Schwerpunkte und Unterschiede im SOX-Framework der CS

Schwerpunkte

Die Credit Suisse unterteilt die generellen IT-Kontrollen in „Computer Operations“, „Program Changes“, „Access to Programs and Data“ und „Program Development“. Zu jeder Gruppe werden jeweils entsprechende Kontrollziele und Massnahmen formuliert.[81]

Schwerpunkte setzt die Credit Suisse in ihrem SOX-Framework in den Bereichen „Vergabe und Überprüfung von Zugriffsrechten“, bei ausgewählten Kontrollen zum Change Management sowie bei Datenbackups. Konkret handelt es sich um die folgenden ISO/IEC 27002 Kontrollen: User registration (11.2.1) & Review of user access rights (11.2.4), Change control procedures (12.5.1) & Change management (10.1.2), Information backup (10.5.1).

Hinweis: Die spezifischen IT-Applikationskontrollen werden im CS-Framework strikt von den generellen IT-Kontrollen getrennt und sind deshalb nicht in die obige Auswertung beziehungsweise Aufzählung eingeflossen. Diese Kontrollen haben im CS-Framework aber an einer anderen Stelle ebenfalls eine erhebliche Bedeutung.

---

77 CSG (2007b)
78 CSG (2007a)
79 vgl. mit Kapitel „4.4, SOX und ISO/IEC 27002” in dieser Arbeit
80 SOX-Framework der Credit Suisse und des IT Governance Institutes
81 in Anlehnung an: PCAOB (2004); SEC (2006); SEC (2007a), Sec. A.1.d

Unterschiedliche Gewichtung

Die regelmässige Überprüfung von Zugriffsrechten spielt im CS-Framework nicht nur eine zentrale Rolle, diese Kontrolle wird auch häufiger erwähnt als vom IT Governance Institute (2006a). Hinzu kommt, dass die CS im SOX-Framework sehr stark auf privilegierte Zugriffsrechte achtet, was in der Abbildung auf ISO/IEC 27002 nur begrenzt berücksichtigt werden kann.[82]

Überproportional häufig werden im CS-Framework auch die physische Sicherheit und das Thema „Daten-Backup“ erwähnt.

Die folgenden Themen spielen in der Credit Suisse eine wichtige Rolle, werden im Zusammenhang mit SOX jedoch weniger häufig in Form von Schlüsselkontrollen erwähnt:[83] Kontrollen zur Anmeldung am System und zum Umgang mit Passwörtern (11.3.1, 11.5.1, 11.5.3), Monitoring & Logging (10.10.1, 10.10.4) und spezielle Netzwerk und Systemkontrollen (10.6.1, 12.6.1).[84]

Weiteres

Im CS-Framework ist unter anderem vorgesehen, dass die Weisung zum Change Management kommuniziert wird. Ebenso unterstreicht das CS-Framework die Bedeutung der Methoden zur Software-Entwicklung.[85] Beide Themen sind ganz im Sinne des IT Governance Institutes (2006a) und von COBIT; die Themen werden aber in ISO/IEC 27002 nur punktuell berücksichtigt.

5. Zusammenfassung der Ergebnisse

5.1. Gemeinsamkeiten von SOX und ISO/IEC 2700x

Die Vorgehensweise zur Umsetzung der geforderten Massnahmen stimmt bei SOX und ISO/IEC 27001 im Wesentlichen überein. In beiden Fällen spielen Risikomanagement, regelmässige Überprüfung der Kontrollen und Nachvollziehbarkeit eine erhebliche Rolle. Die Zielsetzung in Bezug auf die IT-Umgebung gehen bei SOX und ISO/IEC 2700x ebenfalls in die gleiche Richtung, indem Vertraulichkeit, Verfügbarkeit und insbesondere Integrität der Daten gefordert wird. Zudem können eigentlich alle 133 Kontrollen aus ISO/IEC 27002 einen Beitrag zur Erfüllung der SOX-Anforderungen leisten.

---

[82] Im CS Framework werden privilegierte Zugriffsrechte mit zusätzlichen, speziellen Kontrollen verwaltet. ISO/IEC 27002 Kontrollen gehen demgegenüber davon aus, dass privilegierte Benutzer grundsätzlich den gleichen Verwaltungsprozessen unterliegen und machen deshalb diese spezielle Unterscheidung nur ansatzweise.

[83] wiederum im direkten Vergleich mit dem IT Governance Institute (2006a), abgebildet auf ISO/IEC 27002 Kontrollen

[84] Das Thema „Vertraulichkeitsvereinbarung“ (6.1.5) wird vom IT Governance Institute mehrfach generell erwähnt. Im Zusammenhang mit SOX dürften diese Kontrollen jedoch geringere Bedeutung haben, was sich mit den Ergebnissen aus der Analyse des CS Frameworks deckt.

[85] CSG (2007a), Ref. 4.1

5.2. SOX-Relevanz ausgewählter Kontrollen aus ISO/IEC 27002

5.2.1. Spezifische IT-Applikationskontrollen und logische Zugriffskontrollen

Sowohl das IT Governance Institute als auch das CS-Framework und der Artikel von Dwight. A. Haworth und Leah R. Pietron zeigen, dass die wichtigsten SOX-Kontrollen im IT-Umfeld aus den Bereichen „spezifische IT-Applikationskontrollen“ und „logische Zugriffskontrollen“ stammen. Je nach Autor wird dem einen Thema etwas grössere Bedeutung zugemessen als dem anderen, doch grundsätzlich stimmen sie hervorragend überein. Bei den logischen Zugriffskontrollen besteht auch Einigkeit über die sehr grosse Bedeutung von Kontrollen zur Benutzerverwaltung, zum Umgang mit privilegierten Zugriffsrechten und zur regelmässigen Überprüfung der Zugriffsrechte.

Widersprüchliche Aussagen werden zu Kontrollen bezüglich „User Responsibilities“ gemacht: Während Haworth & Pietron hier von Schlüsselkontrollen sprechen, erwähnt das IT Governance Institute nur noch den Umgang mit Passwörtern, und im SOX-Framework der Credit Suisse werden die entsprechenden Kontrollen nicht mehr direkt erwähnt. Ähnliche Unstimmigkeiten ergeben sich im Detail bei logischen Zugriffskontrollen im Netzwerk und teilweise beim Betriebssystem.

5.2.2. Kontrollen bei Änderungen an IT-Systemen

Kontrollen bei Änderungen an IT-Systemen werden in ISO/IEC 27002 an zahlreichen Stellen erwähnt. Die verschiedenen Autoren sind sich einig, dass diese Kontrollen wichtig sind. So sind insbesondere die Detailkontrollen „Change Control Procedures“ und „Change Management“ stets konsistent erwähnt. Spezialthemen in diesem Bereich werden dann aber ebenfalls uneinheitlich gewichtet, wie beispielsweise der Umgang mit Testdaten.

5.2.3. Umgebungssicherheit[86] und Business Continuity

Eine geringere Bedeutung für SOX haben die Kontrollen zur Umgebungssicherheit und zum Business Continuity Management. Trotzdem weisen Haworth & Pietron darauf hin, dass die Kontrollen nicht vollständig zu vernachlässigen sind. Sie argumentieren, dass diese Kontrollen benötigt werden, weil gemäss SOX eine Unternehmung stets die Fähigkeit zur finanziellen Berichterstattung haben muss. In Anbetracht der momentanen Tendenzen, die SOX-Umsetzungen zu vereinfachen und sich auf das Wesentliche zu konzentrieren, dürften diese Bereiche jedoch weiter an Bedeutung verlieren.

5.2.4. Weitere ISO/IEC 27002 Kontrollen

Physische Sicherheit[87] wird sowohl vom IT Governance Institute als auch vom SOX Framework der Credit Suisse sowie von Haworth & Pietron erwähnt. Die entsprechen-

---

[86] Beispiele von Kontrollen zur Umgebungssicherheit sind: Schutz der Verkabelung, um Abhören und Beschädigungen zu vermeiden; Schutz der Geräte vor Stromausfall (z.B. mittels unterbrechungsfreier Stromversorgung) usw.

[87] Hier wird physische Sicherheit im engeren Sinne verstanden, d.h. „Physical Security“ wie im Kapitel 9.1 von ISO/IEC 27002:2005 beschrieben (vgl. ISO/IEC (2005b)); Umgebungssicherheit (Environmental Security) ist bei dieser engen Interpretation nicht inbegriffen.

den Kontrollen haben nicht allerhöchste Priorität, sollten aber auch nicht vernachlässigt werden, da ansonsten logische Zugriffskontrollen umgangen werden könnten.

Übergeordnete Kontrollen[88] haben insbesondere seit den Änderungen der SEC (2007a) an Bedeutung gewonnen. Gemeinsame Schwerpunkte, abgebildet auf Kontrollen aus ISO/IEC 27002, lassen sich bei den verschiedenen Autoren nicht erkennen. So werden die Kontrollen aus dem Bereich „Organization of information security" unterschiedlich gewichtet. Dies mag daran liegen, dass einerseits die Bedeutung der übergeordneten Kontrollen anfangs von SEC (2003) und PCAOB (2004) nicht so sehr hervorgehoben wurde und dass andererseits diese Kontrollen nicht zwingend IT-spezifisch sind und somit möglicherweise an anderen Stellen in den betreffenden SOX-Frameworks behandelt werden.

Spezialthemen in ISO/IEC 27002 werden aus verständlichen Gründen ebenfalls seltener und unregelmässig durch das IT Governance Institute, das SOX Framework der Credit Suisse und von Haworth & Pietron genannt. Beispiele sind Zeitsynchronisation oder kryptographische Kontrollen.

5.3. Unterschiede bei SOX und ISO/IEC 2700x

5.3.1. Wo geht SOX weiter als ISO/IEC 2700x?

Der Fokus von SOX liegt auf den Prozessen zur Erstellung des Finanzausweises. Dieser Bereich wird von ISO/IEC 2700x zwar nicht ausgeschlossen, aber eben auch nicht speziell hervorgehoben. Es ergeben sich unterschiedliche Schwerpunkte, die bereits bei der Risikobeurteilung erkennbar sind. So konzentriert sich das Vorgehen bei SOX von Beginn weg darauf, welche Risiken bei der Finanzberichterstattung wesentlich sind und mit welchen aufeinander abgestimmten Kontrollen darauf geantwortet werden soll. Die Zusammenarbeit mit dem Fachbereich und die Berücksichtigung der Individualität dieser Geschäftsprozesse sind dabei von zentraler Bedeutung und werden stärker hervorgehoben als bei ISO/IEC 2700x. Dabei sind vor allem die spezifischen IT-Applikationskontrollen angesprochen, welche in ISO/IEC 27002 summarisch im Kapitel „Correct Processing in Applications" erwähnt werden. ISO/IEC geht hier nicht speziell darauf ein, wie diese Kontrollen gestaltet und definiert werden. Aus ähnlichen Überlegungen fordert SOX bei der Beurteilung der Kontrolleffektivität, dass zwischen der sogenannten „Design und Operating Effectiveness" unterschieden wird. Das IT Governance Institute unterstreicht selbst bei der Beurteilung der gefundenen Schwachstelle, dass stets die Zusammenarbeit mit dem Fachbereich gesucht werden soll.

Eine vergleichsweise grössere Bedeutung hat bei SOX die Definition der Zuständigkeiten, wiederum vor allem zwischen Fachbereich und IT im Zusammenhang mit spezifischen IT-Applikationskontrollen.

Weiter gehören Anwendungsprogramme, welche durch den Fachbereich selbst entwickelt worden sind, eindeutig in dessen Verantwortungsbereich. Prinzipiell gelten für diese Applikationen die gleichen Kontrollen und werden somit auch in ISO/IEC 2700x abgedeckt. Trotzdem ist hier bei SOX ein spezielles Augenmerk und Unterstützungshilfe von der IT-Abteilung notwendig: Bei der finanziellen Berichterstattung werden näm-

[88] Entity-Level Controls; vgl. insbesondere: SEC (2007a), Sec. II.A; PCAOB (2007), Paragraph 22-44;

lich häufig eigene Tabellenkalkulationsprogramme verwendet und die notwendigen IT-Kontrollen vernachlässigt.

ISO/IEC 2700x ist auf Informationssicherheit ausgerichtet und dementsprechend sind die vorgeschlagenen Kontrollen gewählt. Dadurch werden übergeordnete Kontrollen nur teilweise und nicht so ausführlich abgedeckt wie dies beispielsweise im breiter gefassten COBIT Framework erfolgt. Als Folge davon werden Themen wie „Kommunikation der generellen Aufbau- und Ablauforganisation“ und „Methoden zur Applikationsentwicklung“ in ISO/IEC 27002 nicht direkt erwähnt. Nur knapp angedeutet ist bei ISO/IEC die generelle Schulung von Mitarbeitern im Umgang mit Applikationen.

5.3.2. Wo geht ISO/IEC 2700x weiter als SOX?

Der Fokus von ISO/IEC 2700x geht über die finanzielle Berichterstattung hinaus. Zudem sind die ISO/IEC Standards systematischer aufgebaut und präziser formuliert als die Formulierungen in den Gesetzestexten.[89] Hinzu kommt, dass die Kontrollen in ISO/IEC 27002 verbindlich sind, während die illustrativen Kontrollen des IT Governance Institutes (2006a) nur Empfehlungen sind.

Zu jeder Kontrolle aus ISO/IEC 27002 werden sich Argumente finden lassen, weshalb die betreffende Kontrolle für SOX relevant ist. Es ergeben sich somit keine Kontrollen in ISO/IEC 27002, welche eindeutig über die SOX-Anforderungen hinausgehen. Allerdings beinhalten die ISO/IEC Standards wertvolle Detailangaben, die bei der Umsetzung von SOX-Kontrollen zur Informationssicherheit weiterhelfen.

6. Schlussbemerkungen und Ausblick

Der Sarbanes-Oxley Act lässt insbesondere im Bezug auf die IT viel Interpretationsspielraum offen. Daran ändern auch die kürzlich geänderten Vorgaben von SEC (2007a, 2007b) und PCAOB (2007) nicht viel. In dieser Arbeit wurde anhand der wenigen konkreten Anforderungen sowie Publikationen und Praxiserfahrungen aufgezeigt, wo Gemeinsamkeiten zu den verhältnismässig präziseren Anforderungen aus ISO/IEC 27001 & 27002 bestehen. Ebenso wurde gezeigt, wo sich Schwerpunkte in den ISO/IEC-Kontrollen in Bezug auf SOX ergeben und worauf speziell zu achten ist. Die SOX-Anforderungen wurden im Rahmen dieser Arbeit relativ streng und unter Einbezug der ursprünglichen Gesetzestexte interpretiert.

Bei der Abbildung der SOX-Anforderungen auf Kontrollen in ISO/IEC 27002 zeigt sich, dass sich verschiedene Autoren[90] bezüglich der Themenbereiche und Bedeutung ausgewählter Kontrollen einig sind. Es gibt jedoch auch konkrete Kontrollen in ISO/IEC 27002, bei denen die Abbildungen widersprüchlich sind. Gründe für diese Widersprüche dürften sein: Individualität der Geschäftsprozesse, geänderte Gesetzgebung, kompensierende Kontrollen sowie der bereits erwähnte Interpretationsspielraum ganz generell.

---

89 SEC (2003, 2007a, 2007b); PCAOB (2004, 2007); US Congress (2002)

90 Im Rahmen dieser Arbeit sind es IT Governance Institute (2006a), CSG (2007a), Haworth Dwight A. und Pietron Leah R. (2006)

Die geänderten Vorgaben von SEC und PCAOB (2007) bestätigen und unterstützen den Trend zur Reduktion des SOX-Aufwands. Durch die 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 weitreichende SOX-Forderung abgeschwächt und somit der Unterschied hinsichtlich Dokumentationspflicht zwischen SOX und ISO/IEC 27001 verringert.

Im Zuge der Reduktion des SOX-Aufwands werden wohl viele Unternehmen ihre ausgewählten Kontrollen nochmals hinterfragen und gegebenenfalls anpassen. SEC (2007a) und PCAOB (2007) heben die Bedeutung der übergeordneten Kontrollen hervor, unterstreichen aber zugleich, dass auch Kontrollen an der Basis zwingend notwendig sind.[91] Während bei spezifischen IT-Applikationskontrollen eine auf den konkreten Geschäftsprozess ausgerichtete Analyse notwendig sein wird, kann bei den generellen IT-Kontrollen die vorliegende Arbeit zusätzliche Hinweise geben, welche Kontrollen stärker zu gewichten sind.

Zusammenfassend kann festgehalten werden, dass Massnahmen aus ISO/IEC 27001 & 27002 einen wesentlichen Beitrag zur Erfüllung der SOX-Anforderungen im IT-Umfeld leisten, dass jedoch die Individualität der Geschäftsprozesse zur finanziellen Berichterstattung speziell berücksichtigt werden muss. Die Vorgehensweise in der Umsetzung stimmt im Wesentlichen überein, und mit den Gesetzesänderungen von SEC und PCAOB reduzieren sich die Zusatzanforderungen aus SOX gegenüber den ISO/IEC Standards hinsichtlich Dokumentationspflicht. Aufgrund der aktuellen Diskussion über zu hohen Aufwand bei der Umsetzung von SOX ist zu erwarten, dass die Anforderungen künftig weniger streng interpretiert werden und eventuell sogar weiter gesenkt werden. In diesem Fall ist es aber umso wichtiger zu wissen, wo Schwerpunkte liegen und wo nochmals gekürzt werden kann.

---

[91] Die sogenannten Entity-Level Controls werden beschrieben in: SEC (2007a), Sec. II.A; PCAOB (2007), Paragraph 22-44;
vgl. auch Entity- und Activity-Level Controls in IT Governance Institute (2006a), Seite 57

Anhang A - Detailvergleich ISO/IEC 27001:2005 und SOX

Das IT Governance Institute (ITGI, 2006a) beschreibt in Form einer sogenannten „Road Map“, wie ein Unternehmen aus IT-Sicht vorgehen sollte, um die Anforderungen aus der Sarbanes-Oxley Gesetzgebung erfolgreich umzusetzen. Dabei stützt sich ITGI primär auf die Vorgaben aus dem Sarbanes-Oxley Act gemäss US Congress (2002), auf PCAOB (2004), aufs COSO-Framework und auf bisherige Erfahrungen aus der Praxis. ISO/IEC 27001 beschreibt im Zusammenhang mit der Informationssicherheit ebenfalls ein Vorgehensmodell für die Erstellung und den Betrieb eines Managementsystems.

Im Folgenden werden nun diese beiden Vorgehensmodelle miteinander verglichen und Abweichungen diskutiert.

Die weiter unten aufgelisteten Anforderungen orientieren sich an der Struktur von ISO/IEC 27001, sind aber nicht abschliessend aus dem Standard übernommen worden und stellen lediglich eine Zusammenfassung von ISO/IEC 27001 dar. Die Anforderungen sind zudem mit Vorgaben aus ITGI (2006a) ergänzt worden. Zu jeder Anforderung wird kommentiert, inwieweit sie mit dem jeweils anderen Vorgehensmodell übereinstimmt. Darauf basierend wird summarisch der Übereinstimmungsgrad geschätzt.

Referenzen auf ursprüngliche Literaturquellen sind angegeben. Zur besseren Lesbarkeit sind Beschreibungen auf der Grundlage von ISO gelb markiert; Angaben auf der Basis von ITGI sind blau gekennzeichnet. Die konkreten Quellen sind:

- ISO/IEC (2005a), ISO/IEC 27001:2005; Internationaler Standard, First Edition; Genf, 15.10.2005
- ISO/IEC (2005b), ISO/IEC 27002:2005; Internationaler Standard, Second Edition - renumbered 07/2007; Genf, 15.06.2005
- IT Governance Institute (2006a), IT Control Objectives for Sarbanes-Oxley; Online-Publikation, 2nd Edition; Illinois, September 2006

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
Generell – PDCA		
G-1	**Anforderung**: Kontrollen werden systematisch definiert, umgesetzt, überprüft und gegebenenfalls angepasst. Dieser Prozess ist iterativ und regelmässig zu durchlaufen.	ISO 27001-4.1
	Kommentar: Die IT SOX Compliance Road Map stellt den iterativen Charakter nicht so sehr in den Vordergrund und beschreibt diesen Prozess nicht ganz so systematisch. Es wird jedoch ebenfalls auf die Überprüfung des Kontrollumfelds hingewiesen. SOX wird auch bei der Road Map nicht als ein befristetes Projekt verstanden, sondern als ein regelmässiger Prozess, wo das Kontrollsystem sukzessiv optimiert wird. Zudem müssen die Kontrollen im Rahmen der Berichterstattung regelmässig bestätigt werden.	ITGI-S.27, 44-45 
PLAN – Scope, Weisungen, Risikomanagement und Auswahl der Kontrollen		
P-1	**Anforderung**: Der Fokus (Scope) des Kontrollsystems ist klar zu definieren und zu dokumentieren.	ISO 27001-4.2.1.a, 4.3.1.b
	Kommentar: Die IT SOX Compliance Road Map hebt die Wichtigkeit zur Eingrenzung des Fokus ebenfalls hervor.	ITGI-S.27, 33 
P-2	**Anforderung**: Es sind ausschliesslich Systeme im Zusammenhang mit der finanziellen Berichterstattung zu berücksichtigen.	ITGI-S.28
	Kommentar: ISO 27001 grenzt den Fokus prinzipiell nicht auf bestimmte Geschäftsprozesse und Systeme ein.	ISO 27001-4.2.1.a 

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
P-3	**Anforderung**: Zur Definition des Scopes sind die relevanten Prozesse, Applikationen und Systeme zu identifizieren und in einem Inventar aufzulisten. Dies soll helfen, den Prozess zur Erstellung der finanziellen Berichterstattung zu verstehen und eine bessere Grundlage für die Risikobeurteilung zu erhalten.	ITGI-S.28
	Kommentar: ISO 27001 erwähnt zwar „Assets and Technology“, geht aber nicht derart detailliert auf das Vorgehen zur Festlegung des Scopes ein. An anderer Stelle wird als generelle Massnahme die Erstellung eines Inventars gefordert. Die Dokumentation von Geschäftsprozessen geht über die Anforderungen von ISO 27001 hinaus, da sich der ISO-Standard auf Informationssicherheit konzentriert.	ISO 27002-7.1.1 
P-4	**Anforderung**: Es ist ein systematisches Risikomanagement durchzuführen. Dazu gehören unter anderem: 1) Definieren des Konzepts fürs Risikomanagement, 2) Identifizieren der Risiken, 3) Beurteilen der Risiken und 4) Entscheid für den Umgang mit Risiken.	ISO 27001-4.2.1.c, d, e, f ,h, 4.2.2.a, 5.1.f
	Kommentar: Die IT SOX Compliance Road Map stellt ebenfalls diverse Anforderungen zum Risikomanagement. Der Ansatz von ISO 27001 ist jedoch systematischer aufgebaut.	ITGI-S.32, 59 
P-5	**Anforderung**: Beim Risikomanagement sind die Auswirkungen auf die finanzielle Berichterstattung zu berücksichtigen, wobei vor allem inhärente Risiken wie Technologie, Personen und Prozesse beachtet werden sollten.	ITGI-S.32
	Kommentar: ISO 27001 geht nicht spezifisch auf Risiken zur Erstellung des Finanzausweises ein. Generell wird das Risikomanagement in ISO 27001 jedoch abgedeckt.	ISO 27001-4.2.1.c, d, e, f 
P-6	**Anforderung**: Es sind Massnahmen zu ergreifen, um den identifizierten Risiken angemessen entgegen zu treten.	ISO 27001-4.2.1.g
	Kommentar: Die IT SOX Compliance Road Map stellt ebenfalls die Anforderung, dass die Auswahl der Kontrollen	ITGI-S.99-101

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	auf den Ergebnissen der Risikobeurteilung basieren muss.	
P-7	**Anforderung**: Bei der Wahl der Kontrollen ist darauf zu achten, dass die Kontrollen aus sämtlichen der folgenden Kategorien stammen: Übergeordnete Unternehmenskontrollen (Entity-level controls), spezifische IT-Applikationskontrollen in den Geschäftsprozessen, generelle IT-Kontrollen sowie Kontrollen zur Aufdeckung von kriminellen Handlungen.	ITGI-S.33-36
	Kommentar: ISO 27001 fordert diese spezifischen Kategorien von Kontrollen nicht, verweist jedoch auf sämtliche Kontrollen aus ISO 27002. Das Schwergewicht in ISO 27002 liegt bei den generellen IT-Kontrollen. Übergeordnete generelle Unternehmenskontrollen werden im Rahmen von Weisungen zur Informationssicherheit in ISO 27002 teilweise abgedeckt. Spezifische IT-Applikationskontrollen und Kontrollen zur Aufdeckung von kriminellen Handlungen werden punktuell aufgegriffen.	ISO 27001-4.2.1.g; ISO 27002
P-8	**Anforderung**: Wenn eine Unternehmung mehrere geografische Standorte hat, ist bei der Projektplanung zu berücksichtigen, welche Abhängigkeiten bei den Kontrollen existieren. Dieser Aspekt ist bei der Schätzung des Projektaufwands relevant.	ITGI-S.30
	Kommentar: ISO 27001 geht nicht spezifisch auf diesen Aspekt ein; eine Schätzung der benötigten Ressourcen wird erwähnt.	ISO 27001-5.2.1
P-9	**Anforderung**: Das Kontrollumfeld von wichtigen externen Dienstleistungsanbietern (Outsourcing) ist zu berücksichtigen. Typischerweise sind entsprechende Compliance-Bestätigungen (sogenannte SAS 70, Type II Berichte) von den Dienstleistungsanbietern einzufordern.	ITGI-S.31
	Kommentar: ISO 27001 nennt mit dem Hinweis auf ISO 27002 ebenfalls mehrere Anforderungen an Kontrollen bei Dienstleistungsanbietern. Ein expliziter SOX-Compliance Nachweis wird nicht speziell erwähnt.	ISO 27002-6.2.1, 10.2, 10.6.2,

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
		12.5.5 
DO – Umsetzung der Massnahmen und Betrieb		
D-1	**Anforderung**: Die ausgewählten Kontrollen sind umzusetzen. Dabei sind die Mitarbeiter zu schulen und zu sensibilisieren.	ISO 27001-4.2.2.b, c, e, f, g
	Kommentar: Die IT SOX Compliance Road Map erwähnt den Schritt „Umsetzung“ nicht in einer separaten Phase. Aufgrund des Ablaufs ist jedoch klar, wo dieser Schritt zu erfolgen hat. Zudem beschreibt die Road Map ausführlich, wie das Personal auf die Änderungen vorzubereiten ist.	ITGI-S.19-21, 27 
D-2	**Anforderung**: Es ist festzulegen und zu dokumentieren, wie die Effektivität der Kontrollen zu messen ist.	ISO 27001-4.3.1.g, 4.2.2.d, 4.2.3c
	Kommentar: Die IT SOX Compliance Road Map nennt das Thema „Messung der Kontrolleffektivität“ nicht explizit. Aufgrund der detaillierten Anforderung an die Dokumentation ist dies indirekt zu einem grossen Teil abgedeckt.	ITGI-S.36-40 
CHECK – Überprüfen der Massnahmen		
C-1	**Anforderung**: Die Organisation muss derart aufgebaut sein, dass regelmässig die Effektivität des Kontrollsystems überprüft wird.	ISO 27001-4.2.3.b
	Kommentar: Die IT SOX Compliance Road Map stellt die gleiche Anforderung wie ISO 27001. Beide Standards he-	ITGI-S.37-42

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	ben hervor, dass das Management die Kontrollen überprüfen muss. Der Begriff „Management“ ist jedoch nicht genau definiert und so kann bereits bei einer tiefen Hierarchiestufe von Management gesprochen werden.	
C-2	**Anforderung**: Es sind Kontrollen durchzuführen, welche Fehler, Sicherheitsvorfälle und kriminelle Handlungen zeitnah erkennen.	ISO 27001-4.2.3.a
	Kommentar: Die IT SOX Compliance Road Map hebt klar hervor, dass präventive Kontrollen wichtiger sind als detektive. Trotzdem empfiehlt auch die Road Map detektive Kontrollen und weist an verschiedenen Stellen auf schnelles Reagieren hin.	ITGI-S.35, 37, 60, 76
C-3	**Anforderung**: Das Management muss in der Lage sein, zu beurteilen, ob die festgelegten Kontrollen wie erwartet funktionieren.	ISO 27001-4.2.3.a3
	Kommentar: Diese Anforderung entspricht dem Kerngedanken von SOX, denn am Ende muss das Management ja schriftlich eine Beurteilung des internen Kontrollsystems abgeben.	ITGI-S.50-51
C-4	**Anforderung**: Das Management muss mindestens einmal jährlich das Kontrollsystem betreffend Effektivität überprüfen. Das Ergebnis dieser Überprüfung, die Schlussfolgerungen und die daraus resultierenden Massnahmen sowie geplanten Änderungen müssen klar dokumentiert sein.	ISO 27001-7.1, 7.3
	Kommentar: Die IT SOX Compliance Road Map sieht eine regelmässige Überprüfung durch das Management ebenfalls vor. Die Bestätigung des internen Kontrollsystems hat jährlich zu erfolgen, weshalb auch die Überprüfung mindestens in diesem Intervall erfolgen muss, eventuell sogar häufiger. ISO 27001 gibt die Struktur der Review-Ergebnisse ein wenig kompakter und geordneter vor. Die Dokumentation nimmt bei SOX generell eine wesentliche Stellung ein und so wird auch bei der Road Map konkret gefordert, dass Schlussfolgerungen und abgeleitete Massnahmen zu dokumentieren sind.	ITGI-S.37-42, 51

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
C-5	**Anforderung**: Das Management muss beim Review des Kontrollsystems die folgenden Dokumente und Informationen berücksichtigen: Resultate von Audits, Status von präventiven und korrigierenden Massnahmen, bisher noch nicht berücksichtigte Schwachstellen und Gefahren und weiteres.	ISO 27001-4.2.3.f, 7.1
	Kommentar: Die IT SOX Compliance Road Map setzt im Detail einen anderen Schwerpunkt und nennt die oben genannten Dokumente und Informationen nicht explizit.	ITGI-S.37-42 
C-6	**Anforderung**: Die Effektivität der Kontrollen ist in zwei Schritten zu beurteilen: Sowohl die Gestaltung der Kontrollen (Design) als auch die Durchführung/Umsetzung der Kontrollen (Operating) ist systematisch zu bewerten.	ITGI-S.37-41
	Kommentar: ISO 27001 macht diese Unterscheidung nicht. Die Road Map unterstreicht demgegenüber die Bedeutung bezüglich der Gestaltung von Kontrollen. Dies kommt vermutlich daher, dass bei SOX die Bedeutung auf die finanzielle Berichterstattung zentral ist und somit die Kontrollen aus dieser Perspektive sehr genau ausgewählt werden müssen (insbesondere die spezifischen IT-Applikationskontrollen). Demgegenüber setzt ISO 27001 vor allem bei den generellen IT-Kontrollen einen Schwerpunkt.	ISO 27001 
C-7	**Anforderung**: Bei der Beurteilung der Kontrollen reicht in den meisten Fällen eine Befragung alleine nicht aus. Häufig wird als Methode der sogenannte Walkthrough erwähnt.	ITGI-S.38, 41
	Kommentar: ISO 27001 nennt als Grundlage für die Beurteilung der Kontrollen: Audit-Ergebnisse, Feedback von Dritten, Mess-Ergebnisse, Vorfälle. Eine Beurteilung der Kontrollen aufgrund vom Hören-Sagen reicht somit auch bei ISO 27001 nicht aus.	ISO 27001.4.2.3.b 
C-8	**Anforderung**: Die Risikobeurteilung ist in regelmässigen Abständen erneut zu hinterfragen und gegebenenfalls anzupassen.	ISO 27001-4.2.3.d
	Kommentar: Die IT SOX Compliance Road Map stellt mehrmals die Anforderungen, dass das Kontrollsystem regel-	ITGI-S.44

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	mässig überprüft und angepasst wird. Dadurch ergibt sich indirekt auch die Forderung nach einer regelmässigen Neubeurteilung bezüglich des Risikos. Ein expliziter Hinweis fehlt jedoch in der Road Map.	
C-9	**Anforderung**: Es sind regelmässig (interne) Audits durch unabhängige Personen durchzuführen. Dabei ist zu prüfen, ob Kontrollziele, Massnahmen und Prozesse die gestellten Anforderungen abdecken und wie erwartet umgesetzt worden sind. Die Audits sind geordnet durchzuführen (Risiko basiert, mit klarem Scope und dokumentierten Prüfprogramm, unter Berücksichtigung von vorhergehenden Audit-Ergebnissen und vordefiniertem Vorgehen bei der Berichterstattung etc.). Die Zuständigkeiten und Anforderungen bezüglich der Planung und Durchführung von Audits sind zu dokumentieren.	ISO 27001-4.2.3.f, 6
	Kommentar: Die IT SOX Compliance Road Map erwähnt diesen Aspekt nicht in einem eigenen Punkt. Die Anforderung zur Durchführung von unabhängigen Revisionen ergibt sich im SOX-Umfeld jedoch zwingend, da die Revisoren eine Aussage zum internen Kontrollsystem machen müssen. Dabei existieren diverse Vorgaben zur Durchführung von Audits. ISO 27001 zielt hier natürlich auf die Zertifizierung ab, indem durch interne Zwischenbeurteilungen der Reifegrad abgeschätzt werden muss.	z.B. Sarbanes-Oxley Act, Sec. 201ff
ACT – Aufrechterhaltung und Verbesserung des Kontrollsystems		
A-1	**Anforderung**: Bei den identifizierten Schwachstellen sind die Ursachen zu ermitteln, um künftige Abweichungen zu vermeiden. Präventive Kontrollen sind gegebenenfalls zu implementieren.	ISO 27001-8
	Kommentar: Die IT SOX Compliance Road Map stellt die Beseitigung der Schwachstelle in den Vordergrund und geht weniger auf die Ursachenforschung ein. Trotzdem wird dieser Aspekt ebenfalls angedeutet. Die Bedeutung von präventiven Kontrollen wird in der Road Map hervorgehoben.	ITGI-S.35, 43-45
A-2	**Anforderung**: Die identifizierten Schwachstellen sind in Zusammenarbeit mit der Finanzabteilung zu beurteilen. Dabei sind die Abhängigkeiten der Kontrollen untereinander zu ermitteln. Schliesslich sind Prioritäten für die Beseitigung	ITGI-S.43

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	der Schwachstellen festzulegen. **Kommentar**: ISO 27001 fordert das Festlegen von Prioritäten und die Zusammenarbeit mit dem Fachbereich nicht explizit. Durch die konsequente und regelmässige Risikobeurteilung wird dieser Punkt aber sicherlich zu einem gewissen Grad abgedeckt. Die Road Map deutet hier wiederum die Individualität der jeweiligen Geschäftsprozesse und die Bedeutung im Zusammenhang mit der finanziellen Berichterstattung an.	ISO 27001-4.2.1.d, 4.2.3.d 
A-3	**Anforderung**: Die identifizierten Schwachstellen und Verbesserungsmöglichkeiten sind durch geeignete Massnahmen umzusetzen. **Kommentar**: Die IT SOX Compliance Road Map stellt prinzipiell die gleichen Anforderungen.	ISO 27001-4.2.4.a, b, d, 8.1 ITGI-S.43-44 
A-4	**Anforderung**: Die Korrektur- und Verbesserungsmassnahmen sind allen involvierten Personen stufengerecht zu kommunizieren. **Kommentar**: Die IT SOX Compliance Road Map fordert die konsequente Einbindung der beteiligten Personen. Der Sarbanes-Oxley Act selbst fordert in Section 302, dass wesentliche Schwachstellen den Revisoren und im jährlichen Bericht zum internen Kontrollsystem gemeldet werden.	ISO 27001-4.2.4.c ITGI-S.19-21, 50 
Dokumentation		
R-1	**Anforderung**: Die Dokumentation muss beinhalten: Management-Entscheide, implementierte Massnahmen/Kontrollen und Testergebnisse zur Effektivität der Kontrollen. Der Zusammenhang zwischen ausgewählten Kontrollen und der Risikobeurteilung muss nachvollziehbar sein. **Kommentar**: Die IT SOX Compliance Road Map stellt prinzipiell die gleichen generellen Anforderungen an die Do-	ISO 27001-4.3.1 ITGI-S.32, 36-37

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	kumentation.	
R-2	**Anforderung**: Es muss festgelegt und dokumentiert werden, wie die (zahlreichen) Dokumente verwaltet werden. So soll beispielsweise klar definiert werden: Genehmigung, Version und Status von Dokumenten, Zugang zu Dokumenten, Aufbewahrungsdauer, Vernichtung etc.	ISO 27001-4.3.2, 4.3.3
	Kommentar: Die IT SOX Compliance Road Map stellt keine derart spezifischen Anforderungen ans Dokumenten-Management. Implizit wird aber wohl auch von einem solchen System ausgegangen.	ITGI-S.33-37
R-3	**Anforderung**: Es ist zu begründen, wenn gewisse vom Standard vorgeschlagenen Kontrollen nicht umgesetzt werden. (vgl. Verweis von ISO 27001 auf ISO 27002)	ISO 27001-4.2.1.j; ISO 27002
	Kommentar: Die IT SOX Compliance Road Map macht Vorschläge zu möglichen Kontrollen im Zusammenhang mit SOX. Es handelt sich dabei jedoch nicht um zwingende Vorgaben. Als Konsequenz sind Abweichungen zu den Vorschlägen nicht explizit zu dokumentieren. Zudem weisst die Road Map explizit darauf hin, dass nicht alle Kontrollen zu dokumentieren sind, sondern nur Schlüsselkontrollen im Zusammenhang mit der finanziellen Berichterstattung.	ITGI-S.57-95
R-4	**Anforderung**: Eine übergeordnete Richtlinie beziehungsweise Dokumentation des Managementsystems (vgl. ISMS Policy) ist zu erstellen. Ebenso ist die Methode fürs Risikomanagement zu dokumentieren.	ISO 27001-4.2.1.b,c, 4.3.1a,d
	Kommentar: Die IT SOX Compliance Road Map unterstreicht ebenfalls die Wichtigkeit einer guten Dokumentation. Auf eine Meta-Dokumentation im Sinne einer ISMS-Weisung und Risikomanagement-Methode wird jedoch nicht derart umfassend eingegangen.	ITGI-S.36-37
R-5	**Anforderung**: Die Geschäftsprozesse und dazugehörende Sub-Prozesse sind zu beschreiben (typischerweise mittels	ITGI-S.36

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	Ablaufdiagrammen). **Kommentar**: ISO 27001 fokussiert auf die Risiken und Kontrollen. Indirekt werden dadurch die Geschäftsprozesse sicherlich auch berücksichtigt. Eine entsprechende Dokumentation fordert ISO 27001 allerdings nicht.	ISO 27001-4.3 
R-6	**Anforderung**: Die Risikobeurteilung und der Umgang mit Risiken muss dokumentiert sein. **Kommentar**: Die IT SOX Compliance Road Map fordert ebenfalls eine entsprechende Dokumentation. Der Bezug zu den Geschäftsprozessen wird dabei erneut hervorgehoben.	ISO 27001-4.2.1.c,f,g, 4.3.1.e ITGI-S.32, 36 
R-7	**Anforderung**: Die ausgewählten und implementierten Kontrollen sind zu dokumentieren. Dabei ist pro Kontrolle anzugeben: Kontrollziel, Kontrollaktivität (konkrete Massnahmen) und Häufigkeit der Kontrolle. **Kommentar**: Gemäss ISO 27001 sind die Kontrollen ebenfalls zu dokumentieren. ISO 27002 nennt sowohl Kontrollziel als auch Kontrollaktivität, wodurch diese Beschreibungen auch die Anforderungen der Road Map abdecken. Auf die Häufigkeit einer Kontrolle geht ISO 27001 nicht ein.	ITGI-S.36-37 ISO 27001-4.2.1.g,j, 4.3.1.c,g 
R-8	**Anforderung**: Das Management muss detailliert dokumentieren, wie die Beurteilung des Kontroll-Designs und der Effektivität der Kontrollen stattgefunden hat und was die Ergebnisse waren. Die Dokumentation sollte unter anderem beinhalten: Zeitpunkt und Ausmass der Tests, Resultate der Tests, Schlussfolgerungen, durchführende Testperson, Stichprobenumfang und Grundmenge sowie Referenz auf Zusatzdokumentation. Die Dokumentation sollte einer unabhängigen Stelle ermöglichen, die Beurteilung der Kontrollen nachzuvollziehen. Es sollte dokumentiert werden, welche Daten bei den jeweiligen Kontrollen verwendet worden sind (Supporting Evidence).	ITGI-S.37-40

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Übereinstimmungsgrad
	Kommentar: ISO 27001 stellt die generelle Anforderung, dass Unterlagen aufbewahrt werden, um die Effektivität der Massnahmen nachvollziehbar zu machen. Die Dokumentationsanforderungen an die Beurteilung der Kontrolleffektivität gemäss Road Map sind jedoch detaillierter und decken weitere Aspekte ab.	ISO 27001-4.2.3.g, h , 4.3.1.g, 4.3.3 
Management		
M-1	**Anforderung**: Die Unternehmensleitung muss sich zum Kontrollsystem bekennen und es unterstützen. Das Management muss sicherstellen, dass die notwendigen Weisungen und Pläne erstellt werden, Verantwortlichkeiten klar definiert sind, die Bedeutung des Systems den Mitarbeitern kommuniziert wird und die Überwachung wie vorgesehen durchgeführt wird.	ISO 27001-4.2.1.i, 4.2.2.g, 5.1.a-d, g-h
	Kommentar: Die SOX-Anforderungen richten sich stark an die oberste Unternehmensleitung. Somit kann sich das Management dieser Verantwortung nicht entziehen. Die IT SOX Compliance Road Map erwähnt bisherige Erfahrungen und betont, wie wichtig die Einbindung der Mitarbeiter (sprich Kommunikation) ist. Ebenso wird eine klare Definition von Verantwortlichkeiten gefordert. Dokumentation und Überwachung (Effectiveness Testing) sind sowieso Kernelemente von SOX.	ITGI-S.19-21, 28, 33-42 
M-2	**Anforderung**: Die Verantwortlichkeiten sind insbesondere bezüglich spezifischen IT-Applikationskontrollen klar festzulegen.	ITGI-S.30
	Kommentar: ISO 27001 fordert eine klare Definition der Rollen und Verantwortungen bezüglich Informationssicherheit. Auf spezifische IT-Applikationskontrollen wird nicht gesondert eingegangen. Dieses Thema ist im SOX-Umfeld jedoch sehr wichtig, da es genau die Schnittstelle von IT und Fachbereich betrifft; Unklarheiten an dieser Stelle sind kritisch für eine erfolgreiche SOX Implementation.	ISO 27001-5.1.c 

ID	Anforderung und Kommentar betreffend Übereinstimmung	Referenzen und Überein-stimmungsgrad
M-3	**Anforderung**: Das Management muss genügend Ressourcen zur Verfügung stellen und die Mitarbeiter angemessen schulen. **Kommentar**: Die IT SOX Compliance Road Map erwähnt die Themen „Ressourcen“ und „Mitarbeiterschulung“ in ähnlicher Form. Die Anforderungen gemäss ISO 27001 sind ein wenig strukturierter und detaillierter.	ISO 27001-5.1.e, 5.2 ITGI-S.19-21, 29 

Anhang B - Mapping SOX requirements to ISO/IEC 27002:2005 using a 2-step transition

Introduction

The Sarbanes-Oxley Act (SOX) defines general rules which companies must comply with. However, requirements deriving from this Act as well as from entitled bodies (such as SEC and PCAOB) are not very detailed with regard to IT related questions. The IT Governance Institute (2006a) closed this gap by issuing the guideline „IT Control Objectives for Sarbanes-Oxley“. This document describes control objectives and illustrative controls from a SOX-IT point of view. In addition, it refers to the COBIT 4.0 standard. The IT Governance Institute (2006b) also published a mapping from COBIT 4.0 to ISO/IEC 27002 (synonymously used for ISO/IEC 17799:2005).

In the following, these two mappings have been combined in order to assess the extent SOX requirements are covered by ISO/IEC 27002. Please note that the mapping below only represents a raw combination of these two documents. Interpretations are not included but discussed in the subsequent appendix C.

Detailed Mapping

< Table removed due to copyright restrictions >

Anhang C - Vergleich der illustrativen SOX-Kontrollen gemäss IT Governance Institute mit ISO/IEC 27002:2005

Das IT Governance Institute (ITGI, 2006a) beschreibt detaillierte Kontrollziele, die im Zusammenhang mit der IT beachtet werden sollten, um die Anforderungen aus dem Sarbanes-Oxley Act erfüllen zu können. Dazu werden auf der Basis von COBIT ausgewählte und teilweise abgeänderte Kontrollen vorgeschlagen.

Mit Unterstützung des bereits existierenden Vergleichs von ISO 27002 (bzw. ISO/IEC 17799:2005) und COBIT 4.0 wird im Folgenden untersucht, inwieweit die Kontrollen aus ISO 27002 die SOX Kontrollziele gemäss ITGI (2006a) abdecken können. Das Ziel ist dabei, Lücken im ISO 27002 Standard betreffend SOX-Anforderungen zu finden.

Im eingangs erwähnten Dokument (ITGI, 2006a) werden neben ausführlichen Kontrollzielen zudem illustrative Kontrollen, Beispiele fürs Testen der Kontrollen und Referenzen zu COBIT angegeben. Die nachfolgende Tabelle fasst die Kontrollziele und Massnahmen zusammen und zeigt Abweichungen zu ISO 27002 auf (gegebenenfalls unter Berücksichtigung von ISO 27001). Dies entspricht der Interpretation und Meinung des Autors. Weiter ist zu beachten, dass es sich bei den Kontrollen des ITGIs um illustrative SOX-Kontrollen handelt, welche nicht zwingend umgesetzt werden müssen. Der nachfolgende Vergleich geht trotzdem detailliert durch sämtliche illustrativen Kontrollen durch und nennt Differenzen. Dadurch soll aufgezeigt werden, wo möglicherweise weitere Abklärungen und Überlegungen notwendig sind, wenn mit Hilfe von ISO 27002 die SOX-Anforderungen erfüllt werden sollen.

Zur besseren Lesbarkeit und Nachvollziehbarkeit sind Beschreibungen auf der Grundlage des ITGIs blau gekennzeichnet; Angaben mit Bezug zu ISO sind gelb markiert. Referenzen auf die ursprünglichen Literaturquellen sind jeweils angefügt. Die konkreten Quellen sind:

- ISO/IEC (2005a), ISO/IEC 27001:2005; Internationaler Standard, First Edition; Genf, 15.10.2005
- ISO/IEC (2005b), ISO/IEC 27002:2005; Internationaler Standard, Second Edition - renumbered 07/2007; Genf, 15.06.2005
- IT Governance Institute (2006a), IT Control Objectives for Sarbanes-Oxley; Online-Publikation, 2nd Edition; Illinois, September 2006
- IT Governance Institute (2006b), COBIT Mapping: Mapping of ISO/IEC 17799:2005 with COBIT 4.0; Online-Publikation; Illinois, 2006
- IT Governance Institute (2005), COBIT 4.0; Online-Publikation; Illinois, 2005

ISO/IEC 17799:2005 und ISO 27002 werden synonym verwendet.

ID	Kontrollziel, Massnahmen und Kommentar zum Deckungsgrad	Referenzen und Deckungsgrad
Übergeordnete Kontrollen (Entity-Level Controls, EL)		
	Kontrollumgebung (COSO: Control Environment)	
EL-1	**Strategische IT-Planung**: Kontrollen stellen sicher, dass die strategische IT-Planung auf die Geschäftsstrategie abgestimmt ist. Dazu wird in der Planungsphase systematisch mit den Anspruchsgruppen zusammengearbeitet. Die IT-Planung wird den involvierten Gruppen kommuniziert. Regelmässig findet mit dem CEO und CFO ein Informationsaustausch betreffend Massnahmen und Risiken statt.	ITGI-S.58
	Kommentar: ISO 27002 kann für sich alleine diese Anforderungen nicht vollständig abdecken. So wird die Abstimmung mit der Geschäftsstrategie und speziell die Zusammenarbeit mit CEO und CFO nicht erwähnt. In Kombination mit ISO 27001 werden die Anforderungen jedoch bis zu einem gewissen Grad adressiert, da bei ISO 27001 eine systematische Risikobeurteilung und eine Berücksichtigung des Geschäftsumfelds gefordert wird.	ISO 27001-4.2.1, 4.2.3.d 
EL-2	**Aufbau- und Ablauf-Organisation der IT**: Kontrollen stellen sicher, dass die Verantwortlichkeiten innerhalb der IT und zum Fachbereich klar definiert und kommuniziert sind. Dazu werden unter anderem die Assets in einem Inventar erfasst und den Eigentümern zugewiesen. Weiter ist sicherzustellen, dass die IT-Führung genügend Wissen und Erfahrung zur Bewältigung ihrer Aufgaben hat.	ITGI-S.58
	Kommentar: Die Anforderung zielt übergeordnet auf die gesamte IT-Organisation und deren Funktionen ab. ISO 27002 konzentriert sich demgegenüber auf die Verantwortlichkeiten und Schulungen im Bezug auf Informationssicherheit. So wird beispielsweise in ISO 27002 keine direkte Kontrolle erwähnt, welche sich mit der Definition und Kommunikation der Organisation zur Software-Entwicklung oder Schulungen in diesem Bereich befasst. Analoges gilt für die Zusammenarbeit mit dem Fachbereich: auch hier fokussiert ISO 27002 auf die Informationssicherheit und regelt (mit Ausnahme von ausgewählten Punkten) weniger explizit, wie die Zusammenarbeit generell auszusehen hat.	ISO 27002-6; 7.1.2; 8 

ID	Kontrollziel, Massnahmen und Kommentar zum Deckungsgrad	Referenzen und Deckungsgrad
EL-3	**Unternehmenskultur**: Kontrollen stellen sicher, dass unter anderem der IT-Bereich dazu beiträgt, dass die Wertvorstellungen und ethischen Grundsätze der Unternehmung verstanden und gelebt werden.	ITGI-S.58
	Kommentar: ISO 27002 fokussiert wiederum auf die Informationssicherheit. Im Zusammenhang mit SOX sind jedoch Massnahmen zur Informationssicherheit zentral, und somit leistet ISO 27002 mit der Weisung und Schulung zur Informationssicherheit einen wesentlichen Beitrag zum Thema Unternehmenskultur.	ISO 27002-5.1.1, 8.2.2 
EL-4	**Schulung der Benutzer**: Kontrollen stellen sicher, dass Benutzer bezüglich IT-Aspekten geschult werden.	ITGI-S.58
	Kommentar: ISO 27002 stellt die Anforderung, dass Benutzer bezüglich Informationssicherheit geschult werden. Generelle Benutzerschulung (z.B. Bedienung einer Applikation zur Vermeidung von Fehleingaben) wird dabei nur beiläufig erwähnt.	ISO 27002-8.2.2 
	Information und Kommunikation (COSO: Information and Communication)	
EL-5	**Information und Kommunikation**: Kontrollen stellen sicher, dass aktuelle Informationen sowohl über unternehmensinterne als auch externe Sachverhalte vorhanden und kommuniziert werden.	ITGI-S.59
	Kommentar: ISO 27002 erwähnt ausgewählte Themen wie beispielsweise „Control of Technical Vulnerabilities“. Zudem wird das Thema „Compliance“ in einem Kapitel speziell behandelt. Einen wesentlichen Beitrag zur Erfüllung des oben genannten Kontrollziels liefert jedoch ISO 27001: hier wird nämlich gefordert, dass Informationen über interne und externe Sachverhalte regelmässig und systematisch zu ermitteln und bezüglich Risiken zu beurteilen sind.	ISO 27002-12.6.1; 15 ISO 27001-4.2.1; 4.2.3 

	Risikobeurteilung (COSO: Risk Assessment)	
EL-6	**Risikobeurteilung**: Kontrollen stellen sicher, dass regelmässig und systematisch die Risiken identifiziert, beurteilt und adressiert werden. Dabei ist unter anderem sicherzustellen, dass ein formaler Massnahmenplan zur Reduktion der Risiken existiert und sich das Management über verbleibende Risiken (Residual Risk) im Klaren ist.	ITGI-S.59
	Kommentar: ISO 27002 deckt diesen Aspekt punktuell im Zusammenhang mit „Business Continuity Management“ und „Reporting Information Security Events and Weaknesses“ ab. Ebenso wird in der Einleitung auf die Bedeutung des Risikomanagements eingegangen. Die Anforderung kann aber sicherlich in Kombination mit ISO 27001 erfüllt werden, wo ein systematisches Risikomanagement verlangt wird.	ISO 27002-4; 13.1; 14 ISO 27001-4.2.1; 4.2.3 
	Überwachung (COSO: Monitoring)	
EL-7	**Qualitätsmanagement**: Ein Qualitätsmanagement-System ist für wesentliche IT-Prozesse und Kontrollen implementiert. Die Erfüllung der Anforderungen wird ständig überwacht. Gegebenenfalls wird korrigiert.	ITGI-S.60
	Kommentar: Der Grundgedanke von ISO 27001 ist genau die Erstellung und der Betrieb eines Qualitätsmanagement-Systems. Der Fokus ist dabei auf Informationssicherheit und umfasst dadurch nicht das ganze Spektrum der IT (vgl. zum Beispiel Qualitätsmangement-Systeme bei Software-Entwicklung). ISO 27002 für sich alleine berücksichtigt einzelne Punkte zur Überwachung (vgl. z.B. „Monitoring“), kann aber ohne ISO 27001 die Anforderungen an ein Qualitätsmanagement-System nicht erfüllen.	ISO 27002-10.10 ISO 27001 
EL-8	**Unabhängige Überwachung**: Kontrollen stellen sicher, dass das Management die Einhaltung von Weisungen und Vorgaben überprüft. Zudem ist die IT-Umgebung von unabhängigen Experten zu beurteilen; entsprechende Berichte sind vom Management zu berücksichtigen.	ITGI-S.60
	Kommentar: Wiederum reicht ISO 27002 alleine nicht zur vollständigen Erfüllung dieser Anforderung. Ausgewählte Punkte aus ISO 27002 (z.B. „Compliance with Security Policies and Standards“) in Kombination mit ISO 27001	ISO 27002-6.1.8; 15.2.1

	sorgen jedoch dafür, dass wesentliche Weisungen zur Informationssicherheit, entsprechende Prozesse und Kontrollen überwacht werden.	ISO 27001-4.2.3; 7
Kontroll-Aktivitäten (COSO: Activity-Level Controls, AL)		
AL-1	**Beschaffung und Entwicklung von Applikationssoftware und Systemen**: Kontrollen stellen sicher, dass Applikationen und Systeme beschafft und entwickelt werden, welche die Anforderungen bezüglich der finanziellen Berichterstattung optimal erfüllen. Dazu werden insbesondere die Endbenutzer bei der Beschaffung beziehungsweise Entwicklung von Applikationssoftware eingebunden. Unter anderem sind die Anforderungen an Applikationskontrollen systematisch zu erfassen und zu implementieren. Nach der Umsetzung sind die Applikationskontrollen auf ihre Wirksamkeit zu prüfen.	ITGI-S.61-63
	Kommentar: ISO 27002 enthält ein eigenes Kapitel zum Thema „Beschaffung und Entwicklung von Applikationssoftware“. Darin wird beschrieben, dass zu Beginn die Sicherheitsanforderungen erfasst werden müssen. Weiter wird aufgezählt, welche spezifischen Applikationskontrollen bei der Eingabe, Verarbeitung und Ausgabe vorhanden sein sollten. Da ISO 27002 hier sehr allgemeine Formulierungen verwendet, ist im Zusammenhang mit SOX speziell zu berücksichtigen und nicht zu vergessen, dass die Endbenutzer (insbesondere Vertreter aus der Finanzabteilung) eingebunden werden und deren Anforderungen systematisch und ausführlich erfasst werden (vgl. z.B. COBIT 4.0, AI2.9 „Applications Requirements Management”). Dies muss neben allgemeinen Sicherheitsanforderungen auch spezifische IT-Applikationskontrollen umfassen. Zudem müssen diese Kontrollen vor und nach der Einführung getestet werden, was ebenfalls nicht so direkt in ISO 27002 formuliert ist.	ISO 27002-12
AL-2	**Voraussetzungen schaffen für den Betrieb**: Kontrollen stellen sicher, dass Weisungen und Anleitungen für die Beschaffung, Entwicklung und den Betrieb von Applikationen und Systemen erstellt werden. Diese Dokumente werden regelmässig aktualisiert und von den betroffenen Personen befolgt. Namentlich sind formell zu regeln: Software-Entwicklung, Systemänderungen, Betrieb und Zugriff auf Programmen und Daten.	ITGI-S.63-64
	Kommentar: ISO 27002 erwähnt Weisungen und Anleitungen an verschiedenen Stellen, insbesondere: „Information	ISO 27002-5.1.1;

	Security Policy Document“, „Change Management“, „Access Control Policy“, „Documented Operating Procedures“. Die Einhaltung der Weisungen und Anleitungen werden einerseits in ISO 27002 (vgl. z.B. „Compliance with Security Policies and Standards“) als auch übergeordnet in ISO 27001 (vgl. „Monitor the ISMS“) adressiert. Das Erstellen von Anleitung zur Software-Entwicklung wird von ISO 27002 nicht speziell gefordert.	10.1.1; 10.1.2; 11.1.1; 15.2.1 ISO 27001-4.2.3 
AL-3	**Installation und Genehmigung von Software und Änderungen**: Kontrollen stellen sicher, dass neue Applikationen und Systeme angemessen getestet und abgenommen werden, bevor sie in die Produktion überführt werden. Dadurch soll sichergestellt werden, dass die Prozesse und eingebundenen Kontrollen korrekt funktionieren. Es ist eine Teststrategie zu entwickeln, und es ist zwischen Einzel-, System-, Integrations- und Abnahme-Tests zu unterscheiden. Die Aspekte „Stresstests“, „Datenkonversion“ und „Schnittstellen“ sind ebenfalls zu berücksichtigen. Weiter ist ein Umsetzungsplan zu erstellen. Diese Anforderungen bezüglich der Einführung von neuen Applikationen und Systemen gelten in ähnlicher Form auch bei Änderungen an bestehenden Applikationen und Systemen.	ITGI-S.64-67
	Kommentar: ISO 27002 fordert ebenfalls einen geordneten Änderungs-Prozess inklusiv formeller Abnahme durch die Benutzer. Zudem wird an zahlreichen Stellen die Notwendigkeit von Tests erwähnt (vgl. z.B. „Change Management“; „Separation of Development, Test and Operational Facilities“; „System Acceptance“, „Change Control Procedures“). Diese Anforderungen an das Testvorgehen sind jedoch weniger systematisch und weniger ausführlich als beim IT Governance Institute. Die Aspekte „Datenkonversion“, „Stresstests“ und „Implementierungsplan“ (vgl. COBIT 4.0 AI7) sind in ISO 27002 nicht oder nur teilweise erwähnt.	ISO 27002-10.1; 10.3.2; 12.5 
AL-4	**Definieren und Verwalten von Service Level Agreements**: Kontrollen stellen sicher, dass Service Levels definiert und verwaltet werden, um Klarheit über die Leistungen zu erhalten. Messkriterien für den Leistungserfüllungsgrad sind dabei festzulegen. Service Level Agreements betreffen sowohl interne als auch externe Parteien.	ITGI-S.68
	Kommentar: ISO 27002 erwähnt dieses Thema vor allem im Zusammenhang mit externen Anbietern („Third Party Service Delivery Management“). Zudem werden im PDCA-Modell von ISO 27001 ebenfalls Messkriterien gefordert. Die Anforderungen gemäss IT Governance Institute sind jedoch bei Service Level Agreements in Bezug auf interne Parteien spezifischer (vgl. COBIT 4.0 DS1). Zudem ist bei SOX darauf zu achten, dass Daten zeitgerecht erhalten werden, was in ISO 27002 nur ansatzweise abgedeckt wird.	ISO 27002-10.2 ISO 27001-4.2.2 

AL-5	**Umgang mit externen Dienstleistungsanbietern**: Kontrollen stellen sicher, dass wichtige, extern bezogene Dienstleistungen in Verträgen definiert und formell vereinbart werden. Es ist darauf zu achten, dass die Dienstleistungen zeitgerecht erfolgen und die Datensicherheit beim Dienstleistungsanbieter gegeben ist. Unter anderem muss die Auswahl der Anbieter systematisch erfolgen. Weiter sind Sicherheits-Reviews beim externen Anbieter durchzuführen. Nötigenfalls ist das Kontrollsystem des Dienstleistungsanbieters mittels Compliance-Zertifikat (SAS 70) bestätigen zu lassen.	ITGI-S.69-70
	Kommentar: ISO 27002 behandelt dieses Thema weitgehend im Kapitel „Third Party Service Delivery Management“. Dabei werden unter anderem auch unabhängige Audits angesprochen. Das IT Governance Institute ist bezüglich Anforderungen zur Auswahl der Dienstleistungsanbieter etwas detaillierter. Zudem geht der Compliance-Nachweis bei externen Dienstleistungsanbietern über die Vorgaben von ISO 27002 hinaus.	ISO 27002-10.2 
AL-6	**Gewährleisten der Systemsicherheit**: Kontrollen stellen sicher, dass die Systeme, die für die finanzielle Berichterstattung verwendet werden, geschützt sind. Es soll vermieden werden, dass Daten unberechtigt eingesehen, geändert, beschädigt oder verloren gehen. Unter anderem ist deshalb eine Weisung zur Informationssicherheit zu erstellen, zu genehmigen und zu kommunizieren. Weiter sind Mechanismen zur ordnungsmässigen Authentisierung von Benutzern zu implementiert. Ebenso ist sicherzustellen, dass Kontrollprozesse zur Benutzerverwaltung existieren. Die Systeme sind vor unberechtigten Zugriffen aus öffentlichen Netzen zu schützen und die Überwachung der Systeme erfolgt auf der Ebene Betriebssystem, Datenbank und Applikation. Physischer Zutritt ist kontrolliert.	ITGI-S.71-74
	Kommentar: Es handelt sich bei diesen Anforderungen um sehr wesentliche Punkte im Zusammenhang mit SOX, die zugleich den Kern von ISO 27002 treffen. Die Anforderungen werden durch ISO 27002 abgedeckt.	ISO 27002 
AL-7	**Verwalten der Konfiguration**: Kontrollen stellen sicher, dass IT-Komponenten durch angemessene Konfigurationen geschützt sind und unautorisierte Änderungen vermieden werden. Zudem wird nur genehmigte Software verwendet und Antivirenprogramme werden eingesetzt.	ITGI-S.75-76
	Kommentar: Die Anforderungen, wie sie beim IT Governance Institute (2006a) definiert werden, sind durch diverse	ISO 27002-7;

	Punkte in ISO 27002 abgedeckt (vgl. z.B. „Asset Management“, „Access Control“, „Protection against malicious and mobile Code“ etc.).	10.4; 11 
AL-8	**Umgang mit Problemen und Sicherheitsvorfällen**: Kontrollen stellen sicher, dass bei Problemen und Sicherheitsvorfällen korrekt vorgegangen wird. Auftretende Probleme und Schwachstellen werden aufgezeichnet, analysiert und mit angemessenen Massnahmen beseitigt.	ITGI-S.76
	Kommentar: Das Kapitel „Information Security Incident Management“ von ISO 27002 befasst sich genau mit diesen Aspekten. Zudem geht ISO 27002 auf das Thema „Business Continuity Management“ ein, was ebenfalls zur Erfüllung der oben genannten Anforderungen beiträgt. Weiter unterstützt auch ISO 27001 in den Phasen „Check“ und „Act“ dieses Kontrollziel.	ISO 27002-13; 14 ISO 27001-4.2.3; 4.2.4 
AL-9	**Handhabung der Daten**: Kontrollen stellen sicher, dass Daten während der Weiterleitung und Aufbewahrung vollständig, richtig und nötigenfalls rechtsgültig bleiben. Dazu sind Weisungen und Anleitungen zu erstellen, welche die Verteilung und Aufbewahrung von Daten regeln. Aufbewahrungszeiten sind sowohl für Programme als auch Dokumente, Berichte und übrige Daten zu definieren. Backups sind regelmässig zu erstellen, und das Zurückspielen ist zu testen.	ITGI-S.77-78
	Kommentar: Die folgenden Kapitel aus ISO 27002 stellen die gleichen Anforderungen an die Weiterleitung und Aufbewahrung von Daten: „Information Exchange Policies and Procedures“, „Information Backup“, „Management of removable Media“, „Protection of Organizational Records“, „Physical Media in Transit“ und weitere.	ISO 27002-10.5.1; 10.7.1; 10.8; 15.1.3 
AL-10	**Sicherstellen des Betriebs**: Kontrollen stellen sicher, dass genehmigte Programme wie geplant ausgeführt werden. Abweichungen von der geplanten Ausführung werden identifiziert und mit Gegenmassnahmen berücksichtigt.	ITGI-S.79
	Kommentar: ISO 27002 fordert eine Dokumentation für den Betrieb von IT-Komponenten (vgl. „Documented Operating Procedures“). Ebenso wird an mehreren Stellen eine Überwachung der Systeme gefordert (vgl. „Monitoring“). Das Thema „Job-Steuerung und Überwachung“ wird von ISO 27002 nur indirekt erwähnt.	ISO 27002-10.1.1; 10.10

		
AL-11	**End-User Computing**: Kontrollen stellen sicher, dass IT-Applikationen, welche durch den Fachbereich selbst erstellt worden sind, ordnungsgemäss verwaltet und betrieben werden (vgl. z.B. Tabellenkalkulationsprogramme). Insbesondere sind Weisungen und Anleitungen zum End-User Computing (EUC) zu erstellen. Wichtige EUC-Applikationen sind regelmässig bezüglich Integrität zu überprüfen. Weiter sind Backups zu erstellt und die Zugriffe angemessen einzuschränken. Eine Dokumentation zu jeder Applikation ist erforderlich.	ITGI-S.80-81, 104-106
	Kommentar: ISO 27001 und 27002 unterscheiden nicht zwischen Applikationen, welche durch die IT-Abteilung entwickelt wurden, und Programmen aus dem Fachbereich; es gelten für alle Applikationen die gleichen Anforderungen. Das IT Governance Institute widerspricht diesem Ansatz nicht, schlägt aber trotzdem vor, dieses Thema speziell zu beachten. Insbesondere in der Finanzabteilung werden nämlich häufig selbst erstellte Tabellenkalkulationsprogramme verwendet, bei denen die generellen IT-Kontrollen nicht konsequent angewendet werden.	- 
AL-12	**Applikationskontrollen**: Es ist sicherzustellen, dass spezifische IT-Applikationskontrollen identifiziert, dokumentiert und ordnungsgemäss umgesetzt werden. Dazu ist der Geschäftsprozess entsprechend zu analysieren. Es sind Kontrollen betreffend Existenz, Richtigkeit, Vollständigkeit und korrekter Freigabe von Transaktionen zu implementieren (vgl. auch CAVR-Prinzip von PwC). Die Dateneingabe, Verarbeitung und Ausgabe ist auf mögliche Fehler zu überprüfen. Kontrollen können beispielsweise sein: Vergleich von Summentotalen, Überprüfung von Werteberei-chen, abgestufte Freigabe von Transaktionen aufgrund von implementierten Kompetenzordnungen etc.	ITGI-S.82-96
	Kommentar: Die spezifischen IT-Applikationskontrollen sind oftmals im Verantwortungsbereich der Fachabteilungen und sind ein Schlüssel-Element im Rahmen von SOX. Es handelt sich um massgeschneiderte Kontrollen für die jeweiligen Geschäftsprozesse. ISO 27002 geht im Kapitel „Correct Processing in Applications“ prinzipiell auf diese Kontrollen ein. Das IT Governance Institute hebt jedoch das Zustandekommen dieser spezifischen IT-Applikationskontrollen und deren Bezug zu den Geschäftsprozessen deutlicher hervor. Zudem wird hier die Bedeutung der Kontrollen mit zahlreichen Beispielen untermauert.	ISO 27002-12 

Anhang D - Liste der Kontrollen aus ISO/IEC 27002:2005 und Hinweise zu deren SOX-Relevanz

Das IT Governance Institute (ITGI, 2006a) hat eine Liste mit „illustrativen“ SOX Kontrollen im IT-Bereich zusammengestellt. Sehr wichtige Punkte sind in der Liste speziell gekennzeichnet und zu jeder Kontrolle sind Referenzen auf die entsprechenden Detail-Kontrollziele von COBIT 4.0 angegeben.

Unabhängig von der SOX-Diskussion existiert eine andere Publikation des IT Governance Institutes (2006b), worin die Kontrollziele von COBIT 4.0 mit den Kontrollen von ISO/IEC 27002 verglichen werden.

Diese beiden Abbildungen sind nun wie folgt miteinander verknüpft worden:

ITGI (2006a): IT Control Objectives for SOX; 2nd Edition	ITGI (2006a): IT Control Objectives for SOX; 2nd Edition	ITGI (2005): COBIT 4.0	ITGI (2006b): Mapping of ISO 17799:2005 with COBIT 4.0	ISO/IEC (2005b): ISO/IEC 27002:2005

Als Ergebnis dieser Verknüpfung entsteht eine Liste mit Hinweisen zur SOX-Relevanz von ISO/IEC 27002 Kontrollen. Da Mehrfach-Beziehungen in den Abbildungen vorhanden sind, ergibt sich zudem eine Häufigkeitsverteilung. Um wichtige Kontrollen gebührend zu berücksichtigen, werden jene Kontrollen mit einem Faktor 3 gewichtet, welche gemäss IT Governance Institute von besonderer Bedeutung sind. Es ergibt sich die untenstehende Reihenfolge. Weiter werden die Kontrollen aufgrund der Reihenfolge gleichmässig in die Kategorien 0 bis 4 eingeteilt (0=unwichtig, 4=wichtig; diese Kategorien dienen im Anhang F für eine andere Analyse).

Name of ISO/IEC 27002 control	No. of occurrences in important ITGI-SOX controls (A)	No. of occurrences in other ITGI-SOX controls (B)	Overall rating (C=3*A+B)	Ranking Category (D=f(C))
12.2.2 Control of internal processing	18	6	60	4
12.2.1 Input data validation	15	5	50	4
10.1.3 Segregation of duties	14	5	47	4
12.2.3 Message integrity	14	5	47	4
10.9.2 Online transactions	12	4	40	4
12.2.4 Output data validation	12	4	40	4
10.1.2 Change management	10	8	38	4
5.1.1 Information security policy document	7	13	34	4
6.1.5 Confidentiality agreements	9	6	33	4

Name of ISO/IEC 27002 control		No. of occurrences in important ITGI-SOX controls (A)	No. of occurrences in other ITGI-SOX controls (B)	Overall rating (C=3*A+B)	Ranking Category (D=f(C))
8.1.1	Roles and responsibilities	8	7	31	4
10.1.1	Documented operating procedures	9	2	29	4
12.5.2	Technical review of applications after operating system changes	7	6	27	4
5.1.2	Review of the information security policy	4	14	26	4
10.3.2	System acceptance	8	2	26	4
11.3.1	Password use	8	2	26	4
11.5.1	Secure logon procedures	8	2	26	4
11.5.3	Password management system	8	2	26	4
11.6.1	Information access restriction	8	2	26	4
12.5.1	Change control procedures	6	7	25	4
12.5.3	Restrictions on changes to software packages	6	7	25	4
6.2.1	Identification of risks related to external parties	5	9	24	4
10.8.4	Electronic messaging	6	5	23	4
11.1.1	Access control policy	6	4	22	4
6.2.3	Addressing security in third-party agreements	4	9	21	4
12.1.1	Security requirements analysis and specification	6	3	21	4
13.2.3	Collection of evidence	6	3	21	4
10.9.1	Electronic commerce	6	2	20	4
6.1.1	Management commitment to information security	4	7	19	3
6.1.4	Authorization process for information processing facilities	5	4	19	3
8.2.2	Information security awareness, education and training	3	10	19	3
12.3.1	Policy on the use of cryptographic controls	5	2	17	3
12.4.3	Access control to program source code	4	5	17	3
15.3.2	Protection of information systems audit tools	5	2	17	3
6.2.2	Addressing security when dealing with customers	5	1	16	3
8.3.1	Termination responsibilities	5	1	16	3
8.3.3	Removal of access rights	5	1	16	3
10.1.4	Separation of development, test and operational facilities	4	4	16	3
11.2.1	User registration	5	1	16	3
11.2.2	Privilege management	5	1	16	3
11.2.4	Review of user access rights	5	1	16	3
12.6.1	Control of technical vulnerabilities	3	7	16	3
15.2.1	Compliance with security policies and standards	1	13	16	3
15.3.1	Information systems audit controls	4	4	16	3
11.6.2	Sensitive system isolation	4	3	15	3
6.1.2	Information security co-ordination	2	8	14	3
12.5.5	Outsourced software development	4	2	14	3
10.6.1	Network controls	3	4	13	3

Name of ISO/IEC 27002 control		No. of occurrences in important ITGI-SOX controls (A)	No. of occurrences in other ITGI-SOX controls (B)	Overall rating (C=3*A+B)	Ranking Category (D=f(C))
10.7.3	Information handling procedures	3	4	13	3
10.8.3	Physical media in transit	3	4	13	3
10.8.1	Information exchange policies and procedures	3	3	12	3
11.4.1	Policy on use of network services	3	3	12	3
13.1.2	Reporting security weaknesses	3	3	12	3
13.2.1	Responsibilities and procedures	3	3	12	3
10.5.1	Information backup	2	5	11	3
10.10.2	Monitoring system use	1	8	11	3
12.4.2	Protection of system test data	1	8	11	3
10.10.1	Audit logging	3	1	10	2
10.10.5	Fault logging	3	1	10	2
10.7.4	Security of system documentation	3	1	10	2
11.2.3	User password management	3	1	10	2
11.5.2	User identification and authentication	3	1	10	2
11.5.5	Session time-out	3	1	10	2
11.5.6	Limitation of connection time	3	1	10	2
12.3.2	Key management	3	1	10	2
12.5.4	Information leakage	3	1	10	2
6.1.8	Independent review of information security	1	5	8	2
10.10.4	Administrator and operator logs	1	5	8	2
13.2.2	Learning from information security incidents	2	2	8	2
7.2.1	Classification guidelines	2	1	7	2
9.1.6	Public access, delivery and loading areas	2	1	7	2
10.2.2	Monitoring and review of third-party services	1	4	7	2
10.2.3	Managing changes to third-party services	0	7	7	2
14.1.4	Business continuity planning framework	2	1	7	2
8.1.2	Screening	0	6	6	2
8.1.3	Terms and conditions of employment	0	6	6	2
11.7.1	Mobile computing and communications	1	3	6	2
11.7.2	Teleworking	1	3	6	2
14.1.1	Including information security in the business continuity management process	1	3	6	2
15.2.2	Technical compliance checking	1	3	6	2
10.2.1	Service delivery	0	5	5	2
13.1.1	Reporting information security events	1	2	5	2
15.1.4	Data protection and privacy of personal information	0	5	5	2
6.1.3	Allocation of information security responsibilities	0	4	4	1
9.2.5	Security of equipment off premises	0	4	4	1
10.8.2	Exchange agreements	0	4	4	1
11.5.4	Use of system utilities	1	1	4	1
7.1.2	Ownership of assets	0	3	3	1
9.1.5	Working in secure areas	0	3	3	1
10.10.3	Protection of log information	1	0	3	1
11.4.3	Equipment identification in networks	0	3	3	1

Name of ISO/IEC 27002 control		No. of occurrences in important ITGI-SOX controls (A)	No. of occurrences in other ITGI-SOX controls (B)	Overall rating (C=3*A+B)	Ranking Category (D=f(C))
14.1.2	Business continuity and risk assessment	0	3	3	1
9.1.2	Physical entry controls	0	2	2	1
9.2.4	Equipment maintenance	0	2	2	1
10.6.2	Security of network services	0	2	2	1
10.7.1	Management of removable media	0	2	2	1
11.4.2	User authentication for external connections	0	2	2	1
11.4.4	Remote diagnostic and configuration port protection	0	2	2	1
11.4.5	Segregation in networks	0	2	2	1
11.4.6	Network connection control	0	2	2	1
11.4.7	Network routing control	0	2	2	1
15.1.3	Protection of organizational records	0	2	2	1
6.1.6	Contact with authorities	0	1	1	1
7.1.1	Inventory of assets	0	1	1	1
7.2.2	Information labeling and handling	0	1	1	1
8.2.1	Management responsibilities	0	1	1	1
8.2.3	Disciplinary process	0	1	1	1
9.1.1	Physical security perimeter	0	1	1	1
9.1.3	Securing offices, rooms and facilities	0	1	1	1
9.2.7	Removal of property	0	1	1	1
10.4.1	Controls against malicious code	0	1	1	1
10.4.2	Controls against mobile code	0	1	1	1
15.1.1	Identification of applicable legislation	0	1	1	1
15.1.2	Intellectual property rights (IPR)	0	1	1	1
15.1.5	Prevention of misuse of information processing facilities	0	1	1	1
6.1.7	Contact with special interest groups	0	0	0	0
7.1.3	Acceptable use of assets	0	0	0	0
8.3.2	Return of assets	0	0	0	0
9.1.4	Protecting against external and environmental threats	0	0	0	0
9.2.1	Equipment sitting and protection	0	0	0	0
9.2.2	Supporting utilities	0	0	0	0
9.2.3	Cabling security	0	0	0	0
9.2.6	Secure disposal or re-use of equipment	0	0	0	0
10.3.1	Capacity management	0	0	0	0
10.7.2	Disposal of media	0	0	0	0
10.8.5	Business information systems	0	0	0	0
10.9.3	Publicly available information	0	0	0	0
10.10.6	Clock synchronization	0	0	0	0
11.3.2	Unattended user equipment	0	0	0	0
11.3.3	Clear desk and clear screen policy	0	0	0	0
12.4.1	Control of operational software	0	0	0	0
14.1.3	Developing and implementing continuity plans including information security	0	0	0	0
14.1.5	Testing, maintaining and re-assessing business continuity plans	0	0	0	0
15.1.6	Regulation of cryptographic controls	0	0	0	0

Bemerkungen

Die oben aufgeführte Liste entsteht durch die mechanische Abbildung in zwei Phasen. Die Reihenfolge ist jedoch kritisch zu hinterfragen. So ist beispielsweise das Thema „physische Sicherheit“ stark untergewichtet, obwohl gute Gründe für eine höhere SOX-Relevanz sprechen. Wenn die physische Sicherheit in den Beispielen des IT Governance Institutes nur in einem, dafür aber abschliessenden Fall behandelt wird, so kommt es zu einer Untergewichtung im Vergleich zu Themen wie Change Management, die in mehrere Beispiele einfliessen.

Untergewichtet sind in der Liste vermutlich auch die Kontrollen zu „Unattended user equipment“ und „Clear desk and clear screen policy“; diese Kontrollen leisten nämlich einen wesentlichen Beitrag zum generellen Zugriffsschutz und somit auch zur Datensicherheit und schliesslich zur korrekten finanziellen Berichterstattung. Die Kontrolle „Prevention of misuse of information processing facilities“ lässt eigentlich auch einen engen SOX-Bezug vermuten, ist aber gemäss obiger Liste kaum von Relevanz. Eine mögliche Erklärung ist, dass andere Kontrollen aus dem Standard bereits ähnliche Kontrollziele verfolgen und dass die Kontrolle im Kern „nur“ die private Nutzung von IT-Mitteln einschränken möchte.

Demgegenüber werden gewisse Kontrollen aus ISO/IEC 27002 über die transitive Abbildung sehr häufig erwähnt, obwohl eine derart grosse Bedeutung für SOX fraglich ist. Auffällig ist insbesondere die hohe Gewichtung von „Vertraulichkeitsvereinbarungen“. Es handelt sich dabei um eine generelle, übergeordnete Kontrolle, die vom IT Governance Institute im Zusammenhang mit den Themen „Rollen & Verantwortung“, „Benutzeradministration“ und „IT-Sicherheitsplan“ erwähnt werden. Diese Themen spielen zwar bei SOX eine wichtige Rolle, der Teilaspekt „Vertraulichkeitsvereinbarungen“ wird in diesem Zusammenhang aber vermutlich weniger wichtig sein.

Auf ähnliche Weise dürfte das Thema „Information Systems Audit Considerations“ in der oben aufgeführten Liste zu stark gewichtet sein: Die entsprechenden Kontrollen werden nämlich mehrmals bei den Themen „Monitoring“ und „Software Development Life Cycle (SDLC)“ genannt und dadurch stark gewichtet, obwohl diese Kontrollen nur einen Teilbereich des Monitoring und SDLCs abdecken.

Eine verhältnismässig hohe SOX-Relevanz hat gemäss der oben aufgeführten Liste auch das Thema „Restrictions on changes to software packages“. Der Grund liegt darin, dass dieses Thema beim Change Management und SDLC (zurecht) erwähnt wird. Trotzdem darf hier nicht die Schlussfolgerung gemacht werden, dass bei SOX genau diese Kontrolle von besonderer Bedeutung ist. In der Tat dürften einige Unternehmen diese Kontrolle nicht konsequent einhalten und trotzdem die SOX-Anforderungen erfüllen.

Zusammenfassend kann festgehalten werden, dass die oben genannte Liste nur Hinweise und Tendenzen zur SOX-Relevanz von Kontrollen aus ISO/IEC 27002 geben kann. So spielen tendenziell Kontrollen aus dem Themenbereich „spezifische IT-Applikationskontrollen“, „Logischer Zugriffsschutz“ und „Change Management“ eine wichtige Rolle, während „Umgebungssicherheit“ und „Business Continuity Management“ weniger bedeutend sind. Einzelne Kontrollen sollten aufgrund der oben genannten Reihen-

folge aber nicht von Anfang an ausgeschlossen werden. Tatsächlich wird sich wohl zu jeder Kontrolle ein Argument finden lassen, weshalb sie bei SOX relevant ist.

Anhang E - Abbildung der generellen IT-Kontrollen der Credit Suisse auf ISO/IEC 27002:2005

< Anhang E beinhaltet vertrauliche Daten. Deshalb wurde dieser Teil in der öffentlichen Version der Diplomarbeit entfernt. >

Anhang F - Liste der Kontrollen aus ISO/IEC 27002:2005, abgeleitet aus SOX-Kontrollen der Credit Suisse und Vergleich mit dem IT Governance Institute

< Anhang F beinhaltet vertrauliche Daten. Deshalb wurde dieser Teil in der öffentlichen Version der Diplomarbeit entfernt. >

Eigenständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit respektiv die von mir ausgewiesene Leistung selbständig, ohne Mithilfe Dritter und nur unter Ausnützung der angegebenen Quellen verfasst respektiv erbracht habe.

Luzern, 24. September 2007 Sig. D. Russenberger