Risk & Compliance Management

Contributing editor
Daniel Lucien Bühr

2017

© Law Business Research 2017
1 What legal role does corporate risk and compliance management play in your jurisdiction?

Since the beginning of the financial crisis in 2007, Switzerland has seen many cases of organisational governance, risk and compliance failures, such as certain banks turning a blind eye to competition law or client tax law issues, to conflicts of interest or anti-money laundering compliance or management doing business in a manner that distorts the local, national and international playing field. These cases have triggered an endless stream of new regulations in Switzerland in the past decade. Many new regulations directly or indirectly address integrity, governance, risk or compliance management challenges. And, of course, Switzerland, with its small domestic market in the middle of the European Union, must align its legislation with EU rules and international standards that have become broader and more detailed as well. As a result of these national and international legal developments, warranting that an organisation meets its compliance obligations has become a challenging task for which ultimately the board of directors is responsible.

2 Which laws and regulations specifically address corporate risk and compliance management?

Generally, Switzerland’s legislation does not specifically address corporate risk and compliance management in a technical sense. However, many provisions in various Swiss laws require diligent and compliant business management at all levels. The most important statute in this respect is article 716a of the Swiss Code of Obligations (CO), which lists the non-transferable and inalienable duties of the members of the board of directors of a limited stock company. This provision emphasises the board of directors’ responsibility for compliance with the law throughout the entire company. In addition, article 102 Swiss Criminal Code (SCC) requires all corporations to take all necessary and reasonable organisational (compliance) measures to prevent criminal conduct by its employees. With regard to certain industries, the financial market laws, such as the Swiss Banking Act (BankA), the Swiss Banking Ordinance (BankO) and the Anti-Money Laundering Act, as well as the respective ordinances, stipulate many obligations with regard to risk and compliance management of financial intermediaries. Companies must also abide by competition law - the most important statute in this respect being the Federal Act on Cartels (CartA).

The Swiss Financial Market Supervisory Authority (FINMA), the government body responsible for financial regulation in Switzerland, regularly publishes non-binding circulars. In connection with risk and compliance management measures, FINMA for instance issued circulars on corporate governance for banks and insurance companies as well as on the management of liquidity risks at banks. The latter circular clarifies the requirements stipulated in the Liquidity Ordinance regarding the minimum qualitative requirements for banks’ liquidity risk management.

Other legally non-binding recommendations concerning internal controls, risk and compliance management have been issued by the Ecobusiness, the Swiss Business Federation, in 2014 in the policy paper ‘Fundamentals of effective compliance management’, which is the reference document on best practice compliance governance of the Swiss Code of Best Practice for Corporate Governance. The ‘Swiss Code’ is intended as a list of recommendations based on the ‘comply or explain’ principle for Swiss public limited companies. Non-listed, economically significant companies or organisations (including those in legal forms other than a public limited company) in practice follow the guidance given by the Swiss Code.

3 Which are the primary types of undertakings targeted by the rules related to risk and compliance management?

Compliance and risk management obligations must be fulfilled by all legal entities, regardless of their size or business activity. However, larger companies (in terms of revenues, balance sheet and number of employees) are in general subject to stricter statutory compliance and control or audit regulations. The legal entities targeted by statutory risk and compliance obligations are (in the order of importance in practice): public limited (stock) companies, private limited companies and foundations (in particular in the area of statutory professional insurance). Listed companies and, in general, companies in the financial sector, are subject to overall stricter risk and compliance management obligations.

4 Identify the principal regulatory and enforcement bodies with responsibility for corporate compliance. What are their main powers?

The principal regulatory and enforcement bodies for the private sector are FINMA, the Office of the Attorney General (OAG) and the Competition Commission (COMCO). For the public sector, the main controlling body is the Federal Audit Office.

FINMA supervises and regulates the financial industry (banks, insurance companies, brokers, etc., though not yet asset managers). It has extensive powers, which it exercises itself or through independent examiners (accredited law firms, auditors and forensic experts) by supervising, monitoring, auditing, investigating and sanctioning financial intermediaries and senior management. Financial intermediaries are required to self-report to FINMA all major legal risks. FINMA issues ordinances and circulars and regularly publishes decisions and guidance on legal requirements for financial institutions, in particular on the standard of professional diligence and best practice risk and compliance management.

The OAG, cantonal prosecutors and criminal courts enforce article 102 SCC. According to article 102 SCC, a company can be held criminally liable for failing to take all necessary and reasonable organisational (compliance) measures to prevent certain key crimes (bribery, money laundering, etc). It is important to bear in mind that under the SCC a company may be fined up to 5 million francs, and illicit profits are confiscates. The cantonal and federal prosecutors play an increasingly significant role as enforcement bodies of adequate corporate compliance. With its landmark case against Alstom (OAG order of 22 November 2011), the OAG developed its practice of effectively prosecuting companies that violate article 102 SCC in connection with corruption and money laundering. In the Alstom case, the Swiss subsidiary of Alstom Group (FR) was fined for lack of adequate compliance to avoid bribery of foreign officials and, in addition to a fine of 23 million francs, profits of 36.4 million were disgorged.

The federal and cantonal prosecutors are the competent bodies for conducting criminal investigations and bringing charges for money laundering. Financial intermediaries and traders who suspect that assets stem from a felony or misdemeanour or belong to a criminal organisation must notify the money laundering reporting office which, in turn, can notify the criminal prosecutor (what it actually does in approximately 70 per cent of the cases). The OAG has recently opened
a number of criminal investigations against Swiss banks for violations of anti-money laundering and anti-bribery statutes.

With regard to COMCO, undertakings are sanctioned (under administrative law) if they engage in cartels or illicit vertical restraints, abuse a dominant market position or ‘gun jump’ merger control regulations. For example, one of COMCO’s most recent high-profile probes concerned a number of large international banks for fixing the interest rates Libor, TIBOR and EURIBOR (the banks were fined with over-all approximately 100 million francs in December 2016). Further, recent activities of COMCO include, for example, the fining of one of Switzerland’s largest telecommunications companies, Swisscom, with respect to live sports broadcasting on pay TV, and the prohibition of anticompetitive contract clauses by hotel booking platforms such as Booking.com, Expedia and HRS.

5 Are ‘risk management’ and ‘compliance management’ defined by laws and regulations?

‘Risk management’ and ‘compliance management’ are not explicitly defined in Switzerland’s laws and regulations. However, international standards are being more and more accepted as soft law benchmarks for generally accepted best practice. For instance, COMCO, in its public presentations, refers to ISO Standard 19600 – Compliance management systems as one of their benchmarks should an undertaking raise the compliance defence against a sanction.

6 Are risk and compliance management processes set out in laws and regulations?

Swiss legislation does not outline risk and compliance management processes specifically. There are, however, certain provisions that stipulate the necessary precautions to be taken in that regard. For instance, article 78a CO stipulates that the external auditor must examine whether an internal control system exists and must take the control system into account when carrying out the audit and in determining the scope of the audit. Furthermore, the external auditor must ensure that an adequate risk management system is integrated into the internal control system.

7 Give details of the main standards and guidelines regarding risk and compliance management processes.

Risk and compliance management processes are outlined in non-binding soft law international standards such as ISO Standard 31000 – Risk management and ISO Standard 19600 – Compliance management systems. Some (mainly larger international) corporations also follow the soft law COSO (Committee of Sponsoring Organisations of the Treadway Commission) Enterprise Risk Management framework or the IIA (Institute of Internal Auditors) Three Lines of Defence position paper (which is a basic risk governance concept rather than a soft law standard).

ISO Standard 31000 provides senior management with a framework for designing and implementing an effective risk management system that fosters risk identification, risk analysis and risk evaluation (all together constituting the risk assessment process) and risk treatment. ISO Standard 19600 sets out the compliance responsibilities at all levels of an organisation, as well as the process of planning, implementing and monitoring, measuring and continually improving a compliance management system with its governance, organisation and processes.

8 Are undertakings domiciled or operating in your jurisdiction subject to risk and compliance governance obligations?

Yes, undertakings domiciled or operating in Switzerland are subject to statutory risk and compliance governance obligations. For instance, article 102 SCC (the corporate criminal offence of failing to employ all necessary and reasonable compliance measures to prevent bribery, money laundering, etc.) applies to all undertakings domiciled in Switzerland as well as to all undertakings operating in Switzerland if legal or compliance employees are located in Switzerland. In both cases, the undertaking is liable for its global business conduct.

9 What are the key risk and compliance management obligations of undertakings?

Under article 102 SCC (the corporate criminal offence of failing to prevent), if a felony or a misdemeanour is committed in the undertaking in the exercise of commercial activities and in accordance with its purpose, the felony or misdemeanor is attributed to the undertaking if it is not possible to attribute this act to any specific natural person as a result of inadequate (compliance) organisation of the undertaking. In case of severe felonies (such as bribery), the undertaking is criminally liable irrespective of the liability of any natural person, if the undertaking has failed to take all necessary and reasonable organisational measures that are required in order to prevent such an offence.

With regard to the banking sector, articles 3f and 3g BankA as well as article 12 BankO explicitly require banks to implement an effective internal control system with an independent internal audit function and proper risk management to identify, treat and monitor all material risks.

10 What are the risk and compliance management obligations of members of governing bodies and senior management of undertakings?

Article 716a CO lists the non-transferable and inalienable duties of the members of the board of directors, highlighting their responsibility for the overall management, organisation and (global) compliance of the company. On this statutory basis, the external auditors must provide the board of directors with a comprehensive report on the financial statements and the internal control system of the company (article 716b CO). According to articles 717 and 734 CO, the members of the board of directors and also the members of the executive board are required to manage the company with an increased degree of diligence (members of the board of directors) or with diligence. This standard demands that the members of the board of directors or of the executive board must implement effective risk and compliance management systems.

11 Do undertakings face civil liability for risk and compliance management deficiencies?

Yes, on an extracontractual basis, third parties are entitled to claim civil damages from undertakings if the damages have been caused by employees or other auxiliaries who were not diligently selected, instructed and supervised or if the undertaking does not prove that the employer took all necessary precautions to avoid the harmful conduct (article 55 CO). A similar provision exists regarding causal contractual liability (article 101 CO).

12 Do undertakings face administrative or regulatory consequences for risk and compliance management deficiencies?

An example for administrative consequences for risk and compliance management deficiencies are sanctions under article 102 of the CartA. In case of infringements against the CartA, undertakings can raise the compliance defence, in other words, they can produce evidence that the infringement occurred despite the undertaking’s best practice risk and compliance management. COMCO refers to a number of international standards and best practice guidelines as a benchmark for state of the art compliance management (e.g., ISO 19600 and Organisation for Economic Cooperation and Development and International Chamber of Commerce guidelines). If an undertaking successfully raises the compliance defence, no sanction will be imposed on the undertaking. Institutions that are subject to FINMA’s regulatory financial market supervision may face specific regulatory consequences in case of risk and compliance management deficiencies. FINMA has a broad range of tools to enforce its regulations:

- precautionary measures;
- orders to restore compliance with the law;
- declaratory rulings;
- directors’ disqualification;
- cease and desist orders and bans on trading;
- publication of decisions;
- confiscation of profits; and
- withdrawal of licences and compulsory liquidation.

In the employment of these regulatory enforcement measures, FINMA is guided by the aims of the Swiss financial market laws, namely the purposes of protecting creditors and investors, of ensuring fair market conduct and of maintaining the good standing and stability of the (Swiss) financial system.
### Update and trends

Since the beginning of the financial crisis, Swiss banks have increasingly come under regulatory pressure to improve their risk and compliance management. This pressure is mainly domestic (FINMA) but also foreign (for instance by US regulators such as Department of Justice, Internal Revenue Service, Securities and Exchange Commission, New York State Department of Financial Services, or by European regulators such as the German Federal Financial Supervisory Authority and UK Financial Conduct Authority). Regulators are requiring Swiss banks to have best practice risk and compliance management systems in place to give assurance to them that they meet their legal obligations. For many Swiss banks this is a challenge because historically they have employed governance frameworks for risk and compliance management (such as the Three Lines of Defence framework) instead of generally accepted international methods on substance like the COBIT ERM framework or ISO Standards 31000 and 19600. In contrast to governance frameworks, these standards provide specific guidance on the governance and principles, organisation and processes of state of the art risk and compliance management. Against the background of FINMA's more active regulatory enforcement and the OAG’s criminal investigations against some banks for failure to prevent felonies such as money laundering and bribery in their sphere of influence, the pressure on banks to implement state of the art risk and compliance management systems has significantly increased. And obviously, shareholders of companies that are sanctioned for compliance failures are increasingly likely to recover the companies’ damages from senior managers, who factually are the acting company.

What holds true for banks is true for all other companies, private or public. Here regulatory and enforcement may be less important, but the standard of risk and compliance management diligence required under the failure to prevent offence sets the benchmark as well. And as enforcement agencies become more knowledgeable about best practice risk and compliance management and the respective international frameworks, they will also hold companies and their managers liable to these standards. With increased transparency on financial assets and transactions and beneficial ownership of passive companies, best practice risk and compliance management are more than ever a key responsibility of companies and their senior management.

#### 13 Do undertakings face criminal liability for risk and compliance management deficiencies?

Pursuant to article 102 SCC, undertakings face corporate criminal liability, for organisational weaknesses (the failure to prevent criminal conduct by its employees). According to paragraph 1, if a felony or a misdemeanour is committed by employees of the undertaking in the exercise of its commercial activities in accordance with its purpose, the felony or misdemeanour is attributed to the undertaking if it is not possible to attribute the offence to a specific employee as a result of an inadequate organisation. In the case of paragraph 4, the undertaking is liable to a fine not exceeding 5 million francs (see question 4).

In addition, the company can be convicted under paragraph 2, if the offence committed falls under a list of severe criminal offences such as bribery and money laundering. If a predicate offence is established and if the undertaking failed to employ all necessary and adequate measures to prevent the predicate offence, it is criminally liable for its organisational failure. Fines can amount to a maximum of 5 million francs and illicit profits are disgressed.

#### 14 Do members of governing bodies and senior management face civil liability for breach of risk and compliance management obligations?

Under article 754 CO, the members of the board of directors, senior management and all persons engaged in the liquidation of a limited company face civil liability towards the company, the shareholders and creditors for any loss or damage arising from an intentional or negligent breach of duties of diligence. A key statutory responsibility of members of governing bodies and senior management is to ensure compliance with the law by all employees. It is important to note that not only the members of the company’s formal governing bodies (ie, the members of the board of directors and the members of the executive board) can be held liable, but also factual members of governing bodies who have not been formally appointed but who exercise significant influence on the company’s management.

#### 15 Do members of governing bodies and senior management face administrative or regulatory consequences for breach of risk and compliance management obligations?

Senior members of management only face administrative or regulatory consequences for such breaches in regulated industries, such as the financial industry. Senior members of management at financial institutions regulated by FINMA can face administrative as well as regulatory consequences in case of infringement of their duty of diligence. FINMA can employ administrative or regulatory measures on managers, such as directors’ disqualification, adding a manager to a watch list and the issuance of a business conduct letter. FINMA can enter an individual’s information in a database known as the watch list if the individual’s business conduct is questionable or does not meet the legal requirements. The watch list aims at assessing relevant information with regard to compliance prerequisites, namely, personal details; extracts from commercial, debt enforcement and bankruptcy registers; criminal, civil and administrative court decisions; and reports by auditors and third parties appointed by FINMA. Furthermore, FINMA can send a business conduct letter to those registered in the watch list under specific circumstances. A business conduct letter does not qualify as a decision, but rather simply states that FINMA reserves the right to review compliance with the diligence requirements should the manager change position. In case of directors’ disqualification, FINMA can ban individuals responsible for serious violations of supervisory law from acting in a senior function at a supervised institution for up to five years.

#### 16 Do members of governing bodies and senior management face criminal liability for breach of risk and compliance management obligations?

Individuals can be criminally liable if they fail to implement effective risk and compliance management and turn a blind eye on, for instance, mismanagement (article 158 SCC), embezzlement (article 158 SCC), money laundering (article 201-bis SCC) or bribery (article 322-ter et seq SCC). However, there is no individual criminal liability – sensu stricto – for an organisational compliance failure to prevent criminal offences, as such failure is a criminal offence of the undertaking (see questions 9 and 13).

#### 17 Is there a corporate compliance defence? What are the requirements?

Under article 102(2) SCC, an undertaking is criminally liable for certain felonies committed by its employees if it did not implement the necessary and adequate (compliance) measures to prevent the felonies. The burden of proof for the inadequacy of the compliance measures rests with the prosecutor or court. Still, the defendant undertaking will want to establish that it did implement all necessary and adequate compliance measures. In order to do so, the undertaking will need to submit evidence regarding its compliance policy, its good compliance governance, the overall compliance management system, the processes implementing the compliance management system, the measurement of the effectiveness of the system and regular reporting to senior management and continual improvements, etc.

In competition law cases, COMCO, when determining a sanction, also takes (competition) compliance management of the undertaking into account. The burden of proof rests with the undertaking.

#### 18 Discuss the most recent leading cases regarding corporate risk and compliance management failures.

In May 2016, the OAG opened criminal proceedings against Bank BSI SA, and in October 2016 against Falcon Private Bank Ltd, based on information obtained from the criminal investigations related to the Malaysian State Fund 1MDB and on regulatory offences sanctioned by FINMA in its decision of 23 May 2016. The OAG suspects that both banks failed to prevent money laundering and bribery by its employees. In the context of the substantial number of Petrobras/Lava Jato-related investigations, the OAG convicted the Brazilian company
Odebrecht SA and its subsidiary Braskem on 21 December 2016 for organisational failure to prevent bribery of foreign officials and money laundering under article 102(2) SCC. The OAG stated that Odebrecht SA created slush funds throughout the world in order to pay bribes to government officials, representatives and political parties to obtain business and projects from state-owned companies. As a result, Odebrecht SA was fined 4.5 million francs and the OAG disgorged profits of more than 200 million francs.

Also, in December 2016, the OAG opened criminal proceedings against a former employee of private bank Lombard Odier & Co Ltd. The bank itself is under investigation by the OAG for organisational failure to prevent money laundering under article 102(2) SCC.

19 Are there risk and compliance management obligations for government, government agencies and state-owned enterprises?

With regard to the criminal liability of undertakings, the SCC does not differentiate between private and public undertakings. The term ‘undertaking’ within the meaning of article 107(4) SCC includes entities under both private and public law. Swiss state-owned undertakings such as cantonal banks, hospitals, telecommunications companies, energy companies, railways, defence companies, certain insurance companies, airports, etc, must employ best practice risk and compliance management to meet their compliance obligations and avoid criminal liability if employees engage in misconduct.

Government and government agencies are all obliged to act in accordance with the statute or statutes under which they are established and governed. These statutes all require government and government bodies to comply with their compliance obligations.

20 What are the key statutory and regulatory differences between public sector and private sector risk and compliance management obligations?

The principle that all organisations must meet their compliance obligations is the same for private and public sector organisations. Accordingly, all organisations must implement and maintain best practice (legal) risk management systems and compliance management systems. The main difference between private sector and public sector statutory and regulatory risk and compliance management obligations is the overall purpose, which for public sector organisations covers the good functioning of government and the maintenance of citizens’ trust, and for private sector companies covers the protection of employees, shareholders and creditors, among others.