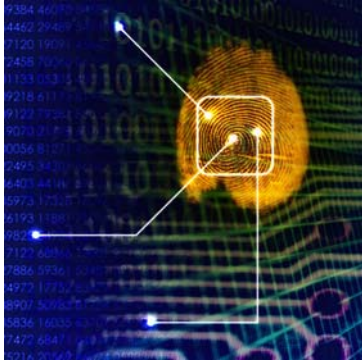


## Internes Kontrollsystem und IT – was man berücksichtigen sollte



**Aus dem neuen Prüfungsstandard 890 zur Prüfung der Existenz eines Internen Kontrollsystems geht klar hervor, dass neben den Kontrollen auf Unternehmens- und Prozessebene auch die IT und ihre Funktion zur Unterstützung der Geschäftsprozesse einen massgeblichen Prüfungsgegenstand darstellt: «Der Abschlussprüfer prüft die Existenz sowohl der Kontrollen auf Unternehmensebene als auch der Kontrollen auf Prozessebene und die generellen IT-Kontrollen.»**

Weiter wird die Geschäftsleitung in die Verantwortung gezogen, in angemessener Art und Weise den aus der IT entstehenden Risiken zu entgegnen, in dem anwendungsbezogene IT-Kontrollen definiert und eingeführt werden. Kontrollmassnahmen im Rahmen der IT sind dann vom Prüfer als wirksam zu taxieren, wenn sie die Integrität und Sicherheit von Daten, die in IT-Systemen in irgendeiner Form verarbeitet werden, aufrechterhalten. Inwiefern IT-Kontrollen im Rahmen des IKS in der jeweiligen Unternehmung gewichtet werden müssen, hängt massgebend davon ab, wie stark der Rechnungslegungs- und Berichterstattungsprozess von IT-Systemen abhängt und wie hoch das Fehlerrisiko im Zusammenhang mit der Verwendung von IT-Systemen ist.

Sowohl kleine als auch grössere Unternehmen verarbeiten Transaktionen im Bereich der Buchführung und Rechnungslegung mittels Unterstützung der Informationstechnologie. Der Einsatz von IT impliziert Risiken, wie beispielsweise dass nicht autorisierte Personen Zugang zu Softwareapplikationen im Finanzbereich und damit Buchhaltungsdaten erlangen. Somit könnten dann diese Daten manipuliert und z.B. fiktive Konten erstellt werden.

Der vorliegende Beitrag behandelt daher wichtige Aspekte bei der Implementierung von unternehmensspezifisch ausgestalteten IT-Kontrollen, die für das Kontrollziel der Sicherstellung einer verlässlichen Finanzberichterstattung von zentraler Bedeutung sind.

### IT-Kontrollen auf Unternehmensebene

IT-Kontrollen auf Unternehmensebene bilden einen Teil des unternehmensweiten Kontrollumfelds und umfassen im Wesentlichen die den IT-Risikomanagementprozess, die IT-Strategieplanung, den Umgang mit rechtlichen und regulatorischen Fragen, die Architektur der IT-Systeme, IT-Regelungen und Weisungen, die IT-technische Ausbildung und das Risikobewusstsein von Mitarbeitenden sowie das Monitoring der IT. Die im Jahreszyklus vorgesehene Prüfung bezieht sich somit auf die Existenz von generellen bzw. unternehmensweiten IT-Kontrollen.

Unternehmensweite Kontrollen gelten als besonders mächtig und wichtig, denn ohne angemessenes Ethikbewusstsein, ausgebautes und umfassendes Leitbild sowie Risikokultur kann kein effekti-

ves internes Kontrollsystem aufgebaut werden. Die Kontrollen auf Unternehmensebene fungieren somit als Grundpfeiler für alle anderen darauf aufbauenden Kontrollen.

## Generelle IT-Kontrollen

Eine funktionierende IT-Infrastruktur und wirksame Kontrollen der IT Prozesse (verstanden als generelle IT-Kontrollen) werden regelmässig als Voraussetzung für die Wirksamkeit von Kontrollen auf der Ebene einzelner Anwendungssysteme (Applikationskontrollen) bewertet. Generelle IT-Kontrollen sind abgeleitet aus den IT-Prozessen. Sie haben unterstützenden Charakter, jedoch keinen direkten Bezug zu den Fachbereichen. Die Dokumentation der allgemeinen IT-Kontrollen zeigt auf, welche Kontrollen sicherstellen, dass die automatisierten IT-Anwendungskontrollen ordnungsgemäss funktionieren, und umfasst regelmässig folgende Bereiche:

- Programmentwicklung; d.h. die Sicherstellung, dass nur IT Systeme entwickelt, konfiguriert und implementiert werden, welche die Anforderungen der Geschäftsprozesse in finanzieller, operationeller und normenkonformer Hinsicht erfüllen.
- Programm- und Datenbankanpassungen; d.h. die Sicherstellung, dass modifizierte oder neue Systeme weiterhin die Anforderungen der Geschäftsprozesse erfüllen. So sind z.B. angemessene Testverfahren für Änderungen an IT-Applikationen und Datenbanken durchzuführen oder Verfahren zur Abwicklung dringlicher Änderungen an Datenbanken zu definieren.
- Zugriffe auf Programme und Daten; d.h. die Sicherstellung, dass einerseits der Zugriff auf Systeme und Daten autorisiert und durch Authentisierungsmechanismen wirksam geschützt ist. Andererseits soll gewährleistet werden, dass der physische Zutrittsschutz zu kritischen IT-Infrastrukturen und Daten vorhanden ist.
- Betrieb der Informatik; d.h. die Sicherstellung, dass produktive Systeme stets verfügbar sind und so betrieben werden, wie sie vom Business genehmigt wurden. Dazu gehört z.B. das korrekte und vollständige Verarbeiten von Datenübertragungen an System-Schnittstellen oder Verfahren zur Handhabung von Zwischenfällen und Problemen.

Um die Existenz der generellen IT-Kontrollen gegenüber dem Revisor zu rechtfertigen, ist es unerlässlich, diese zu definieren und zu dokumentieren. Eine vollständige Übersicht aller relevanten Kontrollen mit den dazugehörigen Kontrollzielen sollte anschliessend an alle IT-Standorte kommuniziert werden, an denen dann das Testen der Kontrollen ebenfalls dezentral erfolgen sollte.

Ein nicht zu unterschätzendes Risiko stellt insbesondere das so genannte End-User-Computing (EUC) dar. EUC bezeichnet den eigenverantwortlichen und freizügigen Einsatz von Software durch Mitarbeiter einer Unternehmung und umfasst typischerweise sowohl Büroanwendungen wie Textverarbeitung und Tabellenkalkulation als auch Anwendungssoftware, die von Benutzern für den Eigenbedarf selber erstellt werden. So werden in vielen Unternehmen beispielsweise Tabellenkalkulationsprogramme ergänzend zur Enterprise Resource Planning Software (ERP) für Up- und/oder Downloads eingesetzt. Hiermit verbunden sind zahlreiche Risiken, da Änderungen in Tabellen beispielsweise von mehreren Mitarbeitern ohne eine korrekte Versionsangabe mitzuführen; fehlende Passwörter ermöglichen überdies auch Nicht-Berechtigten Einsicht oder einzelne Zellen der Tabellen werden nicht schreibgeschützt, was schnell zu unbeabsichtigten oder auch gewollten Manipulationen führen kann. Vor allem das Programmieren von Makros durch End-User, die nicht einem standardisierten Entwicklungsprozess wie bei der Applikationsentwicklung unterliegen, beinhaltet Risiko- und Fehlerquellen. In diesem Zusammenhang ist es Aufgabe des IKS zu verhindern, dass es

nicht zum unkontrollierten Upload fehlerhafter Daten aus solchen Tabellenkalkulationsprogrammen in das produktive ERP-System des Unternehmens kommt.

## Applikationskontrollen

Applikationskontrollen beschäftigen sich mit einer oder mehreren zusammenhängenden Anwendungssoftwaresystemen (Applikationen). Sie kommen regelmässig in spezifischen Geschäftsprozess-Applikationen zum Einsatz und können unterteilt werden in Input-, Verarbeitungs-, Zugriffs- und Outputkontrollen. Die Applikationskontrollen sind nicht unabhängig von den generellen Kontrollen, da sich eine Schwäche bei den generellen Kontrollen auch auf die Applikationskontrollen auswirkt, indem beispielsweise deren Kontrolllogik umgangen werden kann. Nachfolgend wird kurz auf die Inhalte der Applikationskontrollen eingegangen:

- **Inputkontrollen:** Diese Kontrollen stellen sicher, dass die eingegebenen Daten vollständig, fehlerfrei und gültig sind.
- **Verarbeitungskontrollen:** Sie kontrollieren, ob alle Daten verarbeitet werden, keine Daten verloren gehen oder zusätzlich verarbeitet werden, die Verarbeitung mit den korrekten Datenversionen durchgeführt wird und die aus der Verarbeitung resultierenden Berechnungen, Analysen und Zuordnungen korrekt sind.
- **Outputkontrollen:** Sie stellen eine vollständige, fehlerfreie, autorisierte und gültige Datenausgabe sicher.
- **Zugriffskontrollen:** Sie dienen der Gewährleistung des Informationsschutzes und der Vertraulichkeit der Informationen, indem sie Unberechtigten den Zugriff auf eine Applikation verunmöglichen, nur ausgewählten Mitarbeitenden den Zugriff auf bestimmte Funktionen einer Applikation erlauben und nur berechtigten Anwendern den Zugriff auf gewisse Daten ermöglichen.

## Überlegungen beim Outsourcing von IT-Prozessen oder IT-Dienstleistungen

Oftmals werden in zahlreichen Unternehmen IT-Aufgaben ausgelagert, da sie strategisch nicht zu den Kernkompetenzen einer Unternehmung gehören. Werden IT-Prozesse und IT-Dienstleistungen ausgelagert, müssen folgende Überlegungen gemacht werden:

- **Service Level Agreement (SLA):** Wurde im SLA vereinbart, ob der Vertragspartner selbst Audits durchführt oder eine Third Party damit beauftragt wird?
- **SAS70 Report:** Besteht die Möglichkeit der Einsichtnahme in bereits vorhandene SAS70 Reports (Audit-Bericht einer Third-Party zuhanden der Vertragspartner z.B. eines externen Rechenzentrums)?
- Auch bei ausgelagerten Prozessen bleibt die Verantwortung der Kontrollen beim Auftraggeber.

## Rahmenwerke, die bei der Einführung der IT-Kontrollen helfen

Einige wichtige Rahmenwerke in den Bereichen IT Governance, IT Security und Service Management sollen an dieser Stelle kurz genannt werden, da sie Hilfestellungen, Beispiele und Handlungsempfehlungen beim Erstellungsprozess von IT-Kontrollen bieten:

- COBIT: Control Objectives for Information and related Technology. COBIT stellt ein Modell von generell anwendbaren und international akzeptierten Kontrollzielen bereit, die in einem Unternehmen implementiert werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten. Das Framework wendet sich an die drei Zielgruppen Management, Anwender und Auditoren, wobei es Auditoren vor allem bei der Meinungsbildung über das interne IT-Kontrollsystem sowie bei Beratung des Managements bezüglich dieser Kontrollen unterstützen soll.
- ISO/IEC 17799:2005. Der weltweit anerkannte Informations-Sicherheitsstandard ISO 17799 ist eine detaillierte und umfassende Sicherheitsnorm. Dieses Gütesiegel verlangt eine ganzheitliche Informations-Sicherheits-Politik. Es umfasst nicht nur IT-Sicherheit im Allgemeinen, sondern bezieht z.B. auch Gebäude- und Umgebungssicherheit mit ein und deckt damit die gesamte Security-Infrastruktur ab.
- ISO/IEC 27001:2005. Die internationale Norm ISO/IEC 27001:2005 spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
- IT-Grundschatz vom Bundesamt für Sicherheit in der Informationstechnologie. In den IT-Grundschatz-Katalogen werden Standard-Sicherheitsmassnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme empfohlen. Ziel des IT-Grundschatzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. IT-Grundschatz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmassnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen.
- ITIL (IT Infrastructure Library) mit Fokus IT Service Management. ITIL ist die Abkürzung für den durch die OGC (Office of Governance Commerce) in Norwich (England) im Auftrag der britischen Regierung entwickelte Leitfaden IT Infrastructure Library. ITIL ist heute der weltweit De-facto-Standard im Bereich Service Management und beinhaltet eine umfassende und öffentlich verfügbare fachliche Dokumentation zur Planung, Erbringung und Unterstützung von IT-Serviceleistungen.

## Fazit

Nicht wenigen Unternehmen, die in diesem Jahr ein IKS einführen müssen, ist der Handlungsbedarf bei der Umsetzung von IT-Kontrollen noch nicht klar: ergänzend zu den vielfach bereits auf der Ebene einzelner Anwendungsprogramme vorhandenen Kontrollen müssen vor allem die generellen IT-Kontrollen definiert, dokumentiert und umgesetzt werden. Im Mittelpunkt steht dabei die Notwendigkeit einer eindeutigen und vollständigen Regelung, wer Zugriff auf die im Unternehmen eingesetzte Hard und –Software haben soll(te) sowie bei der Programmentwicklung in vorgegebenem Umfang beteiligt sein darf. Da die IT regelmässig den Lebensnerv eines Unternehmens darstellt, ist

vor allem hier das Risiko und damit zugleich der Bedarf nach Kontrollen auf der Unternehmens- und Applikationsebene von enormer Bedeutung.

## Literaturhinweise

- Frei, Patrick: «IT-Kontrollen in der Finanzberichterstattung – Theoretische Analyse und praktische Gestaltung am Fallbeispiel der Crealogix AG», Schulthess Verlag, Zürich 2008.
- Frei, Patrick: IT-Kontrollen in der Finanzberichterstattung, Rechnungswesen&Controlling, Nr. 1, 2008, S. 27-28.

Prof. Dr. Rautenstrauch und Stefan Hunziker, MScBA

Prof. Dr. Thomas Rautenstrauch ist Dozent und Projektleiter am Institut für Finanzdienstleistungen Zug (IFZ) der Hochschule Luzern Wirtschaft und hat darüber hinaus Lehraufträge an der Universität Fribourg sowie weiteren Universitäten in Deutschland und Finnland. Seine Interessen- und Forschungsschwerpunkte liegen im Bereich IKS / Risikomanagement, International Accounting und Controlling. Stefan Hunziker ist Wissenschaftlicher Mitarbeiter und Doktorand am IFZ und verfügt zudem über Erfahrungen aus mehreren IKS-Projekten. Für weitere Informationen: [www.interne-kontrolle.ch](http://www.interne-kontrolle.ch)