

Fundamentals of effective compliance management

dossierpolitik

12. April 2010

Number 7

Integrity as a business policy. The Swiss economy is highly globalized and its value chains are becoming increasingly complex. This development is taking place against a background of increasing regulation and legal enforcement. In this corporate environment, integrity when conducting business is a fundamental requirement of diligent management. If companies want to be successful in the long term, they must nurture a keen culture of integrity and law-abidance. Integrity and compliance are therefore the basis but equally also an opportunity for successful business. economiesuisse and business specialists have drawn up the foundations of effective compliance management. Swiss companies are convinced that by applying binding values and appropriate compliance management they can safeguard their integrity, and avoid or contain breaches of the law. Integrity and effective compliance are therefore unalienable elements of good, diligent business management. Compliance also contributes to the social responsibility borne by the economic players.

economiesuisse position

- ▶ The basic legal responsibilities of any board of directors includes supervising those people entrusted with managing the company, in particular with regard to abidance by the law. Ensuring law-abidance, also known as <compliance>, must be implemented, supervised, and adapted to any amendments by the board of directors with the greatest of care and attention. The aim is to ensure that any breaches of the law are avoided or discovered early enough so that the company can protect itself from claims for financial damages and a loss of reputation.
- ▶ The board of directors determines the company's policy and values and lays down the foundations for compliance within the organization. The corporate management ensures compliance with the law in the company's day-to-day business and provides adequate staff and material resources for it to be done.
- ▶ The management regularly reports to the board about the company's efforts at compliance and how effective they have been.

I. Introduction

► Compliance as a central element of careful business management.

In the business world, compliance is the adherence to laws, standards, and internal rules of behaviour. Within the company, compliance management is the key instrument for ensuring law-abidance and is therefore a vital component of good, diligent management.

► Globalization and regulatory environment require professional compliance.

The Swiss economy is highly globalized and its value chains and products are becoming increasingly complex. While at the same time there is an increase in legislation (for example, laws on competition, corruption, or the financial markets) and its consistent enforcement by the authorities. In addition, the ethical expectations of companies on the part of the media and the general public are steadily rising. Integrity and compliance are therefore a challenge for all companies and their significance should not be underestimated. The most recent economic crisis has shown us that companies without complete compliance run the risk of massive damage in terms of both finances and reputation. However, companies with effective compliance have been able to seize the opportunities presented by the crunch and gain market share. Companies therefore have everything to gain by adopting a culture of complete integrity and professional compliance management.

► Guidelines for effective compliance management.

economiesuisse the umbrella organization of Swiss businesses from all sectors, intends this publication to provide a framework for effective compliance management and contribute to the discussion on compliance. The publication is intended first and foremost for the members of the boards of directors and the executive management in Swiss companies. These guidelines for effective compliance management were inspired by international compliance practice¹, but adapted to the needs and particularities of Swiss businesses. However, on the basis of the essential building blocks, each individual company needs to establish its own compliance plan and put it into long-term practice. The principles presented in the next few chapters are the result of work by the economiesuisse Committee for Legal Issues in collaboration with an experts panel from the SwissHoldings Compliance Group.²

¹ For example, there is reference to UN Global Compact (www.unglobalcompact.ch), the Implementation Guide for the ICC Codes (ICC Document No. 240/619, December 2009), the Ethics and Compliance Book of the Ethics & Compliance Officer Association (Waltham, USA, April 2008) and the guidelines for a good compliance programme as described in the US Federal Sentencing Guidelines Manual of the United States Sentencing Commission (www.ussc.gov).

² The articles have been written by the working group of the economiesuisse Committee for Legal Issues, comprising Dr Daniel Lucien Bühr (Schindler Management AG), Dr Philip Kübler (Swisscom AG), Dr Patrick Sommer (CMS von Erlach Henrici) and Christian Stiefel (SwissHoldings). The experts panel comprised Dr David Frick (Nestlé), Dr Urs Jaisli (Roche), Dr Knut Mager (Novartis), Prof. Dr Othmar Strasser (ZKB), Alfred Gerber (Sulzer), Georg Matiaska (Valora) and Jürg Wyser (PWC).

II. The term 'compliance'

▶ Ensuring law-abidance.

The term 'compliance' basically means ensuring law-abidance. Private and public stakeholders expect that any company will conduct its business in a way that complies with applicable standards. Seen from this perspective, compliance can also be defined as the state of integrity expected by the stakeholders on the basis of the civil responsibility of the companies. Historically, the term 'compliance' and the practice itself are both of US origin, and date back to the legal violations in the American defence industry in the 1980s. Since the early 1990s there has been the recognition in the American economy that each company should be aware of its strategic legal risks and should systematically prevent infringements of the defined core legal areas. Since the late 1990s compliance has also become a key element of diligent corporate management and successful risk management for European businesses. In recent years, increasing emphasis has been placed on integrity in business³. Companies – just like any citizen – are required not only to behave in accordance with the law but also with complete integrity.

▶ Abidance by the law – the board's inalienable duty.

Guaranteeing abidance by the law in the broader sense, as it is described, for example, in Article 716a of the Swiss Code of Obligations as the non-transferrable and inalienable duty of the board of directors of a public limited company, is the starting point of this article. However, beyond law-abidance, a culture of complete integrity should also be maintained. For this the framework is used in which the staff adhere to the corporate ethos and constantly strive for new goals. As shown below, this goal can be achieved with a systematic and efficient compliance management system.

III. Five fundamentals of effective compliance

▶ Compliance as a basic duty.

The fact that companies nowadays are running law-abidance systems or compliance programmes is among the core elements of careful business management. The content of the compliance programme will be different depending on the strategic risk profile ('risk map') of the particular company. Smaller companies that only operate in Switzerland can take clear, straightforward measures to ensure law-abidance, whereas multinationals need to run a comprehensive professional compliance programme. Although there is no single binding model for effective compliance management, there are common fundamental elements for effective compliance as shown, for example, in the 'Compliance House' (cf. figure p. 3).

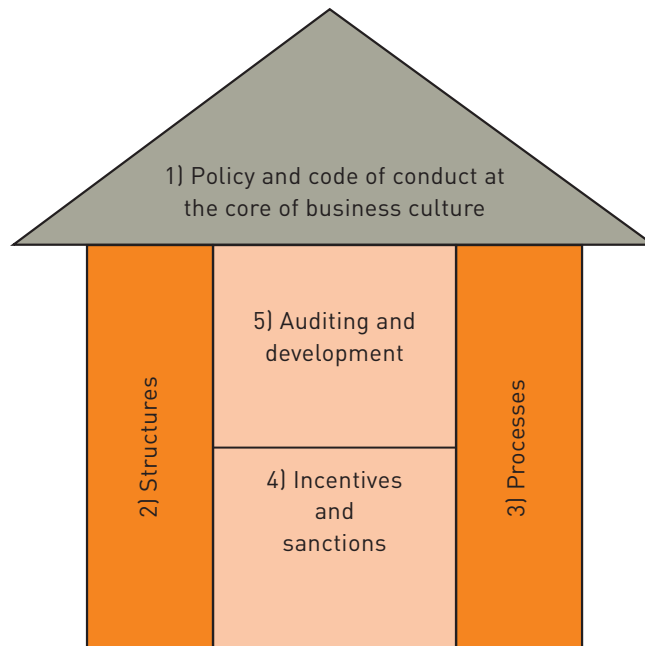
³ Ben W. Heinemann Jr., High Performance with High Integrity, Harvard Business Press, 2008.

Graphic

► The Compliance House, comprising five fundamentals, is one approach to effective compliance.

The Compliance House

Five fundamentals of effective compliance



Source: author's design.

► Commitment by corporate management to integrity as core of business culture; code of conduct issued.

► Corporate management decides on organization and provides adequate resources.

► Regular risk analysis and targeted training.

1) Policy and code of conduct are the roof of effective compliance

The corporate management⁴ commits to complete integrity, in particular to abidance by the law as a key part of its corporate culture and the foundation of its business operations. It issues a code of conduct (code of ethics, code of business conduct, or similar).

2) The structure of the compliance organization is the first pillar of the Compliance House

The corporate management ensures that the code of conduct, in particular the requirement to abide by the law, is effectively implemented by the compliance structure. It makes adequate financial, staff and material resources available. The structural guarantee of the effectiveness of compliance includes the creation of independent bodies to which concerns and infringements can be reported in confidence.

3) The compliance processes are the second pillar of the Compliance House

The compliance processes and the compliance organization together form the company's compliance programme. Planned, systematic processes include, for example, the regular analysis of the legal risks, publishing and implementing internal regulations, training exposed staff, and handling concerns and infringements.

⁴ In public limited companies, the board of directors. When responsibility for running the company is entrusted to third parties (corporate management) the principles also apply to these third parties.

▶ Transparent incentives and sanctions.

4) Appropriate incentives and sanctions complete the Compliance House
Integrity and acting within the law should be the prerequisites for any remuneration. If needs be, particular achievements relating to integrity and compliance, and therefore to the corporate culture, can be rewarded. But under no circumstances should the effectiveness of the compliance programme be sacrificed to conflicting commercial incentives. Culpable breaches of the law should be sanctioned so that punishment and deterrence emphasize the fact that compliance is binding and non-negotiable. The requirement for integrity and compliance together with sanctions in the event of culpable breaches of the law are transparent parts of the staffing and remuneration policy of the company.

▶ Regular audits for effectiveness.

5) Testing the effectiveness and the constant improvement of compliance measures are cornerstones of the Compliance House
The corporate management ensures that the compliance management is regularly tested for effectiveness. Weaknesses in the programme or individual measures are then put to rights. The compliance system must be adapted to take account of any changes in the company (i.e. new products, new markets, etc.).

IV. Comments on the five fundamentals of effective compliance

▶ Corporate management as a role model.

1. Policy and code of conduct – corporate culture
Compliance starts with the commitment of the corporate management to abide by the law as a fundamental condition of all business operations. This commitment to law and order must be genuine, unequivocal, firm and constant; it is the foundation of a compliance-oriented corporate culture. The commitment to law-abidance must be made public within the company and outside, and the corporate management must act as role models in this ('walk the talk').

▶ Corporate management as legislator.

The corporate management issues a code of conduct. The code of conduct belongs to the highest-level regulations ('constitution level') in the company and lays down the ethical and moral framework in which the business operations are conducted.⁵ It is a set of guidelines and a moral reference point for the company. The code of conduct entitles, motivates and obligates the corporate management and all staff.

⁵ In practice, many codes of conduct broadly call for ethical behaviour, i.e. personal integrity and honest, respectful business operations. This takes into account the fact that in many countries legally permitted yet morally reprehensible practices exist (in particular in the corruption sector).

Example 1

▶ Code of conduct.

Example of an elementary code of conduct

As employees of Example Ltd we behave in an ethical manner towards customers, suppliers, competitors, the authorities and our colleagues.

We abide by the following principles:

1. We abide by the laws and standards in force.
2. We respect the human dignity and the rights of every individual.
3. We do not offer bribes to anyone; nor do we accept bribes.
4. We avoid conflicts of interest or declare them at an appropriate time.
5. We maintain the confidentiality of internal data.
6. We respect and safeguard the intellectual property of Example Ltd.
7. We actively support the implementation of this code of conduct.

Example 2

▶ Applying a code of conduct.

Example of the importance of a code of conduct in everyday business

Code of conduct (excerpt):

1. *The employees of the Example Group abide by the laws and standards in force.*

Circumstances: The head of human resources of the Example Group would like to restrict the staff's use of the internet for private purposes in the workplace. In order to understand to what extent the staff use the internet for private purposes, he wants to have the staff's behaviour monitored secretly. Although he is dubious about the legality of this procedure, he asks the IT department – without any further explanation – to secretly monitor and analyse the staff's online behaviour.

Assessment: The head of Human Resources knows that he must obey the law. The legislation includes the labour law that prohibits any secret monitoring of employees unless they are specifically suspected of abuse, and also the data protection law that only permits the collection and processing of personal data if the persons concerned are aware that this is being done. The head of Human Resources is familiar with the broad outlines of this legislation. However, he rates the company's objectives to be more important and omits any clarification of the legal aspects. By doing so the head of Human Resources accepts to break the law. He commits a breach of the code of conduct and through his actions the head of Human Resources puts the Example Group at risk in terms of its liability and reputation.

► Compliance structure.

► Responsibility of board and corporate management.

► Internal ombudsman and external reporting body improve compliance.

Example 3

► Basic structure of a compliance programme.

2. The structure of the compliance organization

The structure and processes of compliance are the main pillars of the Compliance House. They make it possible to implement the principles laid down in the code of conduct. The structure and organization of the compliance programme must be designed from the outset in such a way that illegal behaviour in general is prevented or detected.

The board of directors bears the ultimate organizational responsibility. It organizes the company in such a way that any breaches of the law can as a rule be avoided or detected with appropriate effort and in good time. The board of directors decides the outlines of the staff and structural organization of the legal and the compliance function. Among other things, it decides whether the functions are joined or separate, whether they are handled centrally or not, to whom these functions report (board of directors, audit committee, CEO, etc.) and what resources and tools will be allocated to these functions so that they can do their work effectively and reliably. The board of directors bears the ultimate responsibility for compliance. This responsibility cannot be delegated to any other body. However, the board of directors can delegate compliance tasks to the corporate management, which can in turn delegate the support and supervision of the employees to legal and/or compliance officers. Despite this cascade of responsibility, each member of a body and every employee is personally responsible for compliance within his or her sphere of influence.

To increase the likelihood that reprehensible practices are detected, internal and/or external reporting bodies should be set up. These bodies must be independent in the sense that the staff run no risk of reprisals in the event that they report misconduct. Whistle-blowing must also be protected by guaranteed anonymity and confidentiality. It is conceivable, for example, to have an internal ombudsman for reports of concerns from employees and an external reporting body for confidential or anonymous complaints.

Example of basic structure of a compliance programme

A compliance programme that is effective and integral in its design as a rule features the following basic elements:

- Content and mode of operation of the compliance programme are known to the top management; it supervises how the programme is carried out and its effectiveness.
- The corporate management ensures that the necessary resources, powers and direct reporting lines required to carry out the compliance programme are guaranteed.
- The company informs and regularly trains its staff appropriate to their level in the organization about the principles and rules for complying with the code of conduct. It answers any questions asked by the staff in a timely and competent manner.
- The company checks compliance and effective implementation of the code of conduct in an appropriate way. It ensures that the staff and third-parties can contact a reporting body, maintaining anonymity if requested.
- The company does not establish any commercial objectives that run counter to compliance with the code of conduct. It punishes any infringement of the code of conduct. The compliance programme is regularly and systematically tested for effectiveness.

► Compliance processes: survey, evaluation, advisory and testing activities.

► Training and advising staff.

Example 4

► Training staff.

3. The compliance processes

The compliance processes are the operative component of an effective compliance programme. They are systematic procedures for surveying, evaluating and testing relevant information on compliance with legislation and standards. In addition to this, reliable advice for the staff is a central resource for effective compliance. The processes include in particular establishing and applying a general risk analysis, publishing internal rules and directives, developing and applying concrete risk-minimizing measures, training and support for staff, answering questions about compliance ('speak-up' principle for staff, and 'ask-me' principle for the legal and compliance function), processing reports and conducting checks. In addition to the processes that are specifically compliance-oriented, compliance elements should also systematically be embedded in the business operations.

The regular training of staff creates awareness and understanding of the importance of the code of conduct and the internal rules of behaviour. As compliance with legislation requires a basic knowledge of the law and awareness of the rules of behaviour, the company has an obligation to train its staff thoroughly. The training must be systematic and recurrent. It must consider the specific corporate risks and the current state of employees' knowledge and their responsibilities. In addition to training, advising staff is another key compliance process. Staff must be able to put questions directly or indirectly to the legal and compliance function(s) and receive competent answers within a reasonable period of time.

Example of training in a Swiss multinational

The company holds code-of-conduct training sessions at least once a year for all new employees in each group company. During these sessions the company's values and code of conduct are presented and explained by trained staff (lawyers and compliance officers). In addition, the rules of conduct with regard to bribes and competition law are explained in detail. The company has pinpointed these two sectors as major legal risks.

All staff members must regularly attend a code-of-conduct training session. The training is either in the form of a computer course or as a face-to-face session. Each training session is followed by a confidential electronic compliance survey. In this survey the staff are able to comment on compliance with the code of conduct and alternating specific compliance questions.

The knowledge of the code of conduct is always refreshed whenever there are important management meetings, such as meetings of country or regional managing directors.

If they have questions, staff can contact the legal advisor or the compliance officer of their group company or the group's legal department.

In areas where there are particular legal risks, compliance training sessions are held that tackle those specific legal risks.

▶ Incentives and sanctions: effective ways to implement the code of conduct.

4. Appropriate incentives and sanctions

Staff do not only share responsibility for the financial success of the company but also for the law-abidance of the business operations and maintaining the company's reputation. Incentives for both management and staff are an effective tool in putting the code of conduct into practice. Law-abidance is therefore a requirement of any effective compliance programme and is supported if necessary by incentives. Culpable breaches of the law and internal rules, on the other hand, are punished with a sanction. Sanctions may take the form of a reduction in financial entitlements, an official warning, or even dismissal.

▶ No remuneration without integrity and risk transparency.

A company should not undermine the code of conduct by rewarding commercial success even though legal risks are being ignored. Attention should also be paid to the fact that unrealistic commercial objectives, combined with group pressure, may cause individual employees to break the law and internal directives. The corporate management must therefore make it clear that good performance is not only commercially above average but also systematically takes account of and minimizes the risks associated with any business. In this respect, risk management first and foremost focuses on abidance with the law.

▶ Regular preventative testing.

5. Testing the conceptual effectiveness of compliance

Measures taken by the company to ensure abidance by the law must systematically be tested for effectiveness. The main tool for this is preventative testing, which can be carried out announced or unannounced. Qualified internal or external staff investigate whether corporate management and the staff are abiding by the laws and internal directives. The level of knowledge and business practices must be assessed and business procedures and correspondence examined in detail and evaluated.

▶ Guaranteeing conceptual effectiveness.

The ineffectiveness of a compliance programme in an individual case does not mean that it is ineffective overall, i.e. in the way it is designed. However, if a significant breach of the code of conduct and the rules of conduct is discovered, then the compliance programme must be re-examined. It must be ascertained what caused the breach. If any individual breach is attributable to incomplete or faulty compliance organization, a lack of or unclear rules, or insufficient training or support for employees, then the compliance programme needs to be improved.

▶ Corporate culture and empowering staff as a buffer.

A company's own standard to act with integrity and abide by the law does not mean that every imaginable breach of the law by staff must be prevented by all means possible. Instead, companies should rely on their promotion of ethical conduct, on staff's taking responsibility and on their adequate compliance efforts.

▶ Compliance must consider the principles of risk management.

Corporate compliance is about identifying the strategically relevant risks of not abiding by the law and, applying the principles of risk management, concentrating on preventing serious breaches before they occur. For all companies these risks include offering and taking bribes, breaches of competition law, health and environmental protection regulations, personal rights, and product safety rules. Focusing on serious breaches of the law does not mean that a company might accept culpable breaches of the law by its corporate management and staff in other areas. All companies bear a duty to exercise diligence in the management of their business and therefore a general obligation to obey the law.

▶ Compliance expectations regardless of the type and size of company.

Compliance expectations apply to all companies regardless of their type and size. The details and application of specific compliance measures on the other hand are defined individually. Smaller companies will have straightforward compliance measures. Setting a good example and strength of character of the owner along with a few written rules on the values of the company might suffice. This can be combined with some training sessions with a consultant, external legal support for the business operations and an internal control system. Medium-sized companies as a rule have a higher risk than smaller companies in the event of a serious breach of the law. Consequently the compliance programme must be thought through in greater detail. It must be totally sound. The internal organization, the processes and the control mechanisms should, however, still be straightforward and fit for purpose.

▶ Multinationals with state-of-the-art compliance systems.

Large companies require a professional compliance system (best-practices benchmark). The legal issues are considerably more complex and there are far more people involved than in smaller companies. Since a serious breach of the law can jeopardize the reputation or even the very existence of the company, the commitment to law-abidance must be a prominent part of the corporate culture and the upholding of moral values a constant focus of the corporate management. An effective compliance programme is the concrete proof of the policy and of the expectations of the code of conduct. The corporate management ensures that the compliance organization is provided with appropriate resources and equipped with the necessary internal powers and a direct reporting line to it. Design and conceptual effectiveness of the compliance programme should be checked regularly by experts. If there are any shortcomings the corporate management has the duty of diligence to adapt the compliance programme promptly.

V. Compliance as a challenge

▶ Compliance management needed more than ever.

Setting up and running a compliance management system is more necessary than ever for companies faced with increased legal and societal demands and in a complex economic environment. Effective compliance reduces the danger of legal sanctions, financial losses and damaged reputations. The corporate management's clear and visible commitment to integrity and law-abidance is of key importance. The corporate management must enforce the policy and code of conduct and establish an adequate and functioning compliance organization. Early-warning systems, internal directives, training and targeted incentives and sanctions are important elements for effectively containing and avoiding business risks.

▶ Compliance management to ensure ethically correct conduct – companies as good citizens.

Compliance does not only involve abiding by the law but also ensuring the integrity and socially and ethically responsible conduct of all the company's employees. Effective compliance therefore strengthens a corporate culture, and the business decisions are not taken merely according to economic criteria, but always also include the complete social and ethical responsibility of the company as an equal decision-making criterion. Professional compliance management is therefore a central component of diligent management and a demonstration that the company is not only striving for long-term profitability but that it also maintains a culture of integrity and takes its social responsibility seriously.

▶ Duty of corporate management.

Setting up and running an effective compliance system is a major challenge for a company. Depending on the company's size and business, the compliance measures it requires are more or less extensive. So the compliance programme must be tailor-made to fit the company. However, the expectations of state and society are the same for any company. The corporate management is therefore obliged to constantly and diligently check whether its business and internal organization is in line with the law and the rules of ethical conduct and to correct any shortcomings appropriately and in good time.

Queries:

thomas.pletscher@economiesuisse.ch

Impressum

economiesuisse, Swiss Business Federation
Hegibachstrasse 47, Postfach, CH-8032 Zürich
www.economiesuisse.ch