KANTON
LUZERN

Finanzkontrolle
des Kantons Luzern
Bahnhofstrasse 19
6002 Luzern
Telefon 041 228 59 23
finanzkontrolle@lu.ch
www.finanzkontrolle.lu.ch

Anforderungen der Finanzkontrolle an Informatik-Projekte des Rechnungswesens

Sehr geehrte Damen und Herren

Nachfolgend sind die wichtigsten Anforderungen festgehalten, welche die Finzanzkontrolle aus der Sicht der Revision an Applikationen stellt. Die Anforderungen ergeben sich im Wesentlichen aus den Aufgaben der Finanzkontrolle. Wir verweisen auf das Finanzkontrollgesetz (SRL 615).

Die revisionsspezifischen Anforderungen sind als Zielsetzung zu verstehen, deren möglichst weitgehende Realisierung anzustreben ist. Dabei sind

- die Art, Wesentlichkeit und das finanzielle Risiko der zu verarbeitenden Daten

- die Möglichkeiten der installierten Hardware und

- die personellen sowie organisatorischen Verhältnisse

angemessen zu berücksichtigen.

Finanzkontrolle des Kantons Luzern

Daniel Steffen Ruedi Durrer

Luzern, 12. November 2012

Inhaltsverzeichnis

A Grundsätzliche Anforderungen an das System

1 Struktur und Funktionen

Um eine reibungslose Verarbeitung sämtlicher Geschäftsvorfälle weitgehend sicherzustellen und um das interne Kontrollsystem zu unterstützen, muss sichergestellt sein,

- dass kein Fachbereich Einfluss auf die Arbeiten anderer Fachbereiche nehmen kann
- dass eine ausreichende Funktionentrennung zwischen den einzelnen Fachbereichen besteht
- dass die Funktionentrennung innerhalb der Fachbereiche gewährleistet ist
- dass sämtliche Stellvertretungen geregelt sind.

2 Ordnungsmässigkeit

Bei der Buchführung und Rechnungslegung sind die materiellen und formellen Grundsätze der Ordnungsmässigkeit sowie die geltenden Rechtsgrundlagen zu beachten, insbesondere hinsichtlich der folgenden Aspekte:

- **Belegprinzip:** Dokumentation sämtlicher Geschäftsvorfälle mittels Beleg. Die vom System generierten Buchungen müssen nachvollziehbar sein. Bei Sammelbuchungen und Postenzusammenzügen sind Detailhinweise notwendig, damit auf den einzelnen Urbeleg zurückgegriffen werden kann
- **Grundbuchfunktion:** Chronologische Grundjournalisierung der Buchungen.
- **Kontenführung:** Aufzeichnung der Geschäftsvorfälle in sachlogischer Gliederung. Die Transaktionen müssen eindeutig identifizierbar sein.
- **Aufbewahrung:** Aufbewahrung der Belege, Programme und anderer Unterlagen (siehe Kapitel 4)
- **Internes Kontrollsystem** (IKS; siehe nachfolgendes Kapitel)
- **Prüfpfad:** Nachprüfbarkeit der Buchführung. Der Buchungslauf und einzelne Buchungen müssen vom Beleg bis zur Rechnungslegung (progressiv) und auch umgekehrt (retrograd) verfolgt werden können.

3 Internes Kontrollsystem (IKS)

Die Kontrollen in den Prozessen müssen sicherstellen, dass

- dass alle Geschäftstransaktionen vollständig, richtig, gültig und nachprüfbar erfasst, ins System eingegeben und dort verarbeitet, gespeichert und ausgegeben werden
- dass die Buchführung und die daraus resultierenden Auswertungen vollständig und richtig sind

- dass keine (unbeabsichtigten oder beabsichtigten) Änderungen an den im System gespeicherten Daten vorgenommen werden können

- dass keine unberechtigten Eingaben von Daten oder Zugriffe auf Daten und Programme im System möglich sind.

Diese Kontrollen sind kontinuierlicher Bestandteil des einzelnen Ablaufes.

4 Aufbewahrung

4.1 Bestimmungen des Obligationenrechts (OR)

Art. 957 Abs. 2 des OR besagt:

"Die Bücher, die Buchungsbelege und die Geschäftskorrespondenz können schriftlich, elektronisch oder in vergleichbarer Weise geführt und aufbewahrt werden, soweit dadurch deren Übereinstimmung mit den zu Grunde liegenden Geschäftsvorfällen gewährleistet ist."

Abs. 3 des gleichen Artikels stellt weiter fest:

"Betriebsrechnung und Bilanz sind schriftlich und unterzeichnet aufzubewahren. Die übrigen Geschäftsbücher, die Buchungsbelege und die Geschäftskorrespondenz können auch elektronisch aufbewahrt werden, wenn sie jederzeit lesbar gemacht werden können."

Die Aufbewahrungsdauer beträgt gemäss Art. 962 OR zehn Jahre ab Ablauf des Geschäftsjahres, in dem die letzten Eintragungen vorgenommen wurden, die Buchungsbelege entstanden sind und die Geschäftskorrespondenz ein- oder ausgegangen ist.

4.2 Geschäftsbücherverordnung (GeBüV)

In der Geschäftsbücherverordnung finden sich, gestützt auf Art. 957 des Obligationenrechts (siehe oben), weitere Ausführungsbestimmungen zur Aufbewahrung. Sie enthält folgende Abschnitte:

- Zu führende Bücher
- Allgemeine Grundsätze
- Grundsätze für die ordnungsgemässe Aufbewahrung
- Informationsträger

5 Zugriffsberechtigungen

Die Daten müssen vor nicht autorisierten Zugriffen geschützt sein. Es dürfen ausschliesslich personenbezogene Zugriffsberechtigungen erteilt werden, welche mit dem jeweiligen Aufgaben- und Verantwortungsbereich übereinstimmen. Die Zugriffsberechtigungen müssen aktuell, bewilligt und dokumentiert sein. Sie müssen lückenlos nachvollziehbar sein (Journalisierung). Passwörter dürfen nicht sichtbar sein und müssen verschlüsselt gespeichert werden.

6 Datenschutz

Bei der Bearbeitung von Personendaten ist der Schutz der individuellen Privatsphäre zu gewährleisten. Wir verweisen diesbezüglich auf das Kantonale Gesetz über den Schutz von Personendaten sowie auf das Eidgenössische Datenschutzgesetz. Wir empfehlen, den kantonalen Datenschutzbeauftragten frühzeitig über das geplante Vorhaben zu informieren.

7 Einführung neuer Programme und Change Management

Neu einzuführende Programme sowie Änderungen an bestehenden Anwendungen müssen durch die Verantwortlichen aus den Fachbereichen ausreichend getestet werden, bevor sie in den produktiven Betrieb übernommen werden. Die Tests sind formalisiert, d.h. Testplanung, -durchführung und -dokumentation folgen klaren Richtlinien.

Es gibt formelle Regeln für Änderungen an Programmen und Konfigurationen. Änderungen müssen lückenlos nachvollziehbar und dokumentiert sein und dürfen nur von Berechtigten vorgenommen werden.

8 Anwender-Schulungen

Es besteht ein Schulungsprogramm, um Mitarbeitende in der korrekten und sicheren Benutzung der neuen oder geänderten Anwendung zu schulen.

9 Dokumentation

Es müssen ausführliche Dokumentationen der Anwendung (inkl. Betrieb und Spezifikationen) vorhanden sein. Die Dokumentationen werden nachgeführt.

10 Verfügbarkeit des Source-Code

Der Source-Code der Programme und Programmversionen sowie die jeweiligen Konfigurationen sind umfassend, aktuell und rekonstruierbar zu dokumentieren. Der Zugriff auf den Source-Code bei eingekaufter Software ist nachweislich wirksam sichergestellt (Escrow Agreement).

11 Outsourcing und Cloud Computing

Anwendungen, welche ganz oder teilweise im Outsourcing-Verhältnis betrieben werden und die finanzielle Berichterstattung betreffen, müssen auf Service Level Agreements und klaren Verträgen beruhen, die die Qualität der Leistungen, die Sicherheit sowie die Verfügbarkeit sicherstellen. Der externe Dienstleister muss durch eine unabhängige Stelle hinsichtlich der in den Verträgen festgehaltenen Ziele überprüft werden (der Prüfbericht wird dem Kunden ausgehändigt). Es besteht ein Recht, zusätzliche Prüfungen beim Dienstleister durchzuführen (Right to Audit).

Bei Cloud Computing-Lösungen muss darauf geachtet werden, dass die Daten jederzeit und ohne Eingriffe des Anbieters exportiert werden können.

Sollen personenbezogene Daten bei externen Anbietern bearbeitet und gespeichert werden, muss der Datenschutz gemäss geltenden gesetzlichen Vorschriften von Bund und Kanton gewährleistet sein. Wir empfehlen, den kantonalen Datenschutzbeauftragten frühzeitig über das geplante Vorhaben zu informieren.

12 IT-Notfallplanung

Es müssen bereits in der Projektphase Vorkehrungen für die Umsetzung eines IT-Notfallkonzepts getroffen werden.

B Spezifische Anforderungen an das System

1 Historisierung der Daten

Jede vorgenommene Transaktion muss lückenlos protokolliert und nachvollziehbar sein. Diese Journale müssen unveränderbar sein.

2 Kontrollen im Prozess

2.1 Monitoring des Workflows

Die Daten im Workflow müssen systematisch überwacht werden. Es muss beispielsweise sichergestellt werden, dass

- Daten (Rechnungen) ohne Aktionen entdeckt werden
- Rechnungen ausschliesslich über ????? in den Workflow eingespeist werden (keine manuellen Erfassungen)
- keine unberechtigten Zahlungsempfänger vorhanden sind (Auswertung der Zahlungsempfänger)
- keine Mutationen an Rechnungen vorgenommen werden
- Rechnungen nicht doppelt vorhanden sind
- keine Zahlungsfreigaben ohne Freigabesignal erfolgen
- etc.

Wir empfehlen, gestützt auf eine Risikobeurteilung, entsprechende Auswertungen zu erstellen, welche durch eine verantwortliche Stelle periodisch geprüft werden.

2.2 4-Augenprinzip

Die Freigabe von manuell geprüften Rechnungen soll zwingend im 4-Augenprinzip erfolgen (Rechnungsprüfung und -freigabe).

3 Schnittstellen

3.1 Abfragen Register XY

Automatische Kontrollen müssen sicherstellen, dass die Abfragen erfolgreich durchgeführt werden konnten. Fehler bzw. fehlgeschlagene Zugriffe werden protokolliert.

3.2 Export SAP

Es muss sichergestellt sein, dass die an das System SAP übergebenen Rechnungen vollständig und richtig sind. Die Schnittstelle ist mit geeigneten Auswertungen zu überwachen.

C Schlüsseldokumente eines Projektzyklus

Wir verweisen auf das Dokument 'Empfehlungen der Schweizerischen Finanzkontrollen für Informatikprojekte'. Diese Broschüre bezweckt insbesondere die Erstellung einer Liste der wichtigsten Dokumente aus der Sicht der Revision. Sie will ferner die Fragen definieren, die diese Dokumente beantworten müssen.