

Evaluation von ausgewählten Softwareanwendungen zur Unterstützung eines Internen Kontrollsystems

Diplomarbeit

zur Erlangung des Grades einer Diplom-Ökonomin der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Krause



Vorname: Katja



Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, 22.10.2009

Abstract

For the flood of laws in the last 10 years, many companies feel overstrained to accord identify and to comply with all the relevant formalities. Also the internal controls, mentioned in the companies act from 1977, which were still considered as a compulsory exercise have achieved new attention by the release of the “Bilanzmodernisierungsgesetz (BilMoG)”. The law intensified the disclosure requirements concerning to the internal controls and the amount of the affected companies rose up. In Times, where no company can do its daily business without IT and the amount of data, mainly in accounting increases in volume the question comes up if current softwareproducts can support the internal controls that a functional and effective “IKS” is warranted.

Kurzdarstellung

Nach der Gesetzesflut der letzten 10 Jahre fühlen sich viele Unternehmen überfordert, alle relevanten Regularien zu identifizieren und die Einhaltung zu gewährleisten. Auch das bereits seit 1977 im Aktiengesetz erwähnte Interne Kontrollsystem, das in der Praxis leider immer noch als Pflichtübung angesehen wird, hat mit dem Bilanzmodernisierungsgesetz (BilMoG) neue Aufmerksamkeit erhalten. Die Gesetzgebung verschärfte die Angabepflichten in Bezug auf das IKS und die Menge der betroffenen Gesellschaften wurde erweitert. In Zeiten in denen kein Unternehmen mehr ohne IT sein tägliches Geschäft abwickelt und das zu bewältigende Datenvolumen vor allem im Bereich der Rechnungslegung immer umfangreicher wird, stellt sich die Frage, ob aktuelle Softwareanwendungen das IKS so unterstützen können, dass ein funktionsfähiges und wirkungsvolles IKS gewährleistet ist.

Inhaltsverzeichnis

	Seite
ABSTRACT	I
KURZDARSTELLUNG	I
ABBILDUNGSVERZEICHNIS	IV
TABELLENVERZEICHNIS	VI
ABKÜRZUNGSVERZEICHNIS	VII
1 EINLEITUNG	1
1.1 PROBLEMSTELLUNG UND ZIELSETZUNG	1
1.2 AUFBAU DER ARBEIT	2
2 CORPORATE GOVERNANCE IN DEUTSCHEN UNTERNEHMEN – WICHTIGE REGULARIEN	4
2.1 CORPORATE GOVERNANCE-REGULARIEN: BEGRIFFSDEFINITIONEN UND ENTWICKLUNG	4
2.2 INTERNATIONALE REGULARIEN	7
2.3 NATIONALE REGULARIEN.....	10
2.3.1 Überblick über die nationale Entwicklung	10
2.3.2 Bilanzmodernisierungsgesetz (BilMoG).....	14
2.4 ZWISCHENFAZIT.....	17
3 INTERNES KONTROLLSYSTEM (IKS)	19
3.1 AUFBAU UND AUFGABEN DES IKS.....	19
3.1.1 Begriffliche Einordnung und Aufbau des IKS	19
3.1.2 Aufgaben und Bedeutung des IKS.....	30
3.2 AUSGESTALTUNG UND IMPLEMENTIERUNG DES IKS.....	42
3.2.1 Committee of Sponsoring Organizations of the Treadway Commission (COSO).....	42
3.2.1.1 Bedeutung und Überblick über die COSO-Veröffentlichungen	42
3.2.1.2 COSO I – Die fünf Kontrollelemente des IKS.....	46
3.2.2 Control Objectives for Information and Related Technology (COBIT)	53
3.2.2.1 Einführung und der Zusammenhang mit COSO.....	53
3.2.2.2 IKS-relevante CobIT-Prozesse	57
3.2.3 Rahmenkonzept zur Ausgestaltung und Implementierung des IKS.....	59
3.3 ZWISCHENFAZIT.....	69
4 MODELL ZUR EVALUATION VON SOFTWAREANWENDUNGEN FÜR INTERNE KONTROLLSYSTEME	72
4.1 BEGRIFFLICHE EINORDNUNG UND GRUNDLAGEN DER SOFTWAREEVALUIERUNG	72
4.2 ENTWICKLUNG EINES PHASENMODELLS ZUR EVALUATION	73
4.3 PHASE 1: VORAUSSETZUNGEN FÜR DIE EVALUATION	74

	Seite
4.3.1 <i>Evaluationsziel und –Zweck</i>	74
4.3.2 <i>Evaluationsobjekt</i>	75
4.3.3 <i>Spezifikation des Qualitätsmodelles</i>	76
4.4 PHASE 2: SPEZIFIZIERUNG DER EVALUATION	77
4.4.1 <i>Auswahl der Metriken</i>	77
4.4.2 <i>Festlegung der Einstufungsniveaus</i>	77
4.4.3 <i>Festlegung der Anforderungskriterien</i>	78
4.4.3.1 <i>Formale Anforderungen</i>	78
4.4.3.2 <i>Strategische Anforderungen</i>	82
4.4.3.3 <i>Anforderungen der operativen Geschäftstätigkeit</i>	82
4.4.3.4 <i>Technische Anforderungen</i>	86
4.4.3.5 <i>Anbieterspezifische Anforderungen</i>	86
4.4.3.6 <i>Kosten</i>	87
4.4.4 <i>Anforderungskatalog</i>	87
4.5 PHASE 3: ABLAUF DER EVALUATION	88
4.6 PHASE 4: DURCHFÜHRUNG DER EVALUATION (THEORETISCHE GRUNDLAGEN).....	88
4.7 ZWISCHENFAZIT.....	89
5 EVALUATION VON AUSGEWÄHLTEN SOFTWAREANWENDUNGEN.....	90
5.1 MARKTSICHTUNG	90
5.1.1 <i>Marktanalyse</i>	90
5.1.2 <i>Vorauswahl</i>	91
5.1.3 <i>Auswahl</i>	91
5.2 SOLL-/IST-ABGLEICH DER ANFORDERUNGSKRITERIEN.....	92
5.2.1 <i>Formale Kriterien</i>	92
5.2.2 <i>Strategische Kriterien</i>	92
5.2.3 <i>Kriterien der operativen Geschäftstätigkeit</i>	93
5.2.4 <i>Technische Kriterien</i>	96
5.2.5 <i>Anbieterspezifische Kriterien</i>	96
5.2.6 <i>Kosten</i>	96
5.3 ZWISCHENFAZIT.....	97
6 FAZIT UND AUSBLICK.....	98
LITERATURVERZEICHNIS.....	102
ANHANG.....	112

1 Einleitung

1.1 Problemstellung und Zielsetzung

Wie viele Möglichkeiten fallen Ihnen ein einen Pfannkuchen in einem Restaurant zu essen ohne zu bezahlen? Wahrscheinlich einige. Man könnte schnell essen und weglaufen, sich als Mitarbeiter des Restaurants ausgeben, die Bestellung abholen bevor es der Kellner tut oder den Feueralarm auslösen und in der Küche essen. Was das mit dieser Arbeit zu tun hat? Deutlich wird, dass die meisten Angriffe an Stellen und zu Zeiten passieren, die nichts mit dem Zeitpunkt zu tun haben, an denen das Geld den Besitzer wechseln sollte. Also verhindert das sichern des Zahlungssystems nicht das Stehlen von Pfannkuchen¹. Und das ist der zentrale Gedanke, der es für jedes Unternehmen unerlässlich macht, sich mit seinen Geschäftsprozessen auseinander zu setzen und Risiken zu identifizieren. Vermögensverluste können an jedem Punkt des Unternehmens entstehen auch am Feuerlöscher oder in der Küche. Das zentrale Managementinstrument für diese Aufgaben, wie im Laufe dieser Arbeit dargestellt wird, ist das Interne Kontrollsystem (IKS). Durch die aktuellen Gesetzesänderungen des Bilanzmodernisierungsgesetzes (BilMoG), die eine Beschreibung der wesentlichen Merkmale des rechnungslegungsbezogenen Teils des IKS fordert, in den Mittelpunkt der Aufmerksamkeit der Unternehmen gerückt, stellt das IKS in der Praxis eine Pflichtübung dar. Das vorrangige Ziel ist die Einhaltung und Erfüllung der gesetzlichen Anforderungen. 96% der befragten Unternehmen einer Studie² zum Thema IKS sahen den Nutzen in der Korrektheit und Vollständigkeit der Finanzberichterstattung. Der zusätzliche Nutzen und die Vorteile eines solchen Systems werden in der Praxis nicht erkannt und das Thema wird mit Aufwand und Ausgaben gleichgesetzt³. Obwohl die mangelnde oder fehlende Einrichtung von IKS Unternehmen im Jahr durchschnittlich 5,57 Millionen Euro pro Jahr kosten⁴, da Diebstähle und Betrugsfälle nicht aufgedeckt werden. Dabei ist es so einfach. SAP stellte in einer Produktpräsentation zum Thema Risikomanagement- und Internes Kontrollsystem klar: „Process Control ermöglicht jedem Compliance-Verantwortung zu übernehmen.“⁵ Aus diesem Grund soll in dieser Arbeit der Frage nachgegangen werden, ob bereits Softwareanwendungen existieren, die alle Erfordernisse eines IKS umsetzen und dabei jedem die Möglichkeit geben gesetzliche Anforderungen mühelos umzusetzen und den Diebstahl von „Pfannkuchen“ zu verhindern.

¹ Vgl. Schneier, B.[2001, S.279-280]

² Vgl. Hiendlmeier, A., Maier, B.[2009]

³ Vgl. Expertenbefragung, Auswertung Frage 9

⁴ Vgl. PricewaterhouseCoopers (Hrsg.)[2009, S.12-13, S.29]

⁵ Heckner, M.[2009, S.25]

1.2 Aufbau der Arbeit

Um eine Evaluation von ausgewählten Anwendungssystemen zur Umsetzung eines Internen Kontrollsystems vornehmen zu können und damit die eingangs gestellten Fragen zu beantworten, wird die Arbeit wie folgt vorgehen.

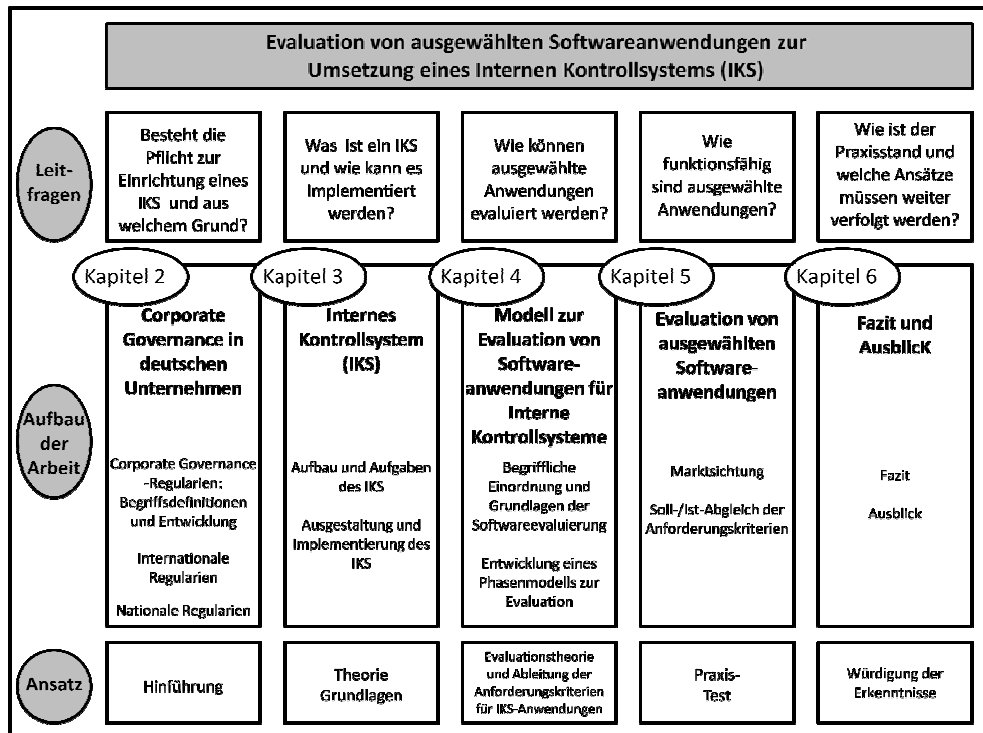


Abbildung 1: Aufbau der vorliegenden Arbeit⁶

Zunächst soll durch die Durchsicht der Gesetzesflut der letzten Jahre geklärt werden, welche Regularien relevant sind und ob sogar die Pflicht zur Einrichtung eines IKS besteht. Und wenn ja, aus welchem Grund. Die umfangreiche Hinführung zu dem Thema dieser Arbeit ist nötig, um sich als Leser ein Bild von der Auswirkung und Mächtigkeit des Managementinstrumentes IKS zu machen und der Überführung in die Anforderungskriterien für die Softwareanwendungen in Kapitel vier folgen zu können. Kapitel drei wird sich dann mit der Frage beschäftigen was ein IKS überhaupt ist und wie es ausgestaltet werden sollte, da der Gesetzgeber diese Antwort schuldig bleibt. Die hier gelegten theoretischen Grundlagen sind mehr als das. Sie sollen vor allem einen umfangreichen Einblick in die Bedeutung des IKS geben und die damit verbundenen Vorteile und Nutzenpotentiale abseits der Gesetzgebung aufzeigen, aber natürlich auch das theoretische Fundament für Kapitel vier legen. Hier werden aus den Erläuterungen der Kapitel zwei und drei die Anforderungskriterien für eine IT-gestützte Unterstützung des IKS abgeleitet und ein Modell zur Evaluation von Softwareanwendungen zur Unterstützung eines IKS vorgestellt, das die Grundlage für den Praxistest in Kapitel fünf liefert. Hier soll im Anschluss die Frage beantwortet werden können, ob bereits Softwarean-

⁶ Graphischer Aufbau orientiert sich an Schäfer, J.[2001, S.11]

wendungen existieren, die alle Erfordernisse eines IKS umsetzen und dabei jedem die Möglichkeit geben gesetzliche Anforderungen mühelos umzusetzen.

Um den Praxisbezug dieser Arbeit zu gewährleisten, wurden im Rahmen einer Reihe explorativer, nicht standardisierter Expertenbefragungen⁷ mit Angestellten von drei der vier großen Wirtschaftsprüfungsgesellschaften und einem IT-Dienstleister eines großen internationalen Konzerns an Hand eines Fragebogens (A.1.1) durchgeführt. Daraus ergaben sich interessante Gespräche, die alle die gleichen Kernfragen beantworteten, aber auch Raum für Nachfragen zu unterschiedlichen Aspekten und Anekdoten aus der Praxis ließen. Die Interviews sind im Rahmen dieser Arbeit als Argumentationsunterstützung in den Text der Arbeit eingeflossen, wodurch jeder Abschnitt der Arbeit einen praxisorientierten Bezug erhielt. Die kompletten Interviewabschriften befinden sich im Anhang unter A.1.

⁷ Die Befragungen waren teilstrukturiert und beinhalten nicht repräsentative, individuelle Sichtweisen der vier Befragten, die sich auf ihren Erfahrungen gründen. Vgl. Atteslander, P.[2008, S.56, 123, 134]

6 Fazit und Ausblick

Die eingangs gestellte Frage dieser Arbeit lautete, ob bereits Softwareanwendungen existieren, die alle Erfordernisse eines IKS umsetzen und dabei jedem die Möglichkeit geben gesetzliche Anforderungen mühelos umzusetzen. Um dies zu beantworten sollte zunächst geklärt werden, ob für diese Arbeit eine Praxisrelevanz besteht und in Kapitel zwei unter Betrachtung der gesetzlichen Entwicklung der letzten 10 Jahre, bzw. speziell der Entwicklung der Corporate Governance-Regularien ein Praxisanreiz zur Umsetzung eines IKS gegeben sein müsste. Um so erstaunlicher war nach Bearbeitung dieses Teilaspektes und dem Wissen um die Angst vor den sogenannten EURO-SOX-Gesetzen (8.Eu-Richtlinie) das Resultat, dass Unternehmen sich schon mit Ende der 1970er Jahre mit diesem Thema hätten beschäftigen müssen. Mit dem BilMoG ergibt sich wie erläutert ein faktischer Zwang zur Auseinandersetzung mit der Effektivität des IKS, der trotz der bestehenden Regularien von allen Experten und auch von meiner Seite dennoch nötig gewesen ist. Es war wichtig den Druck auf die Aufsichtsräte zu erhöhen und die Auseinandersetzung mit der Wirksamkeit und Effektivität der Instrumente zu fördern. Generell gilt: Unternehmen müssen genügend Flexibilität besitzen, um auf Risiken und Chancen schnell und angemessen reagieren zu können. Deshalb müssen in zunehmendem Maße das Steuerungs- und Überwachungskonzept der Unternehmung um betriebswirtschaftliche Konzepte und Methoden ergänzt werden, deren Informationsgehalt über den des betrieblichen Rechnungswesens hinausgeht.³⁹⁴ Sofern Interne Kontroll- und Risikomanagementsysteme nicht funktionieren oder nicht vorhanden sind, können auch die ambitioniertesten externen Corporate Governance- Vorschriften zukünftige Unternehmenskrisen nicht verhindern.³⁹⁵

Dieses Zwischenergebnis rechtfertigt die Auseinandersetzung mit dem IKS und gab die Möglichkeit innerhalb des großen Theorieblocks von Kapitel drei eine ganzheitliche, umfassende Darstellung zu diesem Thema zu liefern. Diese sollte vor allem den eingefahrenen Blick das IKS als Pflichtübung zu sehen lösen und die Potentiale dieses Tools zeigen. Zunächst wurde eine Definition für das IKS hergeleitet und ein Überblick über seinen systemorientierten Aufbau gegeben. In diesem Zusammenhang wurde festgestellt, dass eine isolierte Betrachtung des IKS vom Risikomanagement nicht sinnvoll ist und nur zur Bearbeitung dieser Arbeit durchgeführt wurde. Dies ändert jedoch nichts an der Zulässigkeit der Ergebnisse in Bezug auf das IKS. Auch nicht wenn man im Zuge eines Projektes beide Systeme implementieren wollen würde. Abhängig von Größe, Komplexität und Branche bildet sich ein sehr heterogenes Bild in Bezug auf die Reife des IKS.. Einig waren sich die Experten, dass die Notwendigkeit und die Vorteile des IKS in der Praxis nicht erkannt werden und das Thema mit Geld und Aufwand gleichgesetzt wird. Im folgenden Abschnitt wurde deshalb genau auf die Bedeutung des IKS eingegangen, das trotz gesetzlicher Verpflichtungen und neben den Kernzielen Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit, Ordnungsmäßigkeit der Rechnungslegung und Compliance, erhebliche Vorteile für Interessensgruppen in und außerhalb

³⁹⁴ Vgl. Wich, H.[2008, S.29-30]

³⁹⁵ Vgl. Langenbucher, G,[2003, 56]

des Unternehmens gewährt, z.B. die Vermeidung von Wirtschaftsdelikten und erhebliche potenzielle Ersparnisse. Zur Ausgestaltung und Implementierung wurde im folgenden das anerkannte COSO-Rahmenwerk vorgestellt und erläutert. Bei der Darstellung der Komponente Kontrollaktivitäten wurde durch die Kategorisierung der Kontrollen in automatisch, manuell und detektiv, präventiv ein Einblick in die mögliche Ausgestaltung der Kontrolllandschaft gegeben und erläutert, dass automatische, präventive Kontrollen zwar den effizientesten Kontrolltyp darstellen, dass für eine optimale und wirtschaftliche Kontrolllandschaft das Unternehmen je nach Größe, Komplexität und Branche einen eigenen Mix zusammensstellen muss, der zur Weiterentwicklung beide „Verteidigungslinien“, detektive und präventive Kontrollen, beinhalten sollte. Die Forderung nach automatischen Kontrollen und der Einsatz von ERP-Systemen und Buchführungssysteme in der Praxis macht das IT-IKS, auf Grund der aus der IT entstehenden speziellen Risiken für die Erreichung der drei IKS-Ziele, zu einem wichtigen Bestandteil des IKS. Es wurde erläutert, wie unsichere IT-Systemen zu bestandsgefährdenden Risiken werden können und welche Sicherheitskriterien für die Ordnungsmäßigkeit des IKS erfüllt sein müssen. Da IT in COSO kein expliziter Bestandteil ist, wurde im folgenden Abschnitt, das anerkannte Rahmenwerk CobIT vorgestellt und ein Einblick in den Aufbau des Rahmenwerkes gegeben, das 318 Kontrollziele zur Sicherung, Effektivität und Effizienz des IT-Betriebes definiert und so auch für dessen compliance sorgt. Die Darstellung des praxisnahen Rahmenwerkes zur Implementierung eines IKS bildete den Abschluss des Theorieblocks und fasste auf übersichtliche Weise die praktischen Aspekte des Prozesses IKS noch einmal zusammen. Und bildete damit die Grundlage für den in Kapitel vier entwickelten Anforderungskatalogs Nachdem in Kapitel drei die Bedeutung von automatisierten Kontrollen verdeutlicht wurde, stellte sich die Frage nach dem Praxisstand. Für den Stand der Automatisierung des IKS-Prozesses, bzw. dem Einsatz von IKS-Anwendungen, zeichneten die Experten ein einheitliches Bild. Auch wenn Buchführungssysteme IT-basiert laufen, tut es das IKS noch nicht. Kontrollen werden immer noch vielfach manuell durchgeführt und in Listen dokumentiert und weggeheftet, bzw. es wurden manuelle Schritte in die EDV übertragen ohne eine mögliche Verbesserung zu erreichen. Z.B. liegen Datenbanken für vergebene Berechtigungen vor, die aber durch Emailverkehr zustande kamen, also IT-basiert sind, aber nicht automatisiert. Der erläuterte momentane Praxisstand und den Druck der aktuellen Gesetzlage rechtfertigen den Blick auf den Markt der Software für IKS und die Evaluation ausgewählter Anwendungen in Kapitel vier.

Kapitel vier stellte ein Evaluationsmodell auf Grundlage des ISO/IEC 14598:1999 vor. Als Evaluationsziel wurden die Qualitätsbeurteilung eines Softwareproduktes genannt, das zur Unterstützung des IKS angewendet werden kann. Das Evaluationsobjekt wurde im Folgenden näher bestimmt und als IKS-Anwendung, die Dokumentation, Planung, Steuerung und Überwachung des IKS gewährleisten soll, identifiziert. In Abgrenzung zu den operativen ERP-Systeme, in denen das IKS umgesetzt wird und das die relevanten Daten liefert. Das entwickelte Qualitätsmodell beinhaltet sechs Qualitätsmerkmale, 13 Teilmerkmale und insgesamt 71 Einzelkriterien, womit ein breiter Überblick über die Anforderungen an ein IKS geschaffen wurde der als Anforderungskatalog in A.4. vorliegt. Die Möglichkeit die generell anwendbare

Evaluation auf individuelle Bedürfnisse anzuwenden und zu einer numerischen individuellen Schlussfolgerung zu kommen wurde ebenfalls erläutert.

Zwei Probleme, bzw. Schwachstellen der IKS-Anwendungen ergaben sich bereits bei der Herleitung der Anforderungen. Zum einen die Notwendigkeit einer einheitlichen Datenbasis, die, sofern sie nicht gegeben ist, das IKS unwirksam machen kann. Und zum andern die Feststellung, dass Compliance nicht vollständig zu automatisieren ist und vor allem der Prozess vom individuell gültigen Regularien zum technischen Regelwerk, dass die Compliance garantieren soll, nicht. Die Automatisierung der Regeln setzt gesetzliches Know-How und die Kenntnis von Frameworks wie COSO oder CobIT voraus, um auf die Anforderungen aufbauend Kontrollziele für das IKS zu definieren und im Anschluss diese IT spezifisch zu interpretiert und in formale Regeln zu transformieren. Die größte Schwachstelle der Anwendungen ist somit der Konzeptentwurf. Die Software kann nur so gut sein, wie das Kontrollkonzept und das ist nur so gut, wie es aufgesetzt wurde.

Die Marktsichtung zeigte eine Dreiteilung des Anbietermarktes rund um IKS-Anwendungen. Wirtschaftsprüfungsgesellschaften, Nischenanbieter, aber vor allem ERP-Anbieter bieten zahlreiche Lösungen auf dem neu entstandenen GRC-Markt, der ganzheitliche und effektive Lösungen anbietet, um die Anforderungen des Governance, Risk und Compliance umzusetzen. Das neue der Produktportfolios aus bekannten Anwendungen ist die Verzahnung, der ganzheitliche Lösungsansatz, der Kunden einen großen Effizienzgewinn bringen kann. Bei einem Abgleich der entwickelten Anforderungen mit dem Lösungsportfolios der SAP AG und der Mega International wurde auf einen Blick deutlich, dass die Softwareanbieter alle zentralen Bereiche, die ein IKS IT-gestützt umsetzen kann, zumindest in Angriff genommen haben. Da sich bei dieser Evaluation auf Grund der Datenbasis keine Schwäche herausbilden konnten, wurde im Experteninterview nach Schwächen der Anbieter gefragt. Die Praxis (IT-Dienstleister) zeichnete ein negatives Bild über die Leistung der Anwendungen. Mit Anwendungen von IDS Scheer und SAP im Einsatz hieß es hier: „Beide Produkte sind unzureichend, folgende Anforderungen sind unzulänglich umgesetzt: intuitive Nutzerführung, hohe Verarbeitungsgeschwindigkeit, Schnittstellen zu vor- und nachgelagerten Systemen, upload-/download-Fähigkeit in üblichen Datenformaten, Archivierungsfunktion.“ Was einen wesentlichen Bestandteil des Anforderungskatalogs ausmacht. Die Ursachen für dies Schwächen liegen sicherlich auch an dem Schnittstellenproblem und der Forderung nach einer einheitliche Datenbasis, die durchaus zu Performanceverlusten führen kann. Leider war eine weitere Untersuchung des Praxisstandes nicht mehr möglich. Eine Umfrage unter Unternehmen würde sicherlich interessante Ergebnisse liefern, die mit den Anbietersaussagen verglichen werden könnten. Die Antworten auf die eingangsgestellten Fragen sind somit gefunden. Es existieren durchaus Lösungsstrukturen, die es Unternehmen ermöglichen ihr IKS effizienter und effektiver zu gestalten und die durchaus alle wichtigen Anforderungen abdecken können. Die Frage nach der Handhabbarkeit von Compliance für jeden ist eigentlich durch das Aufzeigen des Automatisierungsproblems der Compliance beantwortet, aber Herr Tenglerth von Deloitte hat schönere Worte gefunden:

„Wenn „jeder“ meint, Personen mit dem entsprechenden Sachverstand in dem jeweiligen Prozessen und mit Kenntnis der vor und nachgelagerten Prozessen sowie der Kontrollen, also ein Sachkundiger, dann muss oder sollte es so einfach sein, dass ein Tool die Mitarbeiter in dieser Hinsicht unterstützt. Wobei auch hier eingeräumt werden muss, dass Compliance-Verantwortung und Kontrollverantwortung bei den Abteilungsleitern zu sehen ist. Also, wenn diese Personen jeder sind, dann ja.“ (A.1.2-Frage 13)

Als Ansatzpunkt für eine weitere Forschung und Weiterführung dieses Themas bietet die Arbeit zahlreiche Ansatzpunkte. SAP bietet 120 vorkonfigurierte Kontrollen an, dessen Untersuchung interessant gewesen wäre. Da ich mir nicht vorstellen kann, wie vorkonfigurierte Kontrollen auf unternehmensindividuelle Prozesse passen sollen. Generell gibt es noch Potenzial für Ideen, wie man das COSO-Modell weiter automatisieren, bzw. digitalisieren kann. Ein Bsp. sind Fortbildungen, die die Komponente Information und Kommunikation fordert, um Mitarbeiter zu fördern und darüberhinaus der Bedarf die Mitarbeiter über wichtigere Änderungen auf dem Laufen zu halten und sie regelmäßig Ethikrichtlinien, etc. bestätigen zu lassen. Hier könnten integrierte E-Learning-Portale eine interessante Idee für die Praxis sein. In der Arbeit ist auch angeklungen wie umfangreich bereits Projekte zu Kontrollen im IKS sind (siehe Siemens³⁹⁶). Die Gestaltung des Projektmanagements von ganzheitlichen GRC-Lösungen wird eine besondere Herausforderung sein. Sowohl was das eigentliche Projektmanagement, als auch die Implementierung neuer Systeme betrifft, die mit bestehender IT-Struktur agieren muss. Und Schlussendlich, um direkt auf dieser Arbeit aufzubauen, würde die Möglichkeit bestehen einen Auswahlkatalog zu entwerfen. Im Internet bestehen Softwaredatenbanken und Auswahltools für viele Softwareanwendungsarten, aber für GRC-Produkte nicht. Eine Datenbank, die Präferenzen strukturiert und Empfehlungen ausgibt in diesem Bereich ist so noch nicht existent.

³⁹⁶ Brauer, M. H., Steffen, K.-D., Biermann, S., Schuler, A. H.: Compliance Intelligence - Praxisorientierte Lösungsansätze für die risikobewusste Unternehmensführung.