

## Fachgutachten

der **Fachsenate für Datenverarbeitung** und **für Handelsrecht und Revision** des Instituts für Betriebswirtschaftslehre, Steuerrecht und Organisation der **Kammer der Wirtschaftstreuhänder** über

# Abschlussprüfung bei Einsatz von Informationstechnik

*(verabschiedet in den Sitzungen des Fachsenats für Datenverarbeitung vom 22. Juni 2004 und des Fachsenats für Handelsrecht und Revision vom 20. Oktober 2004)*

## Inhaltsübersicht

## Seite

A. Vorbemerkungen .....	2
A.1. Anwendungsbereiche des Fachgutachtens .....	2
A.2. Einbindung in die Abschlussprüfung .....	2
B. Ziel und Umfang der Prüfung der Informationstechnik .....	3
C. Tätigkeiten des Abschlussprüfers bei der Prüfung der Informationstechnik .....	5
C.1. Berücksichtigung der Prüfung der Informationstechnik bei der Prüfungsplanung .....	5
C.2. Gewinnung eines Überblicks über die Informationstechnik des geprüften Unternehmens .....	6
C.3. Feststellung der wesentlichen aus dem Einsatz und der Anwendung der Informationstechnik resultierenden Risiken .....	7
C.4. Feststellung der Maßnahmen des geprüften Unternehmens zur Beseitigung oder Verminderung der Risiken .....	8
C.5. Prüfungshandlungen des Abschlussprüfers im Einzelnen .....	9
C.6. Dokumentation der Prüfungshandlungen und Berichterstattung über die Prüfungsfeststellungen .....	11
D. Vorgangsweise bei Auslagerungen im Bereich der Informationstechnik an ein anderes Unternehmen (IT - Outsourcing) .....	12
Beilage	
Das CobiT-Prozessmodell .....	14

## **A. Vorbemerkungen**

### **A.1. Anwendungsbereich des Fachgutachtens**

In diesem Fachgutachten wird die Berufsauffassung dargelegt, die Abschlussprüfer – unbeschadet ihrer Eigenverantwortung – bei der Prüfung der Informationstechnik (IT) im Rahmen von Abschlussprüfungen beachten sollen. Aufgrund der großen Bedeutung der Informationstechnik in zahlreichen, insbesondere in rechnungslegungsrelevanten Unternehmensbereichen, ist deren Prüfung ein wichtiger Bestandteil der Abschlussprüfungen.

Eine Risikoeinschätzung, von der Art und Umfang der weiteren informationstechnik-bezogenen Prüfungshandlungen abhängen, stellt den ersten und immer notwendigen Prüfungsschritt dar. In vielen Fällen werden keine weiteren diesbezüglichen Prüfungshandlungen erforderlich sein; wenn sich im Einzelfall weitere Prüfungshandlungen auf diesem Gebiet als erforderlich erweisen, sind die Ausführungen in den Abschnitten B und C über deren Art und Umfang zu beachten.

Das Fachgutachten bezieht sich insbesondere auf Prüfungen von Einzel- und Konzernabschlüssen; es gilt jedoch auch für sonstige Prüfungen sinngemäß.

### **A.2. Einbindung in die Abschlussprüfung**

Die Prüfung der Informationstechnik ist ein Teilbereich der Prüfung des internen Kontrollsystems und damit ein integrierender Bestandteil einer Abschlussprüfung, bei deren Durchführung nach dem derzeitigen Stand der Erörterung der Grundsätze ordnungsgemäßer Abschlussprüfung die internationalen Prüfungsstandards (International Standards of Auditing = ISA) zu beachten sind. Die Prüfung der Informationstechnik liefert auch einen wichtigen Beitrag zu dem in ISA 315 geforderten Verständnis des zu prüfenden Unternehmens.

Die für die Prüfung der Informationstechnik wichtigen Aspekte sind insbesondere in den folgenden ISA enthalten:

ISA 200	Objective and General Principles Governing an Audit of Financial Statements
ISA 315	Understanding the Entity and its Environment and Assessing Risks of Material Misstatement <sup>1)</sup>
ISA 330	The Auditor' s Procedures in Response to Assessed Risks <sup>1</sup>
ISA 402	Audit Considerations relating to Entities using Service Organisations
ISA 500	Audit Evidence (in Überarbeitung)

Die derzeit gültigen ISA 310 (Knowledge of the Business), 400 (Risk Assessments and Internal Control) und 401 (Auditing in a Computer Information Systems Environment) werden für Prüfungen von Geschäftsjahren, die nach dem 15. Dezember 2004 beginnen durch die ISA 315 und 330 abgelöst.

## **B. Ziel und Umfang der Prüfung der Informationstechnik**

Das Ziel der Prüfung des Informationstechnik-Systems eines Unternehmens besteht hauptsächlich in der Beurteilung der Verlässlichkeit der mit Hilfe von programmgesteuerten Verarbeitungen ermittelten und im Rechnungswesen sowie im Rechnungsabschluss verwendeten Daten.

Ein weiteres Ziel der Prüfung der Informationstechnik besteht in der Feststellung, ob aufgrund der mit dem Einsatz dieser Technik verbundenen Risiken (vgl Abschnitt C3) eine Gefährdung des Fortbestands oder der Entwicklung des geprüften Unternehmens erkennbar ist und aufgrund dieses Umstands die Annahme der Fortführung des Unternehmens bei der Bewertung zulässig ist oder der Abschlussprüfer seine Redepflicht gemäß § 273 (2) HGB auszuüben hat.

Art und Umfang der Prüfung des Informationstechnik-Systems kann nicht allgemein gültig definiert werden; im Einzelfall hängt dessen Prüfung insbesondere von folgenden Umständen ab:

<sup>1)</sup> Für Prüfungen von Geschäftsjahren, die nach dem 15. Dezember 2004 beginnen

**KFS  
DV2**

- Größe, Art und Komplexität des Leistungsprogramms des geprüften Unternehmens
- Art und Komplexität der eingesetzten Informationstechnik-Systeme
- Art und Umfang der Integration von unternehmensweiten Anwendungen
- Vorliegen von automatisch generierten Transaktionen, Vernetzungen mit Kunden, Lieferanten oder anderen Dritten
- Maßnahmen des geprüften Unternehmens zur Beseitigung oder Verminderung von Fehlerrisiken
- bei vorangegangenen Prüfungen gewonnene Erkenntnisse.

Im Sinn der neuen Audit Risk Standards ISA 315 und 330 ist die Prüfung der Informationstechnik wichtig

- bei der Gewinnung des Verständnisses über das Unternehmen und die Unternehmensrisiken
- bei der Beurteilung des Risikos von wesentlichen Fehlern im Rechnungsabschluss und
- bei der Planung der Prüfungshandlungen zur Abdeckung der festgestellten Fehlerrisiken.

Der Umfang der Prüfung des Informationstechnik-Systems ist bei den jeweiligen Prüfungen von der Risikoeinschätzung durch den Abschlussprüfer abhängig.

Über die in Abschnitt A1 geforderten Prüfungshandlungen zur Feststellung allfälliger den Bestand und die Entwicklung des geprüften Unternehmens gefährdender Risiken hinausgehende Prüfungshandlungen bezüglich der Informationstechnik können in der Regel unterbleiben, wenn

- keine prüfungsrelevanten automatisierten Kontrollen bestehen oder
- wegen begründeter Zweifel an der Verlässlichkeit der automatisierten Kontrollen oder aufgrund anderer prüfungsstrategischer Überlegungen ein Prüfungsansatz gewählt wird, der einem hohen Kontrollrisiko Rechnung trägt oder
- auch ohne die Prüfung von automatisierten Kontrollen ausreichende Prüfungssicherheit gewonnen werden kann.

Bei Unternehmen, bei denen die Funktionsfähigkeit der Informationstechnik laufend durch das interne Kontrollsystem überwacht wird oder wesentliche Teile des internen Kontrollsystems in der Informationstechnik realisiert sind, ist die Prüfung dieses Bereichs des Kontrollsystems durch den Abschlussprüfer für die Identifikation von Kontrollrisiken von erhöhter Bedeutung.

Für Art und Umfang der Prüfung des Informationstechnik-Systems ist ferner von Bedeutung, ob der Abschlussprüfer sich dieses Systems zur Unter-

stützung seiner eigenen Prüfungshandlungen bedient (zB durch die Verwendung von CAATs = Computer Assisted Audit Techniques), um auf diese Weise eine erhöhte Prüfungssicherheit oder eine effizientere Prüfungsdurchführung zu erreichen; in diesem Fall ist die Verlässlichkeit und Richtigkeit der zugrunde liegenden Daten besonders wichtig.

Im Rahmen der Abschlussprüfung ist auch die Ordnungsmäßigkeit der Buchführung zu prüfen. Diese Prüfung erstreckt sich bei Verwendung der Informationstechnik im Rechnungswesen auf die Beachtung der im Fachgutachten KFS/DV1 des Fachsenats für Datenverarbeitung (Die Ordnungsmäßigkeit von EDV-Buchführungen) enthaltenen Regeln.

## **C. Tätigkeiten des Abschlussprüfers bei der Prüfung der Informationstechnik**

Die Prüfung der Informationstechnik umfasst die nachstehenden Tätigkeiten des Abschlussprüfers:

- Berücksichtigung der Prüfung der Informationstechnik bei der Prüfungsplanung
- Gewinnung eines Überblicks über die Informationstechnik des geprüften Unternehmens
- Feststellung der wesentlichen aus dem Einsatz und der Anwendung der Informationstechnik resultierenden Risiken
- Feststellung der Maßnahmen des Unternehmens zur Beseitigung oder Verminderung dieser Risiken
- Prüfungshandlungen des Abschlussprüfers im Einzelnen
- Dokumentation der Prüfungshandlungen und Berichterstattung über die Prüfungsfeststellungen

### **C.1. Berücksichtigung der Prüfung der Informationstechnik bei der Prüfungsplanung**

Die Planung umfasst die zeitliche, sachliche und personelle Planung. Die zeitliche und sachliche Planung ist im Zuge der Prüfungsdurchführung zu berichtigen, wenn sich dabei geänderte Feststellungen über die aus dem Einsatz der Informationstechnik resultierenden Risiken und über die Maßnahmen des geprüften Unternehmens zur Beseitigung oder Verminderung dieser Risiken ergeben.

Bei der personellen Planung ist darauf zu achten, dass für die Prüfung der Informationstechnik entsprechend ausgebildete und erfahrene Mitarbeiter eingesetzt oder geeignete externe Sachverständige herangezogen werden.

## **C.2. Gewinnung eines Überblicks über die Informationstechnik des geprüften Unternehmens**

Zur Gewinnung eines Überblicks über die Informationstechnik des geprüften Unternehmens können Informationen über folgende Bereiche sinnvoll sein:

### **Organisation und IT-Prozesse**

- Organigramme und Stellenbeschreibungen
- Einbindung der Informationstechnik in die unternehmensweite Führungs- und Überwachungsstruktur (IT-Governance-Struktur)
- Strategie der Informationstechnik
- Beschreibung der für das Unternehmen wesentlichen IT-Prozesse (zB der Maßnahmen zur Gewährleistung der Datensicherheit)
- Prüfungen der Informationstechnik durch die interne Revision und durch externe Dienstleister
- Auslagerung von Bereichen der Informationstechnik

### **Geräte, Programme und Anwendungen**

- Feststellung der verwendeten Geräte (Großrechner, Client-Server-Systeme, PC und PC-Netzwerke) und Betriebssysteme und der Netzwerkstruktur (Local Area Network, Wide Area Network, Internet, Intranet, Extranet)
- Bezeichnung und Type der Software (Individual, Standard, modifizierter Standard) und deren Hersteller und Versionen sowie deren Aufgabengebiet und die zugrunde liegende Hardware-Plattform
- Verwendete Programmiersprachen und Methode der Datenhaltung (Datenbank- oder Dateioorganisation)
- Wichtige Schnittstellen und Datenflüsse
- Feststellung der Unternehmensabläufe und Geschäftsprozesse, bei denen Infrastruktur und Anwendungen der Informationstechnik eingesetzt werden, und Beschreibung der für die Rechnungslegung wesentlichen Prozesse
- Inhalt der Dokumentationen für Anwender, allenfalls auch Schulungsunterlagen

### **C.3. Feststellung der wesentlichen aus dem Einsatz und der Anwendung der Informationstechnik resultierenden Risiken**

#### **a) Anwendungsunabhängige Risiken**

Aus dem Einsatz der Informationstechnik ergeben sich für die Unternehmen insbesondere folgende Risikofaktoren<sup>2)</sup>:

##### ***Abhängigkeit von der Informationstechnik***

*Die Abhängigkeit der Unternehmen von der Infrastruktur und den Anwendungen der Informationstechnik ist insbesondere bei Vernetzung mit anderen Geschäftspartnern und Behörden sehr hoch. Aufgrund des Automatisierungsgrads und der Komplexität der relevanten Systeme, die häufig ganze Prozessketten unterstützen, sind die Unternehmen in hohem Maße auf die Funktionsfähigkeit und dauernde Betriebsbereitschaft der Systeme und das Fachwissen von Spezialisten angewiesen. Sensible Daten, die für den Geschäftserfolg ausschlaggebend sein können und vielfach auch einen hohen Wert haben, werden vielfach nur in Systemen vorgehalten.*

##### ***Änderungen***

*Größere Änderungen im Bereich der Informationstechnik können sich aufgrund der Einführung neuer Systeme und Technologien oder aufgrund von Restrukturierungen ergeben. Fehlgelaufene Projekte können wesentliche Kosten- und Terminüberschreitungen und Mängel im Verfahrensablauf verursachen. Auch bei der Einführung von Standardsoftware können sich Probleme ergeben, da die Programme häufig an die Anforderungen des Unternehmens angepasst werden müssen (Customizing) und dabei Fehler entstehen können. Größere Änderungen im Bereich der Informationstechnik werden häufig durch Änderungen in der Ablauforganisation (zB Einführung eines durch Informationstechnik gestützten Beschaffungswesens) und Änderungen von Produktionsverfahren verursacht. Die Auswirkungen solcher Änderungen auf die Informationstechnik sind häufig nicht genau vorhersehbar; sie stellen hohe Anforderungen an die Anwender, die den Änderungen mitunter ablehnend gegenüberstehen.*

##### ***Know-how und Ressourcen***

*Wesentlich für einen erfolgreichen Betrieb der Informationstechnik ist das Vorhandensein von Mitarbeitern mit aktuellem und spezifischem Fachwissen. Dies gilt nicht nur für die Spezialisten in den Informationstechnikabteilungen, sondern auch für die Anwender wichtiger Systeme. Die Konzentra-*

<sup>2)</sup> Die anschließenden Ausführungen über die Risiken wurden mit geringeren Modifikationen dem Prüfungsstandard 330 des deutschen Institutes der Wirtschaftsprüfer entnommen

tion des Fachwissens bei einer Person bedeutet erhöhte Abhängigkeit, die nur durch Kommunikation des Fachwissens an mehrere Personen und insbesondere durch eine gute Dokumentation vermindert werden kann. Auch Überlastungen, sowohl im Bereich der Informationstechnik als auch im Anwenderbereich können zur Risikoerhöhung beitragen, wenn dies zu einer Beeinträchtigung der Verlässlichkeit des Systems durch unzureichende Pflege und durch Fehlbedienungen führt.

### **Geschäftliche Ausrichtung**

Wesentlich für die Risikobegrenzung ist die Ausrichtung der Informationstechnik auf die Geschäftsstrategie und die Prozessanforderungen des Unternehmens. Den Geschäftsstrategien muss eine adäquate Strategie für die Informationstechnik entsprechen; diese muss mittel- bis langfristig ausgerichtet, dokumentiert und von der Unternehmensleitung genehmigt sein und konkrete Maßnahmen enthalten. Die geschäftlichen Erfordernisse und die Anwenderbedürfnisse müssen (zB über Fachkonzepte und Pflichtenhefte) klar definiert sein und durch die Funktionalitäten und Prozesse der Informationstechnik weitgehend abgedeckt werden. Auch rechtliche Rahmenbedingungen außerhalb des Handelsrechts (zB Anforderungen des Steuerrechts, des Arbeitsrechts, des Umweltrechts, des Datenschutzes, des Aufsichtsrechts und branchenbezogene Vorschriften) müssen beachtet werden.

Aus der unternehmensspezifischen Ausprägung dieser Risikofaktoren ergeben sich die Risiken für die Organisation, die Infrastruktur und die Prozesse der Informationstechnik des geprüften Unternehmens. Die wesentlichen Risiken und deren Bedeutung für den Geschäftsbetrieb und den Rechnungsabschluss sind zu ermitteln und zu dokumentieren.

### **b) Anwendungsabhängige Risiken**

Weitere Risiken in Bezug auf die Richtigkeit von Daten ergeben sich aus der Anwendung der Informationstechnik.

### **C.4. Feststellung der Maßnahmen des geprüften Unternehmens zur Beseitigung oder Verminderung der Risiken**

Die Unternehmen haben durch geeignete Kontrollen dafür zu sorgen, dass die Risiken, die sich aufgrund des Einsatzes und der Anwendung von Informationstechnik ergeben, nicht zu Fehlern führen.

Die Kontrollen der Unternehmen beziehen sich sowohl auf Risiken, die den einzelnen Informationstechnik-Prozessen zuzuordnen sind (anwendungsunabhängige Kontrollen), als auch auf Risiken, die sich aus den mittels Informationstechnik automatisierten Geschäftsprozessen ergeben (anwendungsabhängige Kontrollen).

Im Zuge der Prüfung des Informationstechnik-Systems ist festzustellen, ob bzw. in welcher Weise das Unternehmen Maßnahmen zur Beseitigung oder Verminderung der für die Richtigkeit des geprüften Jahresabschlusses wesentlichen Risiken getroffen hat.

#### **a) Anwendungsunabhängige Kontrollen der Informationstechnik-Prozesse**

Die wesentlichen Informationstechnik-Prozesse sind sehr häufig unternehmensspezifisch gestaltet.

Das in einer Beilage zum Fachgutachten angeführte CobiT-Prozessmodell bietet einen Überblick über die Informationstechnik-Prozesse und über die Kontrollziele für die einzelnen Prozesse. Die Ausführungen zu den Kontrollzielen sowie diesbezügliche „Audit Guidelines“ können dem Abschlussprüfer Anregungen für konkrete Prüfungshandlungen geben.

#### **b) Anwendungsabhängige Kontrollen der Geschäftsprozesse**

Den Risiken von Fehlern aus den Geschäftsprozessen und den sonstigen rechnungslegungsrelevanten Fehlerrisiken kann durch Maßnahmen begegnet werden, die entweder automatisiert ablaufen (anwendungsabhängige Kontrollen) oder ohne Programmunterstützung durchgeführt werden (sogenannte manuelle Kontrollen). Die manuellen Kontrollen sind nicht Gegenstand dieses Fachgutachtens.

### **C.5. Prüfungshandlungen des Abschlussprüfers im Einzelnen**

Für den Abschlussprüfer ist die Prüfung sowohl von anwendungsunabhängigen als auch von anwendungsabhängigen Kontrollen von Bedeutung.

#### **a) Prüfung der anwendungsunabhängigen Kontrollen**

Bei der Auswahl der Prüfungshandlungen, die auf die Feststellung einer ausreichenden Kontrolle der anwendungsunabhängigen Risiken gerichtet sind, kann sich der Abschlussprüfer an dem CobiT-Prozessmodell und an den den einzelnen Prozessen zugeordneten Kontrollzielen orientieren. Die Prüfung kann sich auf jene Prozesse beschränken, bei denen aufgrund der Struktur des Informationstechnik-Systems des geprüften Unternehmens bei mangelhaftem Funktionieren der unternehmensinternen Kontrollen ein erhöhtes Fehlerrisiko erkennbar ist.

Dabei ist zu beachten, dass Schwachstellen bei den vom Unternehmen durchgeführten Kontrollen von anwendungsunabhängigen Risiken negative Auswirkungen auf sämtliche Anwendungen haben und daher bei allen Anwendungen zu Fehlern führen können.

**b) Prüfung der anwendungsabhängigen Kontrollen**

Anwendungsabhängige Kontrollen sind Kontrollen, durch die die Richtigkeit der Verarbeitungsergebnisse sichergestellt werden soll. Dazu gehören jedenfalls Kontrollen, die im Source Code der Programme enthalten sind, und durch Parameter und Tabellensteuerungen gesteuerte Kontrollen. Die anwendungsabhängigen Kontrollen können in Eingabe-, Verarbeitungs- und Ausgabekontrollen untergliedert werden.

Die Wirksamkeit der anwendungsabhängigen Kontrollen zur Vermeidung von Fehlern hängt in erheblichem Ausmaß von der Wirksamkeit der anwendungsunabhängigen Zugriffsschutzkontrollen und Kontrollen der Software-Änderungsprozesse ab.

Der Umfang der Prüfung der anwendungsabhängigen Kontrollen, die im Sinne der Prüfungseffizienz gleichzeitig mit der Prüfung der anwendungsunabhängigen Kontrollen erfolgen kann, hängt von den bei der Feststellung der Risiken und der Prüfung der anwendungsunabhängigen Kontrollen gewonnenen Erkenntnissen und von der Prüfungsstrategie ab. Der Abschlussprüfer hat zu entscheiden, ob er eine ausreichende Sicherheit für die Richtigkeit der von der Informationstechnik gelieferten Daten durch die direkte Prüfung der Wirksamkeit der anwendungsabhängigen Kontrollen oder durch ergebnisorientierte Prüfungshandlungen erlangt.

Die direkte Prüfung und Beurteilung des Funktionierens der anwendungsabhängigen Kontrollen erstreckt sich auf die Eingabe-, Verarbeitungs- und Ausgabekontrollen der für die Rechnungslegung wichtigen Verarbeitungsprozesse einschließlich der Kontrollen der dazugehörigen Stammdaten, Schnittstellen, Parameter, Berechtigungskonzepte (Funktionstrennungen) und ähnlicher Maßnahmen, durch die Risiken beseitigt oder vermindert werden.

Bei dieser Entscheidung ist auch zu berücksichtigen, ob und inwieweit die Arbeiten der internen Revision oder Kontrollarbeiten von anderen Mitarbeitern des Unternehmens oder von externen Sachverständigen eine Gewähr für die Richtigkeit der von der Informationstechnik gelieferten Daten bieten. Testfälle, Dokumentationen des geprüften Unternehmens und allenfalls vorliegende Softwaretestate anderer Prüfer sind dabei zu würdigen.

Führt der Abschlussprüfer eine direkte Prüfung der Richtigkeit und Wirksamkeit der Programmfunktionen durch, kann die Art dieser Prüfung davon abhängen, ob ihm ein Testsystem des geprüften Unternehmens zur Verfügung steht.

Die Übertragung der Ergebnisse von Kontrolltests auf das Verarbeitungssystem hat zur Voraussetzung, dass im Software-Änderungsprozess ausreichende Kontrollen enthalten sind, aufgrund derer festgestellt werden kann, ob das Testergebnis repräsentativ für die gesamte zu prüfende Periode ist; dh, ob durch ordnungsgemäße Freigabe- und ÜbergabeprozEDUREN die Identität der beiden Anwendungen der Informationstechnik gewährleistet ist.

Sofern kein Testsystem zur Verfügung steht, kann der Abschlussprüfer die Richtigkeit der Verarbeitung etwa durch Beobachtung des Funktionierens von Kontrollen (insbesondere von Eingabe- und Ausgabekontrollen), durch Nachvollziehen der erzielten Ergebnisse oder durch Parallelverarbeitung von Daten mit einem von ihm erstellten Verarbeitungsalgorithmus überprüfen. Die Feststellung der Durchführung von Fachkontrollen und die Durchsicht von Revisionsberichten und von einschlägigen Protokollen kann zur Erlangung einer ausreichenden Prüfsicherheit beitragen.

### **c) Prüfung der Einhaltung der Grundsätze ordnungsmäßiger Buchführung**

Neben der Beurteilung der Wirksamkeit der anwendungsunabhängigen und anwendungsabhängigen Kontrollen ist vom Abschlussprüfer festzustellen, ob bei den Anwendungen die anwendungsbezogenen Grundsätze ordnungsmäßiger Buchführung (Funktionalität, Ordnungsmäßigkeit und Sicherheit) eingehalten werden. Die Vorgangsweise bei dieser Prüfung ist aufgrund der bestehenden Gegebenheiten vom Abschlussprüfer zu entscheiden.

### **C.6. Dokumentation der Prüfungshandlungen und Berichterstattung über die Prüfungsfeststellungen**

Der Abschlussprüfer hat die gewonnenen Erkenntnisse über die wesentlichen Teile des Informationstechnik-Systems und die von ihm vorgenommenen Prüfungshandlungen in den Arbeitspapieren zu dokumentieren. Art und Umfang der Dokumentation ist abhängig von der Komplexität des zu beurteilenden Informationstechnik-Systems.

Die Ergebnisse der Prüfung der Informationstechnik finden Eingang in die Ausführungen über die Rechnungslegung im Prüfungsbericht. Dabei ist zur Ordnungsmäßigkeit der Buchführung und der Datenverarbeitung und zu allfälligen Mängeln bei der Kontrolle der Informationstechnik Stellung zu nehmen.

Über Mängel der formellen Ordnungsmäßigkeit des Informationstechnik-Systems und Mängel, die zu fehlerhaften Daten führen können, sind, wenn sie wesentlich sind, die Aufsichtsorgane und die Geschäftsführung im Wege der Ausübung der Redepflicht des Abschlussprüfers zu unterrichten.

Werden bei der Prüfung Schwächen des Informationstechnik-Systems festgestellt, die zu wesentlichen Mängeln bei der Buchführung und Fehlern bei der Rechnungslegung führen, ist das Prüfungsurteil im Bestätigungsbericht einzuschränken oder gegebenenfalls zu versagen (vgl die Ausführungen im Fachgutachten KFS/PG 3).

Werden im Zuge der Prüfung Verbesserungspotenziale hinsichtlich der Sicherheit und/oder der Wirtschaftlichkeit der Informationstechnik erkannt, ist die Geschäftsleitung in geeigneter Weise (zB im Rahmen des Management Letters) davon zu unterrichten.

## **D. Vorgangsweise bei Auslagerungen im Bereich der Informationstechnik an ein anderes Unternehmen (IT - Outsourcing)**

Wenn ein Unternehmen wesentliche Systeme der Informationstechnik und informationstechnikgestützte betriebliche Funktionen an ein anderes Unternehmen (ein selbständiges Dienstleistungsunternehmen oder ein verbundenes Unternehmen) auslagert, hat der Abschlussprüfer des auslagernden Unternehmens zu beurteilen, wie sich dies auf die Wirksamkeit des internen Kontrollsystems dieses Unternehmens auswirkt. Dabei sind die im internationalen Prüfungsstandard ISA 402 (Audit Considerations relating to Entities using Service Organisations) enthaltenen Anforderungen zu berücksichtigen.

Für die Beurteilung der Ordnungsmäßigkeit der Auslagerungen kann ua wesentlich sein:

- die vertragliche Gestaltung
- die Art der erbrachten Dienstleistung
- das Ausmaß des Zusammenspiels zwischen den internen Kontrollen des auslagernden Unternehmens und des Dienstleistungsunternehmens
- die Art der Kontrollen, die das auslagernde Unternehmen zur Überwachung der ausgelagerten Funktionen eingerichtet hat
- die wirtschaftliche Lage des Dienstleistungsunternehmens
- dessen internes Kontrollsystem.

Stellt der Abschlussprüfer fest, dass die Tätigkeit des Dienstleistungsunternehmens wesentliche Auswirkungen auf die mit Hilfe der Informationstechnik geschaffenen Daten hat, hat er ausreichende Informationen über das interne Kontrollsystem des Dienstleistungsunternehmens einzuholen, um die Kontrollrisiken beurteilen zu können. Gegebenenfalls sollte angestrebt werden, vom Prüfer des Dienstleistungsunternehmens Informationen zu erlangen, und es sollten Erwägungen angestellt werden, ob Prüfungshandlungen vor Ort beim Dienstleistungsunternehmen durchzuführen sind.

Sofern ein Unternehmen das Rechnungswesen ganz oder teilweise an ein Dienstleistungsunternehmen ausgelagert hat, muss sich der Abschlussprüfer von der Erfüllung der Anforderungen an die Ordnungsmäßigkeit der Buchführung durch das Dienstleistungsunternehmen überzeugen. Dabei hat er die Art und Ausgestaltung der Auslagerung wesentlicher Systeme zu beurteilen. Für diese Beurteilung kann der Abschlussprüfer des auslagernden Unternehmens auch die Prüfungsergebnisse des Prüfers des Dienstleistungsunternehmens und von Sachverständigen, die sich auf die Qualität des internen Kontrollsystems des Dienstleistungsunternehmens beziehen, verwenden.

## Das CobiT-Prozessmodell

Im CobiT-Prozessmodell (CobiT bedeutet Control objectives for information and related Technology) der ISACA (Information Systems Audit and Control Association) werden die Informationstechnik-Abläufe in 4 Domänen mit 34 Prozessen eingeteilt.

Für jeden Prozess werden Kontrollziele (insgesamt 314 Kontrollziele) angeführt; die Kontrollziele enthalten die typischen Maßnahmen, durch deren Anwendung die Risiken der betreffenden Prozesse abgedeckt werden sollen.

Die vier Domänen des CobiT-Prozessmodells umfassen die nachstehenden Prozesse:

### Planung und Organisation

PO 1	Definition eines strategischen IT-Plans
PO 2	Definition der Informationsarchitektur
PO 3	Bestimmung der technologischen Ausrichtung
PO 4	Definition der IT-Organisation und ihrer Beziehungen
PO 5	Verwaltung der IT-Investitionen
PO 6	Kommunikation der Führungsziele und der Ausrichtung
PO 7	Personalpolitik und Personalverwaltung
PO 8	Sicherstellung der Einhaltung von externen Anforderungen
PO 9	Risikobeurteilung
PO 10	Projektmanagement
PO 11	Qualitätsmanagement

### Planning and Organization (PO)

Define a Strategic IT-Plan
Define the Information Architecture
Determine technological Direction
Define the IT-Organization and Relationships
Manage the IT-Investments
Communicate Management Aims and Direction
Manage Human Resources
Ensure Compliance with External Requirements
Assess Risks
Manage Projects
Manage Quality

**Beschaffung und Einführung**

- AI 1 Identifikation von automatisierten Lösungen
- AI 2 Beschaffung und Unterhalt der Anwendungssoftware
- AI 3 Beschaffung und Unterhalt der technischen Infrastruktur
- AI 4 Entwicklung und Unterhalt von Verfahren
- AI 5 Installation und Akkreditierung von Systemen
- AI 6 Regelungen von Änderungen

**Acquisition and Implementation (AI)**

- Identify Automated Solutions
- Acquire and Maintain Application Software
- Acquire and Maintain Technological Infrastructure
- Develop and Maintain Procedures
- Install and Accredite Systems
- Manage Changes

**Leistungserbringung und Unterstützung**

- DS 1 Definition und Management von Leistungsebenen
- DS 2 Handhabung der Dienste von Dritten
- DS 3 Leistungs- und Kapazitätsmanagement
- DS 4 Sicherstellung der Kontinuität der Leistung
- DS 5 Sicherstellung der Systemsicherheit
- DS 6 Ermittlung und Zuordnung von Kosten
- DS 7 Aus- und Weiterbildung der Benutzer
- DS 8 Unterstützung und Beratung der Kunden
- DS 9 Konfigurationsmanagement
- DS 10 Umgang mit Problemen und Zwischenfällen
- DS 11 Datenverwaltung
- DS 12 Verwaltung der Ressourcen
- DS 13 Management der Leistungserbringung

**Delivery and Support (DS)**

- Define and Manage Service Levels
- Manage Third-Party Services
- Manage Performance and Capacity
- Ensure Continuous Service
- Ensure Systems Security
- Identify and Allocate Costs
- Educate and train users
- Assist and advise customers
- Manage the configuration
- Manage Problems and Incidents
- Manage Data
- Manage Facilities
- Manage Operations

**Überwachung**

- M 1 Überwachung der Prozesse
- M 2 Beurteilung der Angemessenheit der internen Kontrollen
- M 3 Erlangung unabhängiger Bestätigungen
- M 4 Besorgung von unabhängigen Prüfungen

**Monitoring (M)**

- Monitor the Processes
- Assess Internal Control Adequacy
- Obtain Independent Assurance
- Provide for Independent Audit