GUIDANCE FOR MANAGING ORGANIZATIONAL DUTIES AND OBLIGATORY SUPERVISION

GUIDANCE FOR MANAGING ORGANIZATIONAL DUTIES AND OBLIGATORY SUPERVISION

Prof. Dr. Stephan Grueninger, University of Applied Sciences Konstanz, Germany
Maximilian Jantz, University of Applied Sciences Konstanz, Germany
Christine Schweikert, University of Applied Sciences Konstanz, Germany

Summary

Risk management is an important task for today's businesses. As many of the recent corporate scandals demonstrate, managing the risks emerging from corporate misconduct is essential – even more with regard to the costs as well as internal and external reputational damage these risks can cause. Corporate misconduct does not only comprise risks from legal liability but also risks emerging from economic liability and social non-compliance (disregard of labour and social standards) leading to reputational damage. It is an original management task and organizational duty to manage these risks on the one hand to exculpate the company and its boards from liability but also to prevent corporate misconduct in the future.

In the paper, the authors will present a corporate compliance complexity levels model which forms the basis for the development of specific guidelines on how to appropriately manage organizational duties for various organization types especially with regard to risks emerging from corporate misconduct.

Keywords

risk management, compliance management, integrity management, organizational duty, corporate misconduct, social compliance

1. Introduction and topic

The discussion on corporate governance and the responsible management of organizations is not new. It has always been and still is one of the most important tasks for management boards: the quality of management's decisions and actions decides about the company's continued existence. In order to guarantee the continued existence of the enterprise, management's aim must be to generate and maintain the trust of the different stakeholders into the organization. However, numerous and in some cases spectacular corporate scandals of corporate misconduct and fraud[1] have shaken shareholders', society's and the other stakeholders' faith in responsible management and governance. As a consequence, legislators passed a large number of new laws and regulation as well as tightened existing legislation seeking to set higher standards for good corporate governance.[2] In order to fulfil these more stringent requirements and to restore stakeholders' trust, companies started to develop systems to help meet these challenges. These systems became part of everyday language as compliance or ethics programs. There is no explicit legal obligation to implement such a management system in order to address the requirements (cf. paragraph 4), however, experience showed that a compliance management system (CMS) constitutes a suitable instrument for managing *organizational duties*, the duties for the management of taking care of a good corporate governance.

Although many, in particular big-sized and international companies in the meantime implemented formal compliance management systems, headlines on corruption, bribery and other fraudulent offences have not ended. For example, companies like Enron, WorldCom and Arthur Anderson had *formally*

[1] Despite corporate governance and compliance management comprise a wide variety of aspects, this paper and the research project behind particularly focus on the management and prevention of corporate misconduct and fraud as these can cause tremendous legal, reputational and economic damage to a company (cf. Grueninger (2010), 55).
[2] Grueninger/John 2004, 149

implemented excellent compliance systems.[3] However, these systems failed to prevent corporate misconduct and led to legal, reputational and economic damage for the companies as well as started a discussion on the credibility and effectiveness of corporate compliance programs. Only recently, Siemens and Daimler had to face issues due to non-compliance. From the authors' point of view, many formal and rules-based compliance programs lacked one vital pillar with regard to responsible corporate governance: the systems were not built on and backed by a values-driven corporate culture and integrity. Values provide orientation for all organizational members on how to behave in specific situations in everyday business by setting distinct principles of desirable behaviour.[4] Here, integrity as the fundamental value is of particular importance as it limits the scope of action on the one hand but at the same time opening it and thereby enables the realisation of values-driven compliance management in everyday business.[5]

However, there still is no legislation on how such an *adequate* compliance management system must be designed and orientation and standards on this issue remain rather vague, too. Furthermore, most of the standards implicitly address large, capital market oriented enterprises and provide guidance on how to design a CMS in this kind of companies. Instruments designed on the basis of these guidelines (for MNCs) however, cannot be transferred to e.g. smaller companies as they do not have the necessary resources to properly implement the suggested measures. That is why, according to the prevailing opinion, the design of the elements of a CMS depends on the kind and structure of the specific enterprise who wants to implement them. Companies are faced with the challenge to implement *effective* compliance management measures and processes both to detect as well as to prevent non-compliance. With respect to prevention, it is important to not only focus on rules-based measures and control but to take an integrity and values-based approach giving guidance to desirable and moral behavior. Having implemented company-specific procedures, ensuring their effectiveness constitutes the next imponderability. Proof of the implementation of *adequate* and *effective* procedures may have a mitigating effect for the company in the event of liability. Up to now, the decision on the adequacy and effectiveness of the procedures remains with the company itself or its auditors or – in the event of liability – with the courts.

The circumstances show that there still is a great insecurity on how to implement adequate procedures in an effective CMS which contribute to good corporate governance as well as the fulfillment of organizational duties and which may have a mitigating or even releasing effect in the event of liability. There is a great necessity of more definite guidance on what constitutes an *adequate* and *effective* compliance management in order to ensure good corporate governance and the fulfillment of *organizational duties* within the limits of "reasonable assurance"[6]. In this paper the authors will present first results and insights of the research project "Guidance for managing organizational duties and obligatory supervision"[7] which aims to address this practical and research desideratum by developing specific guidelines on how to appropriately manage organizational duties depending on the respective organizational type which we construe and understand as specific "corporate compliance complexity levels". In section 2, the problem outline of the project will be presented in more detail. Then, relevant international regulation and soft law will be investigated with regard to organizational liability and reputational risks on account of corporate misconduct and social non-compliance (section 3). In section 4, the legal *duties of care* for directors and managers of German corporations will be discussed and a short overview on the state of the art in compliance management standards will be given. Section 5 of this paper gives an outline of the *Corporate Compliance Complexity Levels Model* (C3LM) which forms the basis for the compliance level specific guidelines on effective management of organizational duties with the help of an appropriate compliance management system. Finally, a conclusion will be drawn in section 6.

2. **Problem outline**

[3] Cf. Wieland 2005, 77
[4] Cf. Grueninger 2010, 50f; Paine 1994
[5] Cf. ibid, 52
[6] For the term of "reasonable assurance" cf. ISAE 3000 (http://www.ifac.org/sites/default/files/publications/exposure-drafts/IAASB_ISAE_3000_ED.pdf, 25.05.2012)
[7] The project is sponsored by the German Federal Ministry of Education and Research and led by Prof. Dr. Stephan Grueninger with support of Prof. Dr. habil. Josef Wieland (both Konstanz Institute for Corporate Governance – KICG) and Dr. Roland Steinmeyer (WilmerHale).

Risk management is an essential part of good corporate governance and an important task for today's businesses. As many of the recent corporate scandals demonstrate, managing the risks emerging from corporate misconduct and non-compliant behaviour of the organization's members is particularly essential – even more with regard to the costs as well as internal and external reputational damage these risks can cause. Corporate misconduct which includes offences like corruption, anti-trust violations and fraudulent financial reporting does not only comprise risks from legal liability but also risks emerging from economic liability and social non-compliance (disregard of labour and social standards, e.g. forced or child labour) leading to reputational damage. Therefore, on the one hand companies and their boards need to exculpate themselves from liability but also they need to prevent corporate misconduct to head off economic risks from the organization. Ensuring compliance and avoiding economic damage belongs to management's original assignments and *organizational duties*. One option to address these risks can be the implementation of a business conduct compliance programme.[8]

There is a multitude of guidelines and guidance providing information on best practice of compliance programmes and on elements that need to be implemented to manage risks emerging from corporate misconduct and non-compliance in organizations (e.g. The Bribery Act (UK) – Guidance, OCEG Red Book, COSO Enterprise Risk Management Framework, ComplianceProgramMonitor[ZfW]). However, the guidelines remain vague particularly in respect of the design of specific compliance management measures in companies of different organizational complexity (e.g. size, legal form, internationality, business sector). From the businesses' view it is important to not only list vital elements of an integrative compliance programme but also to precisely identify the organizational requirements, processes and instruments that need to be implemented to carry out the essential organizational duties and management measures in order to minimize liability risks for management and the organization itself. It is important to note that from a risk management perspective not only legal liability risks (e.g. fines, imprisonment) must be addressed but also economic liability risks caused by non-compliant behaviour must be managed. Economic liability risks reveal in reputational damage and may result in falling share prices, termination of business relations, debarments and, furthermore, may cause difficulties when recruiting high-potentials and top managers.[9] In addition, managing economic liability risks is essential with regard to social compliance issues as reputational damage caused by child labour, weak working conditions and not taking responsibility for the supply chain etc. can be tremendous. More specific guidelines on the design of effective compliance programmes which also take into account the organizational complexity of particular types of companies would help companies and their boards to manage their organizational duties more effectively.

Research in this field and the development of compliance level specific guidelines on effective compliance management, on the one hand, is of great importance for the top management and supervisory boards of corporations to provide them clear aids to orientation in respect to their corporate duties. On the other hand, the aim of the intended guidelines is to provide prosecutors and judges - who are active in criminal proceedings - a guidance for the assessment if a company and its managers have disregarded existing laws, rules or regulations.

3. International law and standards in compliance and integrity management

As described in section 1 there have been many corporate scandals in the recent years[10] with the consequence that the companies were sentenced to a fine of hundreds of millions of Euros or Dollars and executives had been laid off and ordered to compensate damages for loss[11] incurred as a result of their misconduct[12]– or in serious cases even were sentenced for several years of imprisonment.[13] Especially in

[8] Cf. Center of Business Ethics 2009
[9] Cf. Grueninger 2010, 40
[10] See for example the scandals of Enron (2001), WorldCom (2002), Siemens (2006).
[11] The compensation for loss mainly has symbolic character and is disproportionate to the damage the company suffered (cf. case Siemens: the former chairman of the Siemens board Heinrich von Pierer shall pay 5 million Euros as compensation to Siemens (http://www.zeit.de/wirtschaft/2009-12/vergleichsweise-guenstig, 31.01.2012) but the total damage Siemens suffered had been more than 2.5 billion Euros (http://www.guardian.co.uk/business/2008/dec/16/regulation-siemens-scandal-bribery, 25.05.2012).
[12] Misconduct in this context means a lack of oversight resulting from an individual responsibility.

respect to corruption and violation of social and ethical standards it should be noted that the legal and economic consequences for companies and its boards can be serious as a closer look at some of the relevant anti-fraud, anti-corruption and anti-misconduct laws shows:

1.1. German Administrative Offenses Act

Section 30 of the German Administrative Offences Act (OWiG) allows the imposition of monetary fines of up to 1 million Euros against the company itself, if company-related duties have been infringed deliberately or negligently. Furthermore, according to section 17 (4) OWiG the confiscation of financial benefits and according to section 29a OWiG the forfeiture of a sum up to the amount of the pecuniary advantage gained may be ordered which in many cases is much higher than the monetary fine.[14]

According section 130 OWiG a violation of organizational and supervisory duties can also be punished with a fine up to 1 million Euros. The fine is directed against the owner of an operation and not against the company. The first sentence of section 130 (1) OWiG provides that "Whoever, as the *owner*[15] *of an operationor undertaking*, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision."

Section 130 OWiG stipulates that the owner of an operation or undertaking is obliged to take proper supervision but does not contain any specification of such proper supervision. The second sentence of Section 130 (1) just specifies the first sentence that "The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel." In the legal literature certain organizational requirements on proper supervision were derived, which are supposed to contribute to the prevention of regulatory infringements within the company. These are the following five steps[16]:

(1) Careful staff selection

(2) Appropriate organization and task delegation

(3) Appropriate information and training of employees

(4) Sufficient supervision and control of employees

(5) Adequate intervention like threat and imposition of sanctions in case of misconduct.

However, still jurisdiction, that deals with the issue if an owner of an operation or undertaking has taken such proper supervision, is missing and remains vague as to what proper supervision, adequate design and implementation of specific measures means in practice from the opinion of the courts.

1.2. US Sentencing Guidelines

---

[13] Cf. case Enron (http://www.chron.com/business/enron/article/2-former-Enron-executives-receive-prison-terms-1898288.php, 31.01.2012) and case Flowtex (http://www.faz.net/aktuell/wirtschaft/wirtschaftskriminalitaet-hohe-haftstrafen-fuer-flowtex-bosse-152035.html, 31.01.2012).

[14] See the Siemens case: In Germany, Siemens made a deal with the prosecutors and paid in one case 201 million Euros: 1 million Euro as monetary fine according to section 30 of the German Administrative Offenses Act and 200 million Euros as confiscation of financial benefits (cf. http://www.transparency.de/Meilenstein-in-der-Aufarbeitun.1379.98.html, 31.01.2012).In the US, Siemens entered into a settlement with the Securities and Exchange Commission ("SEC") and agreed to pay $350 million in disgorgement to settle the SEC's charges, and a $450 million fine to the US DOJ to settle criminal charges. Furthermore, Siemens agreed to pay a fine of approximately $569 million to the Office of the Prosecutor General in Munich to whom the company previously paid an approximately $285 million fine in October 2007 (http://www.sec.gov/news/press/2008/2008-294.htm, 10.05.2012).

[15] *Owner of an operation or undertaking* in the context of section 130 OWiG is not defined by law. Section 130 OWiG considers *owner of an operation or undertaking* as known fixed terminology. For stock companies the *owner*s are not the shareholders but the board of directors who are entitled and obliged to manage the business and therefore have the legal *duty of care* to prevent the company of any damage.

[16] Cf. Rogall 2006, § 130 marginal note 40

According to Chapter 8 of the US Sentencing Guidelines organizations may be subject to criminal prosecution for wrongful acts of its employees. Organizations cannot be imprisoned, but can be fined, sentenced to probation for up to five years, ordered to make restitution and issue public notices of conviction to their victim or be exposed to applicable forfeiture statutes.[17]

However, Chapter 8 has also incorporated mitigating aspects arising from effective compliance programs. If an organization is able to demonstrate the implementation of an effective and adequate compliance program the potential fine range may be mitigated by the Sentencing Commission.[18] *With regard to a systematic effective compliance program the Guidelines outline the following basic principles: (1) oversight by high-level personnel; (2) due care in delegating substantial discretionary authority; (3) effective communication to all levels of employees; (4) reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal; (5) consistent enforcement of compliance standards including disciplinary mechanisms; (6) reasonable steps to respond to and prevent further similar offenses upon detection of a violation. Still, Chapter 8 also does not give further details on how to implement the principles but remains with the description of a corporate "good citizenship" model.*[19]

1.3. **US Foreign Corrupt Practices Act**

The scope of the US Foreign Corrupt Practices Act (FCPA) is interpreted widely and constitutes a risk for companies with international business with relations to foreign officials. An offence against the FCPA **anti-bribery provisions may lead to a** fine up to $2 million per violation for a company. Culpable individuals can be sentenced to a criminal fine of up to $250,000 per violation and/or sentenced up to five years in prison. Even stricter are the "books and records provisions" of the FCPA. Willful violations of these provisions can have serious consequences like a criminal fine of up to $25 million for a company and a criminal fine up to $5 million as well as imprisonment for up to 20 years for culpable individuals. For example in the year 2008, a FCPA record fine of $800 million had been imposed on the Siemens AG due to infringements against that law.[20]

As FCPA does not offer details on effective compliance management measures, guidelines on adequate compliance elements can be drawn from various Deferred Prosecution Agreements (DPA), resulting from FCPA violations issued by the US Department of Justice (DOJ). In the appendix of the DPA – colloquially referred to as "Schedule C" – the DOJ outlines vital elements to an effective compliance program with regard to the respective company. Depending on which DPA is referred to the DOJ identifies 12 to 14 areas which need to be addressed in an effective compliance program. With regard to the Alcatel-Lucent case[21], these elements are:[22] (1) requirement to have a code of conduct, with anti-corruption policy; (2) commitment from the top; (3) standards and procedures on specific areas; (4) risk assessment; (5) update and adapt; (6) senior executive involvement; (7) internal controls; (8) training; (9) internal reporting channels; (10) disciplinary procedures; (11) due diligence; (12) contract provisions; (13) periodic review & testing.

1.4. **German Criminal Code (StGB)**

According to Section 266 StGB (Embezzlement and abuse of trust) an individual who "abuses the power accorded him by statute, by commission of a public authority or legal transaction to dispose of assets of another or to make binding agreements for another, or violates his duty to safeguard the property interests of another incumbent upon him by reason of statute, commission of a public authority, legal

[17] Cf. Desio (n.d.)
[18] Cf. ibid: "The Commission did this by mitigating the potential fine range - in some cases up to 95 percent - if an organization can demonstrate that it had put in place an effective compliance program."
[19] Cf. ibid
[20] Cf. Härig 2009, 69
[21] Available at http://www.justice.gov/criminal/fraud/fcpa/cases/alcatel-etal/02-22-11alcatel-dpa.pdf (20.04.2012)
[22] Taken from a webinar series by Howard Sklar, offered by Thomson Reuters, cf. http://www.world-check.info/Schedule_C_Compliance_Webinar_US.html (20.04.2012). See also Sklar's blog at http://openairblog.wordpress.com/tag/schedule-c/ (20.04.2012).

transaction or fiduciary relationship, and thereby causes damage to the person, whose property interests he was responsible for, shall be liable to imprisonment of not more than five years or a fine."[23]

As outflow of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions Germany amended its anti-corruption provisions of the German Criminal Code in 1998: up to this time the offering, promising or granting a benefit to a *German* public official had been a criminal offence but since then the scope of the German anti-corruption provisions had been extended as well to *foreign* public officials.[24] Consequently, the tax deductibility of bribes had also been banned.

Finally in 2002, the Criminal Code once more was amended regarding the German anti-corruption provisions with the consequence that also the taking and giving bribes in *commercial practice* in international business relations is punishable by law.[25]

1.5. **UK Bribery Act**

An infringementof sections 1, 2 or 6 of the Bribery Act committed by a relevant person or company can have the consequence of imprisonment for up to 10 years and an unlimited fine for an individual and unlimited fine for a company. In contrast to German law, a company itself may be liable to prosecution under the UK Bribery Act if one of its employees commits an act of corruption, and the company failed to establish *adequate procedures* to prevent such acts. Therefore, in case an employee violates antitrust or corruption rules the company has to prove that it had established adequate measures to prevent corruption to avoid a punishable offence. The law itself includes – as well as the FCPA – a wide personal and material scope of application and can apply across international boundaries. So this law represents an additional risk for (German) international acting companies.

In section 9 (1) the Bribery Act determines that "The Secretary of State must publish guidance about procedures that relevant commercial organisations can put in place to prevent persons associated with them from bribing as mentioned in section 7(1)." These adequate measures have been comprised in a "Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)"[26] which was published in March 2011 and contains six vital principles to effectively prevent bribery: (1) proportionate procedures; (2) top-level commitment; (3) risk-assessment; (4) due diligence; (5) communication (including training); (6) monitoring & review.

1.6. **Anti-Trust Laws**

The international antitrust laws have the aim to improve market efficiency, encourage competition, and curtail unfair trade practices. Some of the prohibited business practices are amongst others price fixing, restraint of trade, and monopolization of markets. Anti-trust offences may lead to high payments of

[23] English translation of section 266 of the German Criminal Code (http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P266, 02.05.2012).
[24] Section 334 of the German Criminal Code (*Giving bribes as an incentive to the recipients violating his official duties*) : *"(1) Whosoever offers, promises or grants a benefit to a public official [remark of the authors: the German Law On Combating International Corruption of 10 September 1998 defines the term "public official" of section 334 German Criminal Code as well as any foreign public official], a person entrusted with special public service functions or a soldier of the Armed Forces for that person or a third person in return for the fact that he performed or will in the future perform an official act and thereby violated or will violate his official duties shall be liable to imprisonment from three months to five years. In less serious cases the penalty shall be imprisonment not exceeding two years or a fine..."* (the English version of the German Criminal Code is available under http://www.gesetze-im-internet.de/englisch_stgb/index.html (04.05.2012).
[25] Cf. 299 of the German Criminal Code "Taking and giving bribes in commercial practice"
[26] Available at http://www.justice.gov.uk/legislation/bribery (20.04.2012).

damages, fines and imprisonment.[27] *German corporations, furthermore, bear the risk to be excluded from German public procurement.*[28]

1.7. **International standards in compliance and integrity management**

Finally, companies are also advised to obey international standards like the OECD-Guidelines for Multinational Enterprises, the SA 8000 (Social Accountability), ISO 26000 etc. These regulations encourage companies to support and promote good and responsible corporate governance and to commit to social responsibility such as economic, environmental and social issues (e.g. respect for human rights, fair behaviour towards employees, customers, fair working conditions, ban on child labour).

Although these regulations are not directly legally binding for the companies these urgently should be respected. A violation of these international standards may result in loss of reputation which can lead to significant economic damages for the companies. So a recent study says "70% of consumers avoid buying a product if they don't like the company behind the product"[29] *and "60% of a company's market value is attributable to its reputation."*[30]

Paragraph 4.2 will address different standards and best practice guidelines on how an effective compliance program shall be designed and which elements are necessary in order to successfully fulfil organizational duties and prevent non-compliance.

2. **Companies´ need to reduce risks emerging from corporate misconduct**

Resulting from the existing (international) provisions against corporate misconduct companies are increasingly trying to reduce their liability risk and prevent misconduct as best as possible by establishing a compliance management system (CMS) to ensure compliance with laws and regulations, but also (and no less important) with organizational principles, internal rules and guidelines, the principles of good governance as well as generally accepted ethical norms.[31]In this context many companies, in particular small and medium-sized companies – which may not have established a formal CMS – ask the question, if there is a legal duty to implement a formal compliance management system. Therefore, the *duties of care* for managing directors of corporations will be investigated more closely under the respect of legal philosophical aspects.

2.1. **The legal duties of care for directors and managers of German corporations**

In general, the term "care" is defined as "serious attention or consideration applied to doing something correctly or to avoid damage or risk"[32].The laws describe various duties for managing directors[33]. According to the general clause in section 93(1) of the German Stock Corporation Law the members of the management board have to execute the care required of a prudent and conscientious manager on performing his duties. This may conform to the demands on the duty of care of the laws in other countries: Section 174 (2) of the UK Companies Act 2006 describes the duty to exercise reasonable care, skill and diligence more precisely: "This means the care, skill and diligence that would be exercised by a *reasonably diligent* person with - ...". And according to the American Model Business Corporation Act 2008 directors are expected in carrying out their duties to act in good faith, in the best interest of the corporation, and with the care that a person in a similar position would reasonably deem appropriate.[34]

---

[27] In 2010 the EU Commission in Brussels sentenced several large steel companies to a total fine of 518 million Euros (http://www.spiegel.de/wirtschaft/unternehmen/0,1518,703834,00.html, 10.05.2012); in 2007 the EU Commission fined the Siemens AG to the extent of 396 million Euros due to antitrust violations (http://www.stern.de/wirtschaft/news/kartellverstoesse-400-millionen-rekordstrafe-fuer-siemens-581063.html, 10.05.2012).
[28] Cf. Klusmann 2008, §57 marginal note 110
[29] Weber Shandwick 2012, 8
[30] Ibid, 18
[31] Cf. Center of Business Ethics 2009, 4
[32] Oxford Dictionary online (http://oxforddictionaries.com/definition/care?q=care, 30.01.2012)
[33] Cf. e.g. Section 91 of German Stock Corporation Law – organizational duty/duty to keep accounting records; sections 242 and 264 of the German Commercial Code – duty to prepare an annual report; section 174 (1) of the UK Companies Act 2006 – duty to exercise reasonable care, skill and diligence
[34] Cf. Shu-Acquaye (n.d.), 8

Although the duty of care is subject to different international laws, the legal duties for directors of German corporations arise primarily from German law.

Section 93 (1) of the German Stock Corporation Law does not define the duties of care of a manager of the board in detail so German jurisprudence and legal literature defined them more precisely. According to thisthe duty of care contains amongst others the directors´ obligation for organization and control, for corporate planning and control, financial monitoring and control etc.[35]

German law does not explicitly require companies of the commercial sector to establish a CMS. But the prevailing jurisdiction concludes that a further aspect of the duty of care of any board of management or any owner of an operation or undertaking is to comply with all laws, directives, legal norms and regulations etc.[36] This so called *obligation of legality* requires that a board of management or owner of an operation or undertaking has to establish appropriate organizational measures ensuring that himself and his employees respect all applicable laws by performing their business activities.[37] Resulting from the prevailing opinion a board of management has no discretion in decision-making concerning the question *if* he shall take according organizational measures, because without any corresponding adequate organizational measures a board of management will barely be in the position to ensure that his employees act in accordance with law. However, there are no legal binding guidelines on the question *how* such organizational structure should be carried out. Establishing and implementing a formal CMS is one option in order to assure compliance and prevent non-compliance. The question, whether the managing director is obliged to implement a comprehensive compliance program rather or not, depends on the size and complexity of a company, the diversity and importance of the rules to be followed as well as previous irregularities and misconduct within the company.[38] According to some legal literature small companies with few employees and just one managing director who is able to supervise all company´s corporate activity and holds all decision-making power shall not be obliged to establish a formal compliance organization.[39] The managing director can also meet his obligation of legality other than implementing a formal organizational compliance structure.[40] Nevertheless, here too, the management takes the responsibility that its employees act within the law and therefore must take suitable measures to ensure this.

2.2. Standards and guidelines in compliance management and resulting challenges for companies

Although there is no explicit legal obligation to implement a CMS, CMS have turned out to become best practice and a very broadly used instrument to manage legal and compliance risks as well as to ensure consideration with all the numerous provisions of law. But since the German Law does not contain specific rules in respect of implementing a CMS for commercial companies German companies are faced with the problem of how to design and establish a CMS appropriate to their organization.

There are many standards on compliance management and compliance management programmes which give an overview of the elements of an effective and efficient CMS. In the following, a short overview on some of the relevant compliance and integrity management standards will be given.

2.2.1. *OECD Guidelines for Multinational Enterprises*

The OECD Guidelines for Multinational Enterprises[41] constitute an important instrument to promote good corporate governance on an international basis. The guidelines go back to 1976 and have been comprehensively edited and amended in 2000 and 2011. They provide voluntary principles and standards for responsible business conduct in areas such as employment and industrial relations, human rights,

[35] Cf. Hoelters 2011, § 93 marginal note 42
[36] Cf. Spindler 2008, § 93 marginal note 64
[37] Cf. Fleischer 2012, § 43 marginal note 142
[38] Cf. Fleischer 2010, § 91 marginal note 51
[39] Cf. Fleischer 2012, § 43 marginal note 145
[40] Cf. ibid, § 43 marginal note 145
[41] Cf. www.oecd.org/daf/investment/guidelines (20.04.2012)

environment, information disclosure, combating bribery, consumer interests, science and technology, competition, and taxation.

All members of the OECD as well as Argentina, Brazil, Egypt, Latvia, Lithuania, Morocco, Romania and Peru have signed the Guidelines and thereby committed to urge enterprises in their country to comply with the Guidelines. The Guidelines strive to set a standard for companies; however, they are not legally binding.

With regard to effective implementation of the Guidelines all member states set up so called National Contact Points to which offenses and breaches to the Guidelines are directed. The cases are then discussed within a conciliation process with the respective company and the offense will be published in a communication of the Contact Point.

2.2.2. *OCEG Red Book*

With its Red Book the Open Compliance and Ethics Group (OCEG) provides a comprehensive integrated framework – called "GRC Capability Model" – for what they call "Principled Performance", " a holistic view that addresses the governance, management and assurance of performance, risk and compliance; each with consideration of the other"[42]. The model gives an overview on key components, elements and practices to address management actions and controls which every organization should implement and manage.

Figure 1 outlines the components as well as the different elements of the GRC Capability Model.

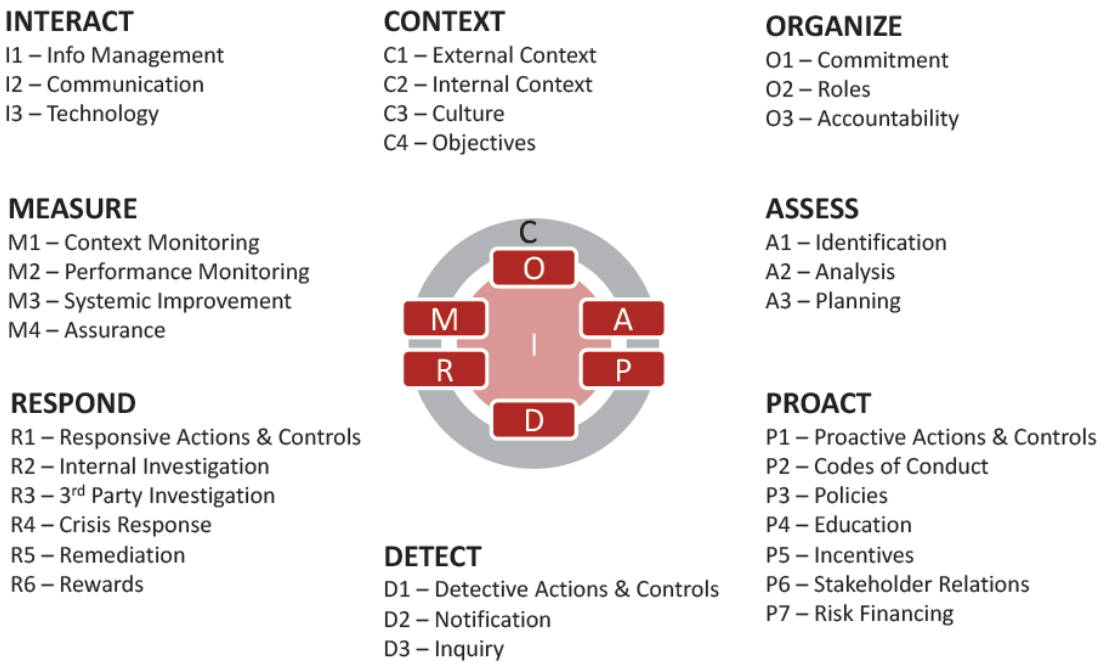

Figure 1: GRC Capability Model Elements View[43]

For each of the listed elements the Red Book provides several principles about what the element should accomplish and gives several practices and sub-practices that outline bundles of activity to effectively and

[42] Cf. OCEG 2012, 2
[43] Cf. OCEG 2012, 6

efficiently address the principles of the elements. Furthermore, the model suggests different actions and controls of proactive, detective and responsive kind in order to ensure effective governance as well as management of risk and compliance.

1.1.1. Australian Standard 3860-2006 Compliance programs

The "Australian Standard (AS) 3806-2006 Compliance programs"[44] was originally introduced in 1998 following a request from the Australian Competition and Consumer Commission. The standard outlines "principles for the development, implementation and maintenance of effective compliance programs within both public and private organizations"[45] in order to provide orientation to organizations for identification and remediation of deficiencies in their compliance program as well as for the development of processes for continual improvement in this area.

The standard is split into different sections: section 2 sets out vital principles for all effective compliance programs regardless of the complexity of the implementing organization, sections 3 to 6 outline guidance with regard to these principles, admitting that the specific measures will strongly depend on the organizational complexity. The principles addressed in the standard are: (1) commitment; (2) implementation; (3) monitoring and measuring; (4) continual improvement.

2.2.3. *IDW PS 980*

In 2011, the Institute of Public Auditors in Germany, Incorporated Association [Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW)] adopted the auditing standard "Principles of proper auditing of compliance management systems" (IDW PS 980).There is no legal duty for the companies to have their CMS audited according to IDW PS 980 but just a voluntary instrument for auditing the CMS according to PS 980.[46] Since the standard describes which elements a CMS shall include as to be considered adequate, companies can use it as orientation and guidance by establishing a CMS. According to the IDW standard the basic elements of a CMS are (1) compliance culture, (2) compliance objectives, (3) compliance risks, (4) compliance program, (5) compliance organization, (6) compliance communication and (7) compliance monitoring and improvement.

2.2.4. *ComplianceProgramMonitor^{ZfW}*

The ComplianceProgramMonitor^{ZfW} (CPM) was developed by the German Centre for Business Ethics in cooperation with the members of Forum Compliance & Integrity (former AfW – Anwenderrat für Wertemanagement^{ZfW}) in 2009.[47]It provides guidance with regard to effective and sustainable *Business Conduct Compliance* which deals with question on how an upright and responsible corporate governance can be developed and promoted. The recommendations are based on relevant international leading practice standards in business conduct compliance and draw on many years of practical experience of the member companies of the Forum Compliance & Integrity. The CPM aims "to make available principles and instructions for supervising and monitoring the development, implementation, maintenance, and improvement of an effective compliance program in both private and public organizations"[48]. It has a broad focus as it addresses not only issues which often are at the center of public debate such as fairness in competition and the fight against corruption, but also encompasses topics such as the environment, human rights, labour and social standards, and other industry-related issues.[49] In addition to guidelines and recommendations on effective compliance management, the CPM also addresses the issue of how to appropriately control and monitor a company's compliance measures that is the design, implementation and application of business conduct compliance programs in everyday business.[50]

---

[44] Available for purchase at http://infostore.saiglobal.com/store2/Details.aspx?ProductID=304437 (23.04.2012).
[45] Cf. AS 3806-2006, 2
[46] The IDW PS 980 is available by payment of a fee at www.idw-verlag.de.
[47] Available at http://www.dnwe.de/complianceprogrammonitor.html (20.04.2012). For more information on the Forum Compliance & Integrity please see http://www.dnwe.de/fci.html (08.05.2012).
[48] Cf. Center of Business Ethics 2009, 4
[49]Cf. ibid,3
[50]Cf. ibid,4

Section C of the CPM lists essential elements of a business conduct compliance program These elements are (1) leadership & corporate culture; (2) conduct principles and conduct guidelines; (3) implementation; (4) responsibility and organization; (5) communication and training; (6) risk assessment and monitoring; (7) integration in HR processes; (8) sales representatives, agents and subcontractors; (9) transparency and documentation.[51]

Besides the description of the different elements of a compliance program the CPM puts emphasis on the monitoring and audit of compliance programs in order to be able to evaluate the adequacy and in particular the efficiency and effectiveness of the program by an internal revision function or with the help of external monitors.[52] A comprehensive compliance monitoring comprises the review "whether a business conduct compliance program has been properly developed and designed (i.), effectively implemented (ii.) and whether it is used and applied (iii.) in a company's (or organization's) everyday business"[53] Whether an element of the compliance program is used and applied (*effectiveness check*) will be confirmed, if the reviewed compliance measure has been used already (at least once).

2.2.5. *Interim result*

As shown above, there are numerous standards on effective and sustainable compliance management systems.[54] However, the short analysis reveals as well that all of the standards and guidelines in compliance management comprise the same elements or kind of elements necessary for an integrated compliance management system: leadership & corporate culture, conduct principles and conduct guidelines, implementation, responsibility & organization, communication & training, risk assessment & monitoring, integration into HR processes, sales representatives, agents & subcontractors, transparency & documentation. This finding implies that all businesses regardless of size or organizational complexity need to address these core issues in order to manage their compliance risks effectively.

However, the specific design of measures for example the design and implementation of compliance training may vary considerably for companies of different organizational and compliance complexity (e.g. a multinational with more than 10.000 employees and branches in many different countries vs. a national company with only 300 employees and mainly national business operation). It was shown that the standards remain undefined regarding the question how the elements shall be designed in detail in order to implement an efficient and effective compliance program aiming for successful prevention of non-compliance as well as for mitigation in the event of liability. Another obstacle with regard to the standards is that there is a great number of standards which leads to uncertainty with regard to finding the relevant standard for a specific company and to a vagueness in how to safeguard the company from liability risks from non-compliance at the best. Figure 2 shows the challenge companies need to address with regard to effective and efficient management of organizational duties and corporate compliance.

[51] Cf. ibid, 7 ff
[52] Cf. ibid,15 ff
[53] Cf. ibid,17
[54] Please note: The list above is only exemplary and is not exhaustive.

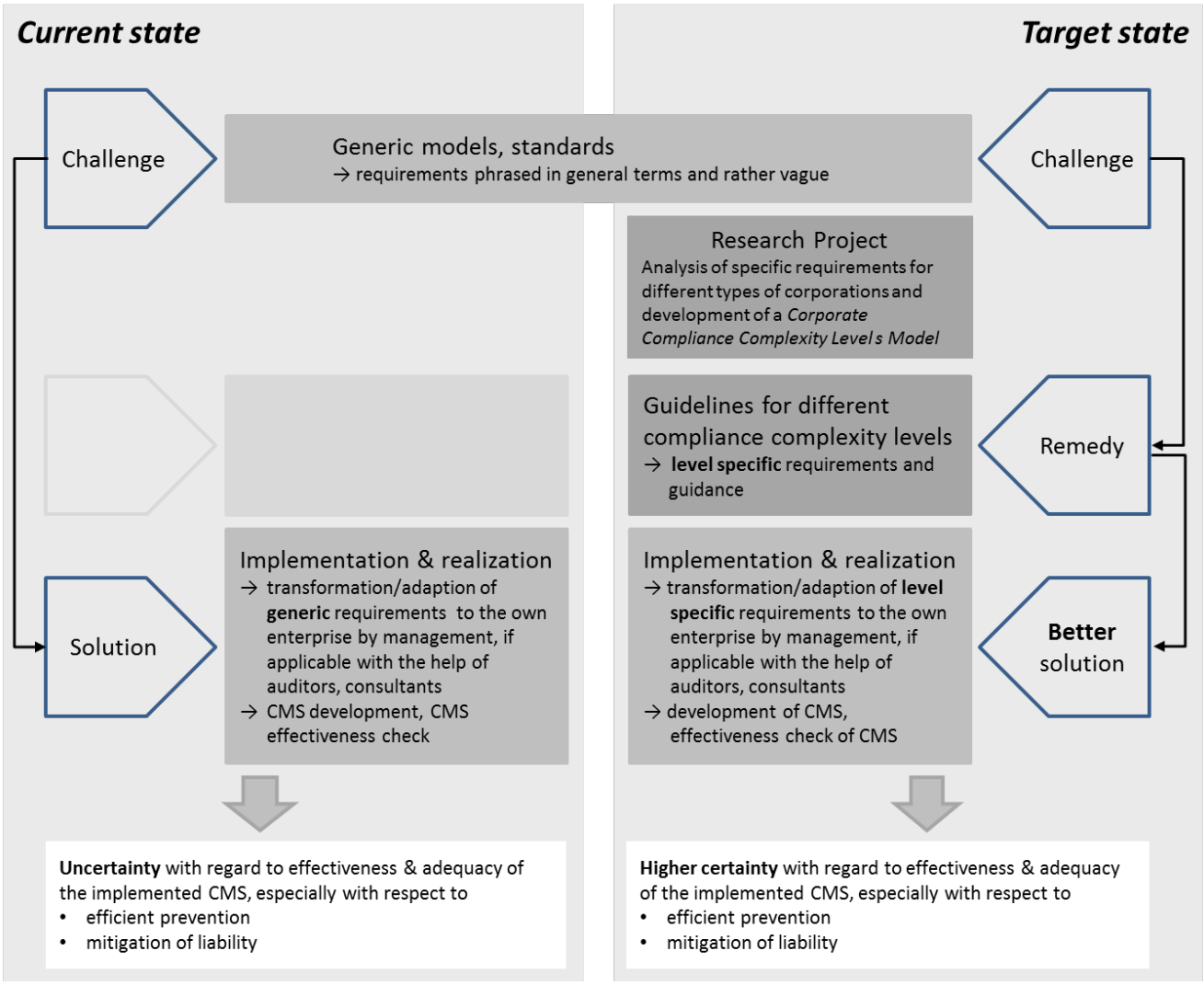

Figure 2: Current and target state of solutions to the challenge for companies and solutions with regard to the management of organizational duties and corporate compliance

In respect of effective and efficient compliance management companies are left alone with generic models and their adaption to the own undertaking which leads to high uncertainty about the effectiveness of the implemented CMS especially with regard to efficient prevention and mitigation of liability (*current state*). The request of the research project is to find a better solution to this challenge by developing specific guidelines for the effective management of organizational duties for companies of different compliance complexity levels. There is no uniform CMS that fits to all different types of companies. The efficiency of a CMS rather depends on the individual risks of a company resulting of its size, kind of (international) business, the number of employed persons, business sector etc. So an effective and efficient CMS must be designed in dependence of the compliance complexity of a corporation. The guidelines provide better orientation for the development of a level specific CMS which leads to a higher certainty about the effectiveness of the implemented CMS especially with regard to efficient prevention and mitigation of liability (*target state*). The development of the guidelines will be based on a thorough review of relevant standards in compliance management and a validation of the determined elements of an effective and efficient CMS. Then, the risks in dependence of the respective company-complexity will be analyzed. This includes a meta-study of evaluating existing studies about companies´ risks, expert interviews (Compliance Officers of companies, experts of audit and accounting firms etc.). From there, specific measures to manage these risks can be developed.

2.3. Rules-based vs. values-based compliance management and the role of integrity management

In the context of compliance management, corporations mostly focus on the prevention of offences which can be subsumed under the term fraud.[55] This is due to the high risk of these offences especially with regard to the substantial financial and severe reputational damages fraudulent actions may cause to the company. Two different categories of fraud can be distinguished: *fraud against the company* and *corporate misconduct*, as preventive measures for these phenomena must take different approaches.[56] *Fraud against the company* means white-collar crime that is directed against the company and causes damage to the company (i.e. fraud, embezzlement, theft), while *corporate misconduct* describes white-collar crime that initially provides benefits to the company like corruption to obtain a concrete contract, cartel agreements and fraudulent financial reporting. *Fraud against the company* can primarily be managed by control mechanisms to reduce the opportunity or possibility of fraudulent actions while the risks of *corporate misconduct* mainly can be mitigated by drafting and implementing of corporate values, rules and compliance compatible incentive systems and its enforcement in the daily business operations.[57]

In the past and even currently many companies have established and carried out rules-based compliance management systems focusing on the definition of rules – in some cases even only reflecting law - and informing the employees thereof.[58] Experience as well as the analysis of relevant literature has shown that misconduct of employees and managers cannot be avoided solely by instructions, rules and control regimes. An integrity-based corporate culture and incentive system are also essential for effective fraud prevention.[59] A values-based compliance management approach is a necessary complement to the rules-based approach as it provides the required guidance and orientation to employees on ethical and desirable (in the sense of compliant) behavior in daily operations.[60] Efforts in this area are often comprised under the term *integrity management*.

According to the definition of the Cambridge University *integrity* means *"the quality of being honest and having strong moral principles that you refuse to change".*[61] Integrity is the most central value for efficient compliance management[62] as it aims to support an ethical corporate culture[63], one of the essential elements to give guidance for moral behaviour and successfully prevent corporate misconduct. This can be reached by managers communicating the values of the corporation and their importance, leading by exemplary behaviour and by integrating ethical aspects into the annual objectives of each staff member and rewarding business behaviour with integrity.[64] For effective implementation of integrity management various factors are significant but the following three elements are particularly important[65]:

a) *Training programs*: First of all it is important to provide high-quality training programs in ethics and compliance management to managers, employees and if necessary also to any external party like sales agents, distributers, suppliers etc. In addition to teaching knowledge on rules of the game and legal standards it is essential to train the participants on how to behave in difficult situations like ethical dilemmas so that they learn that there are situations to which there are only "better" solutions but never "good" solutions. Furthermore, participants need to be given possible courses of action and strategies so they are able to handle difficult situations in their own area in an ethical way.[66]

---

[55] Cf. Grueninger 2010, 45
[56] Cf. ibid, 44
[57] Cf. ibid, 44
[58] Cf. ibid, 59
[59] Cf. Paine 1994; Schweikert/Grueninger 2012
[60] For the two approaches cf. Weaver/Treviño 1999; for further information on values management in enterprises cf. Wieland/Grueninger 2003
[61] http://dictionary.cambridge.org/dictionary/british/integrity_1?q=integrity (09.05.2012)
[62] Cf. Grueninger 2010, 53
[63] Cf. Fuerst 2010, 348
[64] Cf. ibid, 348; Treviño/Brown 2004
[65] In detail cf. Grueninger 2011
[66] Cf. ibid, 10

b) *Incentives*: The second success factor requires a clear attribution of compliance and integrity to the line responsibility. Neither the compliance organization nor the chief compliance officer is responsible for the ethics of the business but the individual managers are. It is important to provide incentives which promote the commitment of the managers to enforcing that topic in their own areas of responsibility.

c) *Leadership ethics*: The compliance culture and leadership ethics must be developed long-term. One option to foster values and culture is to carry out employee questionnaires about the "ethical climate" within the company and to take consistent disciplinary action in case of serious misconduct even if the misconduct had been done by an "important and deserved" manager. All this will only be successful, if the top management and supervisory executive bodies (i.e. management board and supervisory board) set a good example and live an "uncompromising integrity".

5. **Corporate Compliance Complexity Levels Model (C3LM)**

Compliance which shall be specifically defined as the compliance with legal and regulatory demands, with soft law and company internal rules[67] as well as the control and management of risks emerging from non-compliance is essential for a company's existence and future business success. Both, compliance and compliance risk management must be ensured by means of suitable processes and measures by all companies without exemption. With regard to an integrative and appropriate performance of organizational and supervisory duties by the management as well as with regard to prevention and limitation of liability in case of damage, it is necessary to especially examine those measures serving to ensure good conduct and behaviour of the organisation's members in everyday business. These measures are integrated in a so-called business conduct compliance programme.[68]

In order to develop specific guidelines on how compliance management elements should be designed for different types of businesses, the companies to be examinedare classified into different complexity levels. The analysis will focus on businesses of the commercial sector (industry, commerce and trade) with their head offices in Germany. The classification is based on the organizational and compliance complexity of the businesses. In a first screening the following criteria were identified which have an influence on the organizational complexity of a corporation:

- *Legal form of a company*: Depending on the legal form a company has to comply with different acts and regulations. Furthermore, the legal form affects the organization structure (i.e. certain types of companies have to appoint a supervisory board for the company)

- *Multinational concerns*: Not only local but also international law and regulations have to be observed. In a group of companies different types of organizational integration and responsibility models exist (i.e. central vs. decentralized responsibility for compliance). In a multinational environment, the number of generic compliance risks will increase the more complex the company/multinational concern is and the more difficult it is for these undertakings to institute an adequate and effective risk management (identifying the risks, avoiding or mitigating risks).

- *Degree of internationalization*: Enterprises with international/worldwide operations face the risk of different laws, directives and regulations (i.e. FCPA, UK Bribery Act etc.). Also, compliance risks increase depending on in which geographical regions a company does business.

- *Company size*: The larger a company the more complex it becomes with regard to its structure and organisation. It can be expected that along with the increasing size of a company (increasing number of employees, turnover etc.) it will become more difficult for management to oversee the undertaking and to fulfil the organizational duties.

[67] For the definition of the term compliance cf. Grueninger 2010, 39
[68] Cf. Center of Business Ethics 2009, 4

These criteria – which might be supplemented by further criteria – affect companies' risk exposure and form the basis of the Corporate Compliance Complexity Levels Model (C3LM).Due to the high heterogeneity of businesses the number of classes emerging from these complexity criteria theoretically is infinite. However, in order to develop a manageable model of compliance complexity levels the number of company classes needs to be limited. The classification in a particular compliance complexity level will depend on the score a company reaches on account of the ranking in the different complexity criteria. Figure 3 shows a concept of the intended C3LM. Considering the criteria above it can be concluded that enterprises exceeding a certain size need a formal CMS to implement effective prevention of corporate misconduct and to ensure reduction of liability and damages which result from legal infringements/misconduct and also from economic and social non-compliance. However, the design of the CMS elements may vary depending on the complexity level.

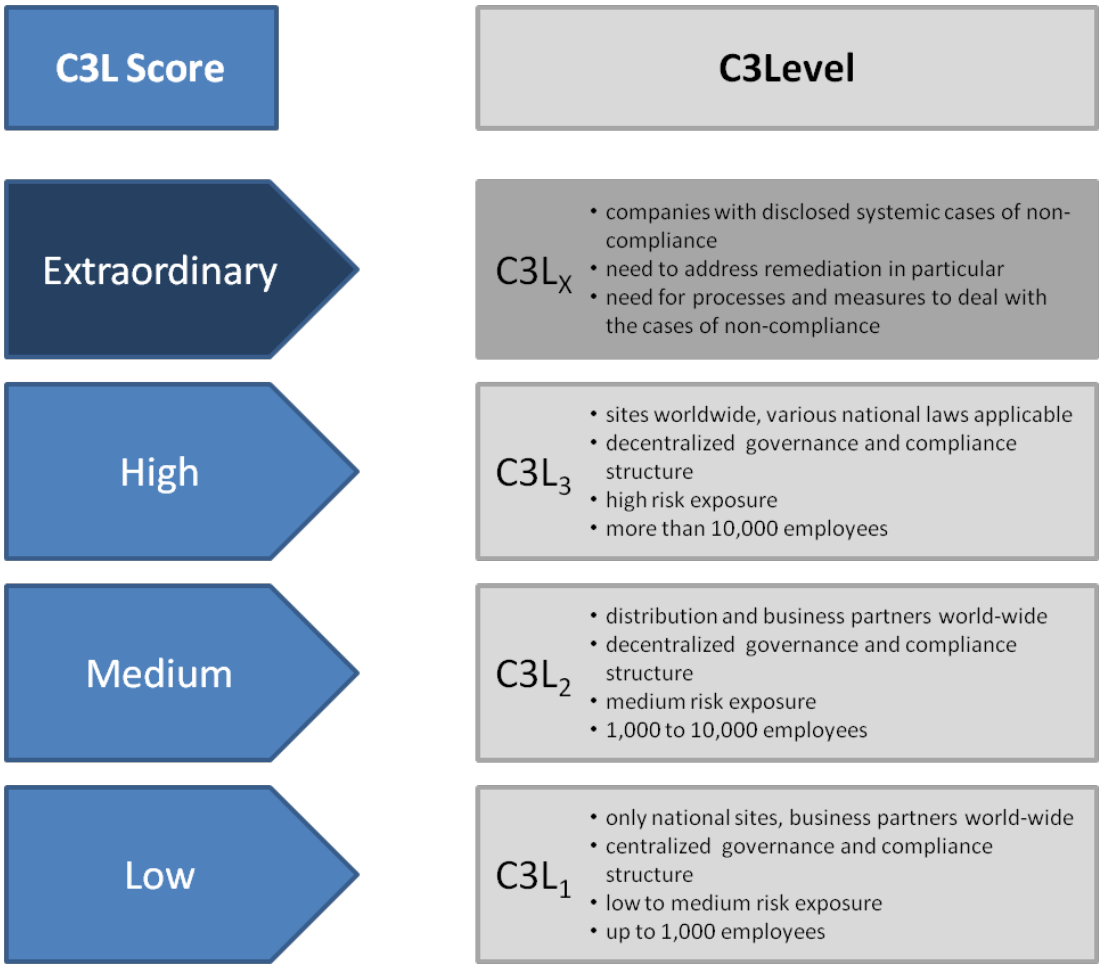

Figure 3: Corporate Compliance Complexity Levels Model (C3LM)

For each compliance complexity level a role model company as well as role model specific compliance complexity guidelines will be developed. These guidelines provide information on the development and design of appropriate compliance management measures performing organizational duties in line with an efficient, sustainable business conduct compliance programme and shall prevent corporate misconduct

and economic damage as well as serve as a reference for businesses and jurisdiction in the event of liability.

However, there are also some weak points which shall be described in short. It should be noted that there are no two enterprises alike. For that reason one bears the risk designing wrong or inappropriate classifications of companies with the consequence designing inappropriate Corporate Compliance Complexity Levels Models. However, it must be considered that due to the variety of company structures today management, (internal and external) auditors, prosecutors and judges, shareholders and stakeholders may have difficulties in evaluating the adequacy and effectiveness of a CMS in a company with a certain individual organization. The C3LM aims to provide an orientation for closing the gap between different organizational structures and the question of how a CMS must be designed to be considered as appropriate and effective.

Conclusion and outlook

Corporations have a need for detailed guidelines on how to design and implement appropriate and efficient compliance management measures in order to prevent non-compliance and reduce their risk of legal and economic liability. Existing laws and standards are too unspecific regarding the question how elements of the CMS have to be designed in detail. The presented research project strives to contribute in closing this gap by developing guidelines in appropriate and efficient compliance management for companies of different organizational complexity (so-called compliance complexity levels). With this paper the authors aim to present the research theses with regard to the management of organizational duties and discuss first research results and the idea of the Corporate Compliance Complexity Levels Model as a basis for complexity level specific guidelines for the management of organizational duties with a broad scientific audience. These guidelines may contribute to start off a broad discussion between companies, auditors but also public prosecutors and judges on appropriate and effective management of organizational duties to prevent corporate misconduct as well as legal and economic liability. Starting such a *multi stakeholder dialogue* between courts and judges, politics, NGOs and industry could be an intended result of the development of a follow-up research project. In the end the guidelines may serve as a basis for a standard legislation and companies can refer to in the event of liability.

Literature

Centre of Business Ethics (Ed.) (2009): ComplianceProgramMonitor^{ZfW}, discussed and developed by the Forum Compliance & Integrity (formerly AfW - Anwenderrat für Wertemanagement^{ZfW}), edited by Josef Wieland, Chairman Forum Compliance & Integrity, and Stephan Grüninger, Director Forum Compliance & Integrity for the Centre of Business Ethics. See: http://www.dnwe.de/complianceprogrammonitor.html?file=tl_files/ZfW/ZfW-CPM-en.pdf (27.01.2012)

Desio, P. (n.d.): An Overview of the Organizational Guidelines. See: http://www.ussc.gov/Guidelines/Organizational_Guidelines/ORGOVERVIEW.pdf (23.01.2012)

Fleischer, H. (2012): In: Fleischer, H./Goette, W. (Eds.): Münchener Kommentar zum Gesetz betreffend die Gesellschaften mit beschränkter Haftung – GmbHG (Band 2,1st Ed.). München: Beck, § 43

Fleischer, H. (2010): In: Spindler, G./Stilz, E. (Eds.): Kommentar zum Aktiengesetz (Band 1, 2nd Ed.). München: Beck, § 91

Fuerst, M. (2010): Werteorientiertes Compliance Management System. In: Wieland, J./Steinmeyer, R./Grueninger, S. (Eds.): Handbuch Compliance-Management. Berlin: Erich Schmidt, pp. 333-358

Grueninger, S., John, D. (2004): Corporate Governance und Vertrauensmanagement. In: Wieland, J. (Hrsg.): Handbuch Wertemanagement. Hamburg: Murmann, pp. 149-177

Grueninger, S. (2010): Werteorientiertes Compliance Management System. In: Wieland, J./Steinmeyer, R./Grueninger, S. (Eds.): Handbuch Compliance-Management. Berlin: Erich Schmidt, pp. 39-69

Grueninger, S. (2011): Integrity Management. In: Hernsteiner 02/2011, pp. 9-10

Haerig, N. (2009): Der US Foreign Corrupt Practices Act (FCPA). In: ZCG 02/2009, pp. 67-70

Hoelters, W. (2011): In: Hölters, W. (Ed.): Aktiengesetz Kommentar (1st Ed.). München: Beck/Vahlen, § 93

Klusmann, M. (2008): In: Wiedemann, G. (Ed.): Handbuch des Kartellrechts (2nd Ed.). München: Beck, § 57

OCEG (Ed.) (2012): OCEG Red Book – GRC Capability Model™. See: http://www.oceg.org/RedBook (23.04.2012)
Paine, L.S. (1994): Managing for organizational integrity. In: HBR, March/April, pp. 106-117
Rogall, K. (2006): In: Senge, L. (Ed.): Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten (3rd Ed.). München: Beck, § 130
Schweikert, C./Grueninger, S. (2012): Anreizsysteme als Element des Anti-Fraud-Management in mittelständischen Unternehmen. In: Zeitschrift für Corporate Governance, 2/12, pp. 82-87
Shu-Acquaye, F. (n.d.): American Corporate Law: Directors' fiduciary duties and liability during solvency, insolvency, and bankruptcy in public corporations. See: http://www.uprblj.com/wp/wp-content/uploads/2011/05/2-UPRBLJ-1.pdf (27.01.2012)
Spindler, G. (2008): In: Goette, W./Habersack, M./Kalss, S. (Eds.): Münchener Kommentar zum Aktiengesetz (Band 2, 3rd Ed.). München: Beck/Vahlen, § 93
Standards Australia (Ed.) (2006): AS 3806-2006 Compliance programs. Available for purchase at http://infostore.saiglobal.com/store2/Details.aspx?ProductID=304437 (23.04.2012)
Treviño, L.K./Brown, M.E. (2004): Managing to be ethical. In: Academy of Management Executive, Vol. 18, No. 2, pp. 69-81
Weaver, G.R./Treviño, L.K. (1999): Compliance and values oriented ethics programs. In: Business Ethics Quarterly, Vol. 9, No. 2, pp. 315-335
Weber Shandwick (Eds.) (2012): The company behind the brand: in reputation we trust. See: http://www.webershandwick.com/Default.aspx/AboutUs/PressReleases/2012/SeventyPercentofConsumersAvoidProductsIfTheyDislikeParentCompanyWeberShandwickSurveyFinds (27.01.2012)
Wieland, J. (2005): Corporate Governance, Values Management, and Standards: A European Perspective. In: Business & Society, Vol. 44, No. 1, pp. 74-93
Wieland, J./Grueninger, S. (2003): Values Management Systems and their Auditing. In: Wieland, J. (Ed.): Standards and Audits for Ethics Management Systems. Berlin et al.: Springer, pp. 119-147