



Impulse für KMU



Aufbau eines IKS – Erfahrungen aus der KMU-Praxis – Teil 2

Nachdem sich das AXALO Telegramm im Februar 2010 den generellen Herausforderungen im Umgang mit IKS-Projekten sowie der Risikobeurteilung gewidmet hat, setzt diese Ausgabe den Fokus auf die Kontrollmassnahmen. Im 2. Teil der Erfahrungen aus der KMU-Praxis werden Herausforderungen im IKS-Projekt während der Definition, Dokumentation, Pflege und Überwachung von Kontrollen beleuchtet.

Die Einführung bzw. Dokumentation des internen Kontrollsystems (IKS) im Umfeld kleiner und mittlerer Unternehmen ist häufig von grundlegenden Fehlentscheidungen geprägt. Die letzte Ausgabe unseres Telegramms widmete sich den grössten Herausforderungen, welche sich zu Beginn eines IKS-Projektes stellen. Dabei schälten wir neben den allgemeinen auch methodische und inhaltliche Themen heraus, wobei insbesondere die Auswahl der Prozesse sowie die Definition der Kernrisiken von zentraler Bedeutung waren. In der aktuellen Ausgabe unseres Telegramms möchten wir uns nun den Themen der nächsten Phasen eines IKS-Projektes widmen. Wir konzentrieren uns dabei auf die manuellen Schlüsselkontrollen, die unternehmensweiten Kontrollen und IT-Kon-

trollen sowie auf die Pflege und die Überwachung eines Kontrollsystems.

Herausforderung 6 – Definition der Schlüsselkontrollen

Die Definition der Schlüsselkontrollen stellt einen wichtigen Schritt im IKS-Projekt dar. Schlüsselkontrollen können zusammenfassend als Kontrollmechanismen beschrieben werden, welche sogenannte Kernrisiken vermindern oder vermeiden. Oder anders ausgedrückt: Durch den Mangel, das Fehlen oder das Versagen einer Schlüsselkontrolle muss innerhalb eines Geschäftsprozesses ein Risiko eingegangen werden, welches dem Unternehmen einen erheblichen finanziellen, operativen, rechtlichen oder strategischen Nachteil verschafft.

EDITORIAL

Die Einführung eines internen Kontrollsystems kann zu unnötigen Problemen führen, sei es bei der methodischen Gestaltung oder bei der fachlichen Umsetzung.

In unserer Ausgabe vom Februar 2010 widmeten wir uns den ersten Schritten innerhalb eines IKS-Projekts. Die darin genannten Erkenntnisse stehen in einem engen Zusammenhang mit denjenigen dieser Ausgabe. Die Definition der Schlüsselkontrollen, der unternehmensweiten Kontrollen sowie der IT-gestützten Kontrollen birgt weitere Gefahren, welche sich dem Unternehmen bei der Auseinandersetzung mit dem internen Kontrollsystem stellen können. Mit diesen Herausforderungen möchten wir uns in diesem Axalo Telegramm beschäftigen.

Trotz aller Widrigkeiten und Herausforderungen, sollten die eigentlichen Ziele eines funktionierenden IKS nicht verloren gehen. Sind diese Ziele laufend im Blickfeld des Unternehmens, kann ein IKS über die reine Dokumentation hinauswachsen und zu einem wirkungsvollen Kontrollinstrument gedeihen.

Oliver Fratschöl
dipl. Wirtschaftsprüfer

Unsere Erfahrungen mit IKS-Projekten zeigen, dass die Wahl bzw. Definition der Schlüsselkontrollen verschiedentlich nicht optimal verläuft. Ein möglicher Grund dafür kann eine Fehleinschätzung der Kontrolle sein. Dabei wird der mutmasslichen Schlüsselkontrolle eine besondere Wichtigkeit und Notwendigkeit beigemessen, obwohl diese Kontrolle weder ein Risiko verhindern noch vermindern kann. Beispielsweise findet sich folgende Situation im Lohnprozess eines kleineren Unternehmens: Dem Risiko einer falschen Lohnzahlung an einen bereits ausgetretenen Mitarbeiter wird mit folgender Kontrolle begegnet: «Lohnzahlungen können nur über das elektronische Visum des Geschäftsführers freigegeben werden». Besteht jedoch, wie in diesem Fall, die Möglichkeit, die Zahlungen nachträglich zu mutieren, sei es irrtümlicherweise oder absichtlich, kann die fehlerhafte Auszahlung nicht (mehr) verhindert werden. Die obenstehende Kontrolle, nämlich das elektronische Geschäftsführer-Visum, wird somit «ausgehoben». Demzufolge wird diese Schlüsselkontrolle wirkungslos.

Die Definition der Schlüsselkontrollen stellt einen Meilenstein des IKS-Projekts dar.

Das vorstehende Beispiel zeigt also, dass die Definition der Schlüsselkontrolle nicht statisch erfolgen darf. Im Mittelpunkt muss deshalb der Geschäftsprozess stehen. Es empfiehlt sich für diesen Schritt, vorgängig eine detaillierte Aufnahme der Abläufe und der bestehenden Kontrollen vorzunehmen.

Ein weiteres Indiz für verbesserungsfähige Schlüsselkontrollen können veränderte Rahmenbedingungen sein. Es kommt vermehrt vor, dass sich durch reorganisatorische Massnahmen die Schnittstellen innerhalb eines Geschäftsprozesses neu gestalten. In einem konkreten Beispiel sähe dies so aus: Der Prozess zum Aus-

lösen und Durchführen des Mahnlaufs erforderte bisher die Kontrolle und Freigabe des zuständigen Key Account Managers. Damit konnte verhindert werden, dass Kunden, trotz Absprache, mit ihrem Kundenbetreuer (z.B. Vereinbarung einer verlängerten Zahlungsfrist für eine erhaltene Abnahmegarantie) zu Unrecht gemahnt werden. Im vorliegenden Fall wird nun eine neue ERP-Software eingeführt, was den automatisierten Mahnlauf erlaubt. Durch diese prozessuale Veränderung wird nun das Risiko einer ungeRechtfertigten Mahnung eines Grosskunden vollends in Kauf genommen. Eine Anpassung der betroffenen Schlüsselkontrolle sollte deshalb in einem solchen Fall ins Auge gefasst werden. Zur Pflege des IKS finden Sie unter ‚Herausforderung 9‘ detaillierte Informationen.

Herausforderung 7 – Dokumentation der unternehmensweiten Kontrollen

Die Dokumentation der unternehmensweiten Kontrollen beginnt mit einer grundlegenden Analyse und Beurteilung der bestehenden internen Regelwerke, Richtlinien und Bestimmungen. Gleichzeitig sind die Prozesse der Risikoanalyse, -beurteilung und -dokumentation des Verwaltungsrates von zentraler Bedeutung. Dabei stehen primär die prozessübergreifenden Risiken im Fokus. Solche übergeordneten Risiken können sein: Markteinbrüche durch Produktinnovationen und Substitutionsgüter, Lieferantenabhängigkeiten, Prozessrisiken aufgrund mangelhafter Produktqualität, Schäden aus deliktischen Handlungen innerhalb des Betriebes oder Liquiditätsengpässe durch Bankenabhängigkeit. Diese Liste lässt sich beliebig erweitern. Die unternehmensweiten Kontrollen werden in der Regel mit Organisationshandbüchern, Mitarbeiterreglementen und Unternehmensrichtlinien abgedeckt. Darüber hinaus gelten Unterschriftenregelungen, Zutrittsbeschränkungen, Archivierungsanweisungen und Whistle-Blowing-Regelungen als klassische unternehmensweite Kontrollen. Wichtige Voraussetzung für die Wirksamkeit dieser Kontrollen ist

das vorbehaltlose Anerkennen der Normen, Werte und Vorgaben durch die Unternehmensleitung.

Der Erfolg von unternehmensweiten Kontrollen beruht zu einem wesentlichen Teil auf der Vorbildfunktion der Geschäftsleitung.

In kleineren und mittleren Unternehmen stützen sich die unternehmensweiten Kontrollen in der Regel auf das 4-Augen-Prinzip, da aufgrund der überschaubaren Struktur viele der vorstehenden Beispiele von Unternehmenskontrollen zu aufgebläht und dadurch nicht praktikabel wären.

Eine grosse Herausforderung bei der Dokumentation der unternehmensweiten Kontrollen bei KMU ist das Erkennen der wesentlichen Kontrollfunktionen. So zeigte sich beispielsweise bei einem Maschinenhersteller mit rund 150 Mitarbeitern, dass die identifizierten Kontrollen auf Unternehmensebene grösstenteils auf das Organisationsreglement verwiesen. Dabei standen Kontrollen wie Zutrittsregelungen, Annahmen von externen Lieferungen und Kassaregelungen im Vordergrund. Die Trennung von Verantwortlichkeiten zwischen der Zahlungseingabe und -freigabe von Lieferantenverbindlichkeiten war hingegen nicht Bestandteil der Dokumentation. Dieses Beispiel zeigt, dass bestehende Kontrollen zu hinterfragen, überprüfen und zu erweitern sind, damit das Gesamtpaket der unternehmensweiten Kontrollen einen wirkungsvollen Bestandteil des IKS bildet.

Herausforderung 8 – Dokumentation der IT-gestützten Kontrollen

Die IT-gestützten Kontrollen lassen sich in generelle IT-Kontrollen («ITGC») und anwendungsbezogene IT-Kontrollen («ITAC») unterscheiden. Letztere beinhalten die implementierten Software-Kontrollen, welche vollständig automatisiert ablaufen.

Diese Kontrollen verfolgen das Ziel, eine vollständige und genaue Datenverarbeitung (von der Dateneingabe bis zur Ausgabe) sicherzustellen. Zudem werden die Datensicherheit und der Datenschutz im Datenverkehr zwischen verschiedenen IT-Programmen gewährleistet. Die anwendungsbezogenen Kontrollen beinhalten neben der typischen Eingabekontrolle, die Kontrolle der Vollständigkeit, der Gültigkeit sowie der Identifikation. Zudem erfolgen Kontrollen für die Authentifizierung und Autorisierung von Informationen. Die anwendungsbezogenen Kontrollen sind insbesondere im KMU-Umfeld vielfach nicht unternehmensspezifisch angepasst. Dies bedeutet, dass diese Kontrollmassnahmen vielerorts im IKS-Projekt nicht speziell thematisiert werden, da die gewünschte Risikoabdeckung in der Regel vom Softwarehersteller oder IT-Anbieter gewährleistet wird.

Anwendungsbezogene Kontrollen bedürfen in der Regel keiner separaten Dokumentation.

Was hingegen hinsichtlich IT-Kontrollen und IKS-Dokumentation von grossem Interesse ist, sind die generellen IT-Kontrollen. Diese Kontrollen verfolgen das Ziel, die Datenverlässlichkeit zu garantieren. Typische Kategorien dieser Kontrollen sind die Kontrollumgebung, IT-Entwicklung, Behebung von Systemausfällen und Zugangsregelungen. Die ITGC beinhalten Funktionen, Massnahmen, Vorgaben und anderweitige Kontrollmechanismen. Dies können Zugriffsrechte, Benutzerprofile, Änderungsverfolgungen oder Passwortregelungen sein. Die Erfahrung zeigt, dass besonders kleinere Unternehmen bei der Dokumentation dieser Kontrollen auf mehrere Hindernisse stossen. Diese zeigen sich sowohl bei der Identifizierung von IT-Risiken als auch bei der Beurteilung der Wirksamkeit und Angemessenheit der entsprechenden Kontrollen. Beispielsweise kommt es vor, dass Unternehmen die Zugriffsberechtigung nicht

benutzerspezifisch vergeben, was dazu führen kann, dass sämtliche IT-Anwender einer Firma auf sämtliche Informationen des gemeinsamen Datenservers zugreifen können (Mangel bei der Identifizierung von Risiken). Hinzu kommt das Risiko von fehlerhaften und deliktischen Datenmanipulationen, die bereits bei einem geringen Ausmass einen verhältnismässig grossen Schaden anrichten können.

Ein weiteres Beispiel eines Hindernisses zeigt sich in der Beurteilung von wirksamen Kontrollen. Es kommt vor, dass KMU-Unternehmen zwar eine laufende und systematische Datensicherung vornehmen, die Aufbewahrung der Sicherungskopien hingegen nicht angemessen implementiert wird. Als Beispiel für eine mögliche Hürde im Bereich der Angemessenheit von Kontrollen kann die Verschlüsselung von E-Mails genannt werden. Diese wird bei vielen nicht als eigentliche Datenschutzkontrolle verstanden und deshalb nicht eingebaut. Stattdessen vertraut das Unternehmen auf einen POP-Server ohne Verschlüsselung, welcher lediglich über einen einfachen Benutzer-/ Passwort-Mechanismus verfügt.

Abschliessend kann festgehalten werden, dass es sich speziell in diesem Thema des IKS lohnt, Expertenunterstützung beizuziehen. Die IT-gestützten Kontrollen stellen nämlich eine erhöhte Schwierigkeit dar, was die Risikoanalyse, die Kontrollzuordnung sowie die Dokumentation und die Überwachung angeht.

Herausforderung 9 – Pflege des IKS

Wie bereits zu Beginn des vorhergegangenen Telegramms erwähnt wurde, soll sich der Nutzen eines IKS auf übergeordnete Werte erweitern. Solche Werte können der Schutz des betrieblichen Vermögens oder die verlässliche Berichterstattung an die Kapitalgeber sein. Aus dieser Tatsache lässt sich ableiten, dass ein Kontrollsystem permanent den veränderten Gegebenheiten angepasst werden muss. Nur so kann gewährleistet werden, dass die Kontrollen weiterhin angemessen und wirksam sind.

Die Angemessenheit und Wirksamkeit des IKS muss laufend geprüft und erfüllt werden.

Beispiele für solche Veränderungen können Geschäftserweiterungen oder Auslagerungen von Tätigkeiten sein. Daneben kann auch ein Wechsel einer bestimmten Schlüsselposition innerhalb des Betriebes zu einer Umgestaltung der Prozesse und natürlich auch der Risikobestände führen. Somit muss sich die verantwortliche Stelle laufend über die wandelnden Verhältnisse des Unternehmens informieren. Unsere Erfahrungen zeigen, dass die Pflege des IKS nicht in allen Fällen als wichtig angesehen wird, wie das folgende Beispiel zeigt: Firma X AG bietet Dienstleistungen innerhalb der Immobilienbranche an. Die wesentlichen und IKS-relevanten Risiken sind analysiert, definiert und dokumentiert. Dank einer günstigen Gelegenheit erwirbt das Unternehmen von einem Mitbewerber eine weitere Sparte, welche das Factoring-Geschäft für die Liegenschaftsvermietung ihrer bestehenden Kunden beinhaltet. Die Firmenleitung verzichtet auf die Pflege des IKS, da sie in der Geschäftserweiterung keine bedeutende Veränderung erkennt. Aufgrund eines Systemausfall, welcher zu einem kompletten Datenverlust der Immobilien-Abrechnungen und der Übersicht aller Mietausstände führt, steht die Firma X AG nach einigen Monaten vor einem enormen Schaden, der nur mit grossem Aufwand beseitigt werden kann.

Wie das vorstehende Beispiel zeigt, stellen die Pflege und der Unterhalt einen bedeutenden Anteil am Erfolg eines internen Kontrollsystems dar.

Herausforderung 10 – Überwachung des IKS

Die Überwachung des IKS unterscheidet sich dahingehend von der Pflege des IKS (siehe Kapitel 9), dass sie den Ist-Zustand von Kontrollmassnahmen dem Soll-Zustand gegenüberstellt. Demge-



genüber widmet sich die Pflege des IKS der Grundlage der IKS-Dokumentation (Prozesse, Risiken, Kontrollen). Somit erfüllt die Überwachung eine abschliessenden und essenziellen Schritt eines IKS-Projekts, der für die ordnungsmässige Umsetzung der definierten Mechanismen notwendig ist.

Problembereiche zeigten sich uns in vergangenen IKS-Projekten vor allem bei manuellen, ereignisbezogenen Kontrollvorgängen, welche besonderer Aufmerksamkeit bedürfen. Folgendes Beispiel verdeutlicht dies: Die Firma Y AG stellt komplizierte kundenspezifische Produkte der Metallbranche (Kupfer) her. Automatisierte Kontrollen existieren abgesehen von der Erkennung des Fingerabdrucks des Geschäftsführer-Notebooks keine. Die Produkte werden individuell fabriziert

und folgen keinem standardisierten Herstellungsablauf. Als eigentliche Schlüsselkontrolle zur Eindämmung des Risikos deliktischer Handlungen (z.B. durch Diebstahl von werthaltigen Rohmaterialien) definiert und dokumentiert die Y AG die tägliche Inventur mit anschliessender Gegenüberstellung des effektiven Verbrauchs innerhalb der abgewickelten Aufträge. Differenzen können sofort beurteilt und erklärt werden, ein möglicher Diebstahl wird dadurch eher erkannt. Die verantwortlichen Personen versäumen der besagten Firma Y AG nun im vorliegenden Beispiel, die Implementierung einer Überwachungsfunktion über das IKS vorzusehen, was dazu führen kann, dass der Prozess- und der Kontrollverantwortliche diese wichtige Massnahme vernachlässigen oder gar auslassen könnte. Diese Kontrolllücke wird im vorliegenden Bei-

spiel einem unzufriedenen Mitarbeiter bekannt, welcher diesen Missstand seinem mit deliktischer Energie geladenen Bekannten mitteilt, welcher möglicherweise zur strafbaren Tat ansetzt.

Dieses Beispiel zeigt, wie fundamental sich die Überwachung des IKS zeigt. Eine Überwachung sollte überdies folgende Grundsätze berücksichtigen: 1) Der Zeitpunkt einer Überprüfung soll für die Betroffenen nicht planbar sein. 2) Die Überwachung soll ebenfalls die Stellvertretung des Kontrollverantwortlichen umfassen. 3) Die Überwachung muss dem Zufallsprinzip folgen. 4) Die Überwachungstätigkeit muss dokumentiert werden. 5) Die Überwachung muss in Konsequenzen münden.

Die beschriebenen zehn Herausforderungen bei IKS-Projekten zeigen die Vielschichtigkeit dieses Themas. Ständen im 1. Teil unserer IKS-Reihe noch einigermaßen berechenbare und rationale Themen im Vordergrund, sind es im 2. Teil Themen, die Ermessensentscheide verlangen. Es empfiehlt sich, bei sämtlichen Herausforderungen eine klare und konsistente Vorgehensweise zu übernehmen, damit ein internes Kontrollsystem nicht nur auf dem Papier, sondern auch am Schreibtisch, an der Werkbank, in der Lagerhalle und im Verkaufsraum lebt. Wir wünschen Ihnen viel Erfolg bei der Umsetzung Ihres IKS-Projekts und stehen Ihnen gerne für tatkräftige Unterstützung zur Verfügung.



AXALO – Unternehmenswachstum, -sanierung und -verkauf

Die Axalo AG ist auf die umsetzungsorientierte Unterstützung von KMU in den Bereichen Unternehmenswachstum, -sanierung und -verkauf spezialisiert. Unsere Ziele sind die Schaffung, Erhaltung und Übertragung von Unternehmenswerten. Dabei ergänzen wir unser unternehmerisches Finanzwissen durch den gezielten Beizug von Spezialisten und bieten unseren Kunden an KMU angepasste Komplettlösungen aus einer Hand an. Typische Anlässe für einen Beizug eines Experten der Axalo AG sind: Strategie-Entwicklung und Neupositionierung, Turnaroundsituationen, Kostenreduktion, Unternehmensbewertungen, Unternehmensverkauf bei Nachfolgelösungen, Finanzplanung (z.B. Budgetierung, Liquiditätsplanung). Ausser-

dem entlasten wir Sie direkt mit unseren Buchhaltungsdienstleistungen. Wir arbeiten mit auf KMU spezialisierten Methoden und haben diese kontinuierlich weiterentwickelt. Da wir selbst auch mehrfache Unternehmer sind, erhalten sie bei uns nachhaltige und unternehmerische Unterstützung.

Hauptsitz

Bartlegroschstrasse 19
FL-9490 Vaduz
T +423 388 29 29
F +423 388 29 20

Zweigniederlassung

Vazerolgasse 2
CH-7000 Chur
T +41 81 733 29 29
F +41 81 733 29 20

www.axalo.com • info@axalo.com