

Grüninger, Stephan; Jantz, Maximilian; Schweikert, Christine; Steinmeyer, Roland

**Research Report**

## Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management

KICG-Forschungspapiere, No. 2

**Provided in Cooperation with:**

Konstanz Institut für Corporate Governance - KICG, Hochschule Konstanz

*Suggested Citation:* Grüninger, Stephan; Jantz, Maximilian; Schweikert, Christine; Steinmeyer, Roland (2012) : Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management, KICG-Forschungspapiere, No. 2, Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG), Konstanz Institut für Corporate Governance (KICG), Konstanz, <https://nbn-resolving.de/urn:nbn:de:101:1-2014012212342>

This Version is available at:

<https://hdl.handle.net/10419/98174>

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

# Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management

Stephan Grüninger, Maximilian Jantz, Christine Schweikert und Roland Steinmeyer

**KICG – Forschungspapiere**  
Nr. 2 (2012)  
ISSN 2198-4913

Konstanz Institut für  
Corporate Governance

Hochschule Konstanz  
Brauneggerstraße 55  
78462 Konstanz

[www.kicg.htwg-konstanz.de](http://www.kicg.htwg-konstanz.de)

## KICG-Forschungspapier Nr. 2 (2012)

### Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management

Stephan Grüninger, Maximilian Jantz, Christine Schweikert und Roland Steinmeyer

*Der folgende Artikel ist im Rahmen des Forschungsprojekts  
„Leitlinien für das Management von Organisations- und Aufsichtspflichten“  
entstanden.*

*Das diesem Artikel zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für  
Bildung und Forschung unter dem Förderkennzeichen 17044X11 gefördert. Die Verantwortung für  
den Inhalt dieser Veröffentlichung liegt bei den Autoren.*

Das KICG ist ein Forschungsinstitut der HTWG Konstanz, Brauneggerstr. 55, 78462 Konstanz.

#### Kontakt

Konstanz Institut für  
Corporate Governance  
Hochschule Konstanz  
Brauneggerstraße 55  
78462 Konstanz  
[www.kicg.htwg-konstanz.de](http://www.kicg.htwg-konstanz.de)

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

## 1 Sorgfalt – eine rechtsphilosophische Analyse

Der Begriff „Sorgfalt“ steht für *Genauigkeit, Gewissenhaftigkeit*<sup>1</sup> und drückt sich in der Verpflichtung zur Wahrung der Interessen anderer aus.<sup>2</sup> Diese Definition zum Begriff „Sorgfalt“ stellt nur auf die Wahrung der Interessen anderer ab und lässt eigene Interessen im Bereich der Sorgfalt unerwähnt. Es dürfte unbestritten sein, dass Sorgfalt auch im Rahmen eigener Interessen eine Rolle spielt (vgl. u.a. § 277 BGB, der von der Sorgfalt in eigenen Angelegenheiten spricht). Dem folgend hieße das, dass ein Betriebsinhaber dann die erforderliche Sorgfalt walten lässt, wenn er genau und gewissenhaft seine Leitungsfunktion ausübt und nicht (nur) die eigenen Interessen, sondern die Dritter – nämlich die der Gesellschaft/des Betriebes – wahrt. Möglich ist sehr wohl auch, dass sich Eigen- und Drittinteresse decken.

Das Gesetz selbst normiert für den Vorstand einer Aktiengesellschaft in der Generalklausel des § 93 AktG die bei der Geschäftsführung anzuwendende Sorgfalt. „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.“ (§ 93 Abs. 1 S. 1 AktG). Unter der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters ist dabei diejenige Sorgfalt zu verstehen, wie sie der Leiter eines Unternehmens vergleichbarer Art und Größe anzuwenden hat, der nicht mit eigenen Mitteln wirtschaftet, sondern wie ein treuhänderischer Verwalter fremden Vermögens.<sup>3</sup>

Auch bei der Unternehmensleitung haben eigene Interessen außer Acht zu bleiben. Gemäß § 76 Abs. 1 AktG hat der Vorstand unter eigener Verantwortung die Gesellschaft zu leiten. Aus der Kompetenzzuweisung erwächst dem Vorstand nicht nur das Recht, die Geschicke des Unternehmens zu leiten, sondern auch die Pflicht, diese Aufgabe wahrzunehmen.<sup>4</sup> Nach allgemeiner Ansicht hat der Vorstand daher seine Geschäftsleitung am Unternehmensinteresse auszurichten, wobei das Unternehmensinteresse sich aus den Interessen der Aktionäre, die der Arbeitnehmer, wie auch der Allgemeinheit zusammensetzt.<sup>5</sup> Der Aufzählung der zu berücksichtigenden Interessen lässt sich somit entnehmen, dass es dem Vorstand nicht gestattet ist, bei der Geschäftsleitung seine persönlichen Interessen zu verfolgen.<sup>6</sup>

Die sorgfältige Geschäftsführung eines angestellten Managers sowie möglicherweise divergierende Interessen zwischen Geschäftsleitung und Eigentümer in Einklang zu bringen, ist Gegenstand des klassischen Theorieansatzes der Corporate Governance, der Prinzipal-Agent-Theorie.<sup>7</sup> Im Vergleich zu einem eigentümergeführten Unternehmen, bei dem davon auszugehen ist, dass sich die Interessen des Unternehmers mit denen des Unternehmens decken, bestehen nach der Prinzipal-Agent-Theorie bei einer fremdgeführten Unternehmung hinsichtlich der

---

<sup>1</sup> <http://www.opentheseaurus.de/synonyme/Sorgfalt>

<sup>2</sup> <http://www.enzyklo.de/Begriff/Sorgfalt>

<sup>3</sup> Spindler, Münchener Kommentar zum Aktiengesetz, 3. Auflage 2008, § 93 Rn. 24

<sup>4</sup> Martin Oltmanns, Geschäftsleiterhaftung und unternehmerisches Ermessen, Die Business Judgment Rule im deutschen und im amerikanischen Recht, Frankfurt am Main [u.a.], 2001, 203 f.

<sup>5</sup> Oltmanns (Fn. 4), 204 f.

<sup>6</sup> Oltmanns (Fn. 4), 205 f.

<sup>7</sup> Vgl. Berle/Means 1932: *The Modern Corporation and Private Property*. New York: Macmillan; Jensen/Meckling 1976: *Theory of the Firm. Managerial Behaviour, Agency Costs and Ownership Structure*. In: *Journal of Financial Economics* (3), S. 305-360

Corporate Governance<sup>8</sup> potenziell unterschiedliche Interessen von Eigentümer (Prinzipal) und angestelltem Manager (Agent) sowie Informationsasymmetrien zugunsten des Managers. Zur Eindämmung des Ausbeutungsrisikos hat der Prinzipal entsprechende Maßnahmen zu implementieren, die für ihn jedoch auch mit bestimmten Kosten verbunden sind (sog. Agenturkosten<sup>9</sup>). Diese Kosten sollen durch eine *Good Corporate Governance* reduziert und minimiert werden. Ziel der Corporate Governance ist demnach die Sicherstellung der Organisations- und Aufsichtspflichten und somit der notwendigen Sorgfalt der Geschäftsführung.

Die Anforderungen an die Sorgfaltspflicht bemessen sich nicht nach einem einheitlichen festen Maßstab, sondern vielmehr nach der *Art und Größe des Unternehmens*, der *Zahl der Beschäftigten*, der *Konjunkturlage*, den *Zeitverhältnissen* sowie den *besonderen Aufgaben des einzelnen Mitglieds*.<sup>10</sup> Dies spricht – wie unter Ziff. 2 näher ausgeführt wird – nach dem Erfordernis, verschiedene Komplexitätsstufen herauszuarbeiten, um die jeweiligen Sorgfaltspflichten identifizieren zu können. Für den Geschäftsführer einer GmbH ist nach §43 Abs. 1 GmbHG Maßstab für seine Pflichterfüllung die Sorgfalt eines ordentlichen Geschäftsmanns, was nach herrschender Meinung dem gleichen Maßstab wie in § 93 AktG entspricht (Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters).<sup>11</sup>

Welche konkreten einzelnen Sorgfaltspflichten nun allerdings dem Vorstand/Geschäftsführer obliegen, regelt das Gesetz nur unzureichend. Insoweit ist vor allem auf die Rechtsprechung zurückzugreifen. Unbestritten ist, dass die Geschäftsleitung dafür Sorge zu tragen hat, dass sich die Gesellschaft in ihren Außenbeziehungen rechtmäßig, d.h. entsprechend den gesetzlichen und vertraglichen Verpflichtungen sowie den anerkannten Grundsätzen der Geschäftsmoral entsprechend verhält.<sup>12</sup> Um dieser Legalitätspflicht gerecht zu werden, dürfte die Geschäftsleitung eines Unternehmens nicht umhin kommen, ein Compliance Management System zu errichten, welches die Begehung von Gesetzesverstößen durch Mitarbeiter der Gesellschaft verhindern soll.<sup>13</sup>

Im Gegensatz zum „Wie“ d.h. der konkreten Ausgestaltung eines Compliance Management Systems dürfte daher das „Ob“ eines derartigen Systems nicht zur Disposition der Geschäftsleitung stehen.<sup>14</sup> Allenfalls in sehr kleinen Unternehmen / Betrieben, deren Geschäftsfelder z.B. keine großen Risiken bergen, dürfte die Pflicht zur formellen Errichtung eines Compliance Management Systems entfallen. Denn bei einer Vielzahl kleinerer Unternehmen wird die Organisationsstruktur nicht derart komplex sein, dass ein umfassendes formalisiertes System erwartet werden kann. Sehr wohl haben aber auch die Betriebsinhaber kleiner Unternehmen die

---

<sup>8</sup> Unter dem Begriff Corporate Governance wird die Führung, das Management und die Kontrolle einer Unternehmung oder Organisation durch formelle und informelle, öffentliche und private Regeln und Regulierungen verstanden. Vgl. Wieland 2005: Corporate Governance, Values Management, and Standards: A European Perspective. In: Business & Society, Vol. 44, No. 1, S. 74-93, hier S. 76

<sup>9</sup> „The costs resulting from managers misusing their position, as well as the costs of monitoring and disciplining them to try to prevent abuse, have been called agency costs.“ (Mallin 2007: Corporate Governance, 2nd Edition. New York: Oxford University Press, S. 13)

<sup>10</sup> Spindler, Münchener Kommentar zum Aktiengesetz, 3. Auflage 2008, § 93 Rn. 24

<sup>11</sup> Zöllner/Noack, Baumbach/Hueck, GmbH-Gesetz, 19. Auflage 2010, §43 Rn. 7

<sup>12</sup> Vgl. BGHZ 129, 236; Fleischer ZIP 2005, 141, 142 ff; Spindler, Münchener Kommentar zum Aktiengesetz, 3. Auflage 2008, § 93 Rn. 64

<sup>13</sup> so auch Ziemons, Oppenländer/Trölitzsch, GmbH-Geschäftsführung, 2. Auflage 2011, §22 Rn.27

<sup>14</sup> wie vor

Legalitätspflicht zu beachten und dafür Sorge zu tragen, dass sich ihre Mitarbeiter an Recht und Ordnung halten.

Die Schwierigkeit besteht daher in der Beantwortung der Frage nach dem konkreten „Wie“. Es stellen sich hierbei insbesondere Fragen wie:

- Wann ist genug der Sorgfalt?
- Wann hat die Geschäftsleitung ihrer Sorgfaltspflicht im Rahmen eines Compliance Management Systems Genüge geleistet – auch wenn neue Verstöße durch Mitarbeiter begangen werden?

Den Risikofaktor Mensch wird es immer geben. Es dürfte auf der Hand liegen, dass selbst die sorgfältigste und gewissenhafteste – und somit der Idealtyp einer Unternehmensleitung – nicht in der Lage sein wird, sämtliche möglichen Verstöße durch Mitarbeiter gegen Recht und Gesetz zu verhindern. Dies darf von einem Unternehmen auch nicht erwartet werden. Diesem Umstand werden auch die US Sentencing Guidelines gerecht, die Haftungsmilderungen bei der Sanktion von Verstößen vorsehen, falls ein Unternehmen ein angemessenes Compliance- und Ethik-Programm installiert hat.<sup>15</sup>

Geht es also bei den Sorgfaltspflichten primär darum, Schaden von der Gesellschaft abzuwenden, erscheint es naheliegend, die Sorgfaltspflichten am konkreten Risikogehalt des jeweiligen Unternehmensgegenstandes auszurichten. In der Sache dürfte es im Rahmen der Sorgfaltspflichten somit vor allem um die Reduzierung derjenigen Risiken gehen, die typischerweise in besonderem Maße dem Unternehmen (erheblichen) Schaden zufügen können.

## 2 Special Compliance Issues vs. Compliance-Komplexitätsstufen

Compliance, d.h. die Einhaltung gesetzlicher und regulatorischer Anforderungen von Soft Law und interner Regelungen,<sup>16</sup> sowie die Steuerung sich daraus potenziell ergebender Compliance-Risiken ist von essenzieller Bedeutung für den Fortbestand einer Unternehmung und somit von ausnahmslos allen Unternehmen mittels geeigneter Maßnahmen sicherzustellen. Im Hinblick auf eine angemessene und umfassende Erfüllung der Organisations- und Aufsichtspflichten durch die Leitungsorgane eines Unternehmens sowie zur Haftungsvermeidung und -milderung im Schadensfall sind vor allem die Maßnahmen zu betrachten, die der Sicherstellung des Wohlverhaltens der Organisationsmitglieder im Geschäftsverkehr dienen. Diese Maßnahmen werden in einem sog. Business Conduct Compliance Programm zusammengefasst.<sup>17</sup>

Für die Entwicklung von Leitfäden für angemessene Management-Maßnahmen im Compliance-Risikomanagement sind zwei Vorgehensweisen denkbar:

---

<sup>15</sup> USSG Manual November 1, 2010, Introductory Commentary of Chapter 8, p. 496

<sup>16</sup> Vgl. Definition des Begriffs Compliance nach Grüninger 2010: Werteorientiertes Compliance Management System. In: Wieland/Steinmeyer/Grüninger (Hrsg.): Handbuch Compliance-Management. Berlin: Erich Schmidt Verlag, 39-69, hier 39.

<sup>17</sup> Vgl. Wieland/Grüninger 2010: Die 10 Bausteine des Compliance Management. In: Wieland/Steinmeyer/Grüninger (Hrsg.): Handbuch Compliance-Management. Berlin: Erich Schmidt Verlag, 111-135, hier 114.

### *Vorgehensweise 1: Leitfäden für Special Compliance Issues*

Dieser Ansatz geht davon aus, dass bestimmte Compliance-Kernfragen (Special Compliance Issues) existieren, die Unternehmen unabhängig von ihrer Organisationskomplexität und dem Geschäftsmodell in gleichem Maße betreffen und in deren Handling, d.h. in der Ausgestaltung der entsprechenden Management-Maßnahmen, keine Unterschiede beispielsweise zwischen einem Groß- und Kleinunternehmen bestehen. Zu den bislang identifizierten Special Compliance Issues gehören:

- Verantwortlichkeit für Compliance
- Business Partner Due Diligence
- Risk Assessment (methodische Vorgehensweise allgemein sowie spezifische Ausgestaltung je nach Branche und genutzten Vertriebskanälen)
- Post Incident Compliance (Umgang mit und Konsequenzen aus einem Vorfall, Remediation, eventuelle Anpassung des CMS, Kontrolle vs. Vertrauen)
- Korruptionsvermeidung (Geschenkerichtlinie)
- Due Diligence Prozesse (Pre Merger, Post Merger)
- Freizeichnungsprozesse

Ferner ist die Thematik der Compliance im Konzern,<sup>18</sup> d.h. die Verantwortung für Compliance im Konzern sowie die Durchgriffsmöglichkeiten hinsichtlich Compliance im Konzern, als eigenes Special Compliance Issue zu diskutieren. Für jede der Special Compliance Issues ist ein spezifischer Leitfaden zu erstellen, der angemessene Maßnahmen zur Steuerung des jeweiligen Compliance-Risikos enthält.

Zusätzlich zu den Leitfäden der einzelnen Special Compliance Issues ist ein weiterer Leitfaden zu entwickeln, der Aufschluss darüber gibt, welche Maßnahmen neben den Maßnahmen zur Adressierung der Special Compliance Issues erforderlich sind, um ein umfassendes und angemessenes Business Conduct Compliance Programm zu implementieren. Dieser Leitfaden darf nicht nur eine Auflistung der notwendigen Compliance-Elemente enthalten, sondern muss Hinweise zur konkreten Ausgestaltung der einzelnen Instrumente und Prozesse im Unternehmen geben. Insbesondere muss dieser Leitfaden dem Umstand Rechnung tragen, dass es Compliance-Issues gibt, die bei Unternehmen mit höherer Organisationskomplexität in stärkerem Maße auftreten als bei Unternehmen mit geringer Organisationskomplexität und die deshalb unterschiedlicher Adressierung bedürfen (vgl. hierzu Vorgehensweise 2).

### *Vorgehensweise 2: Leitfäden für Unternehmenstypen unterschiedlicher Organisationskomplexität*

In diesem Ansatz werden die Leitfäden nicht inhaltlich an den verschiedenen Special Compliance Issues ausgerichtet (vgl. Vorgehensweise 1), sondern die Entwicklung der Leitfäden orientiert sich an der Compliance-Komplexität verschiedener Unternehmenstypen.

Hierzu ist zunächst eine Klassifizierung der zu betrachtenden Unternehmen hinsichtlich ihrer organisationalen Komplexität vorzunehmen. Der Fokus im Rahmen dieses Forschungsprojekts liegt auf Unternehmen mit Hauptsitz in Deutschland, die im sogenannten Commercial Sector

---

<sup>18</sup> Die kleinste Form eines Konzern besteht aus zwei Unternehmen: einem beherrschenden und einem beherrschten Unternehmen.

(Industrie, Handel und Gewerbe) tätig sind. Zu den bislang identifizierten, noch genauer zu untersuchenden Komplexitätskriterien gehören:

- externe Regulierung (Rechtsform, anzuwendende Gesetzgebung z.B. (SOX), etc.)
- Konzernierung des Unternehmens, Verantwortlichkeit im Konzern, Konzerndurchgriffshaftung (dezentrale vs. zentrale Verantwortung für Compliance)
- Risikolage aufgrund der Geschäftstätigkeit/Geschäftsmodell
- Internationalisierungsgrad
- Betriebsgröße
- Leitungsstruktur (eigentümer-/familiengeführt vs. Geschäftsführung durch angestellte (Fremd-)Manager)

Vorgesehen ist, in einem ersten Schritt die eingebundenen Projektpartner entlang der bereits identifizierten Kriterien einzuordnen und auf Basis dessen eine erste grobe Klassifizierung vorzunehmen, die in einem zweiten Schritt durch Einordnung weiterer Unternehmen verfeinert und verfestigt werden soll.

Die Herausforderungen dieses Ansatzes liegen erstens in der Identifizierung der relevanten Komplexitätskriterien. Zweitens kommt erschwerend hinzu, dass zwar einige der Komplexitätskriterien interdependent sind, dass sich jedoch in der Vielzahl deutscher Unternehmen mit gewisser Sicherheit für jede Kombination der Merkmalsausprägungen entsprechende Unternehmen finden lassen. Dies würde zu einer sehr großen Anzahl von Leitfäden führen. Um die Anzahl möglicher Leitfäden zu reduzieren, ist eine Priorisierung der Kriterien, d.h. die Erarbeitung einer Rangreihe der Komplexitätskriterien, denkbar. Daraus ergibt sich eine überschaubare Anzahl an Unternehmenstypen mit unterschiedlicher Compliance-Komplexität, für die im weiteren Verlauf spezifische Compliance-Komplexitäts-Leitfäden entwickelt werden. Diese Leitfäden geben Auskunft über die Entwicklung und konkrete Ausgestaltung angemessener Maßnahmen zur Erfüllung von Organisations- und Aufsichtspflichten im Rahmen eines effizienten, nachhaltigen Compliance Management.

### **3 Wirksamkeit und Angemessenheit eines Business Conduct Compliance Programms**

Von essenzieller Bedeutung für den Erfolg des Forschungsprojekts ist es, herauszuarbeiten, wann ein Business Conduct Compliance Programm wirksam ist und welche Maßnahmen/Elemente – sowie wann diese – als wirksam und angemessen angesehen werden können. Dazu werden verschiedene Standards im Bereich Compliance Management danach untersucht, ob sie Aussagen zur Angemessenheit bzw. Wirksamkeit treffen und unter welchen Umständen ein Compliance Management System demnach als angemessen bzw. wirksam gilt. Die Schwierigkeit der Aussagen zur Wirksamkeit und Angemessenheit besteht darin, dass angemessene Compliance-Maßnahmen die jeweilige Komplexität der Organisationsstrukturen berücksichtigen müssen. Da die deutsche Unternehmenslandschaft hinsichtlich der Komplexität der Organisationsstrukturen relativ heterogen ausgeprägt ist, ist es schwierig, allgemeine Aussagen über Wirksamkeit und Angemessenheit treffen zu können. Eine mögliche Herangehensweise zur Lösung dieser Herausforderung besteht darin, relevante Unternehmensgruppen zu bilden und jeweils für diese Gruppen die Angemessenheit und Wirksamkeit von Compliance-Maßnahmen genauer zu definieren.



Hierzu werden zunächst die bestehenden Standards zu Compliance Management Systemen herangezogen und im Hinblick auf folgende Aspekte analysiert:

- Welche Parallelen weisen die verschiedenen Standards bezüglich der einzelnen Elemente eines Compliance-Management Systems aus?
- Gibt es typische Risiken, die nahezu alle Unternehmen oder Unternehmensgruppen gleichermaßen identifizieren?

Auf Basis dieser Erkenntnisse und insbesondere aus den Erkenntnissen der spezifischen Risiken verschiedener Unternehmenstypen werden – wie bereits unter Abschnitt 2 dargelegt wurde – relevante Unternehmensgruppen gebildet. Für jede Gruppe ist ein sogenanntes ‚Role Model‘ Unternehmen zu entwickeln, das die jeweiligen Spezifika der Unternehmensgruppe in sich vereint.

Im Folgenden könnte für jedes Role Model Unternehmen ein „Prototyp“ eines Business Conduct Compliance Programms abgeleitet werden. Wichtige Fragen, die in diesem Rahmen insbesondere im Hinblick auf die Wirksamkeit und Angemessenheit der einzelnen Elemente zu beantworten sind, sind:

- Gibt es CMS-Elemente, die erst ab bestimmten Betriebsgrößen als erforderlich angesehen werden können – und falls ja – wie bzw. wann verändern sich die einzelnen Elemente in Bezug auf die Betriebsgröße und / oder andere Einflussfaktoren?
- Wie kann die (kontinuierliche) Wirksamkeit geprüft werden (regelmäßige Risk Assessments, Monitoring, Integrity Barometer...)?
- Wie lässt sich die Wirksamkeit vor allem der sog. weichen Kriterien des Sustainable Integrity Managements (z.B. Tone from the top, Leadership, Wertekultur etc.) prüfen? Lassen sich hierzu über Integrity Barometer zuverlässige Aussagen treffen?

Diese Fragen gilt es vor allem im Wege der Expertenbefragung (leitfadengestützte Interviews mit den eingebundenen Projektpartnern) zu klären.

## 4 Ausblick/Next steps

Zur weiteren Bearbeitung des Forschungsprojekts wird zunächst auf Basis internationaler Literatur sowie internationaler Studien zur Wirtschaftskriminalität verschiedener Umfrageinstitute und Beratungsgesellschaften<sup>19</sup> eine Identifikation und Analyse generischer Compliance-Risiken vorgenommen. Ferner werden im Rahmen einer Literaturrecherche Ansätze und Anforderungen für ein wirksames Compliance Risk Assessment aufgearbeitet und in einen umfassenden Best-Practice-Ansatz für effizientes und nachhaltiges Compliance Risk Assessment überführt.

---

<sup>19</sup> Vgl. beispielsweise Ernst & Young (2011): European Fraud Survey; Ernst & Young (2011): Global Fraud Survey; Ernst & Young (2008): Korruption – Das Risiko der Anderen; KPMG (2011): Who is the typical fraudster; KPMG (2011): Global Anti-Bribery and Corruption Survey 2011; KPMG (2010): Wirtschaftskriminalität in Deutschland 2010; Corporate Trust (2009): Studie: Gefahrenbarometer 2010; PWC (2011): Wirtschaftskriminalität 2011; PwC/Martin-Luther-Universität Halle-Wittenberg (2010): Compliance und Unternehmenskultur - Zur aktuellen Situation in deutschen Großunternehmen; Integrity Interactive (2009): 2009 Top Compliance Concerns of Global Companies.

Der Literaturrecherche schließt sich eine empirische Erhebung an. Mittels eines leitfadengestützten Interviews mit den Kooperationspartnern werden die subjektive Einschätzung generischer Compliance-Risiken sowie der Status der in den Kooperationsunternehmen implementierten Compliance Management Systeme erhoben. Die Ergebnisse der Interviews dienen der Verifikation bzw. Falsifikation und der Verfeinerung der Ergebnisse der Literaturrecherchen. Wichtige Fragen, die im Rahmen des Interviews zu erheben sind, sind:

- Welche werden als die größten Compliance-Risiken für die deutsche Wirtschaft bzw. für das eigene Unternehmen wahrgenommen?
- Mittels welcher Maßnahmen werden diese Risiken adressiert?
- Wie viele Mitarbeiter sind in den Bereichen Compliance/Interne Revision im Verhältnis zur Gesamtmitarbeiterzahl beschäftigt?
- Wie sollte das Verhältnis zwischen Mitarbeitern und dem diesen Mitarbeitern überwachenden Mitarbeiter sein? Welche Rolle spielt dabei räumliche Distanz? Wie kann die Kontrolle der Mitarbeiter im Ausland sichergestellt werden?
- Welche Qualifikation besitzen die Personen, die sich um Compliance kümmern?
- Wie sind die Organisationsabläufe im Bereich Compliance strukturiert?
- Wie ist das Berichtswesen im Bereich Compliance organisiert?
- Gibt es Leitlinien, wie Mitarbeiter mit bestimmten Situationen umgehen sollen? Wie werden die Mitarbeiter über solche Verhaltensregeln informiert?
- Ab welcher Betriebsgröße bzw. ab welcher Risikolage ist eine externe Prüfung des CMS wichtig? Wie muss eine solche Prüfung aussehen?

Die empirische Erhebung gibt Aufschluss darüber, wie Unternehmen und insbesondere deren Leitungsorgane derzeit versuchen, die Einhaltung ihrer Organisationspflichten sicherzustellen und wo Unklarheiten und Grauzonen bezüglich der Angemessenheit implementierter Maßnahmen bestehen. Ferner dienen die Ergebnisse der Verfeinerung des Best-Practice-Leitfadens für ein effizientes Compliance Risiko Management und fließen schließlich in die Entwicklung der einzelnen Leitfäden für das Management von Organisations- und Aufsichtspflichten ein.

## **Bisher sind in der Reihe der KICG-Forschungspapiere erschienen:**

Grüninger, S. „Compliance-Prüfung nach dem IDW EPS 980 – Pflicht oder Kür für den Aufsichtsrat?“ (KICG-Forschungspapier Nr. 1/2010)

Grüninger, S.; Jantz, M.; Schweikert, C.; Steinmeyer, R. „Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management“ (KICG-Forschungspapier Nr. 2/2012)