



GEWISSHEIT, DIE IT IM GRIFF ZU HABEN

Der Druck von Gesetzgeber, Regulatorien und Stakeholdern auf die Unternehmensführung hat in den letzten Jahren deutlich zugenommen, so z. B. wegen der Anpassungen des OR in Bezug auf das interne Kontrollsystem oder der kürzlich erfolgten Aktualisierung des Datenschutzgesetzes. Zwar müssen KMUs, welche nicht der ordentlichen Revision unterliegen, die Existenz eines internen Kontrollsystems (IKS) nicht formell bestätigen lassen (OR Art. 728a) – doch ist eine unabhängige Beurteilung der «Gesundheit» der Informatik aus nachfolgend aufgeführten Gründen sehr sinnvoll.

Hat Ihr Unternehmen die Informatik im Griff?

Wurden alle vorgeschriebenen oder notwendigen (Sicherheits-)Massnahmen implementiert? Sind die gesetzlichen Anforderungen hinsichtlich



Peter R. Bitterli

dipl. Math. ETH, CISA, CISM, GEIT*



Ernst Liniger

dipl. Wirtschaftsinformatiker**

Datenschutz und Informationssicherheit ausreichend abgedeckt? Sind die Informatik-internen Prozesse genügend robust, so dass die negativen Auswirkungen bei Zwischenfällen (z. B. Ausfall einer kritischen Geschäftsanwendung) in einem vernünftigen Rahmen bleiben? Unterstützt Ihre Informatik die Erreichung der Geschäftsziele angemessen? Und nicht zuletzt – wissen Sie, welche Kosten gegenwärtig und zukünftig in der Informatik anfallen werden? Wenn Sie auf eine oder mehrere der obigen Fragen mit einem «Nein» oder «Ich weiss es nicht» antworten, besteht sehr wahrscheinlich ein Bedarf nach einer unabhängigen, branchenspezifischen Einschätzung Ihrer Informatik.

Die IT-Querschnittsprüfung – ein Gesundheitscheck der IT (eHealth-Check)

Basierend auf einem Raster mit 91 – zu 20 generellen Themen verdichteten – IT-Kontrollen wird eine eigentliche IT-Querschnittsprüfung durchgeführt. Mit diesem standardisierten Vorgehen erfolgt eine Untersuchung des «Gesundheitszustands» der gesamten Informatik, analog einer generellen Untersuchung beim Hausarzt. Neben einer Zusammenfassung enthält der Bericht für jedes der 20 Themen eine Beschreibung der Erkenntnisse, eine Bewertung der zentralen Fragestellungen, einen Katalog der erkannten Risiken sowie eine Darstellung des Handlungsbedarfs.

Sinn und Zweck einer IT-Querschnittsprüfung (eHealth-Check)

Dem Verwaltungsrat und der Geschäftsleitung bringt ein eHealth-Check Gewissheit darüber:

- ob die Informatik die gesetzlichen und regulatorischen Anforderungen hinsichtlich Datenschutz, Datensicherheit und Datenintegrität erfüllt;
- › Beispiel «Datenschutz/Zugriffsschutz»:

Sie erhalten Gewissheit darüber, ob vertrauliche Informationen nur durch berechtigte (interne/externe) Personen eingesehen oder verändert werden kann;

› Beispiel «Compliance»:

Die für Ihr Unternehmen relevanten Gesetze/Vorschriften sind bekannt und werden eingehalten.

- wo die IT bereits eine solide Grundlage für die aktuelle und künftige Unterstützung der Unternehmensstrategie darstellt und wo Verbesserungen notwendig sind;

› Beispiel «IT-Organisation»:

Neue Technologien werden durch Ihre IT-Spezialisten systematisch auf ihre Bedeutung für die Umsetzung Ihrer Unternehmensstrategie geprüft.

- dass die Risiken im IT-Umfeld erkannt und entsprechend adressiert sind.

› Beispiel «IT-Risikomanagement»:

Weil die definierten Sicherheitsmassnahmen mit Ihren Geschäftszielen abgestimmt sind, ist auch im Ernstfall auf die IT Verlass.

Der Informatikleitung, dem Risikomanagement sowie der internen oder externen Revision zeigt die IT-Querschnittsprüfung auf:

- wie gut die Informatikprozesse (wirklich) sind;
- ob die inhärenten Risiken der Informatik bekannt sind und gemagt werden;
- wo Soll-Anforderungen und Ist-Zustand auseinanderklaffen (und wie weit);
- wo sich Standardisierungs- und Outsourcing-Potential ergeben;
- wo und ob allenfalls vertiefte IT-Prüfungen zur Beurteilung von kritischen generellen IT-Kontrollen notwendig sind.

Vorgehen

Die Analyse und Beurteilung erfolgt in zwei Phasen:

- In Phase I wird in einem ca. einstündigen Gespräch das unternehmens- und branchenspezifische,

minimale Soll-IKS-Profil für die gesamte Informatik ermittelt.

- In Phase II – in der zeitlichen Dimension abhängig von der Grösse und Komplexität eines Unternehmens – erfolgt die eigentliche Querschnittsprüfung, die Erhebung des Ist-IKS-Zustandes und der Vergleich mit dem gemeinsam erhobenen Soll-IKS-Profil der Phase I.

Prüfen und optimieren Sie Ihre Informatik. Wir helfen Ihnen dabei. Wenn Sie an einer unentgeltlichen Erhebung des unternehmens- und branchenspezifischen minimalen Informatik-Soll-Profiles interessiert sind, nehmen Sie mit uns unter Aargauische Kantonalbank, Bahnhofstrasse 58, Postfach, 5001 Aarau, Fax: +41 62 835 72 04, E-Mail: nicole.eilmes@akb.ch Kontakt auf.

* Peter R. Bitterli, dipl. Math. ETH, CISA, CISM, CGEIT, ist seit 25 Jahren als IT-Prüfer im Einsatz, Gründungs- und Vorstandsmitglied des ISACA Switzerland Chapter, Mitglied des Fachstabs für Informatik der Schweiz. Treuhandkammer, Inhaber einer Revisions- und Beratungsfirma sowie einer Ausbildungsfirma.

** Ernst Liniger, dipl. Wirtschaftsinformatiker, ist seit gut 25 Jahren in den verschiedensten Funktionen des IT-Dienstleistungsbusiness tätig, u. a. als Leiter einer internen IT-Revision (und in dieser Zeit als Präsident des ISACA Switzerland Chapter eine der treibenden Kräfte beim nachhaltigen Aufbau der heute über 1000 Mitglieder zählenden erfolgreichen Organisation). Aktuell ist er Geschäftsführer des Startup-Unternehmens BPRES Group AG.

Der Aargauische Gewerbeverband kämpft für bessere Rahmenbedingungen.