

Erfahrungen mit COBIT

Erfahrungen mit der Umsetzung von COBIT in der Internen Informatik-Revision der Winterthur-Gruppe (WGR)

Der folgende Beitrag gibt in einer Einführung den Hintergrund und die Beweggründe an, die dazu geführt haben, dass das IT Audit der WGR COBIT einsetzt. In einem Anwendungsbeispiel wird gezeigt, wie COBIT verwendet werden kann, um einen Prüfungsgegenstand zu fokussieren und zu prüfen.

Einführung

Wettbewerb und Wandel sind zwei der vielen Rahmenbedingungen, welche die Unternehmungen in der heutigen Zeit zwingen, grossen Wert auf effektive und effiziente Informationssysteme zu legen. Die hohen Anforderungen an Funktionalität, Zuverlässigkeit, Geschwindigkeit, Verfügbarkeit und Transparenz müssen im Rahmen begrenzter Budgets erfüllt werden. Entsprechend diesen Entwicklungen hat das Bedürfnis von Management, Benutzern und Revisoren nach Grundlagen und Standards für die Sicherheit und Kontrolle von Informationssystemen zugenommen.

Revisoren benötigen einen Massstab, um Informationssysteme bezüglich verschiedener Kriterien wie Effektivität, Effizienz, Sicherheit und Einhaltung von externen und internen Regelungen beurteilen zu können. Immer mehr werden Revisoren zu Beratungs-

Dienstleistungen herangezogen. Dazu sind Rahmenwerke (Frameworks), die eine gemeinsame Begriffs- und Kommunikationsbasis schaffen und die "Good Practices" darlegen sehr hilfreich.

IT-Management, Fachbereiche und Revisoren stehen nicht nur in der Winterthur-Gruppe einer verwirrend hohen Anzahl von Verfahren und Rahmenwerken gegenüber, die einen sicheren und kontrollierten Einsatz von Informationssystemen in der eigenen Organisation gewährleisten sollen. Die Anwendungsbreite und -tiefe eines Frameworks oder einer Methode variieren stark. Dies erschwert auch die Auswahl einer geeigneten Basis für die Entwicklung und Umsetzung von Informationssystemen.

Mit der Entwicklung von COBIT scheint es gelungen zu sein, eine Art "Landkarte" des Informatikeinsatzes in einer Organisation zu entwerfen. Mit Hilfe dieser Landkarte lassen sich Entwicklung und produktiver Einsatz von Informationssystemen bezüglich Kontrolle und Sicherheit systematisch und von verschiedenen Blickwinkeln her untersuchen. Prinzipien, Struktur und Begriffe von COBIT sind so gewählt, dass sie von Management, IT-Management, Fachbereichen und Revisoren verstanden werden.

Seit etwa drei Jahren wird in der Internen Informatik-Revision der Winterthur-Gruppe konsequent das COBIT-Rahmenwerk eingesetzt [1]. Warum?

- COBIT bildet eine geeignete Basisstruktur für viele Aufgaben. Alle Informatik-Revisoren verwenden die gleiche Landkarte. Kommunikation und Erfahrungsaustausch werden effizienter und eindeutiger. Prüfverfahren und -programme basieren nun auf der Struktur von COBIT und beseitigen so Redundanzen.

- COBIT wird zur Planung und Festlegung des Prüfungsgegenstandes (Scoping) verwendet.

- Oft ist der Soll-Zustand des Prüfungsgegenstandes der geprüften Einheit nicht klar oder gibt zu Diskussionen Anlass. Hier werden die Control Objectives aus COBIT der geprüften Einheit im voraus kommuniziert. Der Soll-Zustand wird für die Auditees transparenter und wird, durch den internationalen Charakter von COBIT und die Darlegung von "Good Business Practices", gut akzeptiert.

- Im Revisionsbericht werden die IT-Prozesse aus COBIT, die den Prüfungsgegenstand betreffen, aufgeführt und mit einer Skala bewertet. Der Informationsgehalt des Revisionsberichtes wird dadurch verbessert.

Aufgrund seiner Struktur ist COBIT für die Verwendung im Self Assessment geeignet. Es ist geplant, COBIT in naher Zukunft dafür einzusetzen.

Anwendungsbeispiel

Das folgende Beispiel zeigt, wie der IT Audit WGR COBIT für einen LAN Audit (Local Area Network) einsetzt.

Festlegen des Prüfungsgegenstandes

Zunächst ist das Ziel der Prüfung festzulegen (Audit Objective). Bei einem LAN Audit geht es primär darum, den Prozess “DS5 Ensure Systems Security” zu sichern. Danach wird eine Auswahl der Control Objectives getroffen, die geprüft werden sollen. Damit diese Auswahl in der Gruppe vorgenommen werden kann, ist es wichtig, dass die daran beteiligten Informatik-Revisoren Struktur und Prinzipien von COBIT und den Inhalt der “Control Objectives” gut kennen. Der Aufwand zum Kennenlernen von COBIT wird leicht unterschätzt. Erfahrungswerte sprechen von ca. 40 Stunden Lernaufwand, um das Wesen und den Inhalt von COBIT gut kennenzulernen.

Neben der Variante, sich direkt auf den primären Prozess DS 5 zu konzentrieren, kann man auch “Top Down” eine Auswahl der Control Objectives treffen. Dabei fängt man beim ersten Prozess PO 1 an und kämmt alle Prozesse und Control Objectives durch. Bei diesem Vorgehen besteht allerdings die Gefahr, zuviele Control Objectives auszuwählen, was zu einem recht hohen Prüfungsaufwand führt. Für erfahrene Informatik-Prüfer spielen die Navigation Aids von COBIT (Information Criteria und IT Resources) eine eher untergeordnete Rolle. Nach einer Weile kennt man den Inhalt der ca. 300 Control Objectives und kann so zielgerichteter eine Auswahl treffen.

Erstellen eines Prüfprogrammes (Audit Program)

Das Prüfprogramm gibt vor, wie der definierte Prüfungsgegenstand untersucht wird. Es besteht aus mehreren Prüfschritten (Audit Steps). Je nach Natur der Control Objectives (CO) müssen diese bei einem LAN Audit mit spezifischen Ressourcen betreffend der untersuchten Plattform ergänzt werden. Während z.B. DS 5.5 (Management Review of User Accounts) ein plattformunabhängiges CO darstellt, muss DS 5.1 (Manage Security Measures) mit geeigneten Komplementär-Informationen konkretisiert werden. Diese zusätzlichen Informationen sind es, die angeben, wie z.B. ein Sicherheitskonzept bei einem Windows NT LAN aussieht, wie dessen Grundschutz gestaltet sein muss, welche Parameter wie gesetzt sein müssen. Das Ergänzen mit Komplementär-Informationen wird heute von einer Reihe guter Quellen unterstützt (z.B. IT-Grundschutzhandbuch des deutschen BSI [2], Sicherheits-Tips [3], Internet etc.).

Die folgende Tabelle zeigt, wie Control Objectives mit Komplementär-Informationen konkretisiert werden. So entsteht z.B. das Prüfprogramm für eine Windows-NT-LAN-Prüfung. Die

Tabelle dient als Beispiel und zeigt nicht das vollständige Prüfprogramm.

Man könnte jetzt argumentieren, das IT-Grundschutzhandbuch direkt und von Anfang an für die Prüfung zu benutzen. COBIT stellt jedoch eine geeignetere Fokussierungshilfe für Informatik-Prüfungen im weiten Sinne dar. Durch das konstante Verwenden von COBIT als Master-Struktur wird zudem ein einheitliches Format aller Prüfprogramme gewährleistet.

Revisoren mit etwas Erfahrung können jetzt bereits mit dem Durchführen der Prüfschritte beginnen. Die COBIT Audit Guidelines sind sehr umfangreich und werden nur für sehr detaillierte Prüfungen herangezogen. Wie ein typischer Prüfschritt aussieht, zeigt Abbildung 1 auf der Folgeseite.

Michael Pongratz, CISA, BSG Unternehmensberatung, St. Gallen

Control Objective aus COBIT	Massnahmen aus dem IT-Grundschutzhandbuch des deutschen BSI
DS 5.1 Manage Security Measures	M 2.91
DS 5.2 Identification, Authentication and Access	M 4.53
DS 5.7 Security Surveillance	M 2.92, M 4.54
DS 11 Manage Data	M 6.44
PO 1 Define a Strategic IT Plan	M 2.93

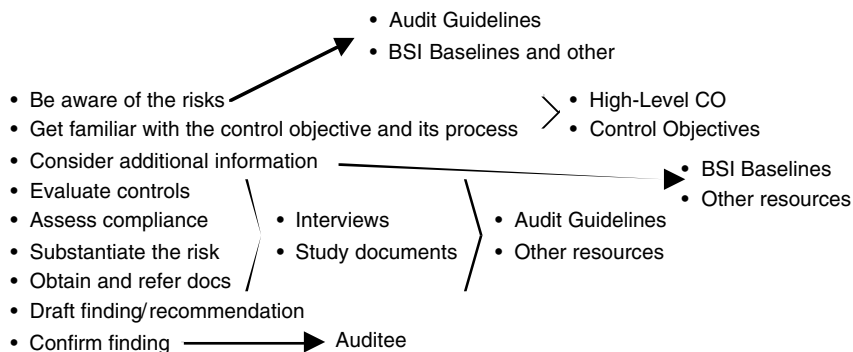


Abbildung 1: Prüfschritt mit COBIT und Komplementär-Ressourcen

Literaturverzeichnis:

■ [1] Pongratz, Michael: Der Einsatz des Rahmenwerkes COBIT in der Informatik-Revision zur Überwachung der Informationssicherheit, in: Bauknecht, Kurt/Büllesbach, Alfred et al. (Hrsg.): Sicherheit in Informationssystemen – Proceedings der Fachtagung SIS '98, Universität Hohenheim, Stuttgart, Zürich: vdf Hochschulverlag, 1998

■ [2] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 1998 – Massnahmenempfehlungen für den mittleren Schutzbedarf, Bonn, 1997 (www.bsi.de)

■ [3] Baer, Rudolf et al.: Informatik-Sicherheit – Praktische Tips, 4. stark erweiterte Sammlung von Tips und Tricks, Publikation der BSG Unternehmensberatung St. Gallen, Band 6, St. Gallen: Fachpresse Goldach, 1998 (www.bsg.ch)

Erfahrungen mit COBIT

Konzernweite Implementierung von COBIT Framework

COBIT Case Study: ein Erfahrungsbericht bei der Rentenanstalt/Swiss Life Gruppe

Hintergrund

Die Rentenanstalt/Swiss Life Gruppe ist als grösste Lebensversicherung der Schweiz zugleich die grösste privatwirtschaftliche Liegenschafteneigentümerin und -verwalterin. Mit über 300 000 Aktionären ist sie auch die grösste Publikumsgesellschaft. Markante Akquisitionen im In- und Aus-

land brachten der Rentenanstalt/Swiss Life Gruppe neue bzw. vertiefte Kernkompetenzen im Private Banking und Asset Management. Die Gruppe beschäftigt momentan über 11 000 Mitarbeitende hauptsächlich im europäischen Raum; davon 1300 in der Informatik (IT Information Technology). Gemeinsam mit über 50 Partnern in 44 Ländern bietet das Swiss Life Netz-

werk Produkte und Dienstleistungen im Bereich internationaler Personalvorsorge, welche auf die Anforderungen multinationaler Kundschaft abgestimmt sind.

Mit der Inkraftsetzung der Corporate Direction for IT Security im Jahre 1998 wurde das COBIT Framework (Governance, Control and Audit for Information and related Technology) als Standard erklärt. Die Anwendung der "Best practices" hat im In- und Ausland durch das Konzernrevisorat und zwangsläufig auch in Zusammenarbeit mit der Revisionsstelle, PricewaterhouseCoopers (PwC), bereits im Jahre 1996 begonnen. Mit dem Beschluss der Konzernleitung wurden die darauf auszurichtende Erstellung eines lokalen IT Security Handbook sowie eines Security Vademecum für alle Mitarbeitenden gefordert, welche in der Zwischenzeit im Konzernbereich Rentenanstalt/Swiss Life Schweiz ebenfalls in Kraft gesetzt wurden.

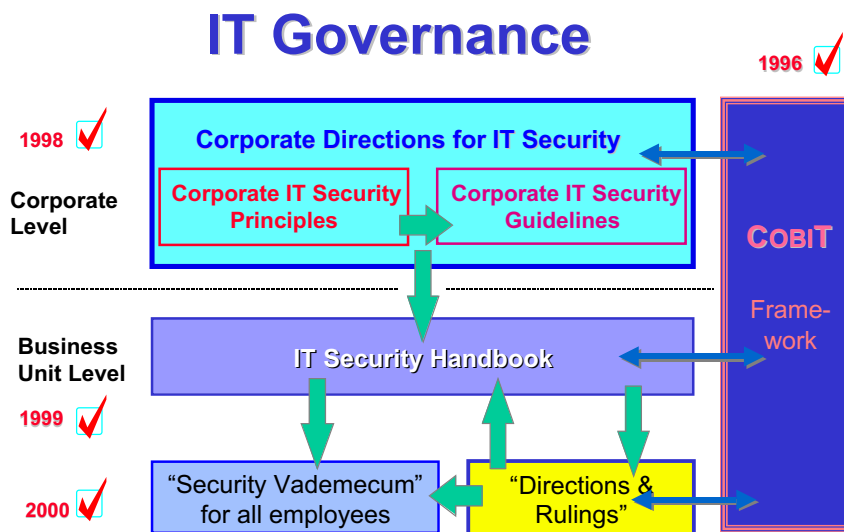
Anwendung

Folgende Entscheidungskriterien gaben für den gruppenweiten Einsatz von COBIT den Ausschlag:

■ *Generell anwendbarer* und von rund 30 im Informatik-, Sicherheits- und Prüfungsumfeld bekannten Instituten akzeptierter Standard

■ *Verstärkte* in strategischer und operativer Hinsicht ausgerichtete Geschäftsanforderungen wie Effektivität und Effizienz (Qualität/Kosten), Vertraulichkeit, Integrität und Verfügbarkeit (Sicherheit), Zuverlässigkeit und Einhaltung rechtlicher Erfordernisse (Ordnungsmässigkeit)

■ *Gemeinsame Nutzung und Verständlichkeit* der COBIT-Kontrollziele



COBIT Framework als Standard der Rentenanstalt/Swiss Life Gruppe

als Baseline für Management, Benutzer, Informatik und Revision (auch mehrsprachig verfügbar)

■ *Garantierte Weiterentwicklung* und Anpassung von COBIT an neue Technologien basierend auf Wissen und Erfahrungen der seit 31 Jahren bestehenden ISACA mit weltweit über 21 000 Mitgliedern, davon rund 300 in der Schweiz.

Mit der Inkraftsetzung wird COBIT nicht nur von der Konzernrevision und der Revisionsstelle bei ex-post und ex-ante Prüfungen im In- und Ausland angewendet, sondern auch bereits bei verschiedensten Aufgaben in Informatik- und Fachbereichen berücksichtigt.

Schlussfolgerungen

Die wesentlichen Vorteile des COBIT-Rahmenwerkes bestehen darin, dass die Implementierung je nach Grösse der Business Unit und auch schrittweise je nach geplanten Vorhaben erfolgen kann:

■ Bei *bestehenden Systemen* (Infrastruktur und Applikationen) können aufgrund der COBIT-Risikoeinschätzung die Kontrollen und Massnahmen den allgemein gültigen Standard "Best practices" angepasst werden.

■ Bei *neuen Systemen* können aufgrund der COBIT-Kontrollziele unter Berücksichtigung der betroffenen IT Ressourcen und Informations-Kriterien die Kontrollen und Massnahmen von Anfang an effizient gestaltet sowie aufeinander abgestimmt werden.

Positive Erfahrungen haben sich beim Einsatz von COBIT sowohl in der Zusammenarbeit zwischen Informatik und Revision, als auch zwischen Informatik und Benutzer gezeigt. Als ausgezeichnetes Kontroll- und Prüfungsinstrument kann COBIT im Zusammenhang mit den in der Rentenanstalt/Swiss Life eingesetzten Modellen für IT Service Management (ITIL = IT Infrastructure Library) und für IT Development (CMM = Capability Maturity Model) genannt werden.

Seit 1998 fanden sieben Tagungen der Interessengruppe COBIT des ISACA Switzerland Chapters statt. Dabei

konnten vermehrt wertvolles Wissen, praktische Erfahrungen in der Anwendung und COBIT-basierende Hilfsmittel, wie Präsentationen, Checklisten etc. ausgetauscht werden. Nebst der ISACA-Homepage www.isaca.org stehen seit dem 1.1.2000 die COBIT-Kontrollziele unter www.isaca.ch auch in deutsch zur Verfügung.

Zukunft und weiteres Vorgehen

In der Informatik-Revisionsplanung 2000 sind konzernweit *Risikoanalysen* im Sinne eines moderierten Self-Assessment durch die Revision vorgesehen. Ziel ist es, die Risiken in allen Business Units der Rentenanstalt/Swiss Life Gruppe für zukünftige Audits zu erkennen und Prioritäten für das weitere Vorgehen der COBIT-Implementierung zu bestimmen.

Um die Beherrschbarkeit der Informatik (IT Governance) zu erreichen, sind weitere Implementierungsschritte notwendig. Diese umfassen einerseits ein top-down *Awareness-Programm* zur Sensibilisierung, Unterstützung und Förderung der Lernprozesse, um die Zusammenhänge hinsichtlich gesetzlicher, finanzieller, sicherheits- und kontrollspezifischer Anforderungen zu kennen und zu beurteilen. Andererseits ist COBIT als konzernweiter Standard für die weitere Implementierung und den Unterhalt des *IT Security Management* (gemäss Diagramm) von besonderer Bedeutung.

Im weiteren wurde im Rahmen des neuen Reglements des Konzernrevisors ein Risiko-Tool unter Einbezug der COBIT-Prüffelder für die Revisionsplanung entwickelt. Ebenso wer-



IG-COBIT-Tagung bei der Rentenanstalt/Swiss Life im Oktober 1999 unter dem Motto: "Get the Swiss Life feeling and the COBIT understanding"

Von links nach rechts (sitzend): D. Gschwend, Swiss Re, Präsidentin CH-Chapter; J. Krebs, UBS; J-P. Brenn ATAG E&Y; M. Galli, Eidg. Finanzkontrolle; (stehend) F. Kräuchi, Bank Sarasin; N. Morgenthaler, Swiss Life; Michael Pongratz, BSG St. Gallen, (Leiter IG COBIT); B. Wiederkehr, Gastgeber, Swiss Life; C. Cavelti, PwC; B. Wildhaber, Wildhaber Consulting, Past Präsident CH-Chapter; Karl Jung, Finanzkontrolle Zürich; M. Schühle, SegalInterSettle.

den COBIT-basierende Verfahrensrichtlinien betreffend IT Audit, Operational Audit und Projektbegleitung erstellt, welche einerseits der Informatikrevision und andererseits in abgestufter Version der Fachrevision zur Verfügung gestellt werden.

In verschiedenen Projektgruppen der ISACA werden die COBIT-Grundlagen weiterentwickelt und laufend den neuen Informatik-Mitteln, -Methoden und -Verfahren angepasst. Die dritte Edition von COBIT wurde für das dritte Quartal 2000 angekündigt. Einzelne Dokumente liegen in Entwurfsform bereits vor. Diese werden einen Beitrag zur Verstärkung und Erreichung der Kontrollziele von Enterprise-, Corporate- und IT-Governance leisten, wie z.B.:

■ *Control Objectives for Enterprise Governance* enthalten high Level and detailed Business Control Objectives

for Business Activities & Enterprise Resources.

■ *Management Guidelines* mit Angaben zum Einsatz von Benchmarking anhand von Key Goal Indicators & Key Performance Indicators, welche durch kritische Erfolgsfaktoren bestimmt sind. Zusätzlich sind Bewertungsrichtlinien für das Control Risk Self Assessment vorhanden.

■ *IT Control Practices* beinhalten alle IT-Prozesse und -Prüffelder mit Fragestellungen zu den Risiken (Warum?) und zur Kontrollpraxis (Wie?).

Wenn es dem Konzernrevisorat gelingt, das Management und die Mitarbeitenden konzernweit auf den Wirkungsgrad und die konsequente Nutzung des COBIT-Framework und der neuen Inhalte zu überzeugen, können nebst Gestaltung der Sicherheit und Einhaltung der *Ordnungsmässigkeit* die Beherrschbarkeit der folgenden

Qualitätskriterien spürbar gesteigert werden:

■ *Effektivität* (Wirksamkeit) bedeutet, dass fehlerfreie und konsistente Informationen, welche für den Geschäftsprozess wichtig sind, rechtzeitig in verwendbarer Form geliefert werden.

■ *Effizienz* (Wirtschaftlichkeit) betrifft die Bereitstellung von Informationen mit einer optimalen Verwendung von Ressourcen.

Dieses kommt wiederum den Vorhaben der Rentenanstalt/Swiss Life www.swisslife.com hinsichtlich den stark wachsenden Bereichen, wie E-Business, Banking und Asset Management zu Gute. Seit April 2000 steht der Profitline Fond-Shop mit erhöhtem Sicherheitsdispositiv für den Direktvertrieb im Internet www.profitline.ch rund um die Uhr zur Verfügung.

Bruno Wiederkehr, Konzernrevisorat, Rentenanstalt/Swiss Life, Zürich

Erfahrungen mit COBIT

Mini Case Study: COBIT Application at a Private Bank in Switzerland

Background

The case concerns a private bank established under Swiss law and regulation (hereafter referred to as The Bank). The Bank belongs to an international group of financial institutions. It operates out of Switzerland, having also branches overseas with off shore subsidiaries.

The banking engine has been outsourced to a “new” host system of somewhat standardised characteristics. The outsourcing process has been closely watched and followed by both, internal as well as external IT audit. Previously, the banking engine had been an upgraded version of an old legacy system. The transition from the “old” to the “new” host had been delayed several times due to lacking functions and migration problems. The final migration was accomplished well ahead of the critical turn of the millennium, still leaving some user requests unfulfilled, though. This led to the situation that certain “old” applications (previously front end to the “old” host) were being kept and some PC solutions were built by users in order to circumvent not yet existing or altogether missing “new” host functions.

The external auditor worked in close collaboration with the internal audit department since more than ten years. A collaboration between the two IT

audit departments was therefore a “natural”.

Application

In the course of the Y2K clean-up, management decided together with internal audit to establish an inventory of all EDP systems in use (especially so-called end user systems). The external auditor was asked to provide certain expert support as well as the quality review for the project. For this purpose a questionnaire was created, already pointing in the direction of COBIT risk analysis and domains.

The stock taking of EDP systems revealed that an enormous number of end user applications was present (close to one hundred). It was then decided to proceed as follows:

- a) Discussion with the owners of the applications in order to identify the need for the systems in question. The aim was to eliminate as many redundant systems as possible for the “new” host system had been enhanced in the meantime now fulfilling many previously lacking functions.
- b) Risk analysis of the systems which could not be eliminated in step a) above.
- c) Tailoring the COBIT framework for end user purposes within the Bank’s organisation.
- d) Finding answers to the checklist questions thus established and discuss-

ing issues with system owners based on the Audit Guidelines.

- e) Reporting issues to management according to the Bank’s specific reporting rules (blank, green, amber, red).
- f) Tailoring the COBIT framework for the host application and following steps in analogous form to steps d) and e) above.

The risk analysis was predominantly based on the answers to the questions of the questionnaire. The deciding issues were:

- The time in which the user judged to be able to continue to perform her/his work without the system’s functioning.
- The impact a loss of the system would cause in primary and secondary levels (monetary terms).
- The impact a loss of the system would cause as far as image of the Bank is concerned.

The tailoring was done in several brainstorming sessions between the internal and external auditors. It resulted in the elimination of certain objectives, in rare cases even entire processes, and the domain *Monitoring* was dropped altogether for this exercise, the intention being to take this domain up at a future point in time.

Conclusion

The expectations were achieved in principle:

- Clear guidance for objectives to be reached.
- Helpful suggestions and hints for solutions.
- Added value to the organisation.

Some difficulties were encountered, such as:

- Tangible help from the Audit Guideline in specific situations often not available (or not found by the auditors...).
- Practically no specific application oriented support (all systems oriented) within the framework was identified.

Future

The Bank intends to continue to use COBIT as a general guideline on a case

by case basis, but will not follow it doggedly. The points addressed (end user computing and banking engine) during this audit will be followed up without any question according to the latest available COBIT standard within the general EDP audit plan of the Bank.

Max F. Bretscher, KPMG Fides Peat, Zürich

wendet. Dabei dienen das Prozess-Framework, die Control Objectives und die Audit Guidelines von COBIT als Baseline.

Mit COBIT's Generic Audit Guideline wurde zudem im Bereich der projektbegleitenden Revisionen eine Vereinheitlichung des Revisionsablaufs erreicht (Anmerkung des Redaktors: Siehe auch *NewsLetter Nr. 49* zum Thema Projektbegleitung).

Innerhalb IA wurde COBIT zum Referenzmodell für Informatikrevisionen definiert.

Erste Kontakte mit Vertretern des Management von CIT zur Präsentation von COBIT fanden statt.

Bedarf für Verbesserungen von COBIT sehe ich vorab bei der fehlenden Flexibilität in der praktischen Anwendung. Bei Angleichungen von COBIT an unternehmenseigene Bedürfnisse ist man auf flexibles Selektionieren und Auswerten angewiesen. Anpassungen an bestehende Strukturen soll man rasch vornehmen können. Der Browser, mit welchem COBIT ausgeliefert wird (Folio Viewer) verfügt nicht über die gewünschte Flexibilität. Die Auslieferung von COBIT in einem maschinell verwertbaren Format (z. B.: RDBMS) erbrächte die gewünschte Verbesserung.

Schlussfolgerungen

COBIT ist ein nützliches Werkzeug für die Informatikrevision. Beschränkt man sich allerdings beim Einsatz von COBIT auf die Optimierung der IT-Revisionsabläufe, wird dessen Hauptnutzen bei Weitem nicht ausgeschöpft.

Erfahrungen mit COBIT

Erfahrungen zum Einsatz von COBIT

bei Internal Audit,

Information & Technology SWISSCOM

Einführung

Die Swisscom AG ist am 1. Januar 1998 aus der früheren Telecom PTT entstanden. Das Unternehmen ist heute der grösste Anbieter im deregulierten schweizerischen Telekommunikationsmarkt. Die Swisscom beschäftigt momentan rund 20 000 Mitarbeitende, davon ca. 2500 in der unternehmenseigenen Informatik, Corporate Information & Technology (CIT).

Die Unternehmensleitung entschied sich für ein Auflösen von Internal Audit (IA) auf den 31. Dezember 1999 und für ein Teiloutsourcing an eine externe Revisionsstelle. Meine Aus-

führungen beziehen sich somit auf die Zeit bis Ende Oktober 1999.

Anwendung

COBIT wurde bei Internal Audit Information Technology (IA-IT) beschafft, weil es sich als umfassendes Werkzeug zur Unterstützung und Standardisierung von Informatikrevisionen präsentierte. Für eine Beschaffung von COBIT sprach weiter die fachlich breite und internationale Abstützung durch den internationalen Fachverband der Informatikrevisoren, ISACA. COBIT besitzt zudem den Vorzug, dass es kostengünstig ist. COBIT wurde versuchsweise beim Erstellen von Prüfprogrammen ange-

Die Stärke von COBIT liegt in der Informatik-Führungsunterstützung. Diese wird erreicht durch Strukturieren der gesamten Informatik-Funktion in überschaubare Prozesse sowie Zuordnen von über 300 vordefinierten Prüf- bzw. Steuerungs-Zielen (Control Objectives).

Die IT-Prozesse von COBIT befinden sich auf einem relativ hohen Abstraktionsniveau. Sie sind durchgängig definiert und von konstanter Granularität. Sämtliche in einem Unternehmen vorkommende IT-Prozesse finden im COBIT Framework Platz. Sie sind so ausgereift, dass, anders als üblicherweise bei ISO 9000 ff Zertifizierungen, die Prozesse gültig bleiben, auch wenn Abläufe innerhalb der Informatik-Funktion ändern (beispielsweise durch Teiloutsourcing, Wechsel von Make zu Buy, Umstellung der Projektmanagement Methode, o.ä.).

Mit den COBIT Control Objectives werden die Zielsetzungen in Bezug auf Sicherheit, Ordnungsmässigkeit, Effizienz und Wirtschaftlichkeit in der unternehmensweiten Informatik festgelegt. Sie sind die Messlatte (Soll) für das IT-Management, mit welcher der Erfüllungsgrad in der Informatik (Ist) kontrolliert wird, sei es durch die Revision (intern oder extern) oder durch die Informatik selber (Self Assessment).

Ein auf Anhieb trivial wirkender, jedoch nicht zu unterschätzender Nutzen liegt darin, dass durch die Durchgängigkeit und Nachhaltigkeit des COBIT-Modells für IT-Spezialisten und Nicht-IT-Professionals auf allen Führungsstufen eines Unternehmens die Chance besteht, ein unternehmensweit einheit-

liches Informatik-Vokabular einzusetzen.

Weiteres Vorgehen/ Zukunft (Mögliche weitere Einsatzgebiete)

Das Thema heisst Beherrschbarkeit der Informatik (IT-Governance). COBIT hilft wirksam und nachhaltig, die Informatik zu beherrschen. Dabei unterstützt COBIT den Einsatz anderer wirksamer Methoden und Verfahren (z.B.: Controlling, Grundschatz des BSI, BS7799, ISO 12207, ISO 15504 u.a.). Mit der Mitte 2000 erscheinenden 3rd Edition von COBIT wird der Einsatz von Kennzahlen (Key Performance Indicators) sowie kritischen Erfolgsfaktoren (Critical Success Factors) ermöglicht. Dies wiederum hilft mit, eine Grundlage für Balanced Score Card Systeme zu schaffen.

Die IT-Manager können Wirkungsgrad und Nutzen ihrer Informatik spürbar steigern, wenn sie COBIT zur Führungsunterstützung einsetzen. Dabei gehört es zu den Aufgaben der Informatik-Prüfer, die Führungskräfte der Informatik auf den Nutzen und optimalen Einsatz von COBIT aufmerksam zu machen und sie bei dessen Einsatz zu unterstützen.

Fritz Kräuchi, Bank Sarasin, Basel