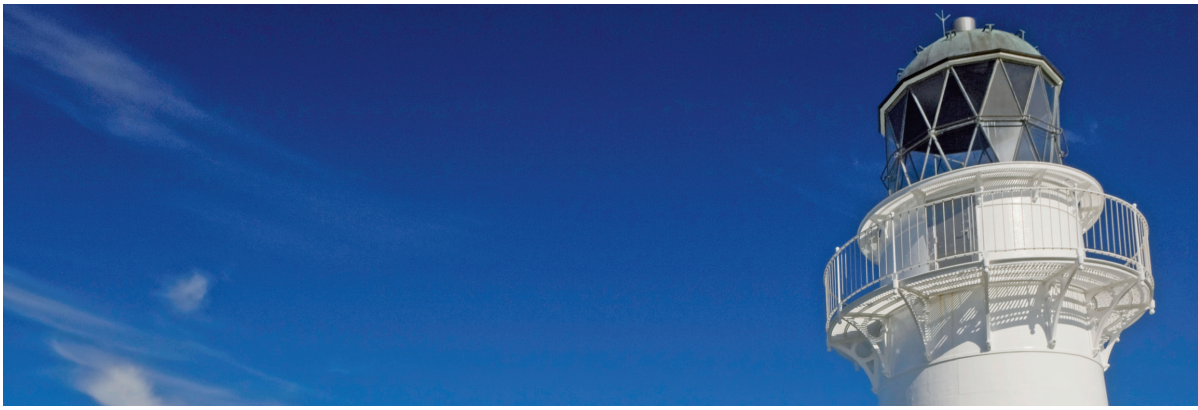
Deloitte.

Center for Corporate Governance
2/2013

Corporate Governance Forum
Information for Supervisory Board and Audit Committee Members



Contents

Focus on compliance

2 The Federal Financial Services Supervisory Authority's requirements of risk management

4 Liability of the Management Board and Supervisory Board in the case of violations of the law by company employees

6 Compliance at Deutsche Telekom

8 Compliance Experts Barometer 2013 – initial results

9 Reform proposals by the EU Committee on Legal Affairs on the statutory audit of financial statements

10 Strategy: What do German companies expect and plan?

12 Governance Code for Family Businesses

14 Scope of the duty to provide information at the General Meeting

16 Federal Cartel Office issues new guidelines on the setting of finds for violations of antitrust law (following a BGH ruling)

17 Reports

18 Interim management report: changes to GAS (DRS) 16

19 A look at IFRS: interim reporting

20 Events/Publications

Compliance at Deutsche Telekom

Manuela Mackert
Chief Compliance Officer
Deutsche Telekom AG
Tel: +49 (0)228 181 22233
manuela.mackert
@telekom.de

Britta Funk
Senior Compliance Expert
Deutsche Telekom AG
Tel: +49 (0)228 181 81283
britta.funk@telekom.de

The duty of the Audit Committee to monitor the effectiveness of the company's internal control systems in accordance with Section 107(3) Sentence 2 of the German Stock Corporation Act (AktG) also extends to the compliance system. Compliance involves adherence to legal requirements and internal company regulations with the aim of avoiding liability risks as well as other legal disadvantages for the company, its executive bodies, and its staff.

Due to the widespread loss of confidence in the economy and the fact that general calls for ethical corporate governance are becoming louder, compliance is about more than simply avoiding liability; it serves as the basis for good corporate governance as well. Only if we all consistently fulfill the highest ethical standards for business operations will we promote trust in Deutsche Telekom – an important foundation for our company's long-term success.

Other functions of compliance are the prevention of breaches of the rules through the implementation of organizational measures as well as the detection and punishment of misconduct. Due in particular to the rising flood of standards, compliance is becoming an increasingly important issue in companies.

In practice, this has led to the development of mechanisms and instruments called compliance management systems that are aimed at ensuring compliance in the company. These take very different forms depending on the industry, the size of the company and its structure, and on company-specific risks.

Audit Standard 980 issued by the Institute of Public Auditors in Germany defines elements of a compliance management system as well as a framework for auditing this system. Irrespective of which standard one uses, certain core elements appear time and again.

1. Implementation of a compliance organization

The compliance organization needs to be set up in accordance with the company's individual needs. At Deutsche Telekom, we have established a compliance organization at Group Headquarters but also set up compliance units in our subsidiaries, staffing these with experts. This is important because knowledge of the individual operating business models and operating processes is required to find individual compliance.

solutions. Which rights, responsibilities, and powers the central and local compliance organizations have needs to be clearly defined. We have drawn up contracts to define this.

2. Preventive elements

a. Creation of a compliance culture

The commitment to compliant behavior must be derived from the corporate culture. This is embodied in particular in the tone at the top and the tone in the middle. Corporate management must make a clear commitment to achieving the level of compliance desired in the company. Compliance needs to be anchored in middle management at the same time. This can achieve a broad impact because middle management is the "first line of defense" and employees go to their supervisors first.

b. Identification of compliance risks

One critical success factor is the compliance risk assessment. Here, the first step is to decide, depending on the business model, which risks may arise and which risks the compliance management system must address. A CMS that focuses exclusively on anti-corruption is one possibility. However, the CMS may also address aspects of antitrust law, capital market issues, and embargos. Its focus may even be broader. This depends on what is relevant in the company and what is not already covered by other areas.

The specific threat that exists for the company and what has already been done to reduce the risk is defined for each risk. Where necessary, other measures will be developed to reduce the risks to a manageable level in line with the risk strategy. The management of the subsidiary or affiliate in question is responsible for performing the compliance risk assessment. The central compliance organization supports the local compliance staff using a suitable methods toolkit and advises the operating units. The compliance unit aggregates the results into a group compliance program and monitors the implementation of the measures resulting from the compliance risk assessment that constitute the compliance program for the following year.

c. Implementation of policies, training, and advice

In multinational corporations, different jurisdictions and different cultural moral values in different countries present a considerable challenge. Building on national and international law, Deutsche Telekom has introduced a large number of compliance-related group policies.

Deutsche Telekom's guidelines have a pyramid structure. As one moves down from the peak to the base of the pyramid, the guidelines become more specific, going

from the very general terms of the Code of Conduct to a much greater level of detail. This includes regulations on anti-corruption, gifts, invitations and events, donations and sponsorship, but also dealings with advisors and agents.

The introduction of group policies is always the responsibility of the management of the subsidiary or affiliate and is accompanied by communication and training measures. In cases of doubt, employees can contact an advice portal. It is important for employees to receive a swift reply that creates certainty of action and provides legally secure room for maneuver.

d. Compliance due diligence

The provisions of the UK Bribery Act have created a growing trend among multinational corporations in particular of selecting their trade partners in line with compliance requirements. For instance, when acquiring equity investments this includes being mindful of "possibly acquiring" compliance risks as early as the M&A process. When considering potential business partners, emphasis is placed on the selection of advisors and sales agents, basing this on a standardized approval process. These days, consulting contracts are probably the most common form of bribery because they may conceal payments for which no actual service or an inadequate service was performed or portions of the payments are passed on to third parties for good conduct. For suppliers too, by writing integrity clauses into the contracts or by the performance of integrity checks, it is assured that there is a similar understanding of values and that the supplier observes the compliance policies.

e. Communication

To increase the awareness of compliance among our staff, we regularly conduct compliance campaigns, both nationally and internationally, involving intranet articles, interviews, and poster campaigns. In addition, the compliance community regularly receives a newsletter with hot topics. What is important from a communication standpoint is to strike the right balance.

Deutsche Telekom's Board of Management and Audit Committee are regularly briefed on the status of the compliance management system and current cases with relevance for the Group. This gives the compliance officer the opportunity to present his or her topics directly to senior management. "Do good and talk about it" is the motto.

3. Repressive elements

The best preventive measures notwithstanding, it is possible that breaches of the law and serious breaches of duty will occur in the company time and again.

To expose non-compliant behavior, companies need both internal and external whistleblowers. It is important that employees are encouraged to report misconduct to their supervisor first. A whistleblower portal will only be effective if the tip-offs are systematically investigated and misconduct is punished, though the whistleblowers must also be protected from reprisals.

Deutsche Telekom has set out clear regulations for investigations and only follows up on tip-offs if a sufficiently individualizable description of the facts and circumstances exists and the allegations of a violation of legal or internal regulations are assumed to be true. If the investigation confirms the reports, action must be taken. This includes punishment commensurate with the act and blame, but also the correction of any existing deficiencies in the internal control system.

4. Continuous monitoring and improvement

The adequacy and effectiveness of the compliance management system must be continuously monitored and improved. For example, Internal Audit may review the implementation of the compliance management system at selected subsidiaries on the basis of clearly defined minimum requirements drawn up in advance by the compliance organization.

Externally, certification may be performed by a public audit firm in accordance with the IDW Auditing Standard (AuS) 980. While this does not release corporate management from liability, it gives it—as well as the Audit Committee and the Supervisory Board—a certain level of assurance that the compliance management system that has been implemented is functioning and is thus effective. Deutsche Telekom had the effectiveness of its compliance organization reviewed as of December 31, 2010 and is seeking certification in accordance with AuS 980 for 2013.