

Internes Kontroll-System im Informatikbereich – auch in KMU erforderlich und sinnvoll!

Auf Risiken und Bedürfnisse ausgerichtete, systematisch aufgebaute und dokumentierte Kontrollen im Informatikbereich erhöhen die Zuverlässigkeit der Geschäftsabwicklung und helfen, die Funktionsfähigkeit, Sicherheit und Wirtschaftlichkeit der Informatik zu gewährleisten - auch in kleineren und mittleren Unternehmen!

Ausgangslage

Gemäss Art. 728a OR hat die Revisionsstelle von wirtschaftlich bedeutenden Unternehmen, die der ordentlichen Revision unterliegen, ab dem Geschäftsjahr 2008 die Existenz eines Internen Kontroll-Systems zu prüfen und zu bestätigen. Beobachtungen zeigen, dass in vielen kleineren und mittleren Unternehmen noch Unsicherheit und Fragen über Umfang und Inhalt sowie insbesondere auch den konkreten Nutzen des IKS bestehen. Dies gilt für das IKS auf Unternehmens- und Prozessebene sowie, in noch stärkerem Mass, auch für die Kontrollen im Informatikbereich.

Der Schweizer Prüfungsstandard "Prüfung der Existenz des Internen Kontrollsystems" (PS 890) definiert die Bedeutung der Informatik für das interne Kontroll-System wie folgt: *„Kontrollen im Informatikbereich sind umso wichtiger, je stärker der Rechnungslegungs- und Berichterstattungsprozess von Informatik-Systemen abhängig ist und je höher das Risiko ist, dass Fehler ihre Ursache im Aufbau von und Umgang mit Informatik-Systemen haben könnten.“*

Informatikeinsatz in KMU

Die Anforderungen an die Informatik weichen in KMU nicht wesentlich von denjenigen in grösseren Unternehmungen ab: Anwendungen mit breitem Funktionsumfang sowie hohe Verfügbarkeit und Sicherheit sind wesentliche Voraussetzungen für die effiziente und zuverlässige Abwicklung der Geschäftsprozesse.

Gegenüber grösseren Unternehmen mit bezüglich Knowhow und Kapazität gut dotierten Informatikabteilungen, ist die Situation in KMU, obwohl die Informatik-Systeme und -Infrastruktur noch „überschaubar“ sind und im Bereich der Kern-Anwendungen Standard-Software eingesetzt wird, oft von folgenden „typischen“ Risiken geprägt:

- fehlendes Knowhow zu Informatik-Anwendungen sowie Daten- und -Werteflüssen (Schnittstellen); daraus resultieren eine fehleranfällige, ineffiziente Nutzung der Software, Schwachstellen in der internen Kontrolle und eine hohe Abhängigkeit von externen Partnern (Lieferanten);
- starke Konzentration des Knowhow auf Einzelne, sehr oft einher gehend mit wenig strukturierten und kaum dokumentierten Prozessen im Informatikbereich; daraus ergibt sich eine hohe Abhängigkeit von solchen Schlüsselpersonen;

- fehlende Funktionen-Trennung zwischen Rechnungswesen und Informatik weil v.a. in kleineren Unternehmen die Verantwortung und z.T. auch die Ausführung in Rechnungswesen und Informatik bei derselben Person liegen;
- angemessener Zugriffsschutz auf Ebene von Netzwerk und Betriebssystem, aber innerhalb der einzelnen Anwendungen kaum differenzierte Zugriffsberechtigungen sowie „schwache“ Passworte und Verzicht auf periodische Passwort-Wechsel;
- Individual-Lösungen und -Auswertungen in Excel oder Access, die von einzelnen Anwendern auf ihrem PC erstellt und kaum dokumentiert werden; deren Weiterentwicklung, Test und Funktionsfähigkeit sowie oft auch deren Nutzung (v.a. im Bereich Kennzahlen und MIS) sind vollumfänglich von dieser einen Person abhängig;
- Schwachstellen im Bereich der physischen Sicherheit (Zutritt, Rauch- und Feuererkennung, Klimatisierung und Stromversorgung) von Rechenzentrum resp. Serverraum;
- regelmässige Erstellung von Datensicherungen, aber oftmals Schwachstellen in deren Aufbewahrung (kein Datenträger-Safe) sowie ungenügende Auslagerung und fehlende Restore-Tests (als Grundlage für Wiederherstellung nach einem gravierenden Ereignis);
- fehlende Vorsorge und Vorbereitung für die Bewältigung von gravierenden Ereignissen (bspw. Zerstörung des Rechenzentrums resp. des Serverraumes), obwohl die Geschäftsprozesse in hohem Mass von der Verfügbarkeit der Informatikmittel abhängig sind.

Fokussieren Sie auf Ihre betrieblichen Anforderungen!

Für ein KMU ist wichtig, auch im Informatikbereich eine angemessene interne Organisation und Kontrolle zu gewährleisten sowie zweckmässige Dokumentationen zu pflegen. Dabei geht es nicht darum, primär den Anforderungen von Obligationenrecht und Revisionsstelle zu genügen - wichtig ist eine klare Fokussierung auf das für Ihr Unternehmen und dessen spezifischen Verhältnisse Notwendige und Zweckmässige!

Es geht in einem ersten Schritt also darum, Klarheit über die **Bedeutung der Informatik für das Unternehmen und die mit dem Informatikeinsatz verbundenen Risiken** zu erlangen. Als Hilfsmittel dafür kann die vom Stab Informatik der Treuhand-Kammer erarbeitete Checkliste dienen:

Kriterium	Risikostufe 1	Risikostufe 2	Risikostufe 3	Risikostufe 4
Geschäftsstrategie und Informatikeinsatz	Die Geschäftsstrategie basiert wesentlich auf der Nutzung des Internets bzw. von neuen Technologien sowie aktivem Informationsaustausch über Datennetze.	Die Geschäftsstrategie basiert teilweise auf der Nutzung des Internets bzw. von neuen Technologien; wichtige Geschäftsprozesse basieren auf Informationsaustausch über Datennetze.	Die Geschäftsstrategie ist nicht von neuen Technologien abhängig; wichtige Geschäftsprozesse nutzen diese Technologien aber bereits.	Die Geschäftsstrategie ist nicht von neuen Technologien (z.B. Internet oder e-commerce) abhängig.

Kriterium	Risikostufe 1	Risikostufe 2	Risikostufe 3	Risikostufe 4
Innovationsgrad beim Informatikeinsatz	Das Unternehmen nutzt eine moderne und komplexe IT-Infrastruktur und adaptiert neue Technologien deutlich vor der Branche.	Das Unternehmen nutzt eine komplexe IT-Infrastruktur und adaptiert neue Technologien ohne Verzögerung.	Das Unternehmen nutzt eine umfangreiche, vorwiegend aus Standardkomponenten bestehende IT-Infrastruktur und adaptiert neue Technologien mit Verzögerung.	Das Unternehmen nutzt eine unkomplizierte IT-Infrastruktur, die vorwiegend aus Standardkomponenten besteht; die IT-Infrastruktur bleibt eher hinter technologischer Entwicklung zurück.
Abhängigkeit von Verfügbarkeit der Informatikmittel	Die IT-Verfügbarkeit ist für das Geschäft (Frontgeschäft resp. Primärprozesse) ein kritischer Faktor; die akzeptierbare Ausfallzeit liegt unter 4 Stunden.	Die IT-Verfügbarkeit ist für das Geschäft (Frontgeschäft resp. Primärprozesse) wichtig; die akzeptierbare Ausfallzeit liegt zwischen 4 Stunden und 2 Tagen.	Die IT-Verfügbarkeit ist für das Geschäft (Frontgeschäft resp. Primärprozesse) bedingt wichtig; die akzeptierbare Ausfallzeit liegt zwischen 2 Tagen und einer Woche.	Die IT-Verfügbarkeit ist für den operativen Betrieb (Frontgeschäft) und die internen Primärprozesse unkritisch; ein Ausfall von mehreren Wochen scheint akzeptabel.
Internes Kontroll-System	Ein internes Kontrollsystem (IKS) ist kaum erkennbar oder ist nicht vorhanden.	Es besteht ein punktuelles, fachbereichsspezifisches IKS; der Dokumentations- und Aktualitätsgrad ist aber unklar.	Es besteht ein formalisiertes, firmenumfassendes IKS; es ist dokumentiert und wird periodisch aktualisiert.	Es besteht ein formalisiertes, firmenumfassendes IKS; es ist dokumentiert und wird jährlich aktualisiert. Das IKS wird durch ein Control Self Assessment ergänzt.
Risikomanagement	Es besteht kein erkennbares Risikomanagement; zur Risikominderung werden ad hoc-Massnahmen eingesetzt.	Es besteht ein punktuelles, anwendungsspezifisches Risikomanagement, das teilweise dokumentiert ist; daraus hervorgehende Massnahmen zur Risikominderung sind nicht (einfach) erkennbar.	Es besteht ein formalisiertes, firmenumfassendes Risikomanagement; es ist dokumentiert und wird periodisch aktualisiert und die daraus hervorgehenden Massnahmen zur Risikominderung sind klar erkennbar.	Es besteht ein formalisiertes, firmenumfassendes Risikomanagement; es ist dokumentiert und wird jährlich aktualisiert und die Risiken werden nachvollziehbar gemindert. Das Risikomanagement wird durch ein Control Self Assessment ergänzt.
Funktions-trennung	Es besteht nur eine rudimentäre, informelle Funktionentrennung; es bestehen (auch im Hinblick auf die IT) abteilungsübergreifende Funktionen.	Es besteht eine Funktionentrennung zwischen IT und Fachbereich; Funktionen <i>innerhalb</i> der Fachabteilungen werden unter Umständen nicht getrennt.	Es wird innerhalb der Fachbereich auf eine funktionale Funktionentrennung geachtet; diese ist in den Aufgabenbeschreibungen dokumentiert, wird jedoch nicht kontrolliert.	Es wird innerhalb der Fachbereiche konsequent auf eine funktionale Funktionentrennung geachtet; diese ist in den Aufgabenbeschreibungen dokumentiert und wird ständig kontrolliert.
Stellvertretung und Knowhow im Rechnungswesen	Im Unternehmen besteht nur eine rudimentäre Stellvertretung; der Ausfall von Einzelpersonen führt bereits im normalen Tagesgeschäft zu Problemen.	Für wichtige Positionen sind Stellvertretungen definiert aber kaum geschult; ein Ausfall von Personen wirkt sich nach einigen Tagen auf das normale Tagesgeschäft aus; die Bewältigung von Problemen und Zwischenfällen ist bei einem Ausfall nicht möglich.	Für alle wesentlichen Positionen sind Stellvertretungen vorhanden und geschult; das normale Tagesgeschäft ist sichergestellt, die Bewältigung von Problemen und Zwischenfällen jedoch schwierig und führt zu Verzögerungen.	Für alle wesentlichen Positionen sind Stellvertretungen vorhanden und geschult, es bestehen entsprechende Dokumentationen; das normale Tagesgeschäft und sowie eine effektive Problembewältigung sind sichergestellt.
Awareness für Informationssicherheit	Die Mitarbeiter sind über ihre Verantwortung zur Einhaltung interner und externer Anforderungen zur Informationssicherheit nicht informiert.	Die Mitarbeiter sind über ihre Verantwortung zur Einhaltung interner und externer Anforderungen zur Informationssicherheit informiert.	Die Mitarbeiter werden wiederholt auf ihre Verantwortung zur Einhaltung interner und externer Anforderungen zur Informationssicherheit hingewiesen und angemessen geschult.	Die Mitarbeiter werden systematisch geschult und die Einhaltung interner und externer Anforderungen zur Informationssicherheit wird regelmässig geprüft.

Kriterium	Risikostufe 1	Risikostufe 2	Risikostufe 3	Risikostufe 4
Software für das Rechnungswesen	Die Rechnungswesen-Anwendung ist eine Eigenentwicklung.	Für das Rechnungswesen wird parametrisierbare Standardsoftware mit Möglichkeiten zur Individualprogrammierung eingesetzt.	Für das Rechnungswesen wird Standardsoftware eingesetzt, welche nur über eingeschränkte Möglichkeiten für Parametrisierung und Individualprogrammierung verfügt.	Für das Rechnungswesen wird Standardsoftware ohne jegliche Parametrisierung und ohne Möglichkeiten für Individualprogrammierung eingesetzt.
Integration Wertefluss im Rechnungswesen	Für Kernanwendungen sind integrierte Lösungen mit hohem Automatisierungsgrad implementiert; der Nachvollzug von Werte- und Datenflüssen bedingt Spezialistenwissen.	Für Kernanwendungen sind integrierte Lösungen mit automatisierten Schnittstellen im Einsatz; Werte- und Datenflüsse sind nachvollziehbar.	Für Kernanwendungen sind verschiedene Insellösungen mit (Batch-) Schnittstellen im Einsatz; Werte- und Datenflüsse sind gut nachvollziehbar.	Es sind mehrere funktionspezifische Insellösungen mit einzelnen (Batch-) Schnittstellen im Einsatz; Werte- und Datenflüsse in Anwendungen und an Schnittstellen sind anhand von Auswertungen und Schnittstellenprotokollen nachvollziehbar dokumentiert.
Programmfehler in Kernanwendungen	Bei den Kernanwendungen treten häufig Probleme auf, die mit grossem Zeitaufwand gelöst werden müssen. Fehler und Ausfallgründe wiederholen sich häufig.	Fehler in Kernanwendungen sind selten, müssen aber mit grossem Zeitaufwand gelöst werden. Störungs- und Ausfallgründe wiederholen sich kaum.	Fehler in Kernanwendungen sind selten und können zeitnah gelöst werden. Fehler und Mängel sind dokumentiert.	Fehler in Kernanwendungen sind sehr selten; Fehler und Mängel werden systematisch, zeitnah und nachhaltig gelöst sowie nachvollziehbar dokumentiert.
Betriebssicherheit der Informatikmittel	Die IT-Mittel (Server, Clients, Netzwerk und Peripherie) sind häufigen Störungen und Ausfällen ausgesetzt; diese wirken sich auf den gesamten Geschäftsbetrieb aus.	Die IT-Mittel ist wiederholt Störungen und Ausfällen ausgesetzt; diese wirken sich auf den gesamten Geschäftsbetrieb aus.	Die IT-Mittel sind kaum Störungen und Ausfällen ausgesetzt; diese wirken sich nur bedingt auf den Geschäftsbetrieb aus.	Die IT-Mittel sind nur selten Störungen und Ausfällen ausgesetzt; diese wirken sich nur auf Teile des Geschäftsbetriebs aus.
Stellvertretung in der Informatikabteilung	Es besteht innerhalb der IT nur eine rudimentäre Stellvertretungsregelung; der Ausfall von Einzelpersonen führt bereits im normalen IT-Betrieb zu Problemen.	Für die wichtigsten Positionen innerhalb der IT sind Stellvertretungen definiert aber kaum geschult; der Ausfall von Einzelpersonen wirkt sich nach einigen Tagen auf den IT-Betrieb aus und die Bewältigung von IT-Problemen ist nicht möglich.	Für alle wesentlichen Positionen innerhalb der IT sind Stellvertretungen vorhanden und geschult, aber nicht dokumentiert; der IT-Betrieb ist sichergestellt, die Bewältigung von IT-Problemen ohne diese Personen jedoch schwierig.	Für alle wesentlichen Positionen innerhalb der IT sind Stellvertretungen vorhanden und geschult, es bestehen entsprechende Dokumentationen; der IT-Betrieb und eine effektive Bewältigung von IT-Problemen sind sichergestellt.
Abhängigkeit von externem Personal	Das Unternehmen ist beim Betrieb der IT weitgehend von externer Unterstützung abhängig; insbesondere bei Problemen ist eine externe Unterstützung unabdingbar.	Der Normalbetrieb der IT ist ohne externe Unterstützung weitgehend möglich; Fehler oder Probleme sind ohne externe Unterstützung kaum lösbar.	Der Normalbetrieb der IT ist auch ohne externe Unterstützung sichergestellt; bei Fehlern oder Problemen muss teilweise auf externe Unterstützung zurückgegriffen werden.	Der Normalbetrieb und die Problemlösung sind jederzeit ohne externe Unterstützung gewährleistet; eine externe Unterstützung ist nur in Krisensituationen erforderlich.
Zeitpunkt der letzten unabhängigen Beurteilung Informatik	Es wurde noch nie eine IT-Prüfung durchgeführt.	Eine IT-Prüfung wurde vor letztmals vor mehr als 5 Jahren durchgeführt.	Eine IT-Prüfung wurde letztmals vor einigen Jahren durchgeführt.	Eine IT-Prüfung wurde im vergangenen Geschäftsjahr durchgeführt.

Grundlagen für das IKS im Informatikbereich

Der Gesetzgeber fokussiert bezüglich internem Kontroll-System auf die Buchführung und Rechnungslegung. Wir sind der Überzeugung, dass bei der Gestaltung der Kontrollen im Informatikbereich auch die "Bedürfnisse" der Leistungserbringungs-Prozesse einbezogen werden müssen – häufig sind Entwicklung, Produktion, Vertrieb und Service in einem viel höheren und direkteren Ausmass abhängig von einem funktionierenden und sicheren Informatikeinsatz als das Rechnungswesen.

Bei der Gestaltung des IKS im Informatikbereich nehmen wir Kontrollziele auf, welche *die Funktionsfähigkeit, Sicherheit und Wirtschaftlichkeit der Informatik* in einem weiteren Sinn unterstützen. Wir adressieren alle wesentlichen Bereiche der Informatik und decken damit auch im PS 890 erwähnten "generellen Kontrollen im Informatikbereich" (Programm-Entwicklung und –Unterhalt, Zugriffe auf Programme und Daten, Betrieb der Informatik) vollumfänglich ab:

Im anwendungs-unabhängigen Bereich , d.h. der Informatik "an sich", sollten Kontrollziele und Kontrollen folgende Themen abdecken:	Im Bereich der Kern-Anwendungen zur Unterstützung der Geschäftsprozesse sollten Kontrollziele und Kontrollen folgende Themen abdecken:
<p>Informatik-Strategie und –Planung Übersicht zum Informatikeinsatz (Anwendungen und Systeme) Organisation und Personal im Informatikbereich Führungsgrundlagen, Richtlinien, Weisungen Risiko-Management Projekt-Management</p> <p>Beschaffung von Informatikmitteln (Hard- und Software) Inbetriebnahme von Informatikmitteln Inventar der Informatikmittel Programm-Entwicklung und –Unterhalt (genereller Prozess)</p> <p>Verträge / Service Level Agreements Versicherungen Konfigurations-Management Physische Sicherheit Logische Sicherheit Datensicherung Archivierung Daten- und Zugriffsschutz (Grundlagen) Notorganisation / Katastrophenvorsorge</p> <p>Leistungen der Informatik (Erwartungen / Beurteilungsgrundlagen) Interne Kontrollen relevante Gesetze, Vorschriften und Verträge</p>	<p>Organisation (Zusammenspiel von Informatik und Fachabteilungen) System- und Benutzer-Dokumentationen Benutzer-Schulung und –Support</p> <p>Systemumgebungen (Entwicklung, Test, Produktion) Antrags-, Genehmigungs-, Test- und Abnahmeverfahren für Programm-Entwicklung und –Unterhalt Antrags-, Genehmigungs-, Test- und Abnahmeverfahren für Pflege Steuerungsparameter (Customizing)</p> <p>Pflege der Stammdaten (Berechtigte, Kontrolle und Nachvollzug) Datenerfassung (Berechtigte, Kontrolle und Nachvollzug) Datenverarbeitung (Kontrolle und Nachvollzug) Datenausgabe (Journale, Kontrolle) Datenspeicherung (Kontrolle und Nachvollzug) (Jahres-)Abschlussarbeiten (Durchführung, Kontrolle und Nachvollzug) Schnittstellen (Kontrolle und Nachvollzug) Zugriffsschutz (Berechtigte, Kontrolle)</p>

Das „ideale“ IKS im Informatikbereich

Ein umfassendes IKS beinhaltet Kontrollziele und Kontrollen auf mehreren Ebenen: Den Geschäftsprozessen d.h. der Aufbau- und Ablauforganisation, den Informatik-Anwendungen und deren programmierten Kontrollen sowie generelle Kontrollen im Informatik-Bereich. Als "Dach" sind unternehmensweite Kontrollziele und Kontrollen in den Bereichen Informatik-Strategie, -Organisation und Personal, Risiko- und Sicherheits-Management sowie Steuerung und Management von (Informatik-)Projekten zu implementieren.

Unternehmensebene Informatik-Strategie, -Organisation und -Personal, Risiko- und Sicherheits-Management sowie Management von Informatikprojekten.
Geschäftsprozesse Aufbau- und Ablauforganisation sowie Kontrollen primär in denjenigen Geschäftsprozessen, die einen Einfluss auf den Wertefluss sowie auf die Buchführung und die Jahresrechnung haben.
Informatik-Anwendungen Kontrollen bei der Erfassung, Eingabe, Verarbeitung und Ausgabe von Transaktionen und Daten sowie Kontrollen an den Schnittstellen zwischen Informatik-Anwendungen.
Informatik-Betrieb Kontrollen bei Programm-Entwicklung und -Änderungen, Betrieb und Änderung der Informatikmittel, der System- und Datensicherheit sowie der Überwachung der Informatik.

Wichtig bei der Gestaltung des IKS, und dies nicht nur im Informatikbereich, ist eine klare Fokussierung auf das für Ihr Unternehmen und dessen spezifischen Verhältnisse Notwendige und Zweckmässige – das IKS darf nicht eine "Pflichtübung" sein, sondern kann einen wesentlichen Beitrag zur "sicheren" (im weitesten Sinn) und effizienten Geschäftsabwicklung leisten!

Peter Steuri

Certified Information Systems Auditor / dipl. Wirtschaftsinformatiker

Partner / Leitender Informatikberater und -prüfer
BDO Visura Solothurn
032 624 65 52 / peter.steuri@bdo.ch