

## Entwicklung eines integrierten IT Compliance Frameworks

### DER NUTZEN FÜR DEN KUNDEN

«Mit weniger als 40 CobiT-basierten Kontrollzielen erreichen wir die Compliance sowohl mit dem Sarbanes-Oxley Act (SOX) als auch mit den Pharma GxP-Richtlinien.

Wir reduzieren damit unsere Compliance-Kosten.

Zudem können wir das Framework flexibel an zukünftige Veränderungen anpassen.»

Dr. Thomas Gigerl  
Senior IT Quality Manager  
Global Information Security  
Officer  
Information Security & IT  
Validation / Quality  
ALTANA Pharma AG\*

\* ALTANA wurde im 2007  
durch Nycomed erworben.

### DER KUNDE

Das IT-Hauptquartier der ALTANA Pharma hatte folgende Aufgaben

- Architektur, Compliance, Security und Service-Management
- Verwaltung der über 300 Geschäftsanwendungen in einem Application Portfolio Management System (APMS), z.B. zur Erstellung der Validierungsmasterpläne (VMP)

### DER HINTERGRUND

ALTANA Pharma begann mit der Dokumentation und Einführung eines SOX-konformen IT-Kontrollsystems. Dabei gab es eine Reihe von Unstimmigkeiten: Die QA- und IT-Mitarbeiter waren bereits mit den vorhandenen Kontrollsystemen so stark ausgelastet, dass die Einführung der SOX-Kontrollen auf Widerstand stieß. Als man die Wirtschaftsprüfungsgesellschaft wechselte, gab es zudem erhöhten Diskussionsbedarf, um das vorhandene Kontrollsystem zu rechtfertigen.

ALTANA Pharma beschloss deshalb, ein integriertes IT Compliance Framework zu entwickeln, das alle relevanten Regulatorien und Best-Practice Ansätze auf einem Minimumniveau umfasst. Das Framework sollte auf einer begründeten und nachvollziehbaren Ableitung der IT-Kontrollen aus den relevanten Gesetzen basieren, um dessen Wiederverwendbarkeit und Erweiterbarkeit zu garantieren.

### DIE ZIELE

- Senkung der Compliance-Kosten insgesamt
- Verringerung der Belastung für die Mitarbeiter und der redundanten Tätigkeiten
- Eine begründete und nachvollziehbare Ableitung der IT-Kontrollen basierend auf den relevanten Gesetzen
- Unabhängigkeit von einzelnen Revisoren
- Durch das IT-Kontrollsystem sowohl Compliance als auch Qualität und Effizienz der IT-Prozesse (Best Practice) sicherstellen

### DAS PROJEKT

Zusammen mit Arcondis entwickelte ALTANA Pharma ein integriertes IT Compliance Framework auf der Basis von CobiT. Dieses umfasst alle relevanten Regulatorien (SOX, GxP), das abgeleitete Minimum-Set von Kontrollen und die daran angebundene Best-Practice Methoden (z.B. ITIL, GAMP, PMI).

Ein Meilenstein war ein mehrstufiges Mapping von Regularien und Best-Practice Ansätzen auf CobiT. Das Ergebnis war ein Set von 35 CobiT-Kontrollzielen mit etwas über 60 Kontrollaktivitäten, das sowohl den Anforderungen von SOX als auch von GxP vollständig gerecht wird. Nur 6 sehr spezifische GxP-Paragrafen des 21 CFR Part 11 musste man über spezifische Kontrollaktivitäten abdecken.

## ARCONDIS - EIN VERLÄSSLICHER PARTNER

Wir strukturieren unser Know-how nach dem Lebenszyklus eines technischen beziehungsweise organisatorischen Systems.

Zuerst werden im Rahmen der Beratung aus Verbesserung- oder Problemlösungsideen unserer Kunden grundsätzliche Lösungskonzepte (Blue Prints) entwickelt.

Wird über die Umsetzung eines Lösungskonzeptes positiv entschieden, sorgen wir mit professionellem Projektmanagement und Unterstützung in der Systementwicklung für dessen Umsetzung.

Da wir unseren Kunden nach Bedarf auch bei der erfolgreichen Umsetzung beziehungsweise Einführung in die Organisation zur Seite stehen, nehmen wir auch Aufgaben im operativen Management wahr.

### Arcondis AG

Christoph Merian-Ring 31A  
CH-4153 Reinach  
Schweiz  
T: +41 61 717 82 00  
F: +41 61 717 82 01

### Arcondis GmbH

Mergenthalerallee 79 - 81  
D-65760 Eschborn  
Deutschland  
T: +49 6196 76 9998 0  
F: +49 6196 76 9998 10

E: [info@arcondis.com](mailto:info@arcondis.com)

[www.arcondis.com](http://www.arcondis.com)

## PROJEKTSTECKBRIEF

Das Gesamtprojekt mit den folgenden Phasen

- Risiko-Assessment zur Ableitung der SOX-Anforderungen auf CobiT basierten Control Objectives und Mapping der SOX- und GxP-Anforderungen auf CobiT Detailed Control Objectives (DCO)
- Ableitung eines auf CobiT ausgerichteten Prozessmodells basierend auf COSO
- Zuordnung des DCO-Set auf vorhandene Guidelines und SOPs (Best Practices)
- Entwicklung und Durchsetzung einer IT-Compliance Policy und Abgleich der

## ERGEBNISSE

Risiko-Matrix für SOX-relevante CobiT-Kontrollziele

Liste von CobiT-Kontrollzielen, die Compliance mit allen relevanten Regularien sicherstellen (SOX und GxP)

Liste von SOX-relevanten Anwendungen und Systemen

Dokumentation der Kontroll-Prozesse

IT Compliance Policy und Guidelines

Zuordnung des Control-Set auf gültige Guidelines und SOPs

## Über Arcondis

Die Arcondis Gruppe ist ein Beratungs-Unternehmen für die Life Science Branche und bietet hochwertige und anwendungsorientierte Dienstleistungen für IT-, Qualitäts- und Informationsmanagement an.

Arcondis steht für *Art of Consulting and Development for Information Systems* und ist ein Sinnbild für die Kunst, die wichtigsten Erfolgsfaktoren von Kundenlösungen zu optimieren und Kundensysteme effizient miteinander zu verknüpfen.

Die Erfolgsfaktoren sind primär die involvierten Menschen, die verwendeten Organisationsmethoden und die technologische Basis.

Detailed Control Objectives mit der Wirtschaftsprüfung

- Entwicklung der Guidelines und SOPs für das interne Kontrollsystem
- Entwicklung der Control Practices und Integration in das Organisationsmodell der ALTANA Pharma
- Evaluation eines Compliance-Tools mit Hilfe eines selbst entwickelten Prototypen
- Aufsetzen einer Rollout-Planung

beanspruchte einen Aufwand von total 18 Mannmonaten.

## NUTZEN

Begründbarkeit der SOX IT-Kontrollen, Unabhängigkeit von Wirtschaftsprüfern

Eliminierung redundanter Kontrollen, Verringerung des Aufwands und der Kosten für die Compliance

Optimale Eingrenzung des regulatorischen Anwendungsbereiches, um die Kontrollaufwände auf das notwendige Mass zu beschränken

Interne und externe Revisions-Fähigkeit

Definition der organisatorischen Abläufe zur kontinuierlichen Pflege des IT Compliance Frameworks, um nachhaltig internen und externen Veränderungen gerecht zu werden

Hilfestellung für die praktische Umsetzung und somit Einhaltung der Kontrollen für das Hauptquartier und die Tochterfirmen