



CPM<sup>ZfW</sup>

ComplianceProgramMonitor<sup>ZfW</sup>

## Contents

FOREWORD	3
A. AIM OF THE GUIDELINES AND DEFINITIONS	4
B. INTERNATIONAL LAWS AND STANDARDS IN BUSINESS CONDUCT COMPLIANCE	5
C. ELEMENTS OF A BUSINESS CONDUCT COMPLIANCE PROGRAM	6
I. Leadership & Corporate Culture	7
II. Conduct Principles and Conduct Guidelines	8
III. Implementation	9
IV. Responsibility and Organization	9
V. Communication and Training	10
VI. Risk Assessment and Monitoring	11
VII. Integration into HR Processes	12
VIII. Sales Representatives, Agents and Subcontractors	13
IX. Transparency and Documentation	14
D. COMPLIANCE MONITORING	15
I. Compliance Monitoring and Compliance Audit	15
II. Extent and Duration	16
III. Purpose and Scope of Monitoring	17
IV. Monitoring Methods and Evaluation	25

## Foreword

From the perspective of "compliance," corporate integrity and probity management and legal compliance in the conduct of business are constantly gaining in importance. As a result, the term has come to be used also outside of the financial services industry to denote the specific demands made on the rules and instruments of business management.

This makes it all the more relevant to define what compliance really means. How does it affect traditional company functions such as legal and internal audit, corporate security, environmental protection or human resources? Which functional and organizational concepts provide appropriate solutions for achieving the legal and ethical compliance objectives within a company? What does compliance mean for the management systems as a whole, such as leadership and compensation processes, training programs, and the internal control system, and how should compliance be monitored? Are social, environmental or corporate social responsibility (CSR) standards a part of compliance?

With the debate in progress, there are as yet no definitive and general answers to all of these questions. Different industries, companies and cultures try different solutions and provide different answers, but there has not yet developed a dominant understanding of or generally accepted blueprint for the "right" compliance solution.

The following compliance monitoring program is a contribution to this global debate; it draws on many years of practical experience of the companies that are members of the Users' Board for Values Management (AfW – Anwenderrat für Wertmanagement<sup>ZfW</sup><sup>1</sup>). The guidelines presented here deliberately focus on the area of "business conduct compliance," i.e. the question of how we can develop and promote probity and legal compliance in business management. The measures proposed here also address the question of how to appropriately control and monitor a company's compliance measures.

On the one hand, we want to provide guideposts to ensure that compliance is not just a declaration of good intentions, but leads to tangible and effective measures that strengthen a company's integrity and legal compliance. On the other hand, these guidelines also seek to undermine efforts to apply to compliance the classical methods of internal control systems, whose many checks and controls risk hampering a pro-active values- and problem-oriented integrity management.

The compliance monitoring approach proposed here does not claim to be exclusive, but leaves room for other and new compliance system developments. Compliance management today is a "work in progress" still requiring many innovative approaches. It cannot be the task of a compliance monitoring program to nip these in the bud. As past cases have shown, a company's integrity and legal compliance ultimately is determined less by the characteristics of its internal control systems, but by a clear focus on the real drivers of conduct such as the integrity and legal compliance practiced and lived by its senior management, the company's compensation and incentive systems, and a corporate culture of open debate. In the final analysis, the key is a corporate and leadership culture that unequivocally and consistently insists on the integrity of business conduct. If these guidelines succeed in contributing to this culture, they have accomplished their purpose.

<sup>1</sup> For more information about AfW<sup>ZfW</sup> see p. 26.

## A. AIM OF THE GUIDELINES AND DEFINITIONS

### Aim of the Guidelines

These guidelines aim 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.

To this end, the guidelines follow relevant international leading practice standards in business conduct compliance, which are listed in section B.

The key elements of an effective business conduct compliance program are described in section C. The explanations on the individual elements are not imperative for the compliance management of companies and other organizations. Rather, they should be understood as introductory remarks on the topic and as possible descriptions of compliance elements. The specific demands made on the compliance elements have to be determined and described for every organization on a case-by-case basis.

The Compliance Program Monitoring itself focuses on the monitoring and control of the design, implementation and application of business conduct compliance programs in everyday business and is described in section D. It also includes a Compliance Program Checklist designed to help conduct the compliance monitoring.

### Definitions

In the context of companies and organizations, the term *compliance* means complying with laws and regulations, organizational principles, internal rules and guidelines, the principles of good governance as well as generally accepted ethical norms.

Thus broadly defined, *compliance management* (i.e. ensuring compliance through appropriate measures) encompasses not only issues such as fairness in competition and the fight against corruption – topics that are frequently at the center of the public debate –, but also the environment, human rights, labor and social standards, and other industry-related issues.

*Compliance programs* describe the package of measures in the context of a company's – or organization's – entire compliance management, as they refer to individual (legal) areas. Accordingly, an environmental management system (e.g. in accordance with EMAS/ISO 14001) is to be understood as (an element of) an environmental compliance program, a social supply chain program (e.g. in accordance with SA 8000) as (an element of) a compliance program ensuring adherence to human rights, labor and social standards, and an anti-bribery compliance program as (an element of) a compliance program ensuring probity in the conduct of business (*business conduct compliance program*).

This differentiation of compliance programs within a company's or organization's compliance management is merely one option, of course. In practice, there are frequently other differentiations, depending on the company's, or organization's, specific requirements. Moreover, individual elements of compliance programs, e.g. the necessary "tone from the top" (commitment and exemplary behavior of the management) and other elements related to leadership and organization, cut across themes and are organized accordingly.

The *ComplianceProgramMonitor*<sup>ZfW</sup> applies solely to the field of business conduct compliance.

Principal International Compliance  
Management Standards

The laws, conventions and standards listed below shall provide orientation about the material and procedural norms that can exist for a company – in the sense of binding legal rules and regulations and voluntary best practice standards in business conduct compliance. The list is not exhaustive. Additional laws, industry standards and other voluntary standards can be relevant, e.g., at all times, the specific anti-corruption and anti-trust laws in the countries where the company does business. On the other hand, not all the laws, conventions and standards listed here need to be relevant for a certain company. Therefore, it is always necessary to analyze the relevant legal and voluntary standards in order to develop and monitor, both internally and externally, a business conduct compliance program.

Selected Laws and Conventions

- Anti-corruption laws
- Relevant criminal law codes (fraud including bidding fraud, extortion, illegal insider trading, money laundering, embezzlement, document forgery, betrayal of secrets, etc.)
- EU Anti-Bribery Law (EUBestG)
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions
- Foreign Corrupt Practices Act (FCPA)
- UN Convention Against Corruption (UNCAC)
- Act Against Competition Restraints
- German Corporate Governance Code
- OECD Guidelines for Multinational Enterprises
- UN Global Compact
- ICC Rules of Conduct and Recommendations on Combating Extortion and Bribery
- World Economic Forum, Partnering Against Corruption Initiative (PACI): Principles for Countering Bribery
- Transparency International/Social Accountability International: Business Principles for Countering Bribery
- Transparency International: "A-B-C of Corruption Prevention" and "Checklist for 'Self-audits' to Prevent Corruption in Companies"
- World Bank, Department of Institutional Integrity: Voluntary Disclosure Program, Protocol 7, II. "Guidance in Revising and Improving the Compliance Program"
- European Bank for Reconstruction and Development (EBRD): "Fraud and corruption – definitions and guidelines for private sector operations"
- United States Sentencing Guidelines: "Effective Compliance and Ethics Program" (§8B2.1)
- Open Compliance and Ethics Group (OCEG): OCEG Guidelines "Red Book"
- Committee of Sponsoring Organizations of the Treadway Commission (COSO): COSO Enterprise Risk Management Framework
- Australian Standard (AS) 8002-2003 – Organizational Codes of Conduct, and Australian Standard (AS) 2860-2006 – Compliance Programs
- ValuesManagementSystem ZfW of the Users' Board for Values Management (AfW – Anwenderrat für Wertemanagement).
- EMB Values Management in the Construction Industry

## C. ELEMENTS OF A BUSINESS CONDUCT COMPLIANCE PROGRAM

The following remarks and comments are based on the above-mentioned laws and standards, the ValuesManagementSystem<sup>ZfW</sup><sup>2</sup>, and the relevant German and international literature on the topic of business conduct compliance. They aim to provide a summary of the possible practical requirements for implementing a business conduct compliance program.

The following remarks and comments do not establish a minimum standard. I.e., the text only serves as an introduction to the topic and as guidance for the development and implementation of a compliance system. The individual elements (see subject headings I to IX of this section), however, are necessary components of a business conduct compliance program.

<sup>2</sup> The ValuesManagementSystem<sup>ZfW</sup> is available at [www.zfw-online.de](http://www.zfw-online.de).

## I. Leadership & Corporate Culture

The company management is responsible for the business conduct compliance program. In particular, it is responsible for constantly communicating, both internally and externally, the company's core values, conduct principles and conduct guidelines (see II.), for acting in accordance with the communicated standards, and for monitoring the implementation and application of the business conduct compliance program.

A business conduct compliance program can only achieve sincerity and credibility if its implementation, application, and public communication are given "top-level" priority. Only the management's continual self-commitment to the company's core values and business conduct compliance program proves the sincerity of the program and thus generates both the ability to act and an environment of reliability and trust for the employees. In this context, it is essential to make clear that complying with the core values and the business conduct compliance program is company policy and that any behavior that does not respect and comply with these values and this program will neither be tacitly expected nor condoned. In addition, monitoring the implementation and application of the business conduct compliance program makes the program more credible in the eyes of business partners and other stakeholders of the company.

In the context of a business conduct compliance program, leadership and corporate culture also help to develop and promote a specific corporate identity, and to provide all employees with the orientation and security required for making difficult decisions in everyday business. In order to live up to this high standard in practice, moral values (e.g. integrity, fairness, honesty, loyalty to the contract, responsibility), cooperation values (e.g. loyalty, team spirit, ability to manage conflict, openness), performance values (e.g. gain, expertise, willingness to perform, flexibility, creativity, innovativeness, quality), and communication values (e.g. respect, belonging, openness, transparency, communication) must be consistent with each other and with everyday business realities. The company values must not contradict one another nor must they make promises to the stakeholders that cannot be kept – ignoring the business realities, so to speak. Only then can a company's core values be credibly communicated to its managers, employees and external stakeholders.

When building a corporate culture defined by integrity, both managers and employees have to develop the skills to recognize and solve values-sensitive problems. The persons involved have to make sure that their conduct and that of their business unit is geared towards compliance in a long-term-perspective. The business conduct compliance program can only be effective in the long term if the top management, the unit managers and the employees make a binding commitment to the program. A business conduct compliance program has to be a high-priority company process that receives constant attention within the organization. To this end, the company must, for example, use coaching methods during an internal or external implementation support in order to ensure the proper conduct of all employees and their units and to bring about changes in behavior in line with the company's core values, conduct principles and conduct guidelines. Only then will the program be effective in the long term and different from short-term and short-sighted activities or delegation to professional contexts. A business conduct compliance program can only be successful if the managers live by and commit to this program at every level of the organization. At the same time, it is equally important to enable and safeguard employees' autonomous decision-making competencies in ethical conflict situations for which there are no explicit conduct principles or guidelines. This allows for the fact that there cannot be specific conduct and procedural principles for every conceivable situation that may arise in a company's, or organization's, daily routine.

## II. Conduct Principles and Conduct Guidelines

A company has to have written conduct principles and conduct guidelines, define the company values, and lay down the business ethics it desires. The primary objective of these conduct principles and conduct guidelines is to prevent criminal and unethical business actions, in particular violations of competition and anti-corruption laws. In addition to unequivocally prohibiting unethical or fraudulent actions, conduct guidelines can also articulate expectations about employees' positive actions (e.g. regarding innovation). Establishing conduct principles and conduct guidelines means that the company should draw up a declaration of values, a code of ethics or similar document. This document is to outline the values that guide the company in its relations with its most important interest groups. Furthermore, this values management (see E.) has to be incorporated into the company's specific business strategy. The business principles and rules of conduct have to be available for all employees and business partners at all times. In addition, all employees should be specifically and explicitly informed about legal compliance. This is all the more important since not every employee is up to date on the current legal situation and knows how to act in accordance with the law.

There are no definitive rules as to what the written compliance regulations have to look like. They can be working instructions, guidelines, instruction leaflets, flyers or handbooks. However, by putting the rules in writing, the company must ensure that its employees know the compliance regulations. Simply publishing the rules, conduct principles and conduct guidelines on the company's intranet or similar platforms will not be enough unless all employees are systematically and notified.

Business conduct compliance programs typically address the following areas, which are regulated as part of the conduct principles (Code of Conduct) and/or by conduct guidelines, working instructions and business process instructions:

- legal compliance, law abidance;
- prohibition of corruption and of violations of anti-trust laws;
- respect for human rights, labor and social standards, prohibition of discrimination and workplace harassment, etc.;
- ensuring legal compliance and compliance with business ethics when dealing with clients and sales intermediaries;
- ensuring legal compliance and compliance with business ethics when dealing with suppliers and subcontractors;
- acceptance and giving of gifts, invitation to meals, drinks or other entertainments, other benefits;
- dealing with conflicts of interests (ensuring the separation of company and personal interests and the priority of company interests over personal interests);
- dealing with donations, not-for-profit activities, and sponsoring;
- prohibition of insider trading;
- protection of company assets (including dealing with information and protection of intellectual property), secondary employment, protection of the assets of business partners.

### III. Implementation

The company should define the target group of every guideline and measure. It should make sure – if necessary, by means of pilot tests or similar means – that the guidelines and measures are easy to understand and apply. The correct application of conduct principles and conduct guidelines, the integration into management processes and the corresponding quality control should be continuously documented. The company should also seek confirmation from relevant company units (management) and employees that the guidelines, measures and controls have been received and understood; it should also establish a helpdesk or information office to be able to field questions about their practical application.

In addition, measures should be taken to recognize and promote exemplary conduct that complies with and reflects the company's values and to impose sanctions for violations of values, especially for gross misconduct in business dealings. This can be done through job instructions, management and staff evaluation systems, and values-sensitive incentive and compensation systems.

The company should use clearly defined, transparent criteria and procedures to recruit, hire and promote employees. Key positions must not be held by individuals who have already committed crimes or come to attention because of major misconduct. Moreover, compliance with the company's core values and conduct guidelines should be part of the evaluation criteria of performance evaluations, compensation systems and bonus regulations or adapt the latter in accordance with its compliance objectives. This is to prevent that company units (management) and employees use means that do not comply with the rules and regulations to strive for or achieve sales and profit targets.

In addition, employment contracts should contain a commitment to legal and in particular anti-corruption compliance. Moreover, it is recommended to include regulations regarding secondary employment and conflicts of interest in the employment contract.

### IV. Responsibility and Organization

Conduct principles and conduct guidelines can only be successful if a company's management demonstrates exemplary conduct and commitment to compliance at every level. The Board of Directors is responsible for compliance.

The company should select individuals who take responsibility for developing and designing the compliance program and support the management in implementing and applying the company standards. To this end, they should have the appropriate resources and powers. In the case of multi-headed company managements, it may be expedient to assign the responsibility for the compliance program to a department. The board member in charge can delegate the above-mentioned responsibility for designing and supervising the compliance program either to an already existing position or to one or more appointed compliance representatives. Moreover, in larger companies, it has proven effective to form a compliance steering committee consisting of the functions that are responsible for important activities and processes in the context of a compliance program (e.g. compliance, legal division, audit, HR, controlling, sales, purchasing, safety). Among other things, this steering committee can be tasked with supporting the management in comprehensively and consistently applying the compliance program and with acting in case of suspected compliance violations.

In addition to appointing individuals in charge, the company should have regulations about how employees can act as "whistleblowers" if they discover or suspect violations of legal and/or internal regulations (e.g. anonymous hotline, ombudspersons). Here, it has to be ensured that the employees know where and how to report misconduct. It also has to be ensured that employees can report suspected criminal activities without fear of negative consequences and without having to resort to hierarchical communication structures. Moreover, the company can offer employees the option to report any ethical dilemmas to existing institutionalized company functions (e.g. legal or human resource departments) – if necessary, anonymously.

## V. Communication and Training

The company has to conduct regular trainings to inform and educate about its conduct principles and conduct guidelines.] Trainings are one of the key instruments of a functioning compliance program.

The company has to make sure that the relevant target groups participate in the trainings and that the learning objectives are communicated with a view to practical application, so that the employees are able to apply the knowledge. Such conduct trainings can in particular include case studies based on ethical dilemmas in everyday practice. The trainings are particularly important for employees in sensitive functions (e.g. sales, purchasing), but should be expanded – at least gradually – to include all company staff and employees (including the company management). Moreover, for certain companies it is reasonable and/or necessary to also inform its sales representatives, sales agents as well as consultants and subcontractors about its compliance rules and to conduct information or training sessions for these groups.

For internal communication, it has proven effective to seek confirmation from the relevant employees (board members, managers and employees in compliance-sensitive functions) that they have taken note of the compliance rules by asking them to sign a written declaration ("compliance declaration"). For the selection of the "relevant employees," all company locations should be taken into account.

In addition, it has to be ensured that the company management and the compliance department/ compliance representative communicate the compliance program within the company continually and continuously, i.e. beyond its introduction stage. In addition to compliance trainings and regular written declarations about having taken note of and complying with the compliance rules, employee polls, for example, can be used to gain information about the staff's perceptions of the status and development of corporate compliance/corporate integrity. If necessary, these surveys can be used to implement further measures for improving the compliance program.

## VI. Risk Assessment and Monitoring

Both best practice standards and the literature on business conduct compliance agree that there have to be controls at irregular intervals. There is as yet no judicial pronouncement on how these controls should be organized and which control measures are necessary, sufficient and reasonable. This offers the advantage that it is possible to flexibly respond to the requirements of the company and its business operations. Controls always fulfill a pro-active function and an investigative function. Announcing and performing controls increases the likelihood of discovering compliance violations while, at the same time, serving as a deterrent, i.e. in a preventive manner.

To this end, the company must evaluate the relevant existing business processes (e.g. in sales and purchasing) and relevant regulations such as the existing signature policy as to whether they promote rule-abiding behavior or encourage or facilitate transgressions. It also has to assess whether the implemented controls are really effective. It is important to have regular risk assessments in all business fields and relevant key departments regarding potential violations of anti-corruption and anti-trust laws and other compliance issues (e.g. labor and social standards throughout the value chain). The company's IT systems have to make sure that no unauthorized third party is able to access the system and that data manipulations can be documented at any time (through logfiles, protocols and controls of all transactions – especially in financial accounting). The two-person rule (or other controls) should be systematically applied during the performance of sensitive functions, e.g. for payment authorization. The company should perform regular controls in order to ensure that all employees taking part in money transactions act in accordance with the generally accepted accounting principles (GAAP; in Germany: Grundsätze ordnungsgemäßer Buchführung, GoB).

In addition to having make sure that the compliance controls of its business processes are functional, the company board is responsible for regularly evaluating the compliance program with a view to its effectiveness and efficiency. This is to guarantee both its quality and its adaptability to changing conditions (e.g. mergers & acquisitions). This evaluation should take place once a year. Moreover, the company should review the compliance program at least once every five years. This review should also include agreements and contracts with agents, sales representatives, subcontractors and subsidiaries.

## VII. Integration into HR Processes

The company has to make sure that individuals who have come to attention for criminal actions or other violations of compliance programs within or outside the company in the past are not promoted to or hired for responsible positions. It has to make sure that no discretionary decisions are delegated to individuals known for having committed fraudulent actions. If criminal actions are discovered, the company has to respond in an appropriate fashion. In case of violations of laws or the compliance program, it has to take appropriate disciplinary measures, also against employees who are responsible for covering up infractions. These measures can range from reprimands to dismissals. Most importantly, the company has to demonstrate its sincerity and will to apply its compliance program. The company will also be judged by the steps it takes in case of a compliance violation.

Until now, few companies have adopted so-called "amnesty programs" (leniency programs) for employees (not for members of the executive management). Here, the company waives claims for damages and refrains from terminating the employment contract if employees who have violated compliance rules bring charges against themselves. Whether such a program makes sense can only be determined by reviewing the particulars of every case.

In addition, there should be positive incentives for complying with the business conduct compliance program and for successfully implementing the program. The target agreements and performance evaluations of managers and executives should include targets that refer to the company's core values and business conduct compliance program. Moreover, the company should make compliance with its core values and conduct guidelines an integral part of the evaluation basis for its performance evaluation and compensation systems.

## VIII. Sales Representatives, Agents and Subcontractors

The hiring of agents, consultants and sales representatives who develop business and do lobby work (especially abroad) has to be thoroughly evaluated (so-called "third-party due diligence"). The same applies to the hiring of subcontractors. In this context, one also has to assess the compliance with laws and compliance programs and the suitability of the business partners selected abroad. When signing contracts, one has to make sure that they include declarations to the effect that the contract partners have not and will not bribe office holders or similar persons to gain any professional or financial advantage. Such declaration is also necessary when entering into joint ventures. Compliance with the prohibition has to be monitored.

The company has to take measures to ensure that all representatives and agents know the compliance program; it also has to make clear that it expects all actions undertaken in its name to be consistent with the existing compliance program.

The company should review the fees and commissions of its representatives and agents at home and abroad with a view as to whether they are reasonable and justifiable. Representatives and agents, too, should be bound to comply with the company's guidelines and conduct rules and be subject to controls.

Secondary employments of employees must be subject to regulation and approval (in particular in companies that are competitors, clients or suppliers). Board memberships are expressly prohibited or subject to regulation and approval. There are clear rules for acquiring company shares/warrants on special terms as well as for granting and giving loans to employees, business partners, subsidiary and holding companies.

Any organizational and/or financial establishment, alteration or liquidation of subsidiary, holding or trust companies at home and abroad is regulated company-wide and subject to approval (purpose of business, management, supervisory bodies, capitalization, ownership structure, etc.). Activities in countries that are considered to be particularly prone to corruption (e.g. according to the Transparency International Corruption Perceptions Index) are subject to particular monitoring and control.

The company has to make sure that its buying processes are documented and transparent at all times, also for competent third parties (by recording procurement specifications, calls for tender, awarding of contracts, complaints, and payment handling).

## IX. Transparency and Documentation

As a matter of principle, payment transactions – in particular for gifts, meal invitations, donations, cash purchases, commissions, and consultancy and trustee services – should be subject to particular control. Moreover, documentation requirements for business transactions and payments should be established and compliance with these requirements should be regularly reviewed, e.g. by internal audits. Donations for political or non-profit causes and sponsoring of any kind should be carefully evaluated, subject to approval and properly documented. There are clear rules for giving and accepting gifts as well as for meal invitations and other benefits, which apply to all employees at home and abroad. Internal budgets for general charitable or social purposes (e.g. company sports club, sponsoring associations, foundations, works council) are to be regularly reviewed.

### I. Compliance Monitoring and Compliance Audit

A compliance audit, i.e. a review of the efficiency and effectiveness of the business conduct compliance program, can be performed either by internal auditors (e.g. by internal audit) or external auditors (e.g. by qualified consulting or auditing companies). In these guidelines, the term *audit* is reserved for cases where a compliance program already exists, i.e. where its implementation has been concluded. That does not mean that all compliance measures, which the company needs from the perspective of best practice and suitability, have to be already implemented and realized. It only means that the internal or external auditor/audit team comes into play after the implementation process has been concluded.

On the other hand, *compliance monitoring* means that the external, independent and objective compliance monitor carries out his/her tasks during the implementation of the compliance program, i.e. s/he accompanies the implementation process. In this context, the compliance monitor expressly does not act as a consultant or trainer, i.e. s/he does not make any decisions about necessary compliance measures nor does s/he design their implementation and application. What the compliance monitor does is to coach the company's management board, internal compliance personnel (compliance representative, compliance committee, etc.) as well as any internal and external consultants along best-practice standards. For example, the whole set of requirements listed in the *Compliance Checklist* (see D. III.) is a best-practice standard.

Among other cases, compliance monitoring takes place when private and in particular public clients or funding institutions (World Bank, European Bank for Reconstruction and Development, etc.) ask a company to establish or improve/update a compliance system. In this case, the independent compliance monitor reports on the progress and status of the compliance system during its development and implementation and submits a final report after the compliance system has been put in place.

In the interest of readability, the term *compliance monitoring* will be used in the following paragraphs to also include the compliance audit, which takes place after the compliance program has been implemented..

## II. Extent and Duration

The extent and duration of a compliance monitoring process cannot be generally defined, but have to be established on a case-by-case basis by the compliance monitor. In any event, the size of the company (turnover, number of employees), the complexity of the organization, and the business model are key criteria for determining the extent and duration of the compliance monitoring process. If applicable, there may be additional, external standards that are relevant for the compliance system.

Basically, the following criteria have to be taken into consideration when planning the extent and duration of a compliance monitoring process (please note that this list is not exhaustive):

- Business volume
- Number of employees; number of employees directly affected by the compliance system (e.g. employees in sensitive company departments or functions)
- Branch of industry
- Business model, e.g. regarding distribution and sales channels
- Level of internationalization/percentage of foreign business/business activities in countries with an increased risk of non-compliance
- Generic risk exposure regarding compliance violations (e.g. risk of corruption)
- Complexity of organizational structure
- Decentralized decision-making powers/possibilities for central control
- Misconduct/criminal behavior in the past
- Opinion of the compliance monitor ("reasonable assurance" or "negative assurance")

### III. Purpose and Scope of Monitoring

A key goal of compliance monitoring is to determine whether the compliance program of a company (or organization) contains the elements that are generally considered necessary to properly protect the company (or organization) from unlawful actions by managers, employees or business partners.

To this end, it has to be established that the company (or organization) has taken the necessary compliance measures, that the compliance program as a whole is integrated into the day-to-day business processes and makes it possible to support the company's values and culture and is thus suited to preventing, uncovering or thwarting crimes and offenses.

The scope of a compliance monitoring program is basically to 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.

#### I. Regarding the **design of the compliance program**, it is reviewed whether

- all **reference standards** relevant for the company **have been taken into account** and whether
- the **compliance measures** are **appropriately designed** for the company (*design check*). The appropriateness is determined by the criteria mentioned in E. II. and, if necessary, by further criteria established by the compliance monitor ("professional judgment").

#### II. Regarding the **implementation or establishment of the compliance program**, it is reviewed whether

- the **elements of the compliance management system** necessary to meet the appropriateness requirements are **functional** (*functionality check*). I.e., in order to achieve the "implemented" status, a compliance measure has to have been adopted and become effective, all accompanying instruments (written forms, technical systems, etc.) have to be available, and the compliance measure has to be able to serve its desired purpose and meet the defined goal.

While monitoring the design focuses on the compliance system's structure, monitoring its implementation focuses on the system's feasibility and ability to function.

#### III. Regarding the **application of the compliance system**, it is reviewed whether

- the **elements of the compliance management system** are applied in day-to-day business practices (*effectiveness check*). To this end, the reviewed compliance measure must have been used already (at least once).

Reviewing the effective application takes on the question of whether the compliance measure is really adhered to and internalized in the company's day-to-day business.

It might not be possible to perform this kind of application monitoring for all compliance measures. Where this is the case, "not applicable (n/a)" should be noted in the checklist. A Code of Conduct, for example, can only be evaluated regarding i. and ii., since it cannot and should not be reviewed in the context of a compliance monitoring program whether the employees follow the guidelines specified in the Code. On the other hand, the integration of compliance into target agreements and performance evaluations is only "effective" once this instrument has been used and not after its planning has been concluded and the process has been fully described.

## Compliance Program Checklist (Business Conduct)

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
I Conduct Principles (Code of Ethics)	Development	1 Definition of company goals and company values	r	i	a	f	e
		2 Definition of the principles of business ethics	r	i	a	f	e
		3 Naming of key stakeholders	r	i	a	f	e
		4 Identification of the applicable reference standards	r	i	a	f	e
II Conduct Guidelines (Code of Conduct)	Development	5 Legal compliance, law abidance	r	i	a	f	e
		6 Prohibition of corruption (zero tolerance), prohibition of anti-trust law violations	r	i	a	f	e
		7 Ensuring compliance with laws and business ethics in dealing with clients and sales intermediaries	r	i	a	f	e
		8 Ensuring compliance with laws and business ethics in dealing with suppliers and subcontractors	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
		9 Acceptance and giving of gifts, meal invitations, and other benefits	r	i	a	f	e
		10 Dealing with conflicts of interests (ensuring the separation between company and personal interests and the priority of company interests over personal interests)	r	i	a	f	e
		11 Dealing with donations, non-profit activities, and sponsoring	r	i	a	f	e
		12 Protection of the assets of the company, secondary employment, protection of the assets of business partners	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
III Policies & Procedures	Development	13 Acceptance and giving of gifts	r	i	a	f	e
		14 Compliance declaration for managers, employees	r	i	a	f	e
		15 Compliance review of third parties (agents, consultants, sales representatives) in sensitive business departments and countries before hiring their services	r	i	a	f	e
		16 Compliance agreement for third parties (compliance declaration, review of suppliers, evaluation of suppliers)	r	i	a	f	e
		17 Supplier compliance (e.g. compliance declaration, review of suppliers, evaluation of suppliers)	r	i	a	f	e
		18 Sanctions in case of non-compliance	r	i	a	f	e
IV Transparency	Development	19 Risk screening for sensitive business areas	r	i	a	f	e
		20 Control of risk management in sensitive business areas	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
		21 Documentation of sensitive payment transactions (e.g. donations, commissions)	r	i	a	f	e
		22 Protection of IT systems against data manipulation	r	i	a	f	e
		23 Two-person rule in sensitive functions	r	i	a	f	e
		24 Control of compliance with generally accepted accounting principles	r	i	a	f	e
V Leadership and Corporate Culture	Implementation	25 Compliance as a strategy of (legal, economic, ecological, social) sustainability	r	i	a	f	e
		26 Orientation towards ethical values	r	i	a	f	e
		27 Leadership style: determination, clarity, reliability, accountability, integrity	r	i	a	f	e
		28 Self-commitment, legality	r	i	a	f	e
		29 Managers serve as role models and take responsibility for compliance ("tone from the top")	r	i	a	f	e
		30 Pro-active and aggressive communication of CMS by company board and management	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
VI Communication and Training	Implement- ation	31 Internal communication (meetings, brochures, newspapers, intranet)	r	i	a	f	e
		32 External communication (e.g. annual reports, reporting, brochures)	r	i	a	f	e
		33 Written and oral information for agents, suppliers, consultants	r	i	a	f	e
		34 Membership and engagement in compliance initiatives and exchange of experiences	r	i	a	f	e
	Implemen- tation	35 Face-to-face training for top-level management and functions with increased compliance risk	r	i	a	f	e
		36 Specific face-to-face training for certain functions and high-risk groups (e.g. purchasing, sales, suppliers)	r	i	a	f	e
		37 Trainings include legal information plus a focus on "real cases"	r	i	a	f	e
		38 Web- or intranet-based training for employees	r	i	a	f	e
VII Compliance in HR	Implement- ation	39 Integrity review and compliance declaration for employees in areas with high compliance risks	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
		40 Integration into employee selection and hiring processes	r	i	a	f	e
		41 Career planning for board members and managers	r	i	a	f	e
		42 Target agreements in sensitive business areas	r	i	a	f	e
		43 Compliance risks in salary systems and bonuses	r	i	a	f	e
		44 Appropriate disciplinary measures (presentation/threat of sanctions in line with labor, civil or criminal law)	r	i	a	f	e
VIII Organization	Implementation	45 Responsibility of top management (board, management)	r	i	a	f	e
		46 Compliance steering committee (e.g. compliance, legal, audit, sales, HR)	r	i	a	f	e
		47 Compliance office with appropriate resources	r	i	a	f	e
		48 External compliance monitor	r	i	a	f	e
		49 Whistleblower systems	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
IX Audit	Review	50 Internal audit of CMS in sensitive business areas	r	i	a	f	e
		51 Control of sensitive payment transactions (e.g. donations, commissions)	r	i	a	f	e
		52 Control of compliance with and implementation of CMS into everyday business practices	r	i	a	f	e
X Monitoring	Review	53 Regular reports to and discussion in the top management	r	i	a	f	e
		54 Self-evaluation of business areas and companies	r	i	a	f	e
		55 External monitoring of the development, implementation and suitability (fit for purpose) of CMS by experts and auditing companies	r	i	a	f	e

## IV. Monitoring Methods and Evaluation

### **Analysis of the Documentation**

As part of the compliance monitoring program, the compliance monitor examines the existing documentation of the compliance system. All measures relevant for the compliance system have to be documented and reviewed.

### **Conduct of Interviews**

The compliance monitor conducts interviews with selected individuals who work for the company. Typically, these always include members of the company's executive management and a group of department heads selected by the monitor. In addition, interviews should be conducted with employees in sensitive functions (e.g. purchasing, sales) and with randomly selected company employees.

### **Evaluation**

The compliance monitor writes a report in which s/he assesses the status of a company's compliance system. S/he evaluates the design, implementation and application of the compliance systems. On all three points, the evaluations should include qualifying remarks.

The evaluation has to include statements about the basic orientation and the aims of the compliance system as well as the program's strengths and weaknesses. In addition, the report has to contain recommendations for the program's further development and improvement and, if applicable, provide information about conditions that have been imposed on the company.

## AfW<sup>ZfW</sup> – Anwenderrat für Wertemanagement<sup>ZfW</sup>

The AfW<sup>ZfW</sup> is a voluntary association of companies and organizations that use and promote the ValuesManagementSystem<sup>ZfW</sup>. Its goal is to advance, enhance and assure the quality of the ValuesManagementSystem<sup>ZfW</sup>. Its practical expertise ensures that the ValuesManagementSystem<sup>ZfW</sup> is highly application-oriented. In addition, the AfW<sup>ZfW</sup> provides its members with a forum for the continuing exchange of experiences and mutual advice. Current AfW<sup>ZfW</sup> members are: ABB, Allianz, BASF, Bilfinger Berger Industrial Services, Bosch, Daimler AG, Deutsche Post, Deutsche Telekom, German Forum for Crime Prevention (Deutsches Forum für Kriminalprävention, DFK), EnBW, Ethics Management of the German Construction Industry (EthikManagement der Bauwirtschaft e.V.), Fraport, Lahmeyer International, Novartis Foundation for Sustainable Development, Schwarz Pharma, Siemens, The Centre for Business Ethics, ZF Marine. Additional information about the AfW<sup>ZfW</sup> is available at **[www.zfw-online.de](http://www.zfw-online.de)**.

This document was discussed in the AfW<sup>ZfW</sup>. The Centre for Business Ethics, Weingarten, is the sole publisher of the ComplianceProgramMonitor<sup>ZfW</sup>.

The Centre for Business Ethics (Zentrum für Wirtschafts-ethik – ZfW gGmbH) was founded in 1998 by the managing board of the German Business Ethics Network (Deutsches Netzwerk Wirtschafts-ethik – DNWE) as its central research institute. Its task is to promote the implementation of business ethics in Germany and Europe in close cooperation with other scientific and economic institutions. At the same time it contributes to the solution of social and entrepreneurial problems that result from economic globalization.

**Zentrum für Wirtschaftsethik gGmbH**  
Wissenschaftliches Institut des  
Deutschen Netzwerk Wirtschaftsethik  
– EBEN Deutschland e. V.

---

**Published by**  
Zentrum für Wirtschaftsethik gGmbH  
Kirchplatz 7  
88250 Weingarten  
Germany

Telefon +49 (0) 751 5686-107  
Fax +49 (0) 751 5686-222  
eMail zfw@dnwe.de

[www.zfw-online.de](http://www.zfw-online.de)  
[www.dnwe.de](http://www.dnwe.de)

---

**Academic Director**  
Prof. Dr. Josef Wieland

**Managing Director**  
Dr. Rainer Öhlschläger

**Project Director**  
Prof. Dr. Stephan Grüninger

**Translation**  
Manuela Thurner, Munich

© Zentrum für  
Wirtschaftsethik gGmbH

---

**dn** DEUTSCHES EUROPEAN  
NETZWERK BUSINESS ETHICS  
**we** WIRTSCHAFTS- NETWORK  
ETHIK DEUTSCHLAND E.V.

## Guidelines for organizations

These guidelines aim 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.