SwissHoldings

Verband der Industrie- und Dienstleistungskonzerne in der Schweiz
Fédération des groupes industriels et de services en Suisse
Federation of Industrial and Service Groups in Switzerland

economiesuisse

fundamentals of effective compliance management

Contents

Effective compliance management

Compliance as a corporate principle

The Swiss economy is highly globalised and its value chains are becoming increasingly complex. This development is taking place against a background of increasing government regulation and legal enforcement. In this environment, professional integrity is a fundamental principle of diligent management. If companies want to be successful in the long term, they must foster a culture of compliance. The term "compliance" generally covers the observance of legal requirements as well as internal behavioural guidelines (codes of conduct, directives); nowadays, it also typically includes a commitment to acting with integrity. Various measures must be taken at all levels (compliance management system) if a compliance culture is to be established in a company. Compliance is primarily the result of effective management; conversely, compliance infringements are often the result of inadequate or deficient management. The compliance working group of SwissHoldings developed the basic elements of an effective compliance management system and published them within an economiesuisse policy document. When the "Swiss Code of Best Practice for Corporate Governance" was revised, this document was updated and referenced as the "Swiss Guidelines for Best Practice in Compliance Management". With systematic compliance management which adequately covers company risks, Swiss companies are convinced that they can avoid statutory violations as far as possible, and promote professional integrity. Effective compliance management is therefore an indispensable component of diligent management. Companies contribute to their social responsibility through good compliance and acting with integrity.

Note about terminology:
In accordance with its function as a supplement to the "Swiss Code of Best Practice for Corporate Governance", the terminology used in this document is geared towards the legal form of the public limited company. However, the principles contained herein also serve mutatis mutandis as guidance for other legal forms using different terminology for the management functions as appropriate.

Position of economiesuisse and SwissHoldings

- One of the core statutory tasks of the Board of Directors is the supervision of persons entrusted with the management of the company, specifically with regard to compliance with the law and internal behavioural guidelines. The Board of Directors must ensure compliance with the law and internal behavioural guidelines as well as ethical business practices, also known as "compliance", and supervise and adapt the aforementioned to any amendments with a high degree of due diligence. The aim is to avoid statutory violations or to discover them in good time and thus to protect the company from financial damage and loss of reputation, as well as to protect the company's employees.
- The Board of Directors determines the credo and values of the company and defines the broad outline of the compliance organisation. The management ensures compliance with the law and behavioural guidelines as well as integrity in daily business, and provides adequate staff and material resources to do so.
- The management regularly reports to the Board of Directors on the compliance efforts of the company and how effective they have been.

Introduction

Compliance as a central component of diligent corporate governance

In the business world, compliance is the observance of laws, standards, and internal rules of behaviour. Nowadays, this is connected with a general commitment to behaviour. Along with strong values and a clear commitment to compliance, company-internal compliance management geared towards the specific risks is one of the integral components of good, careful corporate governance.

Globalisation and the regulatory environment require professional compliance management

The Swiss economy is highly globalised and its value chains and products are becoming increasingly complex. At the same time, there has been an increase in regulation (for example in competition law, data privacy and data storage law, corruption law and in sector-specific regulatory areas) and its consistent enforcement by the authorities. In addition, expectations from investors, non-governmental organisations, employees, the media and the general public that companies will act with integrity in their business dealings are also growing. Ensuring compliance is therefore a challenge for all companies. Companies without complete compliance run the risk of sustaining massive financial damage and loss of reputation, or even losing their licence to operate. On the other hand, effective compliance can lead to comparative advantages over other companies and help companies to better master corporate challenges. Therefore, companies have an inherent interest in a culture of utmost integrity and thus in comprehensive and effective compliance management.

Principles for effective compliance management

With this publication, economiesuisse and SwissHoldings, as the Swiss Business Federation representing all sectors, intend to rewrite the principles for effective systematic compliance management and to contribute to the discussion on Swiss best practice in the area of compliance management as well as on the admissibility of a "corporate defence" in the event that all required and reasonable compliance measures have been taken. This policy document is inspired by international compliance developments; however, it still focuses on the needs and specific features of Swiss companies. On the basis of the essential building blocks, every company must establish an adequate and risk-based compliance concept for itself and implement it sustainably. The principles of effective compliance management presented in the following paragraphs are the result of the work of SwissHoldings' Commission of Experts well as the economiesuisse Commission for Legal Issues and Commission for Competition Issues.[1]

[1] The first edition of the compliance policy document was developed by the compliance working group of SwissHoldings and published by economiesuisse in 2010. As part of the revision of the "Swiss Code of Best Practice of Corporate Governance", it was revised, reprinted and comprehensively referenced therein in 2014. The revision was undertaken by a committee of experts consisting of Jacques Beglinger (SwissHoldings), Daniel Lucien Bühr (LALIVE; ISO expert), David Frick (Nestlé), David Hügin (Clariant), Urs Jaisli (Roche Holding AG), Michael Neff (Kuoni Reisen Holding), Othmar Strasser (ZKB) and Christian Stiefel (SwissHoldings).

The term “Compliance”

Term and development of compliance

To begin with, the term “compliance” means ensuring the observance of applicable legislation as well as commitment to self-regulatory standards (code of conduct, company directives, association codes, etc.). Private and public stakeholders expect every company to do business in accordance with the 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 social responsibility of the companies. Nowadays, the term “compliance” therefore typically involves a strong commitment to acting with integrity (“do the right thing”).

Ensuring observance of the law – the Board of Directors’ inalienable duty

Compliance is achieved if a company abides by all the binding guidelines; this occurs on the one side as a result of a forward-thinking company culture and on the other through value-oriented behaviour from the line managers and the staff.

(For further information on the subject, see the definition of compliance in the ISO standard 19600 – Compliance management systems.)[2]

[2] «Compliance is an outcome of an organization meeting its obligations, and is made sustainable by embedding it in the culture of an organization and in the behaviour and attitude of people working for it. Policies and procedures to achieve compliance must be integrated into all aspects of how the organization operates. Compliance should not be seen as a stand-alone activity, but should be part of the organization’s overall strategic objectives. An effective compliance management system will support these objectives. Compliance management should, while maintaining its independence, be integrated with the organization’s financial, risk, quality, environmental and health and safety management systems and its operational requirements and procedures.»; ISO 19600 – Compliance management systems – Guidelines; s. www.iso.org.

Five basic elements of effective compliance

Compliance as a core corporate duty

The fact that companies nowadays are running law-abidance systems or compliance programmes or – according to the new terminology – compliance management systems is one of the core elements of careful management. The content of the compliance programme will differ depending on the strategic risk profile ("risk map") of the particular company. Companies with risk-inclined business activities or activities in geographical risk zones should pay closer attention to compliance management. Smaller companies will be able to take simpler manageable measures to abide by the law, whereas multinationals will need to operate a comprehensive compliance programme. Although there is no single binding uniform concept for effective compliance management, there are common basic elements for effective compliance as shown, for example, by the "Compliance House" diagram (See Figure 1, page 8).

1

Active commitment and responsibility from the Board of Directors and the executive management form the framework of effective compliance management

Commitment by management to integrity as the core of its company culture; enactment of a code of conduct

Senior management is committed to utmost integrity, in particular to abidance by the law and internal behavioural guidelines as a key part of its corporate culture and an overriding principle of its business operations ("tone from and at the top"). It shall enact a code of conduct (standards of integrity, code of business conduct or similar) and, through consistent management, shall ensure that these guidelines are observed at every level and when necessary also enforced ("walk the talk"). There should be no doubt that it expects its staff to act with integrity and abide by the regulations in all circumstances ("do the right thing").

2

The structure of the compliance organisation is the first pillar of the Compliance House

The management decides on the organisation and provides adequate resources

The management ensures that the code of conduct is effectively implemented by the structural set-up of the organisation. It provides adequate financial, personnel and material resources. In doing so, the compliance function can be organised separately or integrated into other support functions provided that the necessary independence and coordination are ensured. The structural guarantee of the effectiveness of the compliance programme includes the creation of at least one independent body to which concerns, suspicions and infringements can be reported in confidence.

3

The compliance processes are the second pillar of the Compliance House

Regular risk analysis and appropriate training

The compliance processes and the compliance organisation together form the company's compliance programme. Planned, systematic processes include, for example, regular analysis of the legal risks, enacting and implementing internal directives, providing line managers and staff with risk-based training, and handling reports of compliance concerns or infringements.

4

Appropriate incentives and sanctions complete the Compliance House

Transparent incentives and sanctions

Acting with integrity and compliance with the regulations should be the prerequisites for any remuneration. Non-compliance must be appropriately sanctioned. If need be, special efforts to act with integrity and comply with the regulations can also be rewarded. But under no circumstances should the effectiveness of the compliance programme be sacrificed in favour of conflicting commercial incentives. Culpable breaches of compliance must then be sanctioned by the responsible line managers to underscore the company's commitment to compliance on the one hand ("walk the talk"), and to prevent it from being liable in connection with investigations of misconduct on the other hand. The requirement for integrity together with sanctions in the event of culpable breaches should become transparent and consistent parts of the company's personnel and remuneration policy.

5

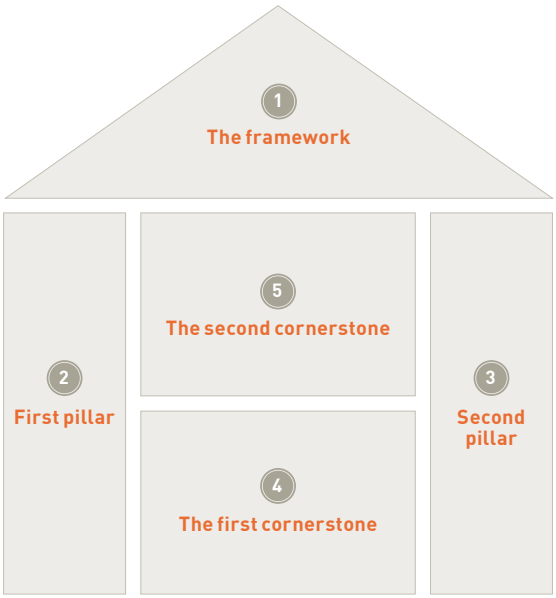
Audits to test effectiveness and constant improvement of compliance measures are the cornerstones of the Compliance House

Regular audits for effectiveness

The management ensures that the company's compliance programme is regularly audited to test its effectiveness. Weaknesses in the programme or individual measures are then remedied. The compliance programme must also be adapted in risk-based terms to take into account any changes in the company (i.e. new products, new markets, etc.).

Figure 1
The Compliance House, comprising five basic elements, is one approach to effective compliance.

The Compliance House
Five basic elements of effective compliance



The framework
Commitment and responsibility on the part of the Board of Directors and the executive management

First pillar
Structures

Second pillar
Processes

The first cornerstone
Incentives and sanctions

The second cornerstone
Auditing and Development

Explanations of the five basic elements

Commitment and responsibility on the part of the Board of Directors and the executive management

Management as a role model

Compliance starts with the commitment of the senior management to abide by the law and internal behavioural guidelines as a fundamental condition of all the company's business operations. This commitment to observe certain standards must be genuine, unequivocal, firm and constant; it is the foundation of a compliance-oriented corporate culture. The commitment to law-abidance and internal behavioural guidelines must be made public within the company and externally, and the management must act as role models on all levels ("walk the talk") and enforce it where necessary. There should be no doubt that it expects its line managers and staff at all levels to act with integrity and abide by the regulations in all circumstances ("do the right thing").

Management as "legislator"

The management should enact a code of conduct. The code of conduct belongs to the highest-level regulations ("constitutional level") in the company and lays down the binding framework in which the business operations should be conducted. It is a guideline and a moral reference point for the company. The code of conduct entitles, motivates and obligates management and all the staff.

The structure of the compliance organisation

Compliance structure

The structure and processes of the compliance programme are the main pillars of the Compliance House. They make it possible to implement the maxims laid down in the code of conduct. The structure and organisation of the compliance programme must be designed from the outset in such a way that illegal behaviour can be prevented whenever possible, or, if it still occurs, quickly discovered and corrected.

Responsibility of management

The management bears the supreme organisational responsibility. It organises the company in such a way that any infringements of the law can usually be avoided or detected in good time. It determines the fundamentals of the personnel and the structural organisation of the legal and compliance function. It decides, among other things, whether the functions are joined or separate, whether they are managed centrally or not, to whom such functions report (Board of Directors, Audit Committee, CEO, etc.) and what resources and tools will be allocated to them so they can do their work effectively and reliably. The Board of Directors bears the supreme responsibility for the observance of compliance in the organisation (See Art. 716a [1] Sect. 5 Swiss Code of Obligations). According to the will of the legislature, the Board of Directors is accorded an extremely important role in comprehensive compliance management; it ensures that the governance principles are

put into practice[3] and it must ask management compliance-relevant questions, i.e. questions on the significant compliance risks in the company and the relevant operative markets for the company, the integrity of the company's line managers, the subsequent compliance assurance and compliance verification measures as well as the appropriate corrective and sanction measures which were undertaken by the management subsequent to a case of non-compliance. However, the responsibility for the operative implementation of the required compliance measures very definitely lies with the management and the line organisation, which can enlist the support of the compliance function to fulfil these duties in a proper and risk-appropriate manner. The guiding rule for compliance responsibility is as follows: Every member of a body and every staff member is personally responsible for compliance within his or her sphere of responsibility and influence. Compliance is therefore the responsibility of each individual staff member involved in the company's daily business. Accordingly, the Compliance support function is also not liable for misconduct by staff or line managers.

Independence and coordination

The compliance function can be freed from other support functions and organised separately or integrated into one or more support functions (such as law, regulatory, HR, quality management, etc.). This has the advantage of giving it structural independence. In the latter case, one recommendation would be to create an interdisciplinary compliance committee which ensures the necessary independence and a coordinated, holistic approach. Corporate governance and risk management may be included as part of an integrated governance, risk and compliance (GRC) model.

Internal speak-up, ombudsman and external reporting bodies improve compliance

Internal and/or external reporting bodies should be set up to increase the likelihood of prohibited practices being detected. This process must be designed in such a way that staff who report suspicion of misconduct or actual misconduct run no risk of suffering reprisals. The reports must also be able to be given anonymously and confidentially. For example, one conceivable approach would be to have an internal ombudsman for reports of concerns from staff and set up a whistle-blower hotline or online portal, or even an independent external reporting body for confidential or anonymous complaints. The motives for a reporting system ("speak up") and setting up a reporting body should be communicated internally openly and without reservation on a regular basis. The staff should be regularly encouraged to use the reporting system in the interests of the company (create a "speak-up" culture).

[3] According to ISO 19600, Section 4.4, the Good Compliance Governance principles are: Direct access for the compliance function to the most senior management body, their independence from the line as well as the guarantee of adequate authority and resources.

Example 1

Basic conceptual structure of a compliance programme

A compliance programme which is effective and integral in its design generally contains the following basic elements:

The senior management ensures that the required management measures have been taken to implement the compliance programme, that the compliance function(s) has/have direct access to it, that it is/they are organisationally independent, and that it possesses/they possess the necessary internal expertise and adequate resources.

The content and mode of operation of the compliance programme are known to the senior management; it ensures that the effectiveness of the programme is regularly and systematically checked by management at all levels with the support of the compliance function(s).

The compliance function(s) has/have the required know-how, expertise and resources to recognise and deal with company-relevant compliance risks.

The company informs and regularly trains its line managers and staff appropriate to their level in the organisation on its values, culture and principles of behaviour. It answers any questions asked by its 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 staff and third parties can contact a hotline or a reporting body, while ensuring their anonymity if requested.

The line managers do not set any commercial objectives which run counter to compliance with the code of conduct. They ensure that any non-compliance with the code of conduct is sanctioned appropriately.

The compliance management system is regularly tested for effectiveness and continuously improved.

The compliance processes

Compliance processes as survey, evaluation, consultancy, and testing activities

The compliance processes are the integral 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 line managers and staff is a central resource for effective compliance. These processes include, in particular, establishing and applying the procedure within the context of a general risk analysis[4], enacting internal behavioural rules and directives, developing and applying concrete risk-minimising measures, training and support for staff, answering questions about compliance ("help & advice" principle and "speak-up" principle), processing reports and conducting checks. In addition to the processes that are specifically compliance-oriented, compliance measures should also be systematically embedded in the company's business operations.

Training and advising staff and line managers

Regular training for staff and line managers creates an 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 is obligated to train its staff and line managers thoroughly. The training must be systematic and recurrent. It must consider the specific corporate risks, the current knowledge of its staff and their responsibilities.

In addition to training, advising staff is another key compliance process. The staff must be able to put questions to the legal and compliance function(s) and receive competent answers within a reasonable period of time.

Executive management is responsible for making sure that the necessary resources are available for training and advising staff.

[4] Public limited companies that are subject to ordinary auditing must have an internal control system. The internal control system deals primarily with operative and financial risks faced by the company. The internal control system may form a component of the company's integral compliance programme. However, the internal control system in no way replaces a compliance programme.

Example 2

Training in a Swiss multinational

The company holds code-of-conduct training sessions (content, processes, responsibilities) for all its new staff at least once a year. Furthermore, the line management is also trained on an on-going basis according to their function. 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 because the legislator has identified these two sectors as major legal risks and has requested that the company take necessary and reasonable measures to avoid cases of non-compliance (see, for example corporate criminal law in accordance with Art. 102 [2] Swiss Criminal Code).

All staff members must regularly attend code-of-conduct training. This training is either in the form of a computer course or takes place as a face-to-face session. Each training session is followed by a compliance survey, in which the staff declare that they have understood and complied with the guidelines on integrity ("compliance assurance").

The topic of compliance is a standard item on the agenda during management meetings and knowledge of the code of conduct is always refreshed with concrete business-internal and external case examples.

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

Appropriate incentives and sanctions

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

The staff not only share responsibility for the financial success of the company but also for the legality of the company's business operations and the conformity of these operations to the in-company guidelines, and responsibility for protecting the company's reputation. In addition to the objectives ("What"), the way of achieving the objectives ("How") should be taken into account during the performance assessment. Incentives for both management and staff are an effective tool to enforce the code of conduct. 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, must be punished with an appropriate 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 if legal or reputational risks are being ignored. Attention should also be paid to the fact that unrealistic commercial objectives, combined with group pressure, may cause individual staff members to break the law and breach internal guidelines. Executive management must therefore make it clear that performance will be assessed in light of the hidden commercial goals but at the same time also on the basis of the set expectations of integrity.

Testing the conceptual effectiveness of compliance

Regular preventive audits

Measures taken by the company to ensure abidance by the law and internal guidelines must be tested systematically for effectiveness. The main tool for this is preventive testing, which can be carried out announced or unannounced ("compliance verification"). Qualified internal or external staff investigate whether the line management and the staff are abiding by the laws and internal guidelines. The level of knowledge and the business practices of the line managers and the staff must be assessed, and business procedures and correspondence must be 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 infringement of the code of conduct and the rules of behaviour is discovered, the compliance programme must be re-examined.

Corporate culture and empowering staff as a buffer

A company's own efforts to act with integrity and abide by the law and internal guidelines does not mean that every imaginable breach of the law by its staff members must be prevented by all means possible. Instead, companies must rely on their promotion of a company culture of integrity, on staff taking responsibility and on an adequate effort to ensure compliance.

Compliance must follow the principles of risk management

Corporate compliance is about each company identifying its strategically relevant risks of not abiding by the law and internal guidelines in advance and, applying the principles of risk management, concentrating on preventing infringements of laws and guidelines relevant to the company before they occur.

Compliance expectations regardless of the type and size of the company

Compliance expectations apply to all companies regardless of their type and size. The details and implementation of specific compliance measures on the other hand must be defined by every company individually. Smaller companies will have straightforward compliance measures. Depending on the circumstances, setting a good example and the strength of character of the owner along with a few written rules on the values of the company might suffice. Nowadays, it is evident that compliance is more often than not the result of good management by the line management at all levels of the company. This involves introducing an effective compliance management system and above all carefully selecting, instructing and supervising staff. Such efficient management is an indispensable requirement for the creation of compliance; furthermore, training sessions with external experts, legal support for the business operations and an internal control system are other practical measures to achieve compliance in the company.

Multinationals with comprehensive compliance programmes

Large companies require a professional compliance system (best practices benchmark). The legal questions to be asked are considerably more complex and there are far more people involved than in smaller companies. Since a serious breach of the law can jeopardise the reputation or even the very existence of the company, commitment to law-abidance and acting with integrity must be a prominent part of the corporate culture and permanently within the focus of the executive management. A risk-based compliance programme, together with correctly understood and observed managerial responsibilities on the side of the line management, will contribute to ensuring that the expectations formulated in the code of conduct are fulfilled. The management ensures that the compliance organisation is provided with appropriate resources and equipped with the necessary internal powers and a direct reporting line to it. The effectiveness of the compliance programme is checked regularly. If there are any shortcomings, the executive management has the duty of diligence to adapt the compliance programme promptly, by e.g. imposing sanctions for cases of non-compliance and, if need be, undertaking the necessary regulatory, organisational and process adjustments.

Compliance as a challenge

Compliance management is needed more than ever

Setting up and running a compliance management system is more necessary than ever for companies faced with increased legal and social demands in a complex economic environment. Effective compliance reduces the risk of sanctions, financial losses, damage to the company's reputation, and the loss of its licence to operate. The management's clear and visible commitment to acting with integrity and law-abidance is of key importance. The Board of Directors and management must take appropriate measures to enforce the policy and code of conduct at all levels, and to establish a risk-based adequate, functioning compliance management system. Risk management, internal guidelines, training concepts and targeted incentives and sanctions are important elements for effectively coping with and avoiding business risks in the area of compliance.

Compliance management to ensure that staff act with integrity – companies as "good corporate citizens"

Compliance not only involves abiding by the law and internal behavioural guidelines but also ensuring that all the company's staff members act with integrity. Effective compliance therefore strengthens a company's culture, which not only makes decisions in accordance with economic criteria but also always takes into account the social responsibility of the company as a significant decision-making criterion. Professional compliance management is therefore a central component of diligent management and a sign that the company is maintaining a culture of integrity and taking its social responsibility seriously in addition to striving for long-term profitability.

Duty of executive management

Setting up and running an effective compliance management system is an important and indispensable task for a company. Depending on the size of the company and its business, the compliance measures that it requires are more or less extensive. Therefore, each compliance management system must ultimately be tailored to fit the company. The compliance expectations of the state and society are the same for any company and must be taken seriously and implemented appropriately. The management is therefore obliged to constantly check whether its business activities and internal organisation are in line with the binding standards of integrity and to correct any shortcomings consistently and in good time. In conclusion, comprehensive compliance management can be described on the one hand as a challenging joint task, and on the other as an important permanent standing order to the management.

This publication is available in English, German and French.
Editorial: Jacques Beglinger, SwissHoldings; Adrian Michel, economiesuisse
Layout and production: Wernlis, grafische Gestalter, Zurich and Basel
Printed by DAZ Druckerei Albisrieden AG, Zurich
Date of publication: September 2014

economiesuisse
Swiss Business Federation
Hegibachstrasse 47
P. O. Box
CH-8032 Zurich

economiesuisse
Fédération des entreprises suisses
Carrefour de Rive 1
Case postale 3684
CH-1211 Genève 3

economiesuisse
Swiss Business Federation
Spitalgasse 4
P. O. Box
CH-3001 Berne

economiesuisse
Federazione delle imprese svizzere
Corso Elvezia 16
Casella postale 5563
CH-6901 Lugano

economiesuisse
Swiss Business Federation
Avenue de Cortenbergh 168
B-1000 Bruxelles

www.economiesuisse.ch

SwissHoldings
Swiss Business Federation
Nägeligasse 13
P. O. Box 402
CH-3000 Berne 7

www.swissholdings.ch