RETHINKING COMPLIANCE – ESSENTIAL CORNERSTONES FOR MORE EFFECTIVENESS IN COMPLIANCE MANAGEMENT*

Stephan Grüninger & Lisa Schöttl

AUTHOR

Stephan Grüninger is Professor for Managerial Economics at the University of Applied Sciences Konstanz (HTWG), Germany. He is Director of the Konstanz Institute of Corporate Governance (KICG) and the Center for Business Compliance & Integrity (CBCI). In addition, he is director of the Forum Compliance & Integrity (FCI) and the Forum Compliance Mittelstand (FCM) which serve as active forums for discussions and exchange of experiences for managers who are responsible for the implementation and realization of Integrity and Compliance Management. He is one of the editors of the German book "Handbook Compliance-Management". From 2002 to 2009, Stephan Grüninger worked in the field of management consulting and advisory, focussing on anti-fraud and Compliance Management as well as fraud investigation; in his last position before being appointed Professor at the HTWG he was a Partner at Ernst & Young (EY) Germany.

Lisa Schöttl is a Senior Consultant in the Risk Consulting unit at PwC. She wrote her doctoral thesis on the topic of Integrity Management in business. Lisa Schöttl completed her studies in Political Science, Management and Business Ethics at the universities of Konstanz, Jena (Germany) and Berkeley (California). From 2013 to 2016 she worked as Project and Institute Manager with Prof Stephan Grüninger at the Center for Business Compliance & Integrity (CBCI) and the Konstanz Institute of Corporate Governance (KICG) in the area of Governance, Compliance & Integrity Management.

* *This article is a revised and extended version of the German article "So geht das nicht – Compliance muss neu gedacht werden: Sechs Thesen für mehr Ernsthaftigkeit und Glaubwürdigkeit im Compliance-Management" by Stephan Grüninger which was published in Compliance Manager 1/2016.*

ABSTRACT

In the past Compliance Management has often failed, the Volkswagen emissions scandal just being one prominent example. Not everything has to be reinvented, and not everything that companies have done in the past regarding Compliance is wrong. But it is about time to think Compliance in new ways. What does "Compliance Management 2.0" really depend on? The following article aims at laying out the cornerstones for enduring effective Compliance which amongst others comprises sincerity and credibility and a moral foundation. Furthermore, the commitment and role model behavior of top managers and the training of line managers are crucial for the effectiveness of any Compliance Management System (CMS). Ultimately, for Compliance to function efficiently the efforts must be adequate for the respective company and realistic regarding the achievable goals.

TABLE OF CONTENTS

I. INTRODUCTION: COMPLIANCE 1.0 DID NOT WORK UND CANNOT WORK

Several past and recent real-life cases illustrate that non-Compliance can often not be prevented despite the existence of professional wide-spread corporate Compliance programs in the respective organizations. Already the textbook-case number one regarding bad corporate governance and corporate ethics, Enron, which was uncovered in October 2001 is a prime example for excessive accounting fraud. It exemplifies that common Compliance programs do not seem to be able to prevent misbehavior in and by companies: „Enron had an extensive and award-winning code of ethics and corporate governance structure. [...] The problem was failure to follow these policies and to develop an ethical, law-Compliance culture within the company."[1]

A not less startling case is the Siemens corruption scandal. It was uncovered in December 2006 and resulted in about € 1.3 billion of paid bribe money, until today an estimated financial damage of € 3 billion for fines and penalties as well as fees for consultants and lawyers and further costs for the internal investigation. This does not even include the so called "management attention", that is the costs for the time of managers and employees invested in interrogations, in revising the Compliance system (Compliance remediation) and applying it to their daily work. "When I started working at Siemens, I analyzed the existing Compliance structure at first. In fact all relevant rules were existent on the enterprise level, but they were not broken down sufficiently in the operational areas", said Dr. Andreas Pohlmann at the beginning of 2008 at a conference – more than one year after uncovering the until then biggest (known) corruption scandal in the economic history. "The ethics rules lay in the drawer, Compliance was a lip service."

Not least Volkswagen (VW) must be mentioned as the company did already have to deal with a veritable corruption case in 2005 and the following years, besides the recently uncovered emissions scandal. As is known, the issue at that time was that work council members had received illegal benefits which included luxury travels and services from prostitutes as well as illegitimate bonuses to the chairman of the work council which had been authorized by the chief human resources officer and labor director (member of the executive board). The momentous decision in the engine development at the headquarters of the company in Wolfsburg was made just at the same time. This then led to the so called "Volkswagen emissions scandal" ten years later. The implemented Compliance structures and measures following the scandal in 2005 were apparently not of a kind that they could prevent committing offenses of environmental laws respectively uncover this misbehavior which is now shaking to the very foundations of VW. Instead in 2013 VW was still listed as a leading company regarding the completeness of their emission state-

1 FREDERICK D LIPMAN & L. KEITH LIPMAN, CORPORATE GOVERNANCE BEST PRACTICES – STRATEGIES FOR PUBLIC, PRIVATE, AND NOT-FOR-PROFIT ORGANIZATIONS, 198 (2006).

ments and their climate protection efforts.[2] So far the VW case is not even slightly clarified, also not what the failure of the CMS or the Compliance organisation exactly was. Nevertheless, it is likely that here too there existed a Compliance system that didn't work. According to reports voices that laws were broken were numerously raised, but they didn't get through to the Chief Compliance Officer or the management board. Or did they?

Anyway, all three cases show more than clearly that companies can get into difficult situations when outdated Compliance 1.0-structures[3] are in place. Enron had implemented a code of conduct and Compliance-structures that were even award-winning, Siemens too had "all necessary Compliance rules" (which is not self-evident at the turn of the millennium) and probably one of the best CMS of big industry in Germany. And in a phase of setting up Compliance structures after a veritable Compliance crisis in 2005 the Volkswagen group even managed to provide for the conditions that led to the VW emissions scandal one decade later – this can be called "maximum credible Compliance accident" without exaggeration.

One could have also chosen ThyssenKrupp (corruption and cartels scandal), Deutsche Bank (money laundering, Libor/Euribor manipulation, fraud in the business of mortgage loans, violation against sanctions etc.) or HSBC (money laundering, assistance in tax evasion etc.) and many more companies as examples. They all have in common that the misbehavior was mostly "systematic misbehavior". But this is exactly what Compliance systems should make impossible. This also makes clear that Compliance Management Systems will never be designed in a way that every single case can be prevented or uncovered, but there definitely are ways to foster the effectiveness of Compliance. These aim at establishing sincere and credible corporate Compliance efforts which are better suited to prevent systematic misbehavior than the old Compliance 1.0 systems.

II. CORNERSTONES FOR ENDURING EFFECTIVE COMPLIANCE

A. Sincerity and Credibility

Compliance 1.0 systems did not work in many cases in the past, i.e. systematic misbehavior couldn't be prevented respectively revealed. So far, so bad. But why did or rather why do Compliance systems not function so often in practice? The reasons obviously vary from case to case. Yet the negative empirical indications suggest a lack of sincerity

---

2 Carbon Disclosure Project: Global 500 Climate Change Report, 8 (2013) (https://www.cdp.net/cdpresults/cdp-global-500-climate-change-report-2013.pdf).

3 For the difference between „Compliance 1.0" and „Compliance 2.0" also see an interview with Donna Boehme, *US-Expertin zu Dieselgate: Compliance bei VW ist veraltet*, JUVE Verlag für juristische Information GmbH (Oct. 26 2015), http://www.juve.de/nachrichten/namenundnachrichten/2015/10/us-expertin-zu-dieselgate-Compliance-bei-vw-ist-veraltet.

and credibility as a cause for the failure of Compliance Management. Both factors, sincerity and credibility, are – as is shown – connected and depend on each other.
The term sincerity refers to an attitude, a disposition with which something is done. Sincerity is threatened by carelessness, superficialness and occasionally also by dilettantism. If one is "sincere", then for the area of Compliance Management this certainly means that measures are only chosen in such a manner that the goal aimed at – the prevention of systematic misbehavior (plus revealing and stopping individual violations) – can potentially be reached. Technically spoken this concerns the appropriateness and functional effectiveness of Compliance systems. Whether Compliance measures are accepted, implemented or followed, whether one has trust in them or not, depends on whether they are being seen as credible. The spectrum of stakeholders who do or don't assign credibility can reach from the own employees (Compliance with a guideline or a business process), over the auditors that examine the CMS as well as customers and business partners up to government agencies (e. g. public prosecution department). If credibility is not transported, stakeholders might get the impression that the Compliance rules and measures are hypocritical, that the company is just pretending its sincerity regarding Compliance.

The consciously ineffective design of a CMS by the management is just one possibility which presupposes sound knowledge of the "criteria of sincerity" on the part of the decision-makers (management board). After all it is possible that this knowledge is not present or is incomplete – the wrong decisions regarding the design of the CMS are made in good faith in their effective implementation. If one thus delimits the "scope of failure" in this still young management topic, then, at one end, it is conceivable that a management board knows exactly what the Compliance risks are and how to mitigate them, but makes decisions concerning the CMS that guarantee its failure. Or – that would be the other end of the scope – an ethically motivated, but bad informed management board makes similarly inapplicable decisions that likewise result in failure of the CMS. Motives and competences, hence wanting and knowing how, play a crucial role here and are not only imaginable, but probably also empirically existent in every possible mix ratio.

A well designed, thus sincerely implemented and therefore credible CMS focuses on promoting the motivation for ethical and legal behavior while at the same time training the competences of the organization and its members. The realization of workshops with managers on the topic of "Compliance & Integrity", in which ethical or Compliance-oriented conflicts or dilemmas are integrated, is essential for enabling decision-makers to handle such conflicts. The training should be designed in a way that participants would have to work on real-life cases for which possible solution strategies have to be found and presented. The discussion of such cases should concentrate less on concrete solutions but focus more on sharpening the attention for moral topics in business and training the decision-making process. The individual's capacity to balance arguments and reasons and judge in appropriate and morally sound ways should be strengthened, also by learning how to integrate different points of view on a topic. In this context Werhane and Moriarty speak of moral imagination which is needed for creatively solving such cases and should be fostered in business: „Moral imagination

enables managers to recognize a set of options that may not be obvious from within the overarching organizational framework; evaluate these options from a moral point of view; and actualize them."[4] Such competences should be trained in regular workshops, but of course also by good leadership.

In daily business, relevant information concerning compliant behavior is often – consciously or unconsciously – overlooked, especially if it serves the interests of the respective person to stay ignorant about certain facts. Such "motivated blindness"[5] can be prevented when leaders consciously use moral language and speak of fairness or honesty in business decisions which stimulates ethical reflection of the situation.[6] The strengthening of ethically sound principles and decision-making frameworks is especially important since research has shown that non-compliant behavior is very often coupled with neutralizing strategies on part of the agent which aim at justifying a certain illegitimate or illegal behavior.[7] In the corporate context such neutralizing techniques such as pointing to a higher authority or to more valuable goals in order to legitimize the own misbehavior is especially dangerous if such a rationale is adopted collectively in a department or the whole company.[8] Compliance workshops where the problem of neutralizing strategies is discussed by using cases taken from the working context of the personnel to be trained can help destabilize such mindsets and rationales.[9] Ultimately, this is a major leadership task which has to be supported by corporate culture in general in order to lead to the desired results.

The positive effect of such Compliance trainings is, on the one hand, that it enhances the competences of ethical-normative reflection and sound decision-making in conflict situations. On the other hand, it "forces" managers to position themselves (in the best case up to the management board and the supervisory board). The managers have to "put their cards on the table" and thereby automatically reveal their true motivation; if they cheat and just pretend their integrity in the training situation, they will be exposed as "noncredible" in foreseeable time and lose their authority as leaders. Of course, such trainings can ultimately only be successful if the strategies and principles to deal with ethically challenging situations are systematically integrated into daily business. As Paine states in her book Value Shift: "Validation occurs through practice and over time as the

---

4 PATRICIA H. WERHANE & BRIAN MORIARTY, MORAL IMAGINATION AND MANAGEMENT DECISION MAKING, 3 (2011).

5 Max H. Bazerman & Ann E. Tenbrunsel, *Ethical Breakdowns. Good people often let bad things happen. Why?,* April, HARVARD BUSINESS REVIEW, 59, 61 (2011).

6 LINDA K. TREVIÑO & KATHERINE A. NELSON, MANAGING BUSINESS ETHICS – STRAIGHT TALK ABOUT HOW TO DO IT RIGHT, 101 (1999).

7 This phenomenon can be traced back to Festinger's theory of cognitive dissonance; LEON FESTINGER, A THEORY OF COGNITIVE DISSONANCE (1957).

8 Hendrik Schneider, *Cognitive Dissonance As A Prevention Strategy – Considerations on the Prospects of Neutralizing the Techniques of Neutralization,* COMPLIANCE ELLIANCE JOURNAL, 18, 29 (Vol.3 No. 2 2017).

9 Ibid, 206.

principle is seen to be an integral and operative force in the organization's activities."[10]

A further example for fostering sincerity and credibility of the Compliance endeavors is the use of an "Integrity Barometer" for measuring the state and quality of the implementation of a CMS and the ethical climate in a company. It should include questions on the role model behavior of managers, the credibility of the management board regarding Compliance activities etc. Such a measuring tool shall not be misunderstood as an exact method for objectively detecting the state of a company concerning Compliance at a certain point in time, but as a dynamic technique that shows trends and developments and gives indications to special problems and to methods of their resolution. An "Integrity Barometer" should focus on questions regarding the implemented management system and the corresponding behavior in the company (see fig. 1).[11]

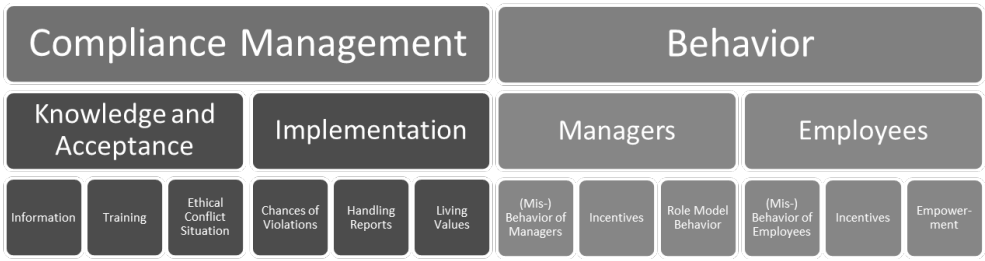

Fig. 1: „Integrity Barometer"

Already the courage of executive management to question managers and employees anonymously testifies their sincerity in this regard – provided that at least some knowledgability on the part of the decision-makers is given and the posed questions are relevant. After all one has to anticipate that the feedback will also illuminate critical points in the corporate and employee behavior and thus consequences have to be drawn. By professionally implementing an "Integrity Barometer" the company respectively the management board communicates that one is sincerely striving towards a successful Compliance Management. This signalized sincerity produces credibility on the part of the stakeholders. Such a recursive relationship between sincerity and credibility also applies to a further important Compliance instrument, the whistleblower system. Companies that commit themselves to implementing, communicating and monitoring such a system signal and actualize sincerity and receive credibility – because and insofar as they have to follow reports on grievances and uncover and stop possible misbehavior. A whistleblower system that is designed and implemented by every trick in the book takes

[10] LYNN S. PAINE, VALUE SHIFT – WHY COMPANIES MUST MERGE SOCIAL AND FINANCIAL IMPERATIVES TO ACHIEVE SUPERIOR PERFORMANCE, 177 (2003).

[11] The Center for Business Compliance & Integrity (CBCI) has developed an approach for an "Integrity Barometer" in cooperation with COMFORMIS (a brand of digitalspirit GmbH). Also known is the so called "Integrity Thermometer" of Prof. Muel Kaptein.

the management board the possibility or at least makes it much more difficult to refuse knowledge of certain behaviors that could bring the company illegal advantages, like business contracts (e. g. by bribing end customers through sales agents) or higher profit margins (e. g. illegal price fixing of retailers). The management will more likely come to know such misbehavior that might provide the company with illegal benefits and therefore has to deal with it.

The appointment of the Chief Compliance Officer (CCO) may serve as a last example regarding its effects on credibility. Is a highly competent, in the company and from business partners respected and to some extent "powerful" person appointed and is she equipped with extensive authority and resources? Or is someone appointed as CCO for whom one could not find a suitable position for quite a while and who is considered as "harmless"? Is it someone who shall "form" Compliance at the fourth or fifth level in the organization and as a start has to request his journey for a "Compliance Check" of a business partner from his supervisor? Even if these questions describe extremes this does not change the fact that the appointment of the CCO is connected with the sincerity and credibility of Compliance Management in the above described manner: A weak CCO cannot manage an (intended) strong CMS. An (intended) weak Compliance Management doesn't tolerate a strong CCO. By appointing a strong CCO the management board signalizes that Compliance Management has priority and shall succeed. This signalized self-enforcement in turn creates credibility inwards (employees) and outwards (external stakeholders). The CCO should directly take care of a certain subset of all Compliance topics with regards to content (as far as possible the high-risk topics which in many companies will often be found in the areas of anti-bribery and corruption as well as anti-trust). Other Compliance topics will only be coordinated by him and possibly consolidated in terms of reporting. Certainly some tasks, competences and responsibilities of the CCO should be defined in written form. But it is more important that it is made clear that "Compliance" is an independent sphere of competence. A good lawyer is not automatically a good Compliance Manager. Also a non-lawyer can be a good Compliance Manager. Selecting the right person is supposedly one of the most significant premises for successful Compliance 2.0.

One can sum up that wherever the step to initiating self-enforcement in Compliance Management is dared, sincerity can be shown internally and externally and credibility is established. Wherever this step is avoided, affected stakeholders may interpret this as a sign of carelessness, superficialness, dilettantism and hypocrisy.

If one accepts the mentioned Compliance measures as examples for certain "criteria of sincerity"[12] and one takes a look at the company landscape, then one can assert that

- high-quality Compliance workshops for managers with dilemma trainings are still an exception; instead one can find instructions on legislation and more or less successful web-based trainings;

[12] High-quality empirical field studies regarding the mentioned "criteria of sincerity" are desirable.

- appropriate, anonymous manager and employee surveys regarding Compliance & Integrity are only conducted in very few cases;
- anonymous whistleblower systems in general are not widespread so far and, if they are installed, are implemented insufficiently (especially regarding communication, training and motivation of relevant stakeholders to use them);
- the position of the CCO is not firmly integrated into the corporate structure. Everything can be found, from the management board to some subordinated middle management position. Corporate flexibility in view of the necessity (e. g. because of uncovered systematic misbehavior), the corporate structure and size, the general risk exposure and internationality is certainly important and correct. But without a respected person with authority Compliance cannot be successful.

B. Moral Foundation of Compliance

"Compliance" refers to conformity with a rule. The verb "to comply [with]" means amongst others "following", "adhering to sth.", "acting on sth.". Hence, Compliance constitutes a restriction and always has to become concrete on the norm which shall be acted upon. The desired behavior is mainly triggered by external pressure. The central question is which behavior can (still) be accepted or is allowed. Posing this question is certainly relevant for Compliance Management, but it is not sufficient for a CMS to function effectively and reliable. Instead, a moral foundation is needed, for example by striving for integrity which refers to the consistency of values and principles, motivation and action.[13] Integrity is tightly connected to honesty and truthfulness and can be understood as the contrary to hypocrisy. It can individually be considered as a "virtue of inner consistency" since the action of the agent has to be consistent with her corresponding inner attitude. In the context of ethics integrity is regarded as an independent moral quality which is defined as acting according to morally sound values and principles out of inner conviction.[14] The right behavior is governed by *recognizing* that it is morally right and because the agent is intrinsically motivated to acting correctly, she cannot avoid acting accordingly. She also asks what is permissible, but especially which behavior is (morally) right. On the basis of this reflection of her behavior she can give good reasons as to why it is right to act this way. Justice and law are also important references for questions of integrity, but not the only ones. In the corporate context integrity rather means that a company commits itself consciously not only to legal, but also to moral behavior. This is realized by consistently acting on morally sound corporate values and principles in daily business.

This can be illustrated with one example: Bribing in order to win a contract in foreign business is prosecuted criminally since quite a while. If one adds to this the – in various

[13] See e. g. DAVID BAUMAN, INTEGRITY, IDENTITY, AND WHY MORAL EXEMPLARS DO WHAT IS RIGHT, 14 (2011).

[14] Cf. RICHARD T. DE GEORGE, COMPETING WITH INTEGRITY IN INTERNATIONAL BUSINESS, 6 (1993).

countries certainly different – investigative pressure, there is sufficient pressure that companies and their employees comply with anti-bribery and corruption rules. In addition, the intrinsically motivated and reflected person will understand and acknowledge that bribery and corruption undermines the (ethically legitimated) principle of competition by which the most productive respectively the cheapest will receive a contract. Corruption hence prevents innovation and undermines the development of the rule of law and democracy especially in developing and emerging nations. These are all *good reasons* to understand that corruption is bad. By this insight (some) people are intrinsically motivated to act in a way that leads to the "right behavior" even in an environment of weak law enforcement, thus continuous effectiveness can be attained. Compliance properly understood as responsible behavior cannot be achieved without a moral foundation of the Compliance rules and measures – also because otherwise every inaccuracy of a Compliance rule and every gap in the legal framework will probably lead to misbehavior.

C. Seizure of results of company-internal investigations

It is crucial to understand that the management board should regularly make strategic and operational decisions which prove the commitment to Compliance and Integrity. The management board and the (top) managers should thus be informed and competent on the topic of Compliance and Integrity. They should know the fundamental Compliance risks in the regions, business divisions and business processes. It is their responsibility to personally inform themselves in conversation with their corresponding managers about the implementation of the CMS and possible conflict situations or ethical dilemmas. The significant Compliance risks and the commitment to Compliance must be addressed regularly inside and outside the company by the management board and the (top) managers (town hall meetings, management meetings, discussions with customers, conferences etc.). An essential condition is that the existing incentives in the company in no case hinder following Compliance rules or even make exactly that impossible. Ensuring this is a management task. For (top) managers it should be checked whether reasonable goals regarding Compliance Management can be found (implementation of the CMS in the own sphere of responsibility, handling revealed cases, bottom-up feedback regarding behavior, values, Compliance commitment). These could be integrated in an existing regular target agreement where appropriate. Misbehavior must be sanctioned according to its severity (financial damage, reputational harm, criminal penalties etc.) irrespective of the person concerned. Summed up, the much quoted "tone from the top" is important, but the "tone at the top" is even more important.

Distinctive incentives to reward Compliance to the law are not required, but appreciating especially moral behavior in the company can be endorsed. This could comprise financial and non-financial benefits but should especially include visible acknowledgment of the model behavior in order to encourage imitation and reinforce ethical behav-

ior.[15] In the same way as it is important to increase the costs for non-Compliance by implementing sanctions it is advisable to lower the individual costs for acting compliant and (morally) right by promoting such decisions, e. g. with a Compliance Scorecard which is taken into account for premiums and promotions.[16]

Albeit the right behavior of top managers is an essential condition for successful Compliance, implementation of Compliance in the company is carried out by line managers, that is the normal hierarchy is obtained. Thus, every manager must ensure Compliance in his own range of command. The Compliance function (the CCO) should support line management in implementing the CMS in daily business and has a consulting role regarding business decisions and transactions (possibly together with further positions, e. g. the legal department). This also points out that Compliance understood like that can only function if line managers (purchasing, sales, production, R&D etc.) are thoroughly trained. As outlined above these trainings have to include practicing ethical decision-making. Then managers will be able to reach independent, well-informed decisions in conflict situations. Furthermore, then they can pass on their knowledge and give orientation. They will be enabled to implement the CMS in their sphere of responsibility, fill it with life and make it a part of business processes. Only those who are able to speak will speak. That means managers trained in such a way will be able to contribute much more to fostering the much-evoked "speak-up culture". This mechanism can be strengthened further when top managers (at least the management board, possibly also the supervisory board) participate in such trainings as well and position themselves clearly to business-based dilemmas.

III. CMS IMPLEMNENTATION GUIDANCE

The question of the effectiveness of a CMS[17] is much discussed. An armada of requirements and standards has been developed in the past years, as e. g. ISO 19600 and IDW PS 980 (for an incomplete listing see fig. 2). But in most cases the standards do not address the specific conditions of companies and the context they act in when giving suggestions on how a CMS should be implemented.

---

15 Cf. Muel Kaptein, *Understanding Unethical Behavior by Unraveling Ethical Culture*, 64, HUMAN RELATIONS, 843, 851 (2011).

16 Hendrik Schneider, *Cognitive Dissonance As A Prevention Strategy – Considerations on the Prospects of Neutralizing the Techniques of Neutralization*, COMPLIANCE ELLIANCE JOURNAL, 18, 32 (Vol.3 No. 2 2017).

17 See Stephan Grüninger & Maximilian Jantz, *Möglichkeiten und Grenzen der Prüfung von Compliance-Management-Systemen – Gestaltung interner oder externer Wirksamkeits und Umsetzungsprüfungen*, ZEITSCHRIFT FÜR CORPORATE GOVERNANCE, 131 (2013).

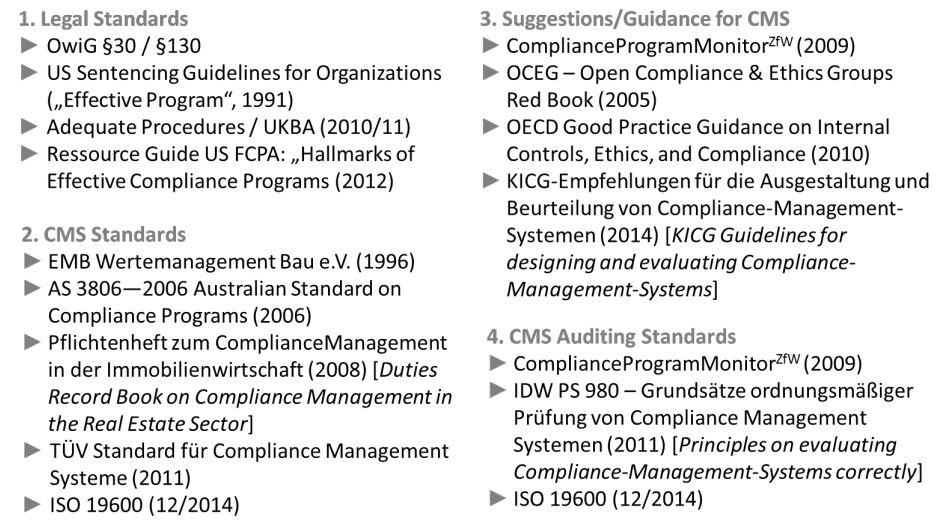

Fig. 2: Requirements of CMS

A project that aimed at addressing the specific questions companies of different size and structure have when implementing a Compliance Management System is the development of the "KICG-Guidelines" which were released in 2014. These represent the first attempt to describe suggestions for the appropriateness of CMS for companies of different levels of Compliance complexity (size, internationality, risk exposure) in detail.[18] Several stakeholder groups participated in this project (representatives of companies of different levels of Compliance complexity, lawyers, accountants/specialists in forensic services). In a follow-up project these project results are verified with members of judicial authorities, scientists, representatives of NGOs etc. in order to achieve a higher degree of reliability[19] and thus an incentive, especially for medium-sized companies, to address the topic of Compliance and invest in prevention. It is likewise important to see that the KICG-Guidelines were developed to give suggestions for both design and evaluation of a CMS and do not intend to establish a new standard (contrary to the intention of e. g. ISO 19600). This project was so important and is mentioned here because the "CMS Best Practice Standard" established in very big companies (e. g. DAX 30) does not fit to medium-sized companies and would completely overburden them. A CMS is ultimately measured at its effectiveness – regardless of whether it is the CMS of a very big or a comparably small company. In view of the question of an "adequate design"

18 STEPHAN GRÜNINGER, MAXIMILIAN JANTZ, CHRISTINE SCHWEIKERT & ROLAND STEINMEYER, EMPFEHLUNGEN FÜR DIE AUSGESTALTUNG UND BEURTEILUNG VON COMPLIANCE-MANAGEMENT-SYSTEMEN (Konstanz Institut für Corporate Governance 2014); STEPHAN GRÜNINGER ET AL., KICG COMPLIANCE ESSENTIALS (Konstanz Institut für Corporate Governance 2017).

19 Reliability regarding the (official) expectations about the appropriateness of corporate Compliance measures.

there exist in fact major differences as the project results show.[20]

In spite of or even because of the many standards and recommendations it is probably necessary that legislators in Germany and all over Europe define general requirements of CMS and incorporate them into positive law. They should specify concisely what is expected from companies and other organizations regarding Compliance. A specification of the OWiG[21], as proposed from different sides[22], would be a viable path for Germany. Guidelines such as the ones from KICG or standards like the IDW PS 980 or ISO 19600 could serve as references for the implementation.

Furthermore, it is essential for companies and can only be decided there that the functioning of CMS measures is ensured in an efficient, that means also cost-efficient, manner. The approach "Compliance as a line function" helps here because it avoids excessive installing of resources in the central Compliance function and prefers a decentral organization instead. For measures in the area of Compliance to work it is important to achieve acceptance. Also for this purpose the manager workshops outlined before are an appropriate approach. The Compliance function has the task to call attention to risks and mitigate these together with line management. But independent controls and process analysis too are important to identify gaps and weaknesses in the implementation of the CMS. As with other central topics in the company it should not only rely on the understanding of the managers and trust in their personal integrity and competences, but should also complement these as necessary by (external) professional expertise in order to guarantee the functioning of the CMS.

Compliance should be limited regarding content and with respect to business relationships. This means that a company pays attention to not promising anything in the code of conduct or other normative texts it cannot hold respectively whose Compliance cannot be controlled. In some code of conduct one can find the statement that "all UN conventions are being followed" which naturally sounds good – at least nobody would want to claim the opposite. But then one should also precisely know to content of all UN conventions. By all means adhering to human rights in the value chain is anything but trivial for globally operating companies. In many countries human rights are not respected at all, violations have an incidence rate of one. One may say that one respects human rights wherever it is in the sphere of influence of the company, but one should also point to the problems and to the limits of the scope of responsibility. In this con-

[20] See *Anforderungen an ein effektives Compliance-Management*, Konstanz Institut für Corporate Governance – KICG (Aug.2, 2017), http://www.htwg-konstanz.de/Compliance-Pflichten.6958.0.html.

[21] Regulatory Offences Act (German: Ordnungswidrigkeitengesetz)

[22] See Bundesverband der Unternehmensjuristen e. V, *Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 des Ordnungswidrigkeitengesetzes (OWiG)*, Frankfurt am Main, 2014; Deutschen Instituts für Compliance – DICO e.V, *Compliance-Anreiz-Gesetz. Ein Vorschlag für den Entwurf eines Gesetzes zur Schaffung von Anreizen für Compliance-Maßnahmen in Betrieben und Unternehmen*, Berlin, 2014.

text, the widely accepted UN Guiding Principles on Business and Human Rights[23] might serve as guidance. They oblige states to protect human rights („State Duty to Protect") and ascribe companies a responsibility to respect human rights („Corporate Responsibility to Respect") which is accompanied by "due diligence". By consciously delimiting and forming the own sphere of responsibility it will become evident whether Compliance is designed sincerely and credibly – or whether the diverse stakeholder demands are adopted without further thought and reflection about how to meet them. Also regarding the prevention of bribery and corruption it should be stated more clearly where the boundaries of Compliance Management in sales and distribution lie. No matter how perfectly a business partner due diligence is managed, a residual risk that the agent bribes the end customer will remain. As of today nobody can tell a company which due diligence standard is adequate for exculpating an incident. Thus, it is even more important that companies clarify what they do and where they see the limits of a thorough due diligence process, also financially.

The Compliance department and especially the CCO should be established as „trusted advisors" who offer a clear additional benefit to the operational business units. This benefit basically consists in locally developing and maintaining the competence of all business units to approach generally risky business with the highest possible degree of legal security and integrity. This naturally includes that some business dealings cannot be done. A Compliance department which merely sets and communicates rules, but runs off when conflicts arise, will not survive in the long run or will lose itself in insignificance. This also points out that Compliance Management should focus on "top risks". Regarding Compliance companies like to deal with the topic of "gifts and hospitality". As interesting as this may be, the real problems lie somewhere else: bribing to acquire business contracts, offenses of environmental law, cartels, avoiding export sanctions, product liability etc. – those are topics that companies have to work on, in fact worldwide, in order to have an effective CMS. The ultimately relevant Compliance risks of a company can only be mitigated if a CMS can give orientation on the topics mentioned. Only then potentially existence-threatening Compliance breaches might be prevented. Only then Compliance is really serving business.

[23] See United Nations Human Rights – Office of the high Commissioner, *Guiding Principles on Business and Human Rights* (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.