

Vorteile und Herausforderungen IT-gestützter Compliance-Erfüllung

(Wirtschaftlichkeit von IT-Risk-Management-Lösungen zur Sicherstellung der Erfüllung von Compliance-Anforderungen)

Prof. Dr. Michael Amberg
Dipl.-Kfm. Kian Mossanen



Eine gemeinschaftliche Studie der
Friedrich-Alexander-Universität Erlangen-Nürnberg
Lehrstuhl für Wirtschaftsinformatik III
und
Novell, Inc.

Friedrich-Alexander Universität Erlangen-Nürnberg
Lehrstuhl für Betriebswirtschaftslehre, insbes. Wirtschaftsinformatik III
Lange Gasse 20, 90403 Nürnberg, www.wi3.uni-erlangen.de

Executive Summary

Der Markt für softwaregestützte Compliance-Lösungen wird von einem zunehmenden Verlangen nach Sicherheit stark vorangetrieben. Sowohl externe als auch interne Bedrohungen geben Anlass, sich mit Compliance auseinanderzusetzen. Nach Möglichkeit sollen Bedrohungen in „real-time“ erkannt, analysiert und abgewendet werden. Neben den von innen heraus getriebenen Aktivitäten zur Gewährleistung eines gewünschten Sicherheitslevels, werden zunehmend Vorgaben zur Auseinandersetzung mit Compliance auf nationaler und internationaler Ebene erlassen.

Der Lehrstuhl für Betriebswirtschaftslehre, insbesondere Wirtschaftsinformatik, der Friedrich-Alexander-Universität Erlangen-Nürnberg und Novell haben sich dieser Studie angenommen, um die aktuellen Anforderungen, Herausforderungen, Ansätze und Strategien sowie Kostentreiber bezüglich compliancebasierter IT-Unterstützung zu identifizieren. Um diese identifizieren zu können, wurde der aktuelle Stand der Literatur umfassend, sowohl quantitativ als auch qualitativ, aufbereitet, wobei der Fokus verschiedenartig gewählt und branchenübergreifend vorgegangen worden ist. Zur Analyse wurden, neben der Aufbereitung des aktuellen Wissenstandes der Literatur, qualitativ-explorative Experteninterviews durchgeführt und diese mit der Literatur abgeglichen. Anhand der gewonnenen Erkenntnisse wurde ein Berechnungsansatz für die Rentabilität von Compliance entworfen und Kostentreiber sowie potentieller Nutzen ermittelt und diese einander gegenübergestellt.

Im Laufe der Studie hat sich gezeigt, dass die Meinungen bezüglich des positiven Nutzens von Compliance sehr stark differieren. Allerdings gab es keinen Gesprächspartner, der die gesteigerten Compliance-Anforderungen in ihrer Gesamtheit ablehnte. Woraus geschlossen werden konnte, dass überwiegend Bedarf an Compliance gesehen wird. Dieser kann mit softwarebasierten Tools zur Erfüllung von Compliance-Anforderungen teilweise gedeckt werden. Eine zentralisierte Aussteuerung in Kombination mit einer Abkehr von der Verwendung von Software-Insellösungen sollten bedarfsorientiert eingesetzt werden. Hierbei ist die Automatisierung durch Software-Unterstützung das Schlagwort zur effektiven und effizienten Erfüllung von Compliance, da Unternehmen zumeist nicht bereit sind, mehr Personal für die Erfüllung von Compliance-Anforderungen einzusetzen.

Durch ein intensives Auseinandersetzen mit den relevanten Gesetzen und Anforderungen wird deutlich, dass eine Vielzahl von Überschneidungen und Redundanzen vorherrscht. Es gilt durch ein Abgleichen interner und externer Anforderungen einen individuellen Anforderungskatalog zu erstellen, der diese überschaubar darstellen lässt und Compliance handhabbar macht.

Gliederung der Studie

1. Einführung

- 1.1 Relevanz des Themas
- 1.2 Problemstellung
- 1.3 Zielsetzung und Aufbau der Studie

2. Einordnung und Abgrenzung von Compliance

- 2.1 Definition von Compliance und weiterer in dieser Studie relevanter Begriffe
 - 2.1.1 Definition von Compliance und IT-Compliance
 - 2.1.2 Definition weiterer relevanter Begriffe
- 2.2 Historische Entwicklung von Compliance
- 2.3 Compliance in unterschiedlichen Branchen
 - 2.3.1 Branchenübergreifende Compliance
 - 2.3.2 Branchenspezifische Compliance

3. Aktueller Stand der Literatur

- 3.1 Aussagen zu Compliance-Anforderungen
- 3.2 Aussagen zu Compliance-Ansätzen
- 3.3 Aussagen zu Software und Anbietern
- 3.4 Aussagen zu Frameworks
- 3.5 Aussagen zu Kosten und Nutzen
- 3.6 Aussagen zu Entwicklungen im Bereich Compliance

4. Relevante Gesetze, Standards und Richtlinien

- 4.1 Verantwortliche Institutionen
 - 4.1.1 Staatliche Institutionen
 - 4.1.1.1 Deutsche staatliche Institutionen
 - 4.1.1.2 Institutionen der Europäischen Union
 - 4.1.1.3 Internationale staatliche Institutionen
 - 4.1.2 Private Organisationen
 - 4.1.3 Auswahl der relevanten Institutionen
- 4.2 Strukturierung der relevanten Gesetze, Standards und Richtlinien
 - 4.2.1 Gesetzliche Anforderungen
 - 4.2.1.1 Gesetzliche Anforderungen in Deutschland
 - 4.2.1.2 Gesetzliche Anforderungen in der Europäischen Union

4.2.1.3 Internationale gesetzliche Anforderungen

4.2.2 Standards

4.2.2.1 Deutsche Standards

4.2.2.2 Internationale Standards

5. Compliance in Verbindung mit Informationstechnologien

5.1 IT-nahe Standards

5.2 Standarderfüllung durch IT

5.3 Übergreifende Anforderungen und Umsetzung mittels Software

6. Qualitative Erhebung mittels einer Expertenbefragung

6.1 Aufbau und Ablauf der Befragung

6.2 Interviewauswertung

6.2.1 Anforderungen an die Compliance

6.2.2 Aktuelle Vorgehensweisen

6.3 Lessons Learned

6.3.1 Fazit der Befragung

6.3.2 Abgleich der Interviews mit der Literatur

7. Rentabilität von Compliance

7.1 Kosten von Compliance

7.2 Kosten von Non-Compliance

7.3 Nutzen von Compliance

7.3.1 Genereller Nutzen

7.3.2 Nutzen generiert durch die IT

7.4 Ergebnisse der ROI-Untersuchung

8. Fazit