Risk & Compliance Management

Contributing editor
Daniel Lucien Bühr

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Risk & Compliance Management 2018

Contributing editor
Daniel Lucien Bühr
Lalive

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2017
Second edition
ISBN 978-1-78915-067-4

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Preface

Risk & Compliance Management 2018

Second edition

Getting the Deal Through is delighted to publish the second edition of *Risk & Compliance Management*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on China, Greece, India, Nigeria and Turkey and an article, written by the editor, on the overlap between the US Department of Justice's assessment of corporate compliance programmes and the International Organization for Standardization's guidance for compliance management systems.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editor, Daniel Lucien Bühr of Lalive, for his continued assistance with this volume.

GETTING THE DEAL THROUGH

London
May 2018

Global overview

Daniel Lucien Bühr
Lalive

This second edition of *Risk & Compliance Management* in the *Getting the Deal Through* series reflects the continued globalisation of the economy and the legal world.

The global economy is services-driven and those services are increasingly available over the internet and new electronic media. Services provided over the internet are by their very nature international and global. With regard to the industrial sector, the global economy has essentially become a components marketplace where assemblers, still often located in the 'old' world, source the most competitive components from around the globe to build end-products under old, well-established brands from another industrial era. Today's economy is also driven by electronic distribution channels for services and new payment procedures. The common denominator in today's economy is therefore the global nature and vitality of its trade.

The worldwide economic model inevitably leads to the globalisation of legal risks and opportunities.[1] Multinational companies, whether large or small, struggle with the diversity of jurisdictions, laws and regulatory bodies. Not surprisingly, they face significantly more complex and material legal risks today than 10 years ago. Yet, if senior managers and general counsel are asked how they have adapted to these changes, they often reply that their work processes and tools have barely changed. Legal and compliance budgets are still small despite ever-increasing duties and risks. Additionally, risk management often remains opaque and is not founded on generally accepted standards,[2] while compliance management is typically shaped by the evolution of the organisation's historic compliance management rather than by modern best practices and a coherent and modern management system design.

To put it simply, nowadays global business opportunities and risks go hand in hand with global legal opportunities and risks. To capture the business opportunities and avoid or limit the business risks, legal risk management must be as good, professional and well-funded as the core business activities. The board of any company should ask top management whether the legal, risk management, compliance and internal audit functions are as sophisticated as its business management.

If a company's finance department applies US generally accepted accounting principles (GAAP) accounting standards, the overall management of the company is certified under 'ISO Standard 9001 – Quality management systems', and if the IT department applies 'ISO/IEC Standard 27001 – Information security management systems', then legal risk management should also be based on a reliable, auditable and generally accepted method. This professionalism and the budgets made available for the business and support functions must reflect the professionalism by which the control functions are designed, implemented, maintained and continually improved. Any company with, for instance, a best practice quality and IT security management system and reporting under US GAAP can therefore reasonably be expected to have an overall legal risk management system that follows generally accepted international standards and practices and is independently audited for effectiveness.

Two questions arise from the requirement that multinational companies (or any organisation with international activities) should follow generally accepted international standards and practices in their legal risk management. The first is what these generally accepted international standards and practices are. The second is whether implementing these standards and practices actually does lead to effective legal risk management by companies in the globalised economy.

The first question (What are the generally accepted international standards and practices?) is quite easy. The only generally accepted international standards and quasi-standards for risk management are ISO Standard 31000 – Risk management (according to the Organisation for Economic Cooperation and Development de facto the global standard for risk management) and the COSO[3] Enterprise Risk Management Framework, a broadly accepted private risk framework. When it comes to compliance management, the only generally accepted standards are ISO Standard 19600 – Compliance management systems and ISO Standard 37001 – Anti-bribery management systems. Both standards are recent and modern in their approach and reflect internationally accepted best practice.

No international standard currently exists for operational legal management; however, there is some guidance available on the principles of good governance of the legal function[4] and, of course, legal management should meet the requirements of ISO Standard 9001 – Quality management systems, namely, adhere to quality management principles, including a strong focus on internal clients (the 'customer'), the motivation and involvement of top management, the process approach and continual improvement.

Finally, internal audit – the 'super' control function that monitors whether legal, risk and compliance management and the internal (financial) control system are effective and achieve the goals set by top management – should follow the well-recognised ISO Standard 19011 - Guidelines for auditing management systems. These guidelines include the principles of auditing, the key aspects of managing an audit programme and conducting management system audits (pre-audit, on-site audit, post-audit). They also address evaluating the competence of the individuals involved in the audit process, including the person managing the audit programme, auditors and audit teams.

The answer to the second question (Does the implementation of the standards and practices lead to effective legal risk management by companies in the globalised economy?) is yes. Applying, maintaining and continually improving generally accepted risk and compliance management standards and practices will normally enable any organisation to manage its legal risks effectively. Of course, this cannot protect from one-off instances of non-compliance, but it will establish effective barriers to long-standing systemic non-compliant behaviour, which is one of the greatest continuity risks for businesses and has in the past decade led to hundreds of billions of dollars in fines and business losses.

To mention just one example of why applying generally accepted standards and processes is effective: ISO Standard 19600 – Compliance management systems names three principles of good compliance governance,[5] the first of which is direct access of the compliance function to the board. If the compliance function has direct (planned, documented and periodic) access, the board will receive first-hand information on the organisation's compliance status (including at top management level) and will be in a position to exercise its ultimate responsibility for effective compliance with the law. As a result, boards that demand best compliance management standards and practices will get the information they need to lead their organisation at the highest level. At the same time, accountability will be fortified because no board member could argue that they did not know about any instances of non-compliance. Under Standard 19600, board members simply must know about such instances when they occur, given that the compliance function has direct access to it. Reporting by a multinational's compliance function

is, by definition, a statement that the organisation is meeting its global compliance obligations, namely, the requirements in all jurisdictions where it operates and under all applicable laws and regulations.

In summary, companies engaging in the global economy must be as engaged, systematic and professional in their legal risk management as they are in their core business activities. They should follow generally accepted standards and practices in their legal, risk and compliance management and in their internal audit, in the same way they apply generally accepted accounting standards when they draw up their annual accounts. Following this path, boards and top management will have a significant competitive advantage to seize the opportunities of the global economy.

I hope you enjoy the 2018 edition of *Risk & Compliance Management* and find it interesting and of value to your business.

Notes

1 Risk, as defined in ISO Standard 31000 (www.iso.org), is the effect of uncertainty on objectives. That effect, which is a deviation from the expected, can be positive or negative. So, risk always includes opportunity.

2 The US Department of Justice (Criminal Division, Fraud Section) demands that companies have a risk management process based on a defined methodology to identify, analyse, and address the particular risks it faces (Evaluation of Corporate Compliance Programs, paragraph 5; www.justice.gov/criminal-fraud/page/file/937501/download).

3 Committee of Sponsoring Organizations of the Treadway Commission, funded and sponsored by the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives International, the Institute of Management Accountants and the Institute of Internal Auditors.

4 Ben W. Heineman Jr, *High Performance with High Integrity*, Harvard Business Press, 2008.

5 ISO Standard 19600, section 4.4 – Compliance management system and principles of good governance.

Argentina

Pedro Serrano Espelta and Gustavo Morales Oliver
Marval, O'Farrell & Mairal

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Certain sets of regulations set forth standards for risk and compliance management. The most relevant are mentioned below.

With regard to corruption risk management, the recent Law No. 27,401, in force since 1 March 2018, criminalises corporate bribery and corruption, and regulates integrity programmes. Such integrity programmes must meet certain requirements imposed by the law such as being appropriate to the specific risks related to the activities, size and economic capacity of the company, and complying with further regulations of this law to be enacted by the relevant authorities. Implementing said integrity programmes based on risk management is mandatory for certain companies contracting with the federal government when, according to applicable regulations, such contracts must be approved by a public official ranked as a minister or above, and when the contract falls under those regulated by:

- article 4 of Decree 1023/01 (eg, procurement, sale and purchase, consulting, services, leases, leasing, swaps, concession for using goods in the public and private domain of the federal government, public works, concessions of public services and licences and all those contracts not specifically excluded from this regime);
- Law No. 13,064;
- Law No. 17,520;
- Law No. 27,328; and
- concession or licensing contracts for public services.

Implementing integrity programmes is voluntary for companies not entering any of the previously mentioned dealings.

With regard to anti-money laundering and anti-terrorist financing, Law No. 25,246 establishes, for certain subjects mentioned in section 20 (Subjects under the Law), the obligation to implement a compliance programme focused on risk management. These provisions are mandatory for the Subjects under the Law so not following them will be considered a breach of the law. In addition, the Financial Information Unit, which is the relevant regulatory agency, issued Resolution 30-E/2017 that specifically adopts the Financial Action Task Force (GAFI) standards for the risk-based approach for financial entities and foreign exchange agencies, and Resolution 21/2018 that specifically adopts GAFI standards for those individuals and entities subject to the capital market's regime as detailed in section 2r of Resolution 21/2018.

As an example of industry regulations, Resolution 38,477 of the National Superintendence of Insurance, which was issued in 2014, establishes that insurance and reinsurance entities subject to the supervision of the National Superintendence of Insurance must approve Rules on Policies, Procedures and Internal Controls to Combat Fraud, which must be based on a risk analysis.

Other examples of industry regulation specifically cover financial entities. Regulation 'A' 5,398 (enacted by the Argentine Central Bank in 2013) and its amendments, establish the obligation for those entities to have an integral process for risk management including the board of directors and high management surveillance for the identifying, assessing, follow-up, control and mitigation of any significant risk.

Regarding companies listed for public offering's regulations, the Argentine Securities Commission, which is the relevant regulatory agency, has enacted General Resolution 606/2012, which establishes guidelines and recommendations of good practices in corporate governance. Although these are only recommendations to listed companies, the companies have to give explanations when they have not followed them.

Despite these particular regulations, companies can implement risk management under other regulations as well as antitrust regulation or international standards such as ISO 37001 to prevent bribery.

Moreover, certain industry associations (eg, the Chamber of Argentine Pharma Companies) have agreed to enact ethics codes that are mandatory for all their members.

In general terms, multinational companies that operate in Argentina usually have corporate risk and compliance management procedures in place; however, local companies usually do not have these measures implemented, with the exception of a few that are listed companies, operate in regulated industries or have business relationships with multinationals that require these measures to be adopted.

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

Corporate risk and compliance management is specifically addressed by certain local regulations. The most relevant are:

- Law No. 27,401, which establishes corporate liability for bribery and corruption crimes;
- Law No. 25,246, which sets forth the obligation for the Subjects under the Law to implement a compliance programme focused on risk management;
- Resolution 38,477 of the National Superintendence of Insurance, which establishes the approval of mandatory Rules on Policies, Procedures and Internal Controls to Combat Fraud for insurance and reinsurance entities subject to the supervision of the above-mentioned entity;
- Resolution 30-E/2017 of the Financial Information Unit, which specifically adopts the GAFI standards for the risk-based approach for financial entities and foreign exchange agencies;
- Resolution 21/2018 of the Financial Information Unit for those individuals and entities subject to the capital market's regime as detailed in section 2r of such Resolution;
- Regulation 'A' 5,398 of the Argentine Central Bank that sets forth the obligation of the financial entities to have an integral process of risk management; and
- General Resolution 606/2012 of the Argentine Securities Commission that approved the Corporate Governance Code for companies listed for public offering.

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

With regard to bribery and corruption, Law No. 27,401 establishes that anti-corruption risk and compliance management is mandatory for private legal entities with national or foreign capital stock, with or without government participation, that engage in certain contracts with the federal government, as described above. Other companies may voluntarily implement integrity programmes under this law. In any case, the integrity programmes will be most relevant in seeking reductions or exemptions from penalties in case of breach.

The anti-money laundering and anti-terrorist financing regulations apply to all legal entities and individuals. However, specific 'know

your customer' and reporting obligations apply only to specific subjects such as:

- financial entities;
- foreign exchange offices and foreign exchange agencies;
- gambling undertakings;
- brokers of stock and other securities;
- brokers of futures and options;
- public registries of legal entities;
- individuals and legal entities engaged in transactions related to real estate, pledges, vessels, aircrafts and vehicles;
- individuals and legal entities engaged in transactions related to works of art, antiques, sumptuary assets, jewels and precious stones;
- insurance companies;
- travellers cheques and credit and debit card issuers;
- companies providing armoured transportation services;
- mailing companies that provide currency transfer services;
- notary publics;
- customs brokers;
- regulatory agencies;
- accountants; and
- trustees, among others.

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

The anti-bribery and corruption regulation is enforced by the criminal courts with the assistance of the Public Prosecuting Ministry. Criminal courts have the power to prosecute, convict, sanction, confiscate and enter into agreements with the defendants.

The Financial Information Unit is tasked with the analysis, investigation, treatment, reporting and communication of information regarding money laundering and terrorist financing. The Financial Information Unit is also authorised to apply sanctions to the undertakings that are subject to 'know your customer' and reporting obligations, and must report to the relevant prosecutors any fact that could reasonably be deemed as a money laundering or a terrorist financing case. Additionally, the Financial Information Unit can ask for the relevant prosecutors' aid and issue mandatory regulations and guidelines for those subject to its authority.

The Central Bank of the Argentine Republic is the main regulatory and enforcement agency for financial institutions. It has regulatory functions, together with auditing and sanctioning powers.

The Argentine Securities Commission has regulatory powers as regards risk and compliance management. It also has sanctioning powers over listed companies.

The National Superintendence of Insurance has regulatory powers over insurance and reinsurance entities. It has regulatory, auditing and sanctioning powers.

The Anti-corruption Office is the body in charge of the enforcement of administrative anti-corruption regulations across the entire public administration and for legal entities with state participation. To do so, the Anti-corruption Office has the power to investigate, report to prosecuting authorities and issue transparency programmes to prevent corruption, among others. Although the Anti-corruption Office has no jurisdiction over private parties (neither legal entities nor individuals who are not public officers), it plays a key role in investigations of corruption crimes and in cooperating with courts in reporting crimes.

All decisions issued by the administrative entities mentioned above are subject to review before judicial courts.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

'Risk management' and 'compliance management' are not defined as such by Law No. 27,401; however, it establishes that integrity programmes shall be implemented or improved according to the results of proper anti-bribery and corruption risk analysis.

The other regulations mentioned above do not provide definitions for risk or compliance management. Nevertheless, the Financial Information Unit's resolutions provide relevant definitions regarding certain factors to be considered when performing risk and compliance management, such as self-evaluation of risk and a risk-based approach in the application of these regulations.

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

In general, the laws and regulations mentioned above provide general and minimum standards and guidelines for risk and compliance management processes, but each entity subject to them must implement its own procedures and mechanisms pursuant to its particular activities and exposure. For example, Law No. 27,401 establishes that a risk-based integrity programme must include a set of actions, mechanisms and internal procedures to promote integrity, supervision and control, with the aim to prevent, spot and correct wrongdoings and illegal acts under Law No. 27,401. It must also, at least, include a code of ethics or integrity policies, training and internal policies to prevent crimes in any interactions with the public sector.

The regulations of the Financial Information Unit establish certain processes that the entities subject to its regulations must follow to implement a risk-based management system to prevent money laundering and financing terrorism. For example, the Financial Information Unit establishes annual internal audits and processes to evaluate the effectiveness of the risk prevention system.

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

Law No. 27,401 establishes that the integrity programme must be appropriate to the specific risks related to the activities, size and economic capacity of the legal entity, in accordance with further regulations of this law to be enacted by the relevant authorities.

Regulation 'A' 5,398 of the Argentine Central Bank provides that each financial entity must issue its own risk management strategies and policies according to the guidelines provided therein regarding:

- credit risks;
- liquidity risks;
- market risks;
- interest rate risks;
- operational risks;
- securitisation risks;
- concentration risks;
- reputational risks; and
- strategic risks.

Regulation 'A' 6,131/2016 of the Argentine Central Bank establishes Guidelines for the Settlement of Foreign Exchange Transactions in order to regulate the risk management of financial institutions by the exposure resulting from foreign exchange transactions, from their negotiation to their final settlement.

Anti-money laundering and anti-financing terrorism standards and guidelines are provided in Law No. 25,246, as amended and, in its implementing, regulations issued by the Financial Information Unit. For example, Resolution 30-E/2017 as well as Resolution 21/2018, both issued by the Financial Information Unit, establish a minimum standard regarding risk and compliance management process, providing that it must be appropriate to the nature and business capacity (considering all business units) of the entities subject to those regulations and also take into account specific risk factors like clients, products and services, distribution channels and geographic zones. All those standards can be fully supplemented with internal standards developed by the particular entity subject to the regulations, based on its activities.

General Resolution 606/2012 of the Argentine Securities Commission only establishes general recommendations for companies that make public offer of securities, but does not provide more detailed standards and guidelines.

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

As mentioned in previous questions, some undertakings domiciled or operating in Argentina are subject to risk and compliance governance obligations.

Financial entities are subject to risk governance obligations pursuant to Regulation 'A' 5398 of the Argentine Central Bank. For example, the regulation establishes that the governance structure implemented must appoint a particular individual or unit that needs to be in accordance with the economic capacity, dimension and nature of the financial entity and may adopt the structure of a committee in which members of the governing body must participate.

Listed corporations are subject to compliance obligations as, although the Corporate Governance Code approved by Resolution 606/2012 of the Argentine Securities Commission is not mandatory, accounting auditors must report on the annual balance sheets of listed companies whether they adhere to the Corporate Governance Code or not.

Law No. 27,401 does not provide governance obligations on anti-corruption risks although it provides guidelines for the related compliance programmes, including clear and affirmative support to the programme by the entity's top management.

Resolution 38,477 specifically addresses the obligation to appoint a regular compliance officer, who must be at least a senior executive.

Law No. 25,246 sets forth the obligation for entities subject to the law to appoint a compliance officer, who must be a member of the governing body. Also, the personal information of the officer must be reported to the Financial Information Unit. This regulatory entity provides in Resolution 121/2011 that the compliance officer will have full independence and autonomy in doing their duties, ensuring unlimited access to all of the information that requires compliance with them.

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

Financial entities, pursuant to Regulation 'A' 5,398, must implement risk management manuals, policies, procedures and strategies duly documented and designed in accordance with the economic size of the relevant financial entity and the nature and complexity of their operations, and provide for business strategies and internal limits applicable to the different kind of risks that the entity faces pursuant to its role in the financial market and its capital stock, assets and financial results and total risks.

According to the Corporate Governance Code approved by Resolution 606/2012 of the Argentine Securities Commission, listed companies must:

- disclose their links with their corporate group and related companies;
- provide the basis for sound management and supervision;
- support an effective policy for identification, assessment, management and disclosure of their business risks;
- preserve the integrity of financial information with independent audits;
- respect the rights of their shareholders;
- maintain direct and responsible links with the community;
- provide for fair and accountable remunerations;
- promote corporate ethics; and
- go in depth to the scope of the ethics code.

Pursuant to Law No. 27,401, undertakings that implement an integrity programme shall conduct appropriate risk analysis as the basis for drafting and updating the integrity programme. The integrity programme must have, as a minimum standard, the following elements:

- a code of ethics or conduct, or the existence of integrity policies and procedures applicable to directors, managers and employees;
- specific rules and procedures to prevent illegal acts within the scope of tenders, public bids, governmental control enforcement or any other engagement with the public sector; and
- periodic training sessions regarding the integrity programme to directors, managers and employees.

According to the anti-money laundering and anti-financing terrorism law, those subject to 'know your customer' and reporting obligations must also approve anti-money laundering and anti-financing terrorism codes that state different measures to adopt and the corresponding assignment of responsibilities to the compliance officer in charge of these issues.

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

Law No. 27,401 does not distinguish the obligations that fall under members of governing bodies and senior management. For those entities that have risk and compliance management obligations, the members of governing bodies and senior management have to approve the relevant code of ethics or code of conduct or the integrity policies. The governing bodies and senior management also have to comply with the general fiduciary standards set forth in section 59 of the General Corporate Law.

Pursuant to Regulation 'A' 5398 of the Central Bank, there are different obligations for members of governing bodies and senior management.

In this regard, the board of directors of financial entities are accountable for the adequateness of the risk management policies, for the credit risks assumed by the entity and for its management. The board of directors must:

- approve and review credit policies and strategies;
- approve the threshold of risk tolerance of the entity;
- approve the staff for the management of the credit risk;
- ensure senior management capacities for managing the credit transactions of the entity pursuant to its strategy and policies;
- guarantee the alignment of the economic incentives granted to its personnel with its risk strategy;
- assess whether the entity's capital is appropriate according to the risks assumed;
- approve new products and activities of the entity;
- follow up the entity's exposure with regard to related companies or individuals;
- approve exceptions to the policies and limits to them;
- receive reports regarding the risks related with the credits granted by the entity and regarding the fulfilment of risk limits; and
- receive reports with timely information in case of adverse risk events and ensure that senior management adopt the appropriate measures to cope with such adverse situations.

Additionally, financial entities' senior management must implement risk management policies, strategies and practices as approved by the board of directors, and must develop written procedures to identify, assess, evaluate, follow-up, control and mitigate credit risks. Senior management must:

- ensure the existence of internal controls and audits;
- regularly follow up market trends that may entail significant challenges for risk management;
- ensure stress tests and contingency plans; and
- ensure that costs, earnings and risks are properly assessed in the process of approving new products.

The Corporate Governance Code provided in Resolution 606/2012 of the Argentine Securities Commission does not distinguish which responsibilities belong to the board of directors and which ones belong to senior management. However, since it refers to the management body of listed companies, it is reasonable to conclude that such obligations mainly belong to the board of directors if it is not provided otherwise in the relevant corporate governance codes that may be adopted by each listed company.

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

No, undertakings do not face civil liability for risk management and compliance management deficiencies as such, as there are no civil obligations for them to establish such risk and compliance management. However, if any actions related to risk and compliance management deficiencies involve tort or breach of contract, civil liability may arise in that regard.

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

Undertakings do not face administrative or regulatory consequences for risk and compliance management deficiencies under Law No. 27,401.

Undertakings face administrative or regulatory consequences for risk and compliance management deficiencies only if regulations issued by administrative regulatory authorities set forth risk and compliance management obligations for those individuals or entities of particular industries subject to its powers.

For example, non-compliance with resolutions issued by the Argentine Central Bank and the Argentine Securities Commission may cause financial entities and listed companies to face regulatory

sanctions for risk and compliance management deficiencies, as these regulatory entities have the power to impose over them administrative sanctions, such as fines, suspensions and disqualifications to operate.

In a similar way, the National Superintendence of Insurance has the power to establish administrative sanctions on insurance and reinsurance entities in case of breach of regulations enacted by such regulatory agency regarding, for example, risk and compliance management. Such administrative sanctions include fines, warnings and suspensions to operate.

Additionally, the anti-money laundering and anti-financing terrorism regulations provide for administrative fines in case of breach of regulations that set forth risk and compliance management obligations.

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

Undertakings do not face criminal liability for risk and compliance management deficiencies under Law No. 27,401. Nevertheless, legal entities may have indirect criminal consequences as they can lose access to the benefits of 'exception from penalties' and 'reduction in penalties' if the risk and compliance management carried out in connection with the integrity programme is deficient.

Additionally, the other relevant laws and regulations mentioned above do not establish criminal liability specifically owing to these deficiencies. However, depending on the facts involved, actions or omissions related to or arising as a consequence of deficient risk management may trigger breaches of administrative, civil, criminal and other regulations.

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

Members of governing bodies and senior management may face civil liability for the breach of risk and compliance management obligations if they do not establish the proper risk and compliance management that is required according to the relevant entity's area of practice and to their fiduciary duties of loyalty and care, set forth in section 59 of the General Corporate Law. As a consequence of this breach, the legal entity, the shareholders or the relevant stakeholders may initiate proceedings against the members of governing bodies and senior management.

Additionally, depending on the facts involved, actions or omissions related to or arising as a consequence of deficient risk management may trigger breaches of administrative, civil, criminal and other regulations.

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

Members of governing bodies and senior management may face administrative or regulatory consequences for breach of risk and compliance management obligations only if those obligations are established in the regulations issued by the relevant administrative regulatory agencies. To illustrate this, the Argentine Central Bank, the Argentine Securities Commission and the Financial Information Unit have the power to impose administrative sanctions on members of governing bodies and senior management of financial entities, listed companies or foreign exchange agencies for breach of certain regulations that set risk and compliance management obligations. Such administrative sanctions generally include fines, suspensions and disqualifications.

Additionally, depending on the facts involved, actions or omissions related to or arising as a consequence of deficient risk management may trigger breaches of administrative, civil, criminal and other regulations.

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

Members of governing bodies and senior management do not face criminal liability as there is no regulation that criminalises them for breach of risk and compliance management obligations.

However, depending on the facts involved, actions or omissions related to or arising as a consequence of deficient risk management may trigger breaches of administrative, civil, criminal and other regulations.

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

There is no corporate compliance defence under Regulation 'A' 5398 of the Argentine Central Bank, Resolution 38,477 of the National Superintendence of Insurance or Resolution 606/2012 of the Argentine Securities Commission.

Law No. 27,401 establishes provisions that are not considered actual defences, but can be considered as factors to extinguish or reduce penalties.

In order to extinguish criminal and administrative penalties the legal entity must:

- spontaneously self-report a crime set forth by this law as a consequence of internal detection and investigation;
- establish, before the facts under investigation occurred, a proper control and supervision system (eg, integrity programme), the breach of which would require an effort by the wrongdoers; and
- return the undue benefit obtained through the crime.

Pursuant to reduction of penalties, the judges will consider:

- compliance with internal rules and procedures;
- number and hierarchy of the individuals involved;
- omission of vigilance on the actions of the authors and participants in the crime;
- damage caused;
- amounts of money involved;
- size, nature and economic capacity of the legal entity;
- spontaneous self-reporting by the legal entity as a consequence of an internal investigation;

Pedro Serrano Espelta **pse@marval.com**
Gustavo Morales Oliver **glo@marval.com**

Av Leandro N Alem 882 Tel: +54 11 4310 0100
C1001AAQ Buenos Aires Fax: +54 11 4310 0200
Argentina www.marval.com

- subsequent behaviour; and
- remediation of damage caused and likelihood of recidivism.

The anti-money laundering and anti-financing terrorism regulations do not provide actual corporate compliance defences but establish the following factors to reduce penalties:

- compliance with internal rules and procedures;
- omission of vigilance on the actions of the authors and participants in the crime;
- damage caused;
- amounts of money involved; and
- size, nature and economic capacity of the legal entity.

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

Since most laws and regulations addressed herein have been recently enacted, there are no leading cases regarding their enforcement. Nevertheless, there are some records that demonstrate what authorities are taking into account to impose sanctions on individuals or entities subject to their power.

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

Regarding risk management obligations, there are no special rules for government, government agencies and state-owned enterprises.

Regarding anti-corruption compliance management, Decree 41/1999 of the federal administration approves the code of ethics for public officials working in such administration that provides compliance anti-corruption obligations. The most relevant are:

- submission of a sworn statement of their heritage and financial situation to the National Public Ethics Office;
- reporting any conflict of interest that can affect the public official's independence and result in the violation of relevant laws and regulations due to placing their own interest before the administration's interest; and
- not asking for or receiving, directly or indirectly, money, gifts, benefits, favours, promises or other advantages:
  - to do, delay or omit something related to their functions;
  - to influence another public official so that they do, delay or omit something related to their functions; or
  - as a consequence of being a public official.

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

The main difference is that the private sector is more regulated than the public sector in terms of risk and compliance management obligations.

Brazil

Bruno De Luca Drago and Fabianna Vieira Barbosa Morselli

Demarest Advogados

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Corporate risk and compliance management have significantly increased in importance in Brazil since the enactment of the Brazilian Clean Companies Act (BCCA, Law No. 12,846/13) and its regulation, Decree No. 8,420/15, which determine that the execution of an effective integrity programme can reduce penalties imposed to legal entities by up to 20 per cent.

Equally important is Law No. 12,850/13, enacted around the same time as the BCCA, which provides for criminal enforcement against a newly created concept of 'criminal organisations' – namely, an association of four or more individuals structurally organised, characterised by a division of tasks, with the object of obtaining, directly or indirectly, any sort of advantage as a result of the practice of certain criminal infringements. An important provision introduced by the Law concerns plea bargaining agreements, which significantly changed the dynamics of criminal investigations in the country.

Partially because of these new pieces of legislation, and partially because of new interpretation of former legislations and burden of proof standards applied by the courts, several Brazilian companies have been dragged into the criminal investigation spotlight – particularly Operation Car Wash, which was largely covered by the local and international media.

The outcomes for Brazilian companies (for their commercial activities in Brazil and abroad) could not be more challenging within this new compliance and governance environment.

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

The main legislation directly addressing corporate risk and compliance management in Brazil is as follows:

- Law No. 12,846/13 –BCCA;
- Law No. 12,850/13 – Criminal Organisations;
- Law Decree No. 8,420/15 – BCCA Regulation;
- Law No. 13,303/16 – Public Companies' Law;
- Law No. 12,529/11 – Competition Law;
- Law No. 9,613/98 – Money Laundering Law;
- Law No. 8,666/93 – Public Bidding Law;
- Law No. 8,429/92 – Improbity Law; and
- Law Decree No. 2,848/40 – Criminal Code.

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

Law No. 12,846/13 applies to any corporation, foundation, association or to foreign companies that have their registered office, branch or representation in Brazil, and that engage in wrongful acts against the public administration. Both foreign governments and public international organisations are described by the term 'public administration'. As for foreign public agents, the law is defined as anyone who holds an office, is employed or is in civil service in public entities, government entities or diplomatic representations abroad. The entity would be controlled by the foreign government or international public organisations.

It is important to note that the BCCA did not establish criminal liability of legal entities, but rather an administrative and civil liability of such entities. Moreover, the Law does not exclude the administrative and civil liability of its directors or officers, that may be held accountable in connection with a tort, to the extent of their culpability. In addition, directors or officers may also be held criminally accountable under the provisions of the Brazilian Criminal Code.

The Law also establishes that, in the event of a merger or amalgamation, the responsibility of the successor will be restricted to a payment of a fine limited to the value of the assets transferred. In addition, parent companies, subsidiaries, affiliates or members of a consortium, within the scope of the contract, may be jointly and severally liable for the infringements perpetrated, such liability being limited to the payment of administrative fines and full compensation of damages caused.

Related legislation such as the Improbity Law and the Brazilian Competition Law have a similar perspective in terms of targeted undertakings. Regarding money laundering, the penalties apply for those who directly engage in illegal conduct, and also 'gatekeepers' who fail in their duty to inform.

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

Under the administrative sphere, the regulatory body responsible for enforcing the BCCA is the higher authority of the corresponding public entity against which the infringement was committed, or a ministry of the state if the conduct is executed against the direct public administration. In such cases, the latter will designate a special commission for the monitoring and judgment of the procedure.

In addition, whenever the infringement involves the Federal Public Administration, the Federal Comptroller's Office (CGU) has delegated powers to enforce legislation. The CGU also holds general powers to take over investigations related to infringements committed against any other public authorities.

In case of procedures for damage compensation, the harmed public agency may file a claim before the judiciary courts, with the assistance of the Attorney General. Public prosecutors also have concurrent jurisdiction to bring damage claims, mainly to enforce administrative fines against legal entities before the courts.

There are also other entities in charge of enforcing different legislation, such as the Federal and State Account Tribunal (over issues of Improbity Law) and the Administrative Counsel of Economic Defence. They deal with competition issues involving bid rigging, among other things.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

Normative Instruction No. 01/2016 issued by the Federal Public Prosecutor and General Controller (now the Ministry of Transparency) define 'risk management' as a 'process, to identify, evaluate, manage and control potential events or situations, to provide reasonable certainty as to the achievement of the objectives of the organisation'.

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

Law No. 13,303/16 defines the processes to be adopted in state-owned companies and mixed-capital entities, while the BCCA and its

Regulation determines the desirable processes to be implemented in private companies.

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

Decree No. 8,420/2015 provides for the minimum requirements for an integrity programme to be considered effective and, thus, to be able to benefit from a reduction in fines for infringements by legal entities.

According to the Decree, a compliance programme consists of:

> *[the] mechanisms and internal proceedings of integrity, auditing and incentives to denounce violations in the context of a corporation, and the effective application of codes of ethics and conduct, policies and guidelines with the objective to detect and correct violations, fraud, irregularities and illicit acts committed against the public administration, either national or international.*

Minimum requirements for the programme to be considered a mitigating factor include:

- engagement of senior management of the company;
- implementation of a code of ethics, code of conduct and compliance policies applicable to all employees and managers;
- extension of the programme to third parties such as suppliers, service providers, agents and associated companies;
- periodic training;
- periodic risk assessment;
- proper accounting registries;
- internal controls that secure trustworthy financial reports;
- internal proceedings that prevent fraud and illicit acts;
- independence, means and delegation of powers to the compliance officer;
- an open communication channel for reporting of irregular activity;
- disciplinary actions in case of violations;
- internal procedures to secure the immediate interruption of the detected violation, and damage remediation;
- appropriate checking measures for hiring third parties; and
- disclosing donations to political parties and candidates transparently.

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

Resolution 4,567/2017, edited by the National Monetary Council, created the obligation for financial institutions to adopt compliance mechanisms. The institutions covered by the Resolution must have a communication channel through which employees, customers, users, partners or suppliers may report any wrongdoing or unlawful action related to the activities of the institution, without identifying themselves. The competent area within the organisation shall prepare semi-annual follow-up reports on the matters reported, containing at least the number of reports received, their nature, the areas responsible for dealing with the situation, the average time to deal with each situation and the measures adopted by the institution with regard to the reported matter.

More recently, the State and the Federal District of Rio de Janeiro enacted State Law No. 7,753/2017 and District Law No. 6,112/2018, respectively. Both items of legislation set forth the mandatory implementation of integrity programmes by companies that execute agreements with the Public Administration, whether it is a contract, consortium, concession or any other type of agreement.

In the case of the Federal District, the rule is valid for any agreements with a term that exceeds 180 days and that has an estimated value equal to or higher than the value established for bids under the price submission procedure (80,000 reais–650,000 reais).

The rules of State Law No. 7,753/2017 apply to any agreement with a term that exceeds 180 days and that has a value that exceeds those established for bids under the competition procedure, currently 1,500,000 reais for construction works and engineering services, and 650,000 reais for acquisitions and services.

Technically, other than for the financial institutions covered by Resolution 4,567/2017 or companies subject to State Law No. 7,753/2017 or District Law No. 6,112/2018, there is no general obligation to implement risk and compliance governance in Brazil; however, there are benefits for doing so. Nevertheless, certain obligations may apply in certain circumstances, such as for participating in the 'new market' of the Brazilian Stock Exchange (higher levels of governance apply).

Update and trends

A noteworthy development is the enactment of Resolution 4,567/2017, which established specific compliance obligations to financial institutions.

Specific rules on other economic sectors will likely follow, owing to the growing awareness of the relevance of integrity programmes by both the government and private initiatives.

In this sense, State Law No. 7,753/2017 and District Law No. 6,112/2018 address a national concern when it comes to agreements with the Public Administration, which has been intensifying since the BCCA came into force. Thus, other states of the federation are expected to adopt similar rules.

Decisions on the application of Decree No. 8,420/15 and the reduction of penalties for legal entities with an effective compliance programme are also to be followed closely.

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

As mentioned above, there are no legal general obligations to implement risk and compliance governance in Brazil. However, each company will determine, on a case-by-case basis, the level of governance it intends to implement, following best guidelines and legal standards provided by the legislation.

In this regard, it is recommended that companies implement mechanisms and internal control proceedings against irregularities on the application of its conduct and ethics statutes. Such mechanisms, referred to as an 'integrity programme', must be suitable and updated according to the activities and requirements of the undertaking. The existence of a well-structured integrity programme helps to diminish penalties in the event of an infraction of the compliance or anticorruption obligations set out by law.

Moreover, the creation of such programmes has been increasingly considered, not only by public authorities but also by the private sector, in order to allow for financing mechanisms, public and private bids and general contracting services.

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

As part of the undertaking's management activities, these individuals may be held liable for infringements of the legislation referred to herein, but only to the extent of their guilt or intent. More precisely, new local criminal theories – such as the Theory of Final Domain of Fact – may expose executives to administrative and criminal prosecution resulting from a failure in their duty (omissive action) to supervise their subordinates once an executive is aware of – and should have acted on – the facts involving the decision-making process of their subordinates.

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

There are no direct consequences for deficiencies in risk and compliance management mechanisms; however, there could be penalties if these deficiencies result in infringement of Brazilian statutes. Moreover, deficiency in compliance controls will prevent undertakings from benefitting from reductions on possible administrative fines.

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

As in question 11, there are no direct consequences for deficiencies in risk and compliance management mechanisms; however, there could be penalties if these deficiencies result in infringement of Brazilian statutes.

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

In Brazil, there is no criminal liability for legal entities except for issues related to the environment. However, it is possible for directors and

officers of an undertaking to be criminally liable for infringements they have committed, but only to the extent of their guilt or intent. In these cases, the applicable procedures and penalties will be the ones provided for in the Criminal Code and related legislation.

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

According to the BCCA, these individuals are liable to the extent of their guilt, regardless of the legal entities' liability. The individual will be subject to the provisions of the Improbity Law that determines that offenders repair the damage or return the goods that were illicitly obtained, as well as the ones provided in the Civil Code and Law No. 6,404/75 (regarding corporations and their partners).

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

The BCCA does not provide for liability of individuals. Regarding the antitrust legislation, individuals may be subject to a fine and may be prevented from exercising commerce for a period of up to five years. According to the terms of the Improbity Law, individuals may be subject to freeze of assets, return of money illegally obtained or a fine of up to three times of the value obtained illegally, in addition to the restoration of the damages caused.

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

To the extent that a criminal infringement (such as corruption, money laundering, fraud, cartel, etc) is proved against a member of a governing body or senior management, criminal liability provided for in the Brazilian statutes may vary according to the nature of the infringement in question.

Criminal liability is only applicable to individuals in Brazil (except for environmental issues where there may be corporate criminal liability). Private corruption is not considered a crime (therefore there must be a public agent or public body involved in order for it to be considered a crime).

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

The offenders may present a defence based on the hypothesis set out in article 18 of Decree No. 8,420/15, such as:

- having a robust compliance programme;
- voluntary self-disclosure;
- collaborating with the investigation, regardless of the execution of a leniency agreement; and
- refunding damages caused.

This defence will not exempt the offender from guilt, but could help diminish the penalties to be applied.

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

In Brazil, the all-time leading cases regarding corporate risk and compliance management failures were brought up by Operation Car Wash. The companies targeted were discovered to be part of a corruption and cartel scandal in several different markets in which they are active, shedding light on the importance of a well-structured compliance programme and regular monitoring. The settlement agreements executed – and still under negotiation – are also serving to determine the structure of such mechanisms.

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

Law No. 13,303/16 provides for obligations to state-owned companies and mixed-economy entities. Government agencies and the government itself are subject to the provisions of the Improbity Law and the Fiscal Management Liability Law (Complementary Law No. 101/2000).

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

The main compliance law applicable to the public sector is the Improbity Law, which punishes improbity acts performed by public agents against the public administration. It can also be applied to private parties if they are proven to have benefited directly or indirectly from the act. It must be proved that the offender acted with guilt (first or second degree) in order for him or her to be penalised.

As for the private sector, the main regulation is the BCCA. It is applicable to legal entities who perform wrongful acts towards national or foreign administration. Contrary to the Improbity Law, there is strict liability provided – meaning it is not necessary to prove intent or guilt.

In addition, the BCCA would arguably provide for a compliance defence, which is not possible under the Improbity Law.

Bruno De Luca Drago **bdrago@demarest.com.br**
Fabianna Vieira Barbosa Morselli **fmorselli@demarest.com.br**

Av Pedroso de Moraes, 1201
Pinheiros
Sao Paulo 05419-001
Brazil

Tel: +55 11 3356 1800
Fax: +55 11 3356 1700
www.demarest.com.br

China

Gary Gao
Zhong Lun

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Corporation is one of the most fundamental units in social economy, as well as a crucial civil and commercial subject. Therefore, various laws and regulations on corporate risk and compliance management and controlling play an irreplaceable key role in the Chinese jurisdiction.

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

Corporate risk and compliance management and controlling is a relatively broad concept, involving all aspects of corporate operation and governance. The most common topics include: strategy risk, finance risk, market risk and operational risk. At present, China does not have a specialised law or regulation integrating all corporate risk and compliance management and controlling. These provisions are spread across laws and regulations governing various fields. For example, the Company Law and Administrative Regulations on Company Registration outline the general requirements for companies; the Law on Enterprise Income Tax, Basic Rules for Enterprise Internal Control and Financial Rules for Financial Enterprises deal with finance risk management; and the Anti-Unfair Competition Law, Labor Contract Law and Interim Regulations on Prohibition of Commercial Bribery govern operation risk management, etc.

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

Because undertakings such as limited companies, listed companies and financial institutions are of great importance to China's economy, all of them are heavily regulated by laws and regulations. In comparison, because listed companies directly affect a wider public interest, they are the most strictly regulated. The major governing laws and regulations in this field include the Securities Law, Guidance for the Articles of Association for a Listed Company and Regulation of Shareholders' Meeting of Listed Company. Furthermore, in recent years, China has strengthened the risk management and controlling of internet financial institutions, such as the management and controlling of shadow and peer-to-peer (P2P) banking for which the main regulations include the Measures for the Liquidity Risk Management of Commercial Banks (Trial) (amended in 2015) and the Implementation Plan of Specific Rectification Work of P2P Internet Credit Risk.

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

The main supervisory authorities in charge of corporate compliance management include:

- the Administration for Market Supervision (and previously the Administration for Industry and Commerce (AIC)): market supervision and management, law enforcement administration;
- the Tax Bureau: classifying the taxpayer, administration of tax collection;
- Customs: port management, bonded supervision and management, customs inspection;
- the Foreign Exchange Authority: supervising the foreign exchange market, managing foreign exchange settlement and sale;
- the China Securities Regulatory Commission (mainly concerning listed companies): centralised and unified supervision and management of the securities and futures market, supervising listed companies and securities market activities performed by the shareholders of listed companies under their obligations stipulated by the laws and regulations;
- the China Banking and Insurance Regulatory Commission (mainly concerning financial institutions and insurance companies): examining and approving the establishment, change, termination and business scope of financial institutions and insurance companies, executing the qualification management of the directors and senior executives of banking financial institutions and insurance companies, inspecting the business activities and the related risks of banking financial institutions and insurance companies;
- the Public Security Bureau: maintaining the social security order, protecting public and private properties, preventing and punishing delinquency activities;
- the Procuratorate: works on behalf of the State in accordance with law, to exercise the procuratorial authority of a State organ. The main duties are investigating criminal responsibility, raising public prosecution and implementing legal supervision; and
- the Supervisory Committee: a new established institution, this is the political organ used to realise the self-supervision of the Party and the State. On behalf of the Party and the State, it supervises all civil servants who exercise public power. It investigates not only illegal behaviours concerning duty, but also criminal behaviours concerning duty.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

Generally, there are some definitions of 'risk management and controlling' and 'compliance management and controlling' in the laws and regulations regarding financial institutions and listed undertakings. For example, the Guidelines on Comprehensive Risk Management for Banking Financial Institutions, Measures for the Compliance Management of Securities Companies and Securities Investment Fund Management Companies, Specification for Compliance Management of Securities Investment Funding Management Companies, Measures on Risk Control Standard Management of Securities Companies, Regulation on the Risk Disposal of Securities Companies, Measures on Risk Control Standard Management of Futures Companies and Guidelines on Reputation Risk Management of Insurance Companies.

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

Generally, concerning financial institutions and listed undertakings, there are rules for the specific process of risk management and controlling and compliance management and controlling stipulated in the rules and regulations (such as the rules and regulations mentioned in question 5). However, in China it is rare that rules are made for the specific process of risk management and controlling and compliance management and controlling for general companies or enterprises unless the State is strengthening the supervision of a specific industry. If so, there may be some specific risk compliance requests for the companies in that specific industry. In addition, owing to the special status of the State-owned enterprise, the State will announce some principal

Update and trends

Before the election of the new government of the People's Republic of China in March 2018, there was some expectation that the new government may to some extent reduce its emphasis on anti-corruption because the anti-corruption struggle since 2014 has already achieved great effects. However, with the new government taking power, they have shown they will continue to strengthen their efforts to combat corruption through public propaganda and practical action.

Among the government's recent anti-corruption efforts, the most notable are the establishment of the Supervisory Committee and the promulgation of the Supervision Law. Pursuant with the Supervision Law, the Supervisory Committee oversees all functionaries who exercise public power; investigates duty-related violations and crimes; conducts the construction of clean governance and anti-corruption work; and upholds the dignity of the Constitution and laws.

It is worth noting that the Supervisory Committee has absorbed the functions of the Anti-Corruption Bureau within the People's Procuratorate and greatly expanded the regulatory target. Under the current legal structure, government workers, ranging from top-tier ministers to frontline clerks, all now fall within the scope of the regulatory target of the Supervisory Committee, which also triggers the change of the criminal justice system of the People's Republic of China.

Against the backdrop of economic globalisation, when Chinese enterprises go abroad to expand their businesses, more and more compliance risks shall be faced and will need to be resolved. For example, due to the current Sino–US trade relationship, how Chinese enterprises try to comply with US regulations and avoid commercial losses is a really pressing issue. Furthermore, with the One Belt and One Road strategy raised by the government, Chinese enterprises may expand their businesses into some countries or regions where they will face serious compliance and corruption risks. How Chinese enterprises conduct their commercial activities within such an environment is a worthy question to explore as well.

Of course, there is no doubt that the Chinese government will keep up the good momentum to perfect its legal system and law enforcement to ensure that businesses from all walks of life can benefit from a fair yet efficient compliance environment.

regulations or guidelines in order to push the State-owned enterprise to conduct risk management and controlling and compliance management and controlling. For example, the Opinion on the Overall Advancement of the Rule of Law Construction of Central Enterprises announced by the State-owned Assets Supervision and Administration Commission of the State Council.

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

Generally, the standards and guidelines concerning the risk management and controlling and compliance management and controlling of financial institutions and listed companies are based on the laws and regulations. For example, the Guidelines on Comprehensive Risk Management for Banking Financial Institutions stipulate the standards and guidelines for the risk system of banking financial institutions from several perspectives, including risk management structure; risk management strategy; risk preference and risk limitation; risk management policy and procedure; management information systems and data qualification controlling mechanisms; as well as internal controlling and audit systems. However, for general companies, there are no standards and guidelines for specific risk control and compliance control stipulated by law. Generally, companies will establish respective risk and compliance controlling systems based on their own business conditions in order to prevent non-compliance activities from occurring. However, not all companies have their own risk and compliance controlling system. In most cases, only comparatively large-scale enterprises will have a risk and compliance controlling system.

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

In China, companies have corresponding risk and compliance obligations (see question 2). There are no laws and regulations that request a company to establish an internal reporting mechanism but, in practice, most large-scale enterprises will actively establish such a mechanism. Generally, the internal reporting mechanism will list the reporting scope, reporting procedure (commonly reporting to an independent department or individual, which means no need for N+1 approval from the informer), award for reporting, punishment for non-reporting and protection for the informer (for example, the informer shall not be demoted or fired, face a reduced salary, etc, because of the reporting).

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

Internal governance

This mainly includes company governance compliance and financial and tax compliance. Company governance compliance includes the compliance of the board of directors and board of shareholders, the rule of procedure of the board of directors, compliance with equity structure, compliance with various policies of the company, etc. Financial and tax compliance includes compliance with revenue accounting, compliance with tax payment, etc.

External operation

This mainly includes business compliance and third-party compliance. Business compliance refers to compliance with business model, compliance with contract signing procedure, etc. Third-party compliance includes the risk audit for transaction, internal audit and third-party audit, regular assessment and rewards, punishments, etc.

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

The risk and compliance management of a company cannot be separated from the establishment, execution and obedience with compliance policy by the management. The main obligations for the management include:

- establishing the compliance controlling strategy;
- establishing the risk compliance system;
- cultivating the risk consciousness of employees and the compliance culture of the company;
- supervising the compliance operation of the company;
- being forbidden to embezzle the property of the company via the advantage of convenience of position;
- being forbidden to take bribes or commit bribery for the benefit of the company or individual;
- being forbidden to violate the obligation of prohibiting on business competition; and
- confidentiality.

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

Yes. If the non-compliance activity infringes a third party, the third party may be able to sue the company. For example, if the company violates the Cyber Security Law to collect sensitive personal information without the consumer's authorisation, the consumer may be able to bring civil litigation against the company in order to make the company compensate for the infringement regarding right to reputation, right to privacy, etc. Another example is, if a company fires an employee who conducted non-compliance activity while such activity has not been stated as a reason for dismissal in the compliance governance documents of the company, the company may be sued by the employee.

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

Yes. If the company's non-compliance activity violates the related laws and regulations, the company may face corresponding administrative punishment. For example, if the company violates the Anti-Unfair Competition Law to bribe a trading party, the administrative organisation can impose a penalty, confiscate illegal gains, revoke the business licence and record in the credit record among other punishments.

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

Yes. If the company's non-compliance activity violates the related laws and regulations and meets the standard of filing a criminal case, the company may face corresponding criminal punishment. For example, if the company violates the Criminal Law to smuggle goods or evade the payable tax, the company will have a penalty imposed on them several times the size of the original payment amount.

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

Yes. If the company's non-compliance activity violates the related laws and regulations, the legal representative of the company and the senior management involved in the non-compliance activity may face corresponding civil liability. For example, if a company is enrolled on the blacklist of dishonesty because of outstanding debt, according to Interpretations of the Supreme People's Court on Certain Issues Concerning Application of Enforcement Procedure of the Civil Procedure Law of the People's Republic of China, the person directly responsible or the person subject to direct liability for affecting the performance of debts may be restricted from leaving the country, staying in a hotel, taking a flight, opening a banking account, etc.

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

Yes. If the company's non-compliance activity violates the related laws and regulations, the legal representative of the company and the senior management involved in the non-compliance activity may face corresponding administrative punishment. For example, a senior executive of a company who also holds a post within the Party or acts as a national civil servant may be dismissed from office or expelled from the Party if the company infringes State-owned property.

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

Yes. If the company's non-compliance activity violates the related laws and regulations and meets the standard of filing a criminal case, the senior management involved in the non-compliance activity may face corresponding criminal punishment. For example, according to the Criminal Law, if the company unlawfully raises funds and the amount involved is huge, as well as the penalty imposed on the company, the person who is directly in charge will be sentenced to fixed-term imprisonment or criminal detention.

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

According to the current laws and regulations in China, there is no generalised compliance defence. However, in judicial practice and law revision, there is some narrow compliance defence. For example, if a company has express policy that prohibits its employees from bribing medical workers to illegally collect the personal information of consumers, the court can identify that the non-compliance activity was individual behaviour conducted by the employee and the company may not face any liability. Another example is, according to the Anti-Unfair Competition Law, if an employer has evidence to prove there is no relation between the transaction opportunities or competition advantage and an employee's non-compliance bribery, including that the employer has not gained any benefit owing to the employee's non-compliance activity, the employer may not be punished.

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

In November 2017, Shanghai YangPu AIC decided that employees of Squibb, in the hope of procuring drug sales, sponsored the business class tickets for flights for a hospital medical director to participate in the European Society of Cardiology Congress in London in 2015. The AIC further discovered that, during that period, the hospital that the medical director worked for did purchase related drugs from Squibb in larger amounts than previously purchased. Such behaviour violates the related provisions of the Pharmaceutical Administration Law of the People's Republic of China. The AIC imposed an administrative punishment on Squibb and the involved individuals, including the confiscation of illegal gains and the imposing of a fine.

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

Yes. For example, the Several Opinions on Promoting Fair Competition and Maintaining Regular Order in the Market, issued by the State Council on 4 June 2014, put forward recommendations to reform the system of market access. These include setting a clear negative list, vigorously reducing administrative examination and approval of items, banning a disguised form for examination and approval, etc.

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

In China, the risk and compliance management obligations for the public sector and private sector are basically the same. However, owing to the different social status, the obligations for the public sector are greater than for the private sector and the punishment for the public sector can be more severe than for the private sector as well. Furthermore, from a criminal perspective, the same behaviour conducted by the public sector or private sector may cause different accusations and criminal punishment. For example, if a public sector employee takes a bribe, the employee may be accused of the crime of taking bribery, which is a specific crime for an employee of the public sector. However, if a private sector employee takes a bribe, the employee may be accused of the crime of non-official servant taking bribery. The standards of criminal punishment for those two crimes are different.

中倫律師事務所
ZHONG LUN LAW FIRM

Gary Gao **gaojun@zhonglun.com**

Level 10 & 11
Two IFC
No. 8 Century Avenue
Pudong New Area
Shanghai 200120
China

Tel: +86 21 6061 3666
Fax: +86 21 6061 3555
www.zhonglun.com

Germany

Barnim von den Steinen
Rotthege | Wassermann

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Corporate risk and compliance management is gaining ever more importance in Germany. The trend started in the late 1990s, when corruption of foreign officials became a criminal offence, fuelled by cases where the European Commission imposed massive antitrust fines and by the German Federal Court ruling that supervisory boards are obliged to assert and claim damage compensation from management board members if damage for the company results from an infringement of their duty of care.

Compliance management was believed to have reached its peak in Germany following the Siemens corruption scandal of 2006. In reality, as recent cases show, a peak has not yet been reached (see question 18). Nowadays, the main drivers are as follows. Firstly, financial industry regulation, which develops risk and compliance management concepts that are also implemented in other industries and in the public sector. Secondly, the commitment of tax and law enforcement authorities, high-volume damage claims as well as civil and criminal court rulings give reason to introduce and improve corporate risk and compliance management systems.

As fines and claims for damages have been causing losses of billions of euros in several cases because of violations of antitrust laws, capital market obligations or anti-corruption laws, this has attracted not only the attention of investors and the media in Germany but also of large companies and led to the introduction of comprehensive risk management and compliance structures. Today, the trend towards introducing systematic corporate risk and compliance management systems is also extending into German Mittelstand (medium-sized companies), particularly as the legal requirements are not predominantly differentiated according to company size.

It is important to note that corporate risk and compliance management is also of fundamental personal importance to management and supervisory board members and responsible employees, since they may personally be held liable – not only for violations of the laws (eg, anti-corruption legislation) but also for infringements of duty of care regarding proper risk and compliance management (eg, insufficient measures to prevent infringement of laws and failure to react when evidence for weaknesses in the systems arises). This in turn may result in damage claims, criminal prosecution and administrative fines against them.

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

The following legal provisions may be regarded as important rules addressing corporate risk and compliance management:

- Each member of the board of directors of a stock corporation is subject to the duty of legality, according to which due care includes both personal compliance with laws and taking care of the company's compliance with laws and internal directives (common understanding based on sections 76 and 93 German Stock Corporation Act). Managers of companies of other legal forms, for example, limited liability companies, are also legally responsible for ensuring that the represented company complies with laws.
- Risk management is a specific duty for the management board of a stock corporation pursuant to section 91 paragraph 2 German Stock Corporation Act: the board must take appropriate measures – in particular, setting up a monitoring system so that developments that threaten the company's existence are detected at an early stage.
- Inadequate supervision by the board of directors or company owner to prevent legal violations by employees of the company can be punished with massive fines against both the responsible manager and the company (sections 30 and 130 German Act on Regulatory Offences).
- Entities in the banking, financial services and insurance sectors are required to set up and maintain risk management and compliance functions in accordance with specific legal requirements.
- The German Corporate Governance Code (DCGK) contains certain recommendations regarding compliance governance for listed companies (see question 8).

Apart from the financial industry for which specific legal requirements exist, corporate law deliberately leaves open the organisational measures necessary to fulfil the compliance obligation. Each individual company is left to decide on the concrete structure governing all its compliance processes and systems and, subject to due examination and preparation, this decision lies within the entrepreneurial discretion of the board of directors.

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

Regulated financial institutions (including insurance companies), certain corporate entities such as stock corporations and limited liability companies, as well as listed companies, are within the focus of authorities that enforce risk management and compliance violations. In general, however, management board members and company owners, irrespective of company legal form, are obliged to take reasonable steps to avoid legal violations from their companies.

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

The Federal Financial Supervisory Authority (BaFin) is authorised to enforce measures with regard to credit institutions and regulated financial firms (including insurance companies). Risk and compliance management deficiencies of banks or other regulated financial institutions may have various consequences, for example, administrative fines, dismissal of the responsible members of the management board and, ultimately, withdrawal of the licence.

Independently from the industry sector, the public prosecutors are responsible for the prosecution of administrative offences, for example, failure to comply with the obligation to take appropriate measures against legal infringements (section 130 German Act on Regulatory Offences).

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

In Germany, there are no general legal definitions for 'risk management' and 'compliance management'.

The DCGK addresses listed companies and provides a definition of compliance in clause 4.1.3 DCGK: The board of directors must

ensure compliance with legal requirements and internal corporate guidelines and ensure that compliance is observed by subsidiaries. The provisions of the Code are not mandatory law, but as a general rule, the requirements are implemented by listed companies.

For credit institutions, a definition of risk management is provided by the BaFin (clause AT1 of the Minimum Requirements for Risk Management): risk management includes the establishment of appropriate strategies and the establishment of appropriate internal control procedures. The internal control procedures consist of the internal control system and internal auditing. The internal control system shall include in particular:

- rules on the organisational and operational structure;
- processes for identifying, assessing, managing, monitoring and reporting risks (risk management and risk control processes); and
- a risk control function and a compliance function.

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

For financial institutions, specific processes and rules are set out by BaFin in the Minimum Requirements for Risk Management (MaRisk). This framework includes specific regulations for risk management processes BaFin regards as standards to be obeyed. Pursuant to MaRisk, each institution must have a compliance function to counter the risks that may arise from non-compliance with legal regulations and regulations.

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

The Institute of Public Auditors in Germany have published an audit standard for voluntary audits of compliance systems (IDW PS 980). It serves as a non-governmental benchmark for examining compliance management processes. This auditing standard serves to orient responsible persons regarding the proper structure of a content management system and its examination. An audit will provide additional assurance as to the adequacy and effectiveness of the principles and measures introduced in the company for the purpose of preventively ensuring proper compliance with laws. At the same time, a corporate body documents that it has had the compliance system checked in accordance with its responsibilities.

One must note that the guidelines are nonbinding and that the board of directors has rather broad discretion in weighing the specific risks of the entity they represent and how to address them.

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

All undertakings

Generally, German law does not provide for specific rules as regards risk and compliance governance. Most larger undertakings implement a risk and compliance structure that reflects adequate governance obligations. However, which rules will be implemented depends on the specific case. Save the individual situation, best practice comprises the following (see also question 9):

- Typically, German companies have a management board and a separate supervisory board. Such two-board structure is mandatory for a German stock corporation, and most European companies also provide a two-board structure. A limited liability company must have a supervisory board if it has more than 500 employees. It is advisable to design a risk and compliance management system in such a way that there is direct access to the supervisory board for the heads of risk and compliance management. This will improve the effectiveness of such a system, in particular because of the possibility of prompt and uninfluenced reporting to the supervisory board, namely, the persons that control the management.
- The independence of the risk and compliance management system is also a decisive factor for a sound corporate compliance defence (see also question 17). This independence can be ensured, for example, by agreeing on longer employer-side notice periods with regard to the head of risk or compliance. Also, a fixed remuneration of the compliance officer, which is not dependent on the prosperity of the respective monitored area, contributes to the integrity of the system.
- Finally, a compliance system must always be equipped with sufficient effective powers and resources to effectively prevent violations. Examples include random and unannounced business process reviews, document controls, email checks (save the data protection and privacy rules), or the introduction of regular reporting obligations to the supervisory board. Last but not least, monitoring by documenting the implementation of measures also plays an important role.

Stock-listed companies

German companies listed on the regulated stock market are subject to risk and compliance 'governance' obligations pursuant to the DCGK. Actually, such listed companies are required to provide a declaration of (non-)conformity regarding the obedience of the recommendations of the Code. If a recommendation is not being applied, the company needs to disclose and explain this in the annual declaration of conformity ('comply or explain'). The largest listed companies in Germany typically obey all recommendations as they represent best practice. The Code states that compliance is a task of the management board and defines it as compliance with legal and internal provisions (section 4.1.3 DCGK). The Code further states that the management board should submit information on risk management and compliance to the supervisory board (section 3.4 DCGK). In addition, the Code recommends a regular exchange between the chairman of the supervisory board and the chairman of the board of directors on matters relating to risk assessment, risk management and compliance (section 5.2 DCGK), and that the supervisory board establishes an audit committee to supervise the effectiveness of the risk management and compliance systems (section 5.3.2 DCGK).

Regulated financial institutions

Financial institutions and other regulated undertakings in the financial industry are subject to specific risk and compliance governance obligations (see question 9, as regards regulated financial institutions).

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

All undertakings

There is no standard set of obligations that must be implemented. Therefore, the implementation of a risk and compliance management system is a business decision of the board of directors. After due diligence, acting within the scope of a careful decision and without any conflict of interests, the board is free to decide on adequate measures without having to fear damage claims ('business judgment rule', section 93 German Stock Corporation Act). This general concept is also applicable to undertakings of other legal forms.

As a general practical approach, save an individual analysis and a set-up of customised rules, a risk and compliance management system is typically characterised by three core attributes:

- Assessment of the key risk areas in the company, addressing the risks through internal rules and living an integrity culture – including the board of directors and the supervisory board ('tone from the top') and also the employees – as well as adequate training and counselling. Thus, systematic misbehaviour can be ruled out.
- Immediate reaction by the responsible manager or board member or members as soon as there is evidence for individual misconduct or non-functioning of the systems; adequate reactions against lawbreakers and responsible supervisors.
- Proportionality: the system must be appropriate for the particular company and its risks (ie, individually tailored in scope, breadth and depth of regulation). It must not lead to risk-aversion or excessive, inappropriate formality.

As regards certain types of risks, typically the following areas are being addressed (alphabetical list): anti-corruption, anti-money laundering, antitrust, capital market issuer obligations (eg, ad hoc notices), data protection, employment, environmental protection, IT, product safety, tax, third parties and work protection.

Regulated financial institutions

Financial institutions and other regulated undertakings in the financial industry are subject to detailed risk and compliance management obligations set forth by BaFin in the Circular MaRisk. Even though this

framework is legally not binding, undertakings de facto are obliged to adopt the rules as key risk and compliance management obligations. Pursuant to MaRisk, each institution shall have a risk control function in place that is responsible for independently monitoring and reporting risks. The risk control function shall be segregated organisationally, up to and including the management board level, from the organisational units that are responsible for initiating or concluding transactions. In particular, the risk control function shall meet the following requirements:

- support the management board in all risk policy issues, in deciding and implementing the risk strategy and evolving a risk limitation system;
- carry out the risk inventory and draw up the overall risk profile;
- support the management board in developing and improving the risk management and risk control processes;
- develop and improve a system of risk ratios and a procedure for the early detection of risks;
- monitor the institution's risk situation and internal capital adequacy as well as compliance with the risk limits in place on an ongoing basis;
- draw up the regular risk reports for the management board; and
- assume responsibility for the processes for passing on material risk-related ad hoc information promptly to the management board, the responsible officers and, where applicable, the internal audit function.

Further key requirements are that the staff of the risk control function shall be granted independence and all necessary means to perform their tasks. The head of the risk control function shall be involved in important risk policy decisions of the management board. Certain powers and independence are required for the head of risk control.

In particular, the compliance function should meet the following requirements:

- Each institution should have a compliance function in place in order to counteract the risks that may arise from non-compliance with legal rules and regulations. The compliance function should ensure the implementation of effective procedures for complying with the legal rules and regulations that are material to the institution, and of corresponding controls. The compliance function should additionally support and advise the management board with regard to complying with these legal rules and regulations.
- The compliance function should regularly identify the material legal rules and regulations, non-compliance with which might jeopardise the institution's assets, in the light of risk factors. The compliance function should be, in general, directly subordinate to and report to the management board. It may also be linked to other control units. It may also be assisted by other functions and units in the performance of its duties.
- The institution shall appoint a compliance officer who is responsible for carrying out the compliance function tasks. Depending on the nature, scale, complexity and riskiness of the business activities, as well as on the institution's size, the compliance officer may in exceptional cases be a member of the management board. Compliance function staff shall be granted sufficient powers and unrestricted access to all information needed to perform their tasks. They shall be notified of instructions and decisions of the management board that are material to the compliance function. The compliance function staff shall be notified in due time of material amendments of the rules that are intended to ensure compliance with the material legal rules and regulations. The compliance function shall report to the management board on its activities at least once a year and on an ad hoc basis. Such reports shall address the appropriateness and effectiveness of the rules that are intended to ensure compliance with the material legal rules and regulations. The reports shall also cover information on potential deficits and on remedial measures. In addition, these reports shall be passed on to the supervisory board and the internal audit function.

The supervisory board shall be notified if the compliance officer or the head of the risk control function is replaced.

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

The members of the board of directors are each personally responsible and liable for a proper risk and compliance management. The members of the management board of a group of companies are also responsible for appropriate measures of the subordinated entities fulfilling risk and compliance obligations.

The responsibilities may be delegated to a certain member of the board, and sub-delegation to a member of the senior management is possible and advisable. However, the ultimate responsibility remains with all members of the board of directors, meaning they have to supervise the person to whom the task has been conferred.

The supervisory board is responsible for supervising the board of directors. This includes checking and monitoring whether the board of directors has established a proper risk and compliance management system.

Risk and compliance manage obligations exist only for those senior managers who have been assigned these tasks (eg, chief compliance officer). Their tasks cannot be described abstractly. It depends on the results of the analysis of the company's risks, which determine the individual tasks and the focus of the compliance measures to be taken.

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

Yes. If there are legal violations owing to inadequate risk and compliance management, customers may file damage claims, for example in cases such as antitrust violations (see truck cartel case, question 18) or bribery of public officials.

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

Yes. The Act on Regulatory Offences is applicable on any entity irrespective of the industry sector. Pursuant to this legislation, the management board or owner of an operation or undertaking shall be deemed to have committed a regulatory offence if they intentionally or negligently omit to take the supervisory measures required to prevent contraventions of laws within the operation or undertaking and such contraventions occur. A regulatory fine may be imposed on both the person and the entity. The fine to be imposed on the entity may generally amount to a maximum of €10 million. However, the regulatory fine shall exceed the financial benefit that the perpetrator has obtained from commission of the regulatory offence; the statutory maximum may therefore be exceeded if it does not suffice for this purpose.

There are specific rules for the financial industry: risk and compliance management deficiencies of banks or other regulated financial institutions may have various consequences, for example administrative fines, dismissal of the responsible members of the management board and, ultimately, withdrawal of the licence.

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

No. In Germany only natural persons may be subject to criminal fines, undertakings may not. There is an ongoing discussion to introduce a criminal liability for undertakings. A major reason against introducing such liability is that administrative fines (see question 12) are considered sufficient.

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

Each member of the board of directors of a stock corporation is responsible for ensuring that his or her company operates within the framework of the laws and internal directives and that any legal violations are avoided as much as possible. This obligation also applies to managers of companies of other legal forms.

If the management board violates these obligations, each individual member may face damage claims arising from this breach of duty by the company if the company suffered damage because of the breach. If tasks are delegated to a certain board member, the others may be held personally responsible for damages if they do not properly supervise

the delegated member and the compliance officer repeatedly reported on compliance failures (eg, the Siemens corruption case). In accordance with the jurisprudence of the Federal Court of Justice (BGH), the supervisory board is obliged to analyse and enforce the company's claims against members of the board of directors. Additionally, if the board of directors does not take actions against compliance failures and, in particular, systematic violations, the supervisory board knowing of such failure must take actions against the board of directors in order to restore proper risk and compliance management. If the supervisory board fails to do so and if damages occur or increase, the members of the supervisory board may be held liable for such damages.

Members of senior management – below the corporate board – may also be held liable by their company for damages resulting from the violation of risk and compliance management obligations. However, according to German judicial jurisprudence, being employees they bear a graduated liability. Liability therefore comes into practical consideration only when employees have deliberately violated their obligations. According to some court rulings, a special responsibility is assumed by the head of compliance.

According to section 93 paragraph 1 German Stock Corporation Act, no breach of duty exists if the member of the board of directors makes an entrepreneurial decision, assuming that he or she could act on the basis of appropriate information for the good of the company.

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

Inadequate supervision by the management or the owner of a company may be sanctioned with massive fines against the responsible person as well as the company (section 130 Act on Regulatory Offences).

Members of senior management also face administrative consequences, if the owner of a business or someone otherwise so authorised had commissioned this senior executive to manage a business or expressly commissioned a person to perform on his or her own responsibility duties that are incumbent on the owner of the business (section 9 German Act on Regulatory Offences).

As regards regulatory consequences, specific rules have to be observed, for example, for managers working in the banking sector (see above).

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

If the members of the management board of a stock corporation violate their duty of diligent care and damages arise therefrom, according to the jurisprudence of the German Federal Court, this may be regarded as a criminal offence pursuant to section 267 German Criminal Code ('infidelity'). Even if this has not been ruled in the respective Court judgment, the failure to establish an appropriate compliance system or to react promptly on evidence for infringements of law may also be deemed a violation of duty in this regard.

Members of governing bodies may be subject to criminal proceedings because they did not prevent (further) infringements out of their corporate entity. This criminal liability may also apply to senior managers (below the board of directors) and to members of the supervisory board if and to the extent that they are responsible for the supervision or the functioning of the compliance system. If, for example, a foreign official has been bribed by a company representative and if the responsible board member has evidence for such bribery but does not react appropriately, this omission to react may be regarded as a criminal offence by the responsible board member. As a result, the board member may be punished for bribery because of an inappropriate compliance practice. As such, in a 2012 court trial the long-term former head of the MAN commercial vehicle division ultimately admitted that he had not done enough to prevent bribery payments in Slovenia in 2004–2005, and was convicted for accessory to corruption by omission.

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

In Germany, there is no general statutory corporate compliance defence enabling a company, for example, to avoid vicarious liability for a violation of an anti-bribery provision by its management, employees or agents when implementing certain rules. Nor do compliance and risk management regulations applicable to financial institutions provide for corporate compliance defence. Hence, a financial institution may face civil liability claims even if it has obeyed all administrative legal compliance requirements.

However, a public prosecutor or court would consider whether an appropriate corporate compliance system was in place to prevent and detect violations of laws by employees and agents when determining the responsibility of the management for the infringement and the level of the financial penalty. Furthermore, they will also credit the firm for correcting the deficiencies in its compliance and risk management framework as part of a remediation programme. This could lead to a lower fine being imposed against the firm.

In the given context, one should recall that each individual company is left to decide on the concrete structure governing all its compliance processes and systems and, subject to due examination and preparation, the decisions on the actual setup of a risk and compliance management system lie within the discretion of the members of the board of directors (see questions 2 and 14). If the board members act within the limits of due care, they cannot be held liable for infringements of laws and resulting losses for the company. This, in a wider sense, may also be regarded as a corporate compliance defence.

Update and trends

Deficient compliance system causes risk for directors' and officers' (D&O) insurance coverage

The trend continues that companies hold liable members (or former members) of governing bodies for damages resulting from a violation of duty of care. We see many cases where such members are facing multi-million euro claims. Whereas the members tend to rely on insurance coverage, reality teaches unpleasant lessons: insurance companies increasingly try to refuse to make D&O insurance payments because a proper compliance management system had not been set up. The (higher) courts have yet to decide on such exclusions for insurance payments. However, it is advisable to regularly check and improve the risk and compliance management system as well as the performance and standing of the chosen insurance partner.

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

Volkswagen (VW) emissions scandal ('Dieselgate')

Public enforcement authorities and private plaintiffs worldwide are holding VW responsible in particular for illegal defeat devices in the engine control, false emission reports as a consequence therefrom and for delayed capital market information. VW CEO Martin Winterkorn has resigned over the scandal. German prosecutors launched an investigation into him and 36 other individuals. VW dismissed several top managers. Stock price damage claims in excess of €1 billion against VW are pending at German courts for violating its duty to publish ad hoc notices. Even if the scandal has not been settled yet, it has become clear that there has been a massive failure in the compliance system and culture at VW, resulting in damages in excess of €25 billion (as of December 2017).

Truck cartel

Four European manufacturers of trucks, DAF, Daimler, Iveco/Fiat and Volvo/Renault, were fined by the European Commission in the summer of 2016 for unlawful collusion on prices and had to pay nearly €3 billion, most of them by Daimler (nearly €1 billion). Regarding other truck manufacturers, Scania has not accepted its fine and MAN remained unpunished as crown witness. First civil lawsuits have been filed by customers for damage compensation in excess of €120 million. The manufacturers had unlawfully agreed on prices for more than a decade, which can be regarded as an example of inappropriate risk preventive measures and a serious lack in compliance culture.

Corruptibility of a public official

One example of how severe personal consequences of violations of anti-corruption laws may be in Germany is a criminal ruling of February 2017 in Düsseldorf: the former head of the North-Rhine Westphalia state-owned BLB construction service company used his

official powers to artificially increase prices for the construction of public buildings in order to enrich himself. He was sentenced to seven and a half years' imprisonment for corruptibility and infidelity. Even if the conviction might be lowered by a higher court, the ruling demonstrates the willingness of the courts to answer non-compliance with high penalties.

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

Typically, the laws regarding risk management and compliance (including those imposing obligations that lead to the de facto obligation to implement such risk management tools) do not distinguish between private or governmental owned enterprises. For example, the key legal provision regarding the violation of obligatory supervision in operations and enterprises, section 130(1) German Act on Regulatory Offences, expressly states that 'an operation or undertaking within the meaning of section 130(1) shall include a public enterprise.'

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

The range of sanctions for criminal offences committed by public officials is slightly increased, for instance in the area of bribery.

Another difference is that rather specific rules exist at federal, state and municipal level regarding the prevention of corruption and the reaction to violations of anti-corruption laws by public officials. For example, the federal government published its 'Directive concerning the Prevention of Corruption in the Federal Administration'. It addresses the key aspects of a preventive strategy, such as identifying administrative activities especially vulnerable to corruption, raising awareness among officials and creating principles for awarding contracts. Pursuant to a respective circular, rewards or gifts must not be accepted. There may be an exception for gifts of a maximum value of €25. However, in this case the recipient is obliged to notify the employer. Another regulation addresses sponsoring and donations.

ROTTHEGE | WASSERMANN

Barnim von den Steinen **b.vondensteinen@rotthege.com**

Graf-Adolf-Platz 15
40213 Düsseldorf
Germany

Tel: +49 211 955991 15
Fax: +49 211 955991 29
www.rotthege.com

Greece

Vicky Athanassoglou
VAP Law Offices

1 What legal role does corporate risk and compliance management play in your jurisdiction?

The focus of the EU on the subject of corporate governance in the past few decades has resulted in the development of some ground rules regarding the Greek corporate environment. More specifically, in early 2000, a series of best practice principles based on recommendations from the Organisation for Economic Cooperation and Development were issued by the Hellenic Capital Markets Committee, and from that point on pieces of legislation regarding corporate governance and risk management began to be adopted gradually, as mentioned below. Nevertheless, it seems that there is no legal role for corporate risk and compliance management defined under the Greek legal framework. Following the world financial crisis in 2008, and as a result of the Greek recession, Greek enterprises prove willing to incorporate in their structure best practices regarding risk and compliance management functions and thus, for this purpose, new pieces of legislation have already been adopted in the form of the incorporation of EU directives and sound amendments to the existing legislation.

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

The main pieces of legislation set out below are considered to be of the highest priority for Greek undertakings:

- Law No. 3016/2002 On Corporate Governance, Remuneration and Other Issues as amended in force, providing the minimum corporate governance requirements for listed companies;
- Law No. 2190/1920 On Public Limited Companies applies to both non-listed and listed public limited liability companies (under the corporate form of a societe anonyme (SA)), setting rules for the general meeting, the roles of the board of directors, relationships between members of the board of directors and the company, rights of minority shareholders, etc;
- Law No. 4490/2017 On the Statutory Audit of the Annual and Consolidated Financial Statements, Public Oversight of the Audit Work is referred to by every undertaking that is obliged to keep financial statements;
- specific legislation containing risk and compliance obligations applies to credit institutions (Law No. 4261/2014) and insurance undertakings (Law No. 4364/2016); and
- for listed companies, apart from the obligations imposed by the above discussed legislation, a set of basic principles and best practices has been introduced by the Hellenic Governance Code For Listed Companies, published in October 2013, by the Hellenic Corporate Governance Council.

Further to the above, the following lists the most important areas related to compliance and risk management applied to and concerning all of the previously mentioned undertakings but mainly the credit institutions and, where relevant, the financial institutions too:

- supervisory framework for credit institutions: Law No. 4261/2014 (as mentioned above), Decision of the Governor of the Bank of Greece No. 2577/2006, Law No. 3746/2009 On the Insurance of Investment and Deposits Fund;
- protection of bank secrecy and confidentiality: Legislative Decree 1059/1971, as applicable, on the protection of bank deposits;
- protection of market abuse: Law No. 3340/2005, as applicable, on insider dealing and market manipulation, in combination with Law No. 4443/2016 on market abuse regulation transposing Regulation (EU) No. 596/2014 and several guidelines of the Hellenic Capital Market Commission;
- markets in financial instruments and transparency (covering areas of investor protection – Markets in Financial Instruments Directive (MiFID) and Inside Trading): Law No. 3606/2007, as amended by Law No. 4514/2018 transposing the MiFID II directive, regarding markets in financial instruments and Law No. 3556/2007, as applicable, on transparency regarding issuers whose shares are admitted to an organised financial market;
- money laundering: Law No. 3691/2008, as applicable on the prevention and suppression of legalising income from criminal activities and financing of terrorist activities, was amended by Law No. 3932/2011, under which the Anti-Money Laundering, Counter-Terrorist Financing Commission was renamed as the Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority. According to this law, as amended by Law No. 4389/2016, the said national authority aims to combat the legalisation of proceeds from criminal activities and terrorist financing, assisting in security and sustainability of fiscal and financing stability by collecting, investigating and analysing any suspicious transactions forwarded to it by legal undertakings and natural persons, under special obligation, together with any other information as regards the relevant crimes. In addition, Banking and Credit Committee Decision No. 281/2009 on the supervision of credit institutions by the Bank of Greece regarding legalisation of income from criminal activities and financing of terrorist activities is also applicable;
- combat against bribery: Law No. 2656/1998, as applicable, on the ratification of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions; and OECD Guidelines (2011) on responsible behaviour of multinational companies globally;
- data protection: Law No. 2472/1997, as applicable, on the protection of natural persons with regard to the processing of personal data; Law No. 3471/2006, as applicable, on data protection in electronic communications: Decisions by the Data Protection Authority; and of course the new law implementing the EU General Data Protection Regulation (GDPR) 2016/679, which is due to be issued in May 2018;
- consumer protection: Law No. 2251/1994, as applicable, on consumer protection; Law No. 3862/2010, as applicable, on payment services in the internal market; Decision of the Governor of the Bank of Greece No. 2501/2002 on the informing of interested parties regarding credit transactions and relevant contract terms; and
- protection of competition: Law No. 3959/2011, as applicable, on the protection of free competition.

Moreover, for undertakings active in financial markets (namely collective investment undertakings and portfolio investment companies), Decision 3/645/30.4.2013, as amended by Decision 10/773/20.12.16, of the Hellenic Capital Market Commission contains detailed provisions regarding risk measurement and prediction of risk exposure and risk for the contracting party.

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

As stated in article 1 of the above-mentioned Law No. 3016/2002, provisions regarding corporate governance in general, and thus, also including types of risk and compliance management, apply to companies in the legal form of an SA (defined and organised by Law No. 2190/1920) which, additionally, are admitted in a regulated financial market (listed companies).

In addition, for specific categories of undertakings, such as financial and credit institutions and insurance undertakings, particular pieces of legislation apply, imposing tailored obligations on them. Specifically, for credit institutions, Law No. 4261/2014, transposing EU Directive 2013/36, includes a set of corporate governance as well as specified risk management provisions. Moreover, for insurance undertakings, Law No. 4364/2016, transposing Directive 2009/138, introduces detailed provisions on governance systems and risk management.

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

The supervisory body for listed companies is the Hellenic Capital Market Commission. It is responsible for monitoring the compliance of listed companies with the provisions of Law No. 3016/2002 and Law No. 4449/2017 on corporate governance and obligatory audits. That said, Decision 5/204/14.11.2000 of the Commission refers to detailed obligations of listed companies regarding the subjects of internal organisation regulation and audit. Non-compliance with the above-mentioned issues results in administrative fines being imposed by the Commission.

By the same token, the Hellenic Competition Commission has broad enforcement powers in the area of collusive practices, abuses of dominance and merger control. This body is empowered to take decisions on finding an infringement of the Competition Act and to impose administrative fines. It also forms a policy for combating anti-trust behaviour, competition distortion, etc, through its reports and opinions.

Moreover, according to the Articles of Association of The Bank of Greece (as applies, after the last amendment by Law No. 4099/2012), the latter is entrusted with the overall monitoring of the financial and insurance sectors as well as of other types of undertakings. In this regard, it is competent for the review of certain procedures regarding risk management (eg, annual review of the cash flow plans of credit institutions according to Law No. 4261/2014) and for the imposing of administrative sanctions according to the relevant legislation. Furthermore, in a transnational context, the European Central Bank through the Single Supervisory Mechanism, is in charge of supervising the systemically significant credit and financial institutions. Moreover, the Bank of Greece is responsible for specifying the recommendations and guidelines conducted by the Committee of European Banking Supervisors and hereafter the European Banking Authority.

Special reference has to be made to the Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority. This authority has been restructured into three individual units: the Financial Intelligence Unit, the Financial Sanctions Unit and the Source of Funds Investigation Unit. The president is an acting Public Prosecutor to the Supreme Court appointed by a Decision of the Supreme Judicial Council, and serves on a full-time basis.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

In the Greek legislation concerning listed companies, there is no definition of the terms 'risk management' and 'compliance management'. However, the results to be attained by the establishment of such systems are indeed described in legislation. For instance, according to Law No. 3016/2002, the audit committee is responsible, among other things, for the monitoring of the internal organisation regulation and the Articles of Association of the company, as well as for the company's compliance with the applicable legislation. Additionally, according to Law No. 4364/2016 for insurance undertakings, the risk management systems in place shall include the strategies and policies suitable for the identification, measurement, monitoring, management and reporting of the risks faced by the company, in an individual or collective manner, along with any interdependencies connected to them.

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

The national legal framework provides a sufficient description of the process followed for risk and management compliance. Specifically in the separate pieces of legislation listed above, the regulatory and supervising bodies shall follow the exact processes to meet their target and achieve their goal.

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

For listed companies, apart from the obligations imposed by the above discussed legislation, a set of basic principles and best practices has been introduced by the Hellenic Governance Code For Listed Companies, published in October 2013 by the Hellenic Corporate Governance Council. The aim of the Code is to enlighten the members of the board of directors of listed companies regarding corporate governance areas that are not covered by legislation, and thus to provide a complete best practices approach.

In general, the standards introduced by the Code are divided into the general principles addressed to all SA companies and the special practices to be applied only by listed companies. Especially for the latter, some of the additional requirements to those of legislation are: the obligation to disclose a statement for the identification of the core risks faced by the company, as well as the main features of the internal control system applied and the adoption of detailed policies regarding conflicts of interest of members of the board of directors.

As for the context, the Code contains four sections, each covering the following areas: the board and its members; internal control; remuneration; and relations with shareholders.

Furthermore, according to the Decision of the Governor of the Bank of Greece No. 2577/2006 concerning credit and financial institutions, these undertakings are obligated to abide by the standards of an efficient organisational structure, and have a sufficient internal audit system with primary focus on the functions of internal review, risk management and regulatory compliance.

Instruction No. 51/13.03.2013 of the Hellenic Capital Market Commission is considered to be a reference point with regard to compliance management for companies providing investment services. The said Instruction contains clarifications about transposing European Securities and Markets Authority guidelines of 6 July 2012 (ESMA/2012/388) into the Commission's supervisory practice. These guidelines are based on two main axes: the competences of regulatory compliance function (risk assessment, supervisory programme, reports submission, etc) as well as the organisational requirements of the regulatory compliance function (efficiency, independency, permanency of the function, etc).

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

According to Law No. 4449/2017 and Act No. 2577/9.3.2006 of the Governor of the Bank of Greece, compliance and risk management apply to undertakings having their registered seat and operating in Greece.

Specifically, Law No. 4449/2017 is applicable to companies that have their shares listed in a regulated financial market in Greece and that are additionally governed by Greek law or the laws of any EU member state.

Regarding credit institutions, according to Act No. 2577/9.3.2006 of the Governor of the Bank of Greece, branches of foreign credit institutions are obligated to disclose to the Bank of Greece the internal audit processes adopted, as well as the results from the audit performed by the home state supervising authority and the external auditors concerning the branch activities with regard to the related provisions (namely prevention and suspension of money laundering, processes aiming to the transparency of transactions and sufficient informing of the interested parties and any other obligation applicable to undertakings under the legislation of the host country).

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

Listed Companies

Law No. 3016/2002 on corporate governance introduced the obligation for participation in the board of directors of non-executive and independent non-executive directors, with certain criteria determining when independence is indeed secured (article 4). Additionally, listed companies became obligated to set an internal audit function characterised by autonomy from the other functions of the company and monitored by non-executive members of the board of directors, without any member of the board of directors to be allowed to also be a member of the audit function. Duties of the audit function include the monitoring of the corporate and legal obligations of the company and referral to the board of directors of cases of interest collision. With regards to consequences of non-conformity with the said provisions, Law No. 3016/2002 provides for an administrative fine issued by the Hellenic Capital Market Commission.

In principle, Law No. 2190/1920, on public limited companies, as in force and amended by Law No. 3873/2010 and Law No. 3884/2010, provides the legal framework for risk and compliance management on listed and non-listed companies, limited by shares. Law No. 3884/2010 focuses on shareholders' rights and additional corporate obligations regarding shareholders' information in the context of general meeting preparation, while Law No. 3873/2010 provides for the drafting and disclosure of a corporate governance statement for all listed companies.

According to Law No. 2190/1920, the members of the board of directors are responsible for fulfilling the scope of company's management and in general the corporate object. They are also entrusted with the duties provided, namely, duty of loyalty, duty of care, obligation for a non-competitive conduct, etc. Furthermore, they are required to disclose and publish the annual financial statement, the annual management report and the corporate governance statement, where applicable (article 22a). The said obligation, in combination with the one that calls for carrying out an internal audit, is of utmost importance for the purposes of the regulatory provisions in force. Reference should be made to the audit carried out in terms of the law, the statute and the decisions of the general meeting (articles 39a, 40 and 40a). The annual management report (article 43a, 43b) should comply with the obligations of risk management and of the battle against corruption and bribery.

According to article 7a, the appointment and the cessation for any reason whatsoever of the following persons are subject to publication: namely, the persons who carry out the management of the company or have the power to represent the company jointly or individually, or are competent to carry out regular audits.

Further to the above, the Articles of Association may specify the matters in respect of which the power of the board of directors is exercised in whole or in part by one or more members thereof, company directors or third parties, as stipulated in article 22. It may also authorise or require the board of directors to entrust the internal audit of the company to one or more members or third parties, without prejudice to other provision of the law. Such persons may authorise other members or third parties to exercise the powers conferred on them. Thus, related to article 22a, every member of the board of directors shall be responsible to the company for any fault committed during their management of the company's affairs. They shall be responsible for any omissions or false entries in the balance sheet concealing the actual position of the company. The annual management report and the corporate governance statement, where applicable, shall be drawn up and are also subject to this kind of obligation to be published.

The content and the information of an annual management report is specified according to article 43a, and may differ depending on the size of the company and depending on whether the company under consideration is a subsidiary of another company that requires a consolidated management report or a separate report. It is further clarified that the provisions for the corporate governance statement under article 43bb regarding, specifically SAs with transferable securities admitted to trading on a regulated market, specifies the content of the corporate governance statement that must be incorporated in the management report of said companies. The content of the corporate governance statement also differs depending on the size of the company.

The duties of board of directors members follow in exactly the same vein, providing that they shall keep absolute secrecy on confidential matters of the company, while refraining from any action pursuing their own interests contrary to the company's interests. They are also required to disclose to the other members of the board of directors their own interests, which may arise from company's transactions falling within their duties.

Furthermore, the company must disclose its remuneration policy, making it available on its website and also including it in the corporate governance statement. Any remuneration paid out of the profits to a member of the board of directors shall be taken out of the balance of the net profits after the deduction of amounts set aside as regular reserves, and of the amount required for the distribution to the shareholders. Any other remuneration or compensation not specified by the Articles of Association, for any reason whatsoever, shall be deemed to be chargeable to the company only if approved by special resolution of the general meeting. The said obligation is enforced by the existence of a Remuneration Committee provided in Law No. 3016/2002 as mentioned above.

There is also a significant obligation for members of the board of directors regarding shareholder information. To be more specific, members of the board of directors should provide the general meeting with extensive information for the election of a candidate to the board of directors with regard to the reasons justifying the nomination, a detailed curriculum vitae (including information on the current activity of the candidate, their participation on other boards of directors and other positions, distinguishing between the positions they hold in companies belonging to the same group and positions they hold in companies outside the group, etc) and the criteria to determine whether the candidate is in a conflict of interest (indicating in particular any relationship between the company in which the candidate works or is mainly employed and the company for whose board they are a candidate). This duty also refers to the obligatory information processes that have to be applied before a general meeting takes place, regarding shareholders' rights. Besides this, pursuant to article 39, rights of minority interest matter greatly.

It has also to be pointed out that the law in question specifies the definition of an affiliated company, something really important for the identification of an independent non-executive member of the board of directors, according to Law No. 3016/2002.

Greek public limited companies (as well as branches and agencies of foreign public limited companies) are audited in respect of drawing up the balance sheet, the financial administration and general operations. Furthermore, the Minister of Commerce may, whenever they deem it necessary, carry out such inspections through the appropriate employees of the Ministry or through the inspectors of public limited companies.

Credit and insurance undertakings

As stated above, Law No. 4261/2014 applicable to credit institutions includes details of corporate governance as well as specified risk management provisions. That said, credit institutions are obligated to establish a sound and efficient corporate governance system that contains a clear organisational structure including efficient division of competences, internal audit systems consisting of appropriate administrative and auditing processes as well as an effective system for the detection, monitoring, management and reporting of risks faced, or possibly faced, by the institution. Moreover, remuneration policies and strategies shall be in line with efficient risk management. The above system shall be appropriate for dealing with the complexity of the risks as well as being suitable for the activities of the institution, and will be closely monitored by the board of directors. Particularly for important credit institutions (as defined in article 68 of Law No. 4261/2014), a risk management committee consisting of non-executive members of the board should be in place, having the obligation to report to the board of directors and to provide assistance throughout risk management.

With regard to insurance undertakings, Law No. 4364/2016 introduces a set of provisions on governance systems and risk management that is very similar to that for credit institutions, as discussed above. As for specific provisions, article 32 of Law No. 4364/2016, among others, provides the minimum of risks targeted by the system. It also foresees that specific risk management policies shall be set out in order to address each one of the risks concerned.

Update and trends

Implementation of MiFID II
Law No. 4514/2018 transposing the MiFID II Directive (2014/65/EU) was published in the Official Gazette in January 2018. As stated in the explanatory memorandum of the new legislation, the purpose of the new legal framework is to establish a stricter context for the operation of activities related to financial instruments. The goal is to achieve greater transparency and security for all interested parties and better coordination of market supervision throughout the EU.

Current issues regarding the GDPR
The new Regulation introduces a common framework of provisions regarding the way personal data of EU citizens are collected, processed, stored, transmitted, utilised and destroyed (either in electronic or physical form) by both private undertakings (irrespective of their size and area of activity) and public sector bodies. The Regulation obliges companies and organisations to reorganise their technical systems through the mapping of procedures related to personal data storage and process. Additionally, the above shall establish appropriate technical mechanisms that will enable them to list and eliminate any possible threats of data leak to malicious users. Undoubtedly some questions regarding the implementation have been raised as some points have not yet been absolutely clarified (eg, any time limitations as regards the storage of personal data, while time pressure is still an issue) and the date set for the final implementation is 25 May 2018.

In conclusion, taking into account how recent the GDPR legislation is and also that there are no guidelines for the proper compliance, the questions raised will be resolved mainly in practice. Undertakings face the inherent risk of high level of fines, which can reach the amount of €20 million or 4 per cent of the annual global turnover (of the group or holding). However, companies and organisations should consider the data protection officer and processor as 'tools', assisting them with their compliance obligations in order to avoid the severe fines that could emerge from data leaks and not as another set of obligations among the numerous already imposed on them.

Social security obligations for shareholders and board of directors members
According to Law No. 4387/2016 regarding the reform of the National Security System, members of the board of directors of an SA with commercial, trading or production scope, who are also holders of at least 3 per cent of the total shares of the company, are obliged to submit financial contributions for social insurance.

Public interest undertakings (listed, insurance, credit and financial undertakings)
Law No. 4449/2017, on the statutory audit of annual and consolidated financial statements, and public oversight of the audit work, is referred to by the undertakings that are obliged to keep financial statements. The audit must be carried out according to the international auditing standards by an auditor, which may be either an auditing accountant or an auditing company. The provisions ensure the objectivity and the independency of the auditor throughout the whole procedure. The auditor conducts an audit report in which they present the conclusions of the audit, having taken into account any reports of third countries' audit work. The audit report must be conducted in writing and must include very specific information and data of the controlling undertaking, as well as the opinion and the conclusions of the auditor, who bears full responsibility for the report. It is worth mentioning that the auditors are also subject to a system of quality assurance (quality control). The competent body for this quality control is the Hellenic Accounting and Auditing Standards Oversight Board.

According to article 44 of the said law, every public interest undertaking has an audit committee, consisting of mainly independent and experienced members. This committee may be either an independent committee or a committee of the board of directors of the controlled undertaking, but the president shall be independent. The committee informs the board of directors about the results of the statutory audit, explains the importance of such an audit and generally monitors the procedure of statutory audit ensuring the procedural integrity. It also monitors the financial informing by submitting recommendations and suggestions, and monitors the efficiency of the internal systems audit as well. The principal regulatory and enforcement bodies for the supervision of compliance with provisions regarding the committee are the Hellenic Capital Market Commission and the Bank of Greece (see question 4).

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

Greek law for an SA (Law No. 2190/1920) foresees, as mentioned above, a broad set of competences for the board of directors and for non-members exercising management duties delegated by the board. In a nutshell, the board is responsible for deciding upon any corporate issue regarding the management of corporate affairs, the company's assets and of course the representation of the company. In that sense, a key obligation of the board is to abide by the duty of loyalty and to always act for the benefit of the company, ensuring that there is no conflict of interests.

Specifically for listed companies, according to Law No. 3016/2002, board members are responsible for aiming at the long-term improvement of the company's value and also for the safeguarding of the general corporate interest. In that sense, the pursuance of personal interests contradicting the ones of the company is not allowed according to the said legislation. The internal audit committee is responsible for monitoring the above issues and non-compliance causes the imposing of administrative sanctions against the board.

Moreover, with regards to public interest entities, mainly listed companies, credit and insurance undertakings, subject to Law No. 4449/2017, the audit committee in place is entrusted with monitoring the quality of the internal audit systems and the risk management systems, subject to the obligations of the board. That said, the board members are subject to administrative sanctions in cases of improper establishment and functioning of the said committee along with the members.

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

Yes, third parties have the right to file a claim for damages against an undertaking according to the laws for civil liability (specifically the provisions for wrongful acts pursuant to the provisions of the Greek Civil Code), in cases where non-compliance of the said undertaking with the applicable legislation has caused damages to the party concerned.

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

In the case of sector-regulated enterprises, namely credit institutions and insurance companies, the special legislation applicable, as discussed above, provides for specific administrative and regulatory sanctions for the undertakings' non-adherence to risk and compliance obligations. That said, for credit institutions, non-operation of a corporate governance system, containing efficient risk management among others, results in a series of severe administrative and regulatory measures and fines imposed by the Bank of Greece (inter alia, dismissal of responsible persons, revocation of the institution's licence, financial fines of up to 10 per cent of the annual finance revenues, etc). Moreover, legislation for insurance institutions (namely, article 256 of Law No. 4364/2016) foresees a reprimand or fine of up to €2 million placed upon the undertaking, the members of the management and any other person responsible for non-compliance with it. Lastly, the Hellenic Capital Market Commission and the Bank of Greece are responsible for imposing administrative sanctions on companies active in the financial markets sector.

As far as listed companies are concerned, deficiencies regarding risk and compliance management are not punishable by an administrative sanction, and other regulatory consequences affecting the undertaking as such do not apply. However, board members do face administrative consequences in some areas of corporate governance covered by the above-mentioned legislation (see question 15).

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

No, there is no such provision for criminal liability of legal persons in Greek law. Instead, natural persons are subject to criminal liability (see question 16).

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

Members of the board of directors of an SA are liable against the company for any fault that occurred during the exercise of their competences as managers of the corporate affairs (article 22a of Law No. 2190/1920). However, proving that they have acted as a prudent business person would have excludes the above liability. Additionally, the law was amended in recent years to include cases of non-compliance with board obligations regarding the drafting and disclosure of annual economic statements, the management report and the corporate governance report (in cases that are applicable), according to the applicable laws.

Thus, the company has a right to claim for damages towards the members of the board in cases where their decisions and actions have caused the said damages. With regard to the board's liability against the company creditors, the former are held liable for the damages they have caused by fault to the latter, according to the civil legislation for wrongful acts, as provisions of Law No. 2190/1920 serve the purpose of safeguarding the creditors' interests and thus, non-compliance with them during the exercise of their duties, forms a wrongful act. Lastly, it is of importance to mention that the legal entity of the company is jointly and severally liable along with the board members against its creditors.

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

As discussed in question 10, board members of listed companies face administrative sanctions for non-compliance with the corporate governance obligations of Law No. 3016/2002 and Law No. 4449/2017. The Hellenic Capital Market Commission is responsible for imposing a reprimand or fine ranging from €3,000 to €1 million on the persons performing the duties of board members (members of the audit committee might also be sanctioned according to Law No. 4449/2007), except for credit and insurance companies, for which the Bank of Greece is the supervisory authority (see question 12).

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

According to the Greek legal system, the persons faced with civil liability are those entrusted with the representation of the company as well as with the management of its corporate affairs. Therefore, members of the board of directors of an SA face criminal liability for breach of their legal obligations, according to articles 54-seq of Law No. 2190/1920 (inter alia, submission of false statements regarding the payment of corporate capital and the issuing of shares, omission of the annual balance sheet completion), as well as being accused of committing the crimes of articles 375 (embezzlement) and 390 (infidelity) of the Penal Code. Criminal liability of the responsible persons is also incurred for the breach of tax and social insurance law obligations, as well as for non-compliance with competition law.

With regard to credit institutions, the relevant legislation (article 59 of Law No. 4261/2014) foresees the criminal liability of the board members, the president, the auditors and the responsible directors and employees of the credit institution whose actions have caused (among other things): the omission or forgery of the appropriate listing of an important transaction; the submission of false or inaccurate reports or data to the Bank of Greece; or the obstruction of the company practices review by the Bank of Greece.

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

As discussed above, the Hellenic Corporate Governance Code has been published for listed companies. As regards the implementation of the Code, it is voluntary and based on a 'comply or explain' approach, meaning that in cases where a listed company deviates from the Code standards, it has to provide detailed reasoning regarding such necessity. Additionally, a company has to provide specific information about the alternative measures followed by it in order to tackle the issues for which a deviation from the Code provisions has been chosen. Among other things, risk mitigating actions have to be described in detail and should be in line with the overall principles enshrined in the Code.

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

Novartis

According to the testimonial evidence of the protected witnesses, it is alleged that the multinational pharmaceutical company Novartis has applied a system of bribery of doctors and officials to promote the use of Novartis medicines by patients, thereby multiplying company profits and succeeding over other competition in the pharmaceutical market. It is also presumed that Greek politicians may be involved in this case. In addition, this bribery is alleged to have involved illegal exports of pharmaceuticals in consultation with doctors and pharmaceutical

VAP LAW OFFICES

ATHENS | DÜSSELDORF

Vicky Athanassoglou **va@vaplaw.eu**

4 Karagiorgi Servias Street
105 62 Athens
Greece

Tel: +30 210 32 54 237
Fax: +30 210 32 54 237
www.vaplaw.eu

warehouses. It is considered to be a crucial case as Greece is a reference country for drug pricing in 29 countries around the world.

This case is still pending, but was selected to be analysed because it constitutes a matter of particular concern to Greek society. What precedes is more of a news and current affairs circumstantial recording rather than unassailable proof of what has taken place.

Fines to construction companies

Another representative example derives from a ruling of the Hellenic Competition Commission, based on Greek antitrust law, that had a severe impact on the earnings of companies involved. Its judgment on the case found that 15 major Greek construction companies had formed a trust against public construction competition. The fines incurred following the 626/2016 judgment of the Commission were approximately €80 million, which were the highest fines among similar cases within the EU. Considering that the combined earnings of the four major companies for 2016 were €2.4 million after provisions of approximately €79 million were realised for the above fine, it is evident that its impact on their viability was crucial.

Siemens

A typical example involving bribing of public officials is the well-known *Siemens* case that was revealed in 2008 in Greece. According to the given facts, a series of bribes were paid to a number of public officials and politicians concerning the purchase from the Hellenic Telecommunication Company of several telecommunication systems and security systems used by the Greek authorities to ensure public safety during the Olympic Games held in Athens in 2004. The case is under scrutiny by the Greek judiciary system.

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

As discussed above, the Greek legal framework, in which risk and compliance management provisions are included, addresses companies of the legal form of an SA. Additionally, the obligations imposed on the undertakings differ according to their form as listed or non-listed. Additionally, as already noted, there is specific regulation of certain types of activities of companies, such as credit and insurance providing. That said, whether the ownership of the undertaking is private or public does not play a role in defining the obligations concerned.

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

One of the key differences between the private and public sectors is that for the latter there is a special supervisory framework. Specifically, for public administrative entities, the General Inspector of Public Administration, appointed by the government for a specified period of time, is the authority responsible for ensuring the efficient and effective functioning of public administration, the monitoring of its performance and the detection of any corruption and maladministration phenomena. Some of the main competences of the said authority are the conducting of all kinds of inspections, post-inspections and investigations in the civil service and the public sector, including public enterprises and other state-controlled enterprises, and the conducting of annual auditing of the financial statements of the inspecting and controlling bodies of public administration and other categories of civil servants.

India

Junia Sebastian, Arindam Basu and Richika LRS
ALMT Legal

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Although, at present, India as a country is still awaiting comprehensive legal guidelines with respect to corporate risk and compliance management, in recent times, compliance with labour, industrial, financial and corporate laws has gathered enormous momentum within the corporate sector.

Labour compliance

India being a country with a significant labour force, one of the major challenges of any company in the corporate sector is with respect to labour compliance. As labour law is considered a 'specialised area', non-compliance of labour laws carries with it considerable legal implications and risks.

To keep up with the emerging needs with regard to corporate risk and compliance management, companies in India need to establish effective contract management with their employees and any other related third parties as per the provisions of the Indian Contracts Act 1872.

Another integral part of corporate risk and compliance management in India that has recently emerged is the aspect of pre-emptive screening of employees. There are no dedicated laws governing the pre-emptive screening of employees in India, hence, there are no legal requirements for conducting background checks on prospective employees, except in certain cases such as banks, schools, etc, under certain notifications by various state governments within the country.

Financial compliance

In the wake of the *Satyam* scandal (a high-profile corporate scandal affecting India-based company Satyam Computer Services in 2009 wherein the chairman, Mr Ramalinga Raju, confessed to having manipulated the accounts to the tune of 70 billion rupees) along with the collapse of some of the largest companies in the world, India has brought in stringent financial compliance that is to be strictly adhered to by every company. It is a well-known fact that India as a country has a complex and bureaucratic accounting, tax and regulatory system, which makes it an onerous challenge for all companies to remain compliant with each and every financial compliance required by the applicable laws. However, the government has from time to time relaxed many such regulations for ease of business and attracting foreign investments. For example, the Goods and Services Tax regime was introduced in India on 1 July 2017 by subsuming dozens of state and central indirect taxes to transform India into a single market and thus promote the ease of doing business in India.

Corporate compliance

Besides compliance with labour and financial laws, companies are also required to strictly adhere to all corporate compliance as per various other laws including, but not limited to, the Companies Act 2013, Reserve Bank of India guidelines, the Foreign Exchange Management Act 1999, the Securities and the Exchange Board of India Act 1992. However, the government has deregulated and relaxed various laws for ease of business and promoting foreign investment in India. For example, foreign direct investment in 'single brand retail trading' has recently been allowed up to 100 per cent under the automatic route.

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

Keeping in mind the plethora of laws with regard to labour, financial and corporate laws in India, which a company is required to be compliant with, below are certain laws and regulations that we believe are required to be complied with on the highest priority with respect to each sector.

Labour law

There are specific central acts that are required to be strictly adhered to by a company, which are mentioned below, but are not limited to:

- the Industrial Disputes Act 1947;
- the Employees State Insurance Act 1948;
- the Employees' Provident Funds and Miscellaneous Provisions Act 1952;
- the Payment of Bonus Act 1965;
- the Factories Act 1948;
- the Contract Labour (Regulation and Abolition) Act 1970;
- the Child Labour (Prohibition and Regulation) Act 1986;
- the Maternity Benefit Act 1961;
- the Payment of Gratuity Act 1972; and
- the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act 2013.

As well as the abovementioned acts, there are certain state-specific acts that are required to be adhered to by companies, such as the Professional Tax Act and the Shops and Establishment Act that are applicable to a particular state.

Financial and corporate compliance

When it comes to corporate and financial compliance, both compliance and risk management go hand in hand. Below are some of the specific regulations that are to be adhered to at the highest priority:

- the Companies Act 2013;
- the Income Tax Act 1961;
- the Reserve Bank of India and its subsequent guidelines;
- the Banking Regulation Act 1949;
- the Foreign Exchange Management Act 1999;
- the Securities and Exchange Board of India 1992 and its subsequent guidelines; and
- the Goods and Services Tax Act 2017.

The Competition Act 2002 also lays down several provisions to promote fair competition in the market and mitigate business-related risks, though its applicability is dependent upon certain thresholds, which are enumerated under this legislation.

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

Risk and compliance management is significantly dependent on various factors of a business such as the sector, size, scale, nature of the business and the activities being carried out. Any legal person or entity who indulges in any kind of commercial activities will have to adhere to the rules of risk and compliance management, as may be applicable. A good corporate governance policy is a commitment by an organisation to adopt various good ethical practices and values and this should

necessarily encompass the entire value chain of stakeholders, namely, shareholders, management, employees, bankers, customers, vendors and regulators.

Thus, all persons, organisations and undertakings are targeted at varying degrees by the rules of risk and compliance management.

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

The Indian legal system recognises sector-specific regulatory and enforcement agencies and bodies that are responsible for corporate compliance in a particular sector. The government of India has enacted various acts, and inter alia created various statutory bodies to regulate and implement the provisions specified therein. The following are a few examples of the principal regulatory and enforcement bodies in India with responsibility for corporate compliance:

- The Registrar of Companies (ROC) is the designated authority that deals with the administration of the Companies Act 2013, and falls under the ambit of the Ministry of Corporate Affairs. It is mandatory for companies incorporated under the Companies Act 2013 to file various forms, returns and documents with the ROC with respect to their day-to-day corporate compliance and activities.
- The Reserve Bank of India (RBI) is the central bank of the country and the key authority that lays down the compliance functions for banks throughout India. The RBI, via its notification RBI/2006-2007/335 dated 20 April 2007, has laid down certain mandatory compliance functions including but not limited to strict observance of all statutory provisions contained in various legislations such as Banking Regulation Act 1949, Reserve Bank of India Act 1934, Foreign Exchange Management Act 1999, Prevention of Money Laundering Act 2002, etc, as well as ensuring observance of other regulatory guidelines issued from time to time such as standards and codes prescribed by The Banking Codes and Standards Board of India, Indian Banks Association, Foreign Exchange Dealers Association of India, Fixed Income Money Markets and Derivatives Association, etc, and also each bank's internal policies and fair practices code. The RBI also sets out the rules and regulations for exchange control transactions in India, eg, foreign investment and outbound investment related regulations.
- The Securities and Exchange Board of India (SEBI) promotes and regulates the securities market in India. In order to protect the interests of investors, SEBI has laid down various compliances required to be followed by listed entities. In addition to this, SEBI has directed the stock exchanges to implement various measures to ensure corporate compliances including inter alia setting up of a separate monitoring cell to monitor compliances with the provisions of corporate governance and listing of public issues.
- The Competition Commission of India was established under the Competition Act 2002 to eliminate practices having adverse effect on competition, to promote and sustain competition, and to protect interests of consumers and ensure freedom of trade by other participants.
- The prime objective of the Enforcement Directorate is the enforcement of two key acts of the government of India, namely, the Foreign Exchange Management Act 1999 and the Prevention of Money Laundering Act 2002. The officers of the Directorate perform an adjudication function so as to impose a penalty on persons for the contravention of the said acts.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

The Indian laws have been designed to implement risk and compliance management. While there is no specific law or regulation in India that defines 'risk management' and 'compliance management', the same has been widely recognised under various statutes in the manner that has been described in earlier questions.

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

Yes. As stated above, Indian laws set out various provisions for risk and compliance management. For example, the Companies Act 2013, requires a board of directors to develop and implement a risk management policy and identify risks that may threaten the existence of the company. Further, the Companies Act 2013 has made the requirement of compliance very explicit by stipulating a mandatory requirement of positive affirmation from the directors as part of the directors' responsibility statement under section 134, stating that the directors have devised a proper system to ensure compliance with the applicable laws and that such systems are operating effectively.

It is to be noted that section 205 also requires a company secretary to provide a report to the board about compliance with the provisions of the said act, the rules made thereunder and other laws applicable to the company.

The most significant regulation in this context is Regulation 27(2) of the SEBI Listing Obligation and Disclosure Requirements (LODR) Regulations 2015, which defined significant tighter personal responsibility of top management for the accuracy of reported corporate governance and inter alia stipulates the preparation of a compliance report of all laws applicable to a company and the review of the same by the board of directors periodically, as well as to take steps by the company to rectify instances of non-compliance and to send reports on compliance to the stock exchanges quarterly. The stock exchanges have been directed by SEBI to set up a separate monitoring cell with identified personnel to monitor compliance with the provisions of the revised Regulation 27(2) of SEBI (LODR) 2015 on corporate governance and to submit a consolidated compliance report to SEBI within 15 days from the end of each quarter.

As per LODR, read with section 134(5)(f) of the Companies Act 2013, the relevant provisions mandate the present corporate bodies to incorporate and implement a legal compliance management system:

- Regulation 4(1) of LODR requires that the listed entity shall abide by all the provisions of the applicable laws and other guidelines;
- Regulation 4(2)(f) of LODR directs that the board of directors of the listed entity shall ensure that a system for compliance with the law and relevant standards are in place; and
- Regulation 17(3) of LODR provides that the board of directors shall periodically review compliance reports pertaining to all laws applicable to the listed entity, prepared by the listed entity, as well as steps taken by the listed entity to rectify instances of non-compliance.

There are a number of other acts and regulations besides the SEBI guidelines such as the Information Technology Act 2000, Companies Act 2013, etc, that mandate the corporate bodies both in public and private sectors to maintain and conduct a periodic review of the regulatory functions and processes of the organisations to ensure that the company's goal, structure and ongoing operations are consistent with the latest developments in business and corporate laws and regulations. This then lowers the compliance risk profile, reduces fines, reassigns headcounts, enables a better and higher use of the limited law department's resources, saves measurable costs and improves effectiveness and ensures due diligence.

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

There are no specific standards or guidelines regarding risk and compliance management processes in India. However, the same has been laid down in various forms of law and regulation. For example, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 state that companies must have 'reasonable security practices and procedures' and that companies are deemed in compliance if they have a documented security programme with managerial, technical, organisational and physical controls. ISO 27001 is provided as a reference standard.

The basic guidelines for risk and compliance management processes are:

- reporting: the reports from management to the board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing the risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, or may have, on the company and the actions being taken to rectify them; and
- roles and responsibilities: all employees have some responsibility for internal control as part of their accountability for achieving

objectives. The employees collectively should have the necessary knowledge, skills, information and authority to establish, operate and monitor the system of internal control.

A strong risk and compliance management system framework can mitigate risks if it can:
- identify the risk inherent in achieving goals and objectives;
- establish risk appetite across the entire risk spectrum;
- establish and communicate risk management frameworks;
- build accurate and consistent risk assessment;
- establish and implement measurement reporting standards and methodologies;
- build a risk profile;
- establish the key control processes, practices and reporting requirements;
- monitor the effectiveness of control;
- ensure all the exposures are adequately identified, measured and managed in accordance with board-approved frameworks;
- provide early warning signals;
- ensure risk management practices are adequate and appropriate for managing the risks;
- report areas of stress where crystallisation of risks is imminent;
- present remedial actions to reduce or mitigate such risks;
- report on sensitive and key risk indicators;
- communicate with relevant parties;
- review and challenge all aspects of the company's risk profile;
- advise on optimising and improving the company's risk profile; and
- review and challenge risk management practices.

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

Yes, as explained above, undertakings operating in India are subject to risk and compliance governance obligations. As per section 134(5)(f) under the Companies Act 2013, the directors have to state in the yearly directors' responsibility statement that they have devised proper systems to ensure compliance with the provisions of all applicable laws and that such systems were adequate and operating effectively.

On failure to comply with the above requirement, the company shall be punishable with fines ranging from 50,000 rupees to 2.5 million rupees and every officer of the company who is in default shall be punished with imprisonment for a term of up to three years or with a fine ranging from 50,000 rupees to 500,000 rupees, or with both.

Further, corporate governance lays down the foundation of a properly structured board and strives for a healthy balance between management and ownership that is capable of taking independent decisions for creating long-term trust between the company and external stakeholders of the company. It creates space for open dialogue by incorporating transparency and fair play in strategic operations of the corporate management. The significance of corporate governance lies in:
- accountability of management to shareholders and other stakeholders;
- transparency in basic operations of the company and integrity in financial reports produced by the company;
- checks and balances as an integral part of good corporate governance;
- adherence to the rules of company in law and spirit;
- code of responsibility for directors and employees of the company; and
- open dialogue between management and stakeholders of the company.

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

Key compliances under the Companies Act 2013 are as follows:
- consolidated financial statements are to be prepared where a company has subsidiaries and associates. Intermediary subsidiaries are exempted provided shareholders of the parent have consented to the same;
- uniform financial year has been implemented for all companies as April to March. Specific approvals for deviation can be obtained from the National Company Law Tribunal for certain classes of companies;
- as per section 138 of said Act and Rule 13 of Companies (Accounts) Rules 2014, the following companies are required to appoint an internal auditor in a board meeting:
  - listed companies;
  - a public company with a paid-up share capital of more than 500 million rupees and a turnover of 2 billion rupees, loans and borrowings of more than 1 billion rupees and outstanding deposits of more than 250 million rupees; and
  - a private company with a turnover of 2 billion rupees, loans and borrowings of more than 1 billion rupees;
- the provisions on reporting fraud have been laid down under section 143(12) of the Act and provides that if the auditor of a company, in the course of the performance of their duties as auditor, has reason to believe that an offence involving fraud is being or has been committed against the company by officers or employees of the company, they shall report the matter to the central government;
- as per section 204(1) of said Act, read with Rule 9 of the Companies (Appointment and Remuneration of Managerial Personnel) Rules 2014, the following companies are required to obtain a secretarial audit report:
  - every listed company;
  - every public company having a paid-up share capital of 500 million rupees or more; and
  - every public company having a turnover of 2.55 billion rupees or more.

Key compliances under the Foreign Exchange Management Act 1999:
- a foreign liabilities and assets return is required to be submitted mandatorily by all companies resident in India that have received foreign direct investment or made outward direct investment (ODI) in any of the previous year or years, including the current year; in other words, who holds foreign assets or liabilities in their financial statements as of 31 March; and
- an Indian party or resident individual that has made an ODI has to submit an annual performance report in Form ODI Part II to the authorised dealer bank by 31 December every year in respect of each joint venture or wholly owned subsidiary outside India.

Key compliances under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Data Protection Rules):
- any person or entity that collects, receives, stores, processes or handles personal or sensitive personal information must provide a privacy policy on the company's website that should be accessible to the provider of information;
- the Data Protection Rules mandate companies to obtain express consent from the provider of sensitive personal information regarding the purpose and use of the information. The consent can be obtained through any electronic media;
- the company should ensure that the data providers are made aware of the purpose for which the sensitive personal information is collected, the intended recipients of the information, the agency collecting the information, the agency retaining the information, etc. Further, the data provider should be given an option not to provide the information or to revise or withdraw the information;
- the companies must have 'reasonable security practices and procedures'. The companies are deemed in compliance if they have a documented security programme with managerial, technical, organisational and physical controls. ISO 27001 is provided as a reference standard; and
- all discrepancies or grievances reported to companies must be addressed in a timely manner. Companies must appoint a grievance officer and publish their name and contact details on the company's website. The grievance officer must redress all the data subjects' grievances within one month of receiving the grievance.

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

As per the Companies Act 2013, the board of directors is required to develop and implement a risk management policy and identify risks that may threaten the existence of the company. Further, the Act has

made the requirement of compliance very explicit by stipulating a mandatory requirement of positive affirmation from the directors as part of the directors' responsibility statement under section 134, stating that the directors have devised a proper system to ensure compliance with the applicable laws and that such systems are operating effectively. It is to be noted that section 205 also requires a company secretary to provide a report to the board about compliance with the provisions of the said Act, the rules made thereunder and other laws applicable to the company.

Further, SEBI issued the revised clause 49 that would be applicable to all listed companies with effect from 1 October 2014. The revised clause 49 requires senior management to make disclosures to the board relating to all material financial and commercial transactions where they have personal interest that may have potential conflict with the interest of the company at large. The term 'senior management' shall mean members of the core management team. This will include all members of management one level below the executive directors including all functional heads.

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

Compliance in general means compliance with laws and regulations. These laws and regulations may stipulate penalties for non-compliance of provisions. While there are no direct consequences for deficiencies in risk and compliance management mechanisms, penalties may be imposed if the same results in infringement of the said laws.

Below are a few examples of penalties imposed:

- As per section 88 of the Companies Act 2013, if a company fails to maintain a register of members, the company and every officer of the company in default shall be punishable with a fine ranging from 50,000 rupees to 300,000 rupees. Further, as per section 92 of the Act, if a company fails to file a copy of annual return within the prescribed timeline, the company shall be punishable with a fine ranging from 50,000 rupees to 500,000 rupees.
- Section 13 of the Foreign Exchange Management Act 1999 imposes a penalty on every person who contravenes any provision of this Act, or contravenes any rule, regulation, notification, direction or order issued in exercise of the powers under this Act, or contravenes any condition subject to which an authorisation is issued by the Reserve Bank. The said penalty can equal up to three times the sum involved in such contravention where the amount is quantifiable, or up to 200,000 rupees where the amount is not quantifiable. Where such contravention continues, further penalties can be levied of up to 5,000 rupees for each day after the first day during which the contravention continues.
- Section 21 of the Maternity Benefit Act 1961 states that every employer who does not comply with the provisions of the Act shall be punishable with imprisonment of up to three months, with a fine of up to 500 rupees or with both.
- Section 22A of the Minimum Wages Act 1948 imposes a penalty on every employer who contravenes any provision of this Act or any rule or order made thereunder with a fine of up to 500 rupees.
- Via its circular dated 15 June 2017, SEBI has imposed certain penalties for non-compliance with certain provisions of the SEBI (Issue of Capital and Disclosure Requirements) Regulations 2009, which includes inter alia a penalty of 20,000 rupees a day for delay in completion of bonus issue, until the date of actual compliance.
- Section 43A of the Competition Act 2002 imposes penalties on any person or enterprise who fails to give notice to the commission with respect to forming a combination. The penalty imposed may extend to one per cent of either the total turnover or the assets, whichever is the higher amount.

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

Yes, undertakings do face administrative and regulatory consequences for risk and compliance management deficiencies.

For example, under the Aircraft Rules 1937, powers have been conferred on the central government and the Director General of Civil Aviation (DGCA) to grant various licences, permits, certificates, approvals, etc. At the same time, these rules empower them to suspend, cancel, withdraw or modify them, if the document holder contravenes certain provisions of these rules or does not comply with the directions issued by the DGCA or does not observe the terms and conditions of the relevant document. This can be termed as administrative action.

Further undertakings in India have been governed by various regulators such as the RBI, SEBI, Insurance Regulatory and Development Authority (IRDA), Pension Fund Regulatory and Development Authority, National Bank of Agriculture and Rural Development, Telecom Regulatory Authority of India, etc.

In addition to the penalties imposed by the RBI and SEBI as explained above, please note that section 105B of the IRDA stipulates the penalty for failure of an insurer to undertake life insurance business and general insurance business in the rural or social sector. In such an event, an insurer shall be liable to a penalty of up to 500,000 rupees for each such failure and shall be punishable with imprisonment for up to three years or with a fine for each such failure.

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

Yes, undertakings face criminal liability for risk and compliance management deficiencies in India. The Companies Act 2013 prescribes the penalties for offences committed by companies. Under the Income Tax Act 1961, the Customs Act 1962, the Central Sales Tax 1956 and the Central Excise Act 1944, various tax-related crimes such as tax evasion, smuggling, customs duty evasion, value added tax evasion and tax fraud are prosecuted.

Further, the Environment (Protection) Act 1986 is an act under which the central government is empowered to protect and improve the quality of the environment. A significant statutory rule framed under this Act is the Hazardous Waste (Management and Handling) Rules 1989. It is to be noted that any violation of any rule framed under the provisions of the said Act renders the offender liable for imprisonment for a term of up to five years with a fine, and if the contravention continues beyond a period of one year, the term of imprisonment may be increased by another five years.

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

Yes, the members of governing bodies and senior management face civil liability for breach of risk and compliance management obligations. For example, section 35(1) of the Companies Act 2013 imposes civil liability on every director, promoter or other senior management personnel for any mis-statements in the prospectus.

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

Yes. See question 12.

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

The Companies Act 2013 prescribes punishments for offences committed by companies under the Act. Liability for an offence leads to conviction or punishment by way of imprisonment or fine or both, and the punishment is inflicted on the company, the directors and other officers of the company who were accused and found guilty of the offence by a court.

In most cases, the persons liable for the offences are 'officers who are in default' and the said term is defined exhaustively under the Act. For the purpose of any provision under that Act, an 'officer of the company' means any of the following:

- a whole-time director;
- key managerial personnel, who include:
  - a managing director, or chief executive officer or manager and, in their absence, a whole-time director;
  - the company secretary; and
  - the chief financial officer (CFO);
- where there are no key managerial personnel, such director or directors as are specified by the board on its behalf who have given their consent in writing to the board to such specification, or all of the directors if no director is so specified;

- any person in accordance with whose advice, directions or instructions the board of directors of the company is accustomed to act, other than a person who gives advice to the board in a professional capacity;
- any person who, under the immediate authority of the board or any key managerial personnel, is charged with any responsibility including maintenance, filing or distribution of accounts or records, and who authorises, actively participates in, knowingly permits or knowingly fails to take active steps to prevent, any default;
- in respect of a contravention of any of the provisions of the Act, any director who is aware of a contravention by virtue of receiving any proceedings of the board or participating in such proceedings without India objecting to the same, or where such contravention had taken place with their consent or connivance; and
- in respect of the issue or transfer of any shares of a company, the share transfer agents, registrars and merchant bankers to the issue or transfer.

Section 439 of the Act provides that, notwithstanding anything contained in the Code of Criminal Procedure 1973, every offence under the Act shall be deemed to be non-cognisable within the meaning of the Code of Criminal Procedure and that no court (as defined under the 2013 Act) shall take cognisance of any offence under the Act that is alleged to have been committed by any company or any officer thereof, except on the complaint in writing of the companies registrar, a shareholder of the company or a person authorised by central government.

In *Anath Bandhu Samanta v Corporation of Calcutta* (AIR 1952 Cal 759), the Calcutta High Court held that there is nothing in Indian law that precludes the trial of a company for an offence except where it was physically impossible for the company to have committed the offence in question; mens rea is essential. Furthermore, if the only punishment for the offence in question is imprisonment, a company can be tried for that offence and, if found guilty, punished by imposing a suitable fine.

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

There is no such defence for corporate compliance under the Indian laws. Every undertaking needs to comply with applicable laws. As is the case under common law principles, ignorance of law is no justification for non-compliance and corporate entities and their management bodies are required to be aware of the various compliances demanded of them.

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

The Satyam case

The fraud committed by Ramalinga Raju and Satyam Computers is the biggest corporate fraud in India and it is also an example of failure of corporate governance. On 24 June 1987, Satyam Computer Services Ltd (popularly known as Satyam) was incorporated by the two brothers, B. Rama Raju and B. Ramalinga Raju, as a private limited company with just 20 employees for providing software development and consultancy services to large corporations (the company went public in 1991). In 1996, the company promoted three more subsidiaries including Satyam Renaissance Consulting Ltd, Satyam Enterprise Solutions Pvt Ltd and Satyam Infoway Pvt Ltd. In 2001, Satyam became the world's first ISO 9001:2000 company certified by Bureau Veritas Quality International. In 2003, Satyam started providing IT services to World Bank and signed a long-term contract with them. In 2005, Satyam was ranked third in the Corporate Governance Survey by Global Institutional Investors.

Suddenly, on 7 January 2009, B. Ramalinga Raju confessed to more than 78 billion rupees worth of financial fraud and he resigned as chairman of Satyam. His emotionally charged four and half page letter of startling revelations shook the entire corporate world when he admitted to cooking the accounts and inflating the figures by 50.4 billion rupees. He committed this fraud and tried to hush it up through an abortive bid to purchase Maytas Infra, a company he had created and that was run by his son Teja Raju. A week after his scandalous confession, Satyam's auditors Price Waterhouse finally admitted that its audit report was wrong as it was based on incorrect financial statements provided by Satyam's management. On 22 January 2009, Satyam's CFO Srinivas Vadlamani confessed to having inflated the number of employees by 10,000. He told Criminal Investigation Department officials interrogating him that this helped in drawing approximately 200 million rupees per month from the related but fictitious salary accounts. Satyam had inflated the revenue of the company by infusing false and fictitious sales invoices and shown the amount received and deposited as fixed deposits in various scheduled banks.

Update and trends

The Companies Act 2013 has put a greater emphasis on corporate governance measures through the different provisions that are incorporated within it.

The Sahara case

The Sahara Group was accused of failing to refund over 200 billion rupees to its more than 30 million small investors that it had collected through two unlisted companies of Sahara. In 2011, SEBI ordered Sahara to refund this amount with interest to the investors, as the issue was not in compliance with the requirements applicable to the public offerings of securities. Later in 2014, Mr Subrata Roy, the chairman of Sahara was arrested for the said fraud. His proposal to settle the matter was rejected by the court and SEBI.

Punjab National Bank (PNB) fraud case

India's second largest state-owned lender Punjab National Bank (PNB) disclosed on 14 February 2018 that it was the victim of the country's largest bank fraud. PNB revealed that fraudulent transactions by billionaire jeweller Nirav Modi and related entities (ie, M/s Diamonds R Us, M/s Solar Exports and M/s Stellar Diamonds) amounted to US$1.77 billion or over 110 billion rupees.

In a complaint to the Central Bureau of Investigation, PNB said that Modi and the companies linked to him colluded with its officials to get guarantees or letters of undertaking to help fund buyer's credit from other overseas banks. PNB alleged that the funds, ostensibly raised for the purchase and sale of diamonds, were not used for that purpose. Later, it was revealed that the fraud extended past PNB to other lenders such as State Bank of India, Union Bank, Axis Bank Ltd and Allahabad Bank, all of whom had exposure to the case. The preliminary investigations showed two officials of the bank had fraudulently issued letters of undertaking to the said firms without following the due process. These fraudulent letters of undertaking were then transmitted across the Society for Worldwide Interbank Financial Telecommunications (SWIFT) messaging system, and based on these, credit was offered to the said firms.

This case is the most recent classic example of risk and compliance management failure by PNB and several bankers wonder how the delinking of SWIFT from Core Banking Solution could have been achieved without it being detected by the bank's information technology department. This suggests a possible breach of the security system (eg, passwords and authentication) and the fact that the approval for issuance of letters of undertaking was forged for such huge amounts without it being captured in the system or red-flagged, indicates a major failure of the internal control systems of PNB.

In light of the above, it is pertinent to note that a company's system of internal control reflects its control environment and should be capable of responding quickly to evolving risks to the business arising from factors within the company and to changes in the business environment. Internal controls are the core of a company's corporate governance practice and the main means of controlling, offsetting and mitigating most types of risk, especially those associated with reckless and fraudulent financial decisions.

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

Yes, there are risk and compliance management obligations for government, government agencies and state-owned enterprises. The Department of Public Enterprises (DPE) has issued mandatory governance guidelines to Central Public Sector enterprises and state-owned enterprises.

For example, the DPE requires Central Public Sector enterprises to submit quarterly progress reports with regard to compliance of corporate governance guidelines. Further, the guidelines also require the Administrative Ministries to consolidate the information received from such enterprises and submit a comprehensive report on the status of compliance of corporate governance guidelines to the DPE.

In addition to the above, the DPE also provides for certain other policies to regulate risk and compliance management that include but are not limited to personnel policies, vigilance policies, financial policies, corporate social responsibility, etc.

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

The introduction of the Companies Act 2013 has imposed certain additional compliance requirements mandated for private companies that, until then, were mandated only for public companies and private companies that are subsidiaries of public companies. These include the following:

- appointment of director to be voted individually;
- option to adopt principle of proportional representation for appointment of directors; and
- the provisions pertaining to the ineligibility for appointment of director are also extended to cover appointment or reappointment of a director in a private limited company.

Certain provisions of clause 49 of the Listing Agreement are very specific with regard to risk and compliance management obligations for public companies. Clause 49 I(D) of the Listing Agreement with the stock exchanges requires companies to institute a code of ethics for the board and senior management and affirm compliance to the same on an annual basis. Although institution of the whistle-blower mechanism is not mandatory at present, clause 49 II(D) requires an audit committee to review procedures for the receipt, retention and treatment of complaints (including confidential and anonymous submissions by employees) received regarding accounting, internal accounting controls or auditing matters, providing for adequate safeguards against victimisation of employees who avail of the mechanism and also provide for direct access to the chairman of the audit committee in exceptional cases. The stock exchanges' corporate governance listing standards require listed companies to incorporate the code of ethics for directors and senior management and public disclosure of the code on the company's website. The guidelines changed focus away from compliance toward a broader assessment of corporate efforts to create an ethical and organisational culture.

Schedule IV, read with section 149(8) of the Companies Act 2013, lays down the code for professional conduct for independent directors. The duties of an independent director elaborated in Part III of Schedule IV include ascertaining and ensuring that the company has an adequate and functional vigil mechanism and that the interests of the persons using it are not harmed. The independent directors are also entrusted with the task of reporting concerns over unethical behaviour, actual or suspected fraud or violation of the company's code of conduct or ethics policy. Such changes made by the Act with regard to governance, transparency, disclosures, the position of the serious fraud investigation office, etc, under section 211 of the Companies Act 2013 is expected to make companies shift from being complacent to playing compliant roles.

In particular, the amended guidelines require boards of directors and executives to assume responsibility for the oversight and management of ethics and compliance programmes. The provisions will help in developing a valuable framework for the design of effective ethics and compliance programmes.

ALMT Legal
ADVOCATES AND SOLICITORS

Junia Sebastian **jsebastian@almtlegal.com**
Arindam Basu **abasu@almtlegal.com**
Richika LRS **richika@almtlegal.com**

No 2 Lavelle Road
Bangalore 560001
India

Tel: + 91 80 4016 0036
Fax: + 91 80 4016 0001
www.almtlegal.com

Italy

Andrea Fedi and Marco Penna

Legance – Avvocati Associati

1 What legal role does corporate risk and compliance management play in your jurisdiction?

In Italy, corporate risk and compliance management play an increasingly key role. Italy was one of the first countries to enact laws on legal entities' criminal responsibility for offences committed by their directors, representatives, executives, managers, agents and employees. Legislative Decree 231/2001 has placed such responsibilities on legal entities for more than 15 years, and embraces a large variety of crimes that go far beyond anti-bribery and corruption. At the same time, enforcement of privacy rules has become increasingly effective. Naturally, sensitive legal sectors, such as banks, insurance companies and listed companies, are very specifically regulated and deeply scrutinised (according to the Banking Act 385/1993, the Insurance Act 209/2005 and the Financial Act 58/1998).

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

Article 2381 of the Italian Civil Code vests with the chief executive officer (under the continuing supervision of the board of directors) the task of ensuring the adequacy of the organisational, administrative and accounting set-up of the corporation. The above provision, which is interpreted as a general principle and is therefore applied to limited liability companies too, is intended to establish the duty of the directors to organise the business in a way that reduces the risk of non-compliance.

As far as listed companies are concerned, the Italian legal and regulatory framework provides for certain additional corporate bodies and procedures aimed at addressing corporate risk and compliance management. In particular:

- pursuant to article 154-bis of the Financial Act 58/1998, listed companies shall appoint a manager in charge of preparing the company's financial reports and ensuring that appropriate administrative and accounting procedures are put in place in connection therewith;
- pursuant to article 123-bis of the Financial Act 58/1998, the board of directors of listed companies shall publish, on a yearly basis, a report on corporate governance providing information on, inter alia, the risk management and internal audit systems adopted by the company in relation to the financial reporting process; and
- article 7 of the Code of Conduct for Listed Companies – which sets forth best practice standards for listed companies' corporate governance on a 'comply or explain' approach – recommends adoption of an internal control and risk management system that shall consist of policies, procedures and organisational structures aimed at identifying, measuring, managing and monitoring the main risks concerning listed companies.

Moreover, pursuant to the above-mentioned provisions, it is recommended that listed companies set up a control and risk committee. The committee shall be charged, among other things, with supporting the evaluations and decisions made by the board of directors in relation to the company's internal control and risk management system. For further information concerning the laws and regulations on corporate risk and compliance management of listed companies, see questions 6 and 7 below.

With respect to banks, the Bank of Italy's Regulation 285/2013 establishes a comprehensive regulatory framework in connection with banks' risk and compliance management. The general aim of the relevant provisions is setting up an integrated and effective internal control system in order to:

- regularly monitor business operations and ongoing compliance with the applicable laws and regulations, and check the adequacy of the banks' organisation and accounting arrangements;
- adequately monitor all business risks; and
- ensure information flows that allow management to make informed decisions.

Also, with regard to insurance companies and in line with the new Solvency II regulatory framework, Legislative Decree 209/2005 and Institute for the Supervision of Private Insurance and Collective Interest (ISVAP) Regulation 20/2008 provide for the implementation of an appropriate internal controls system, ensuring:

- the efficiency and effectiveness of corporate processes;
- adequate control of present and perspective risks;
- the reliability and integrity of accounting and management information;
- protection of assets from a medium and long-term perspective; and
- compliance of the insurance companies' activities with current legislation.

Large undertakings are also subject to Legislative Decree 39/2010 (on the auditing of their accounts), which, effective from 1 January 2017, now provides, for those exceeding certain dimension thresholds, the obligation to publish a non-financial statement containing information on the undertaking's activity impact on environmental, social and employee matters, respect for human rights, anti-corruption and bribery matters.

Compliance violations may trigger a broad range of consequences. First of all, pursuant to article 2049 of the Italian Civil Code and article 185 of the Italian Criminal Code, legal entities are responsible for civil damages resulting from violations committed by their representatives and employees in the exercise of their functions or roles.

Moreover, pursuant to article 197 of the Italian Criminal Code and article 6 of Law 689/1981, legal entities are jointly liable for the fines levied against their representatives and employees for offences committed in the exercise of their functions or roles.

Since 2001, pursuant to Legislative Decree 231, a legal entity is also criminally liable for certain offences committed by its directors, representatives, executives, managers, agents and employees when the crime has been committed in the interests or to the benefit of the legal entity. Legal entities may exculpate themselves from such criminal responsibility only if very strict conditions are satisfied. The long list of crimes that trigger the criminal responsibility includes bribery; corporate crimes; forgery; money-laundering; health and safety and environmental crimes; cybercrimes; conjuring; insider trading and market abuse; copyright crimes; and many others. Legislative Decree 231 applies to legal entities incorporated in Italy, Italian branches of foreign legal entities, partnerships and associations with or without legal personality.

Specific additional rules apply to state-owned companies (Law 190/2012) that must adopt specific anti-corruption measures.

From 25 May 2018, the General Data Protection Regulation 679/2016 has direct application in Italy.

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

The primary focus is on banks and financial institutions, insurance companies and listed companies. As mentioned above, a specific set of anti-corruption rules applies to state-owned companies. However, compliance rules are increasingly designed to apply to all types of companies and even to unincorporated associations.

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

Banks are supervised by the Bank of Italy and the European Central Bank (ECB). Following the implementation of the Single Supervisory Mechanism in accordance with Regulation (EU) No. 1024/2013, the ECB retains monitoring powers on all 'significant' Italian banks and specific tasks relating to the prudential supervision of all the banks, in cooperation with the Bank of Italy (eg, the decision on acquisition of qualifying holdings in banks). The other 'less significant' Italian banks are supervised by the Bank of Italy. In this respect, in addition to on- and off-site controls aimed at verifying compliance with banking and financial regulatory provisions (including anti-money laundering provisions), the Bank of Italy's supervisory actions extend to the adoption of administrative measures mainly relating to prudential supervision (eg, adoption of non-standard risk method assessment by the banks). The ECB and the Bank of Italy also retain sanctioning powers. Generally speaking, with regard to 'significant' banks, the ECB can impose pecuniary and administrative sanctions for violations of directly applicable European rules. For 'less significant' banks the said sanctioning powers are generally attributed to the Bank of Italy. Finally, following the implementation of Directive 2014/59/EU (BRRD), the ECB and the Bank of Italy also exercise extensive powers in relation to banks' crisis management.

With regard to insurance companies, the Italian Insurance Supervisory Authority (IVASS) is the competent supervisory authority charged with ensuring the stability of the Italian insurance market and the protection of insurance. In this context, IVASS retains inspection and investigation powers on technical, financial and capital management of insurance companies, verifying compliance with laws and regulations. IVASS also adopts regulatory provisions relating to different areas: internal controls systems, capital adequacy, valuation of technical provisions, accounting, etc. In line with banks' regulatory framework described above, IVASS also has the power to impose administrative and pecuniary sanctions over insurance companies.

The Italian Securities and Exchange Commission (Consob) and Borsa Italiana are in charge of supervision of listed companies. Consob is an independent authority that is responsible for supervising the Italian regulated financial markets and financial intermediaries. In particular, Consob has the power to enact regulations to implement provisions of law on matters regarding regulated financial markets and financial intermediaries, and to impose administrative sanctions to the supervised entities. Borsa Italiana, a commercial company, is responsible for the organisation and management of the Italian stock exchange – its main responsibilities include supervising the transactions carried out on the markets and defining the rules and procedures for admission to listing of companies' financial instruments.

While the enforcement of Legislative Decree 231/2001 on legal entities' criminal responsibilities is in the hands of the criminal courts, the national anti-corruption authority is appointed to scrutinise anti-corruption legislation on state-owned companies.

Finally, the Italian Data Protection Authority is the independent authority that is responsible for supervising the compliance of data processing; receiving claims, reports and complaints; blocking illicit processing; and carrying out inspections.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

With reference to banks and insurance companies, 'risk management' is not defined in the applicable regulatory provisions. However, the idea of risk management is widely used with general reference to risk monitoring and verification activities to be carried out by a specific internal function implemented within the banks and insurance companies. Also 'compliance management' is not defined in the applicable regulatory provisions. Compliance is used mainly in reference to the internal function, implemented within the banks and insurance companies, verifying – on a continuous basis – compliance with laws and regulations.

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

The Italian Civil Code only provides that the organisational, administrative and accounting set-up of a corporation be 'adequate' to the corporation's size and business. Some more indications are provided for listed companies. Indeed, the Financial Act 58/1998 contemplates specific additional corporate bodies (such as the manager in charge of the accounting documentation) and generally refers to the guidelines of the Code of Conduct for Listed Companies, which is a soft law set of rules for which the Financial Act establishes the principle of 'comply or explain'. Listed companies and, from 2016, state-owned companies also have the obligation to publish a corporate governance yearly report.

With reference to banks and insurance companies, risk and compliance management processes are deeply regulated under the applicable law and regulations (see question 2). Said regulatory provisions provide for a detailed framework relating, among other things, to organisational structures involved in said processes; ongoing control of aggregate exposure to relevant risks; and assessment of compliance status with the applicable laws and regulations, revision and reporting activities (conducted internally and with regard to the supervisory authorities).

Risks linked to data processing are to be addressed in compliance with the General Data Protection Regulation (GDPR) 679/2016.

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

Listed companies can voluntary adopt the Code of Conduct for Listed Companies issued by the committee for corporate governance. The Code of Conduct describes, inter alia, the main features of an effective internal control system and risk management; in particular, it requires companies to:

- adopt a control system consisting of rules, procedures and an organisational structure aimed at identifying, monitoring and managing compliance risks; and
- promote cooperation and communication between the executives and control bodies (ie, the statutory auditors, internal audit, control and risk committee, etc).

It is important to note that if a listed company decides not to adopt the Code of Conduct (wholly or partially), it is bound to the 'comply or explain' principle and the directors will be required to explain the reason for non-application.

The association of entrepreneurs has issued guidelines that provide a methodological approach in order to identify and address compliance risks and draft compliance shields to benefit of the exemption from criminal responsibility pursuant to Legislative Decree 231/2001. Indeed, legal entities can be exempt from criminal responsibility for offences committed by their directors, managers, agents or employees in the interest or to the advantage of the legal entity only if they adopt and effectively implement internal policies, rules and procedures and appoint a special supervisory body (a 231 compliance shield). The association of entrepreneurs' guidelines require, inter alia:

- assessing risks of crime, mapping the company's risk areas and identifying potential gaps;
- adopting and implementing a code of ethics and a disciplinary code;
- establishing a whistle-blowing procedure;
- training employees and executives;
- carrying out monitoring and inspections; and
- regularly updating and upgrading the compliance rules and the functioning of the system.

In that respect, it is worth remembering that Italian law 179/2017 has recently implemented a general regulation for whistle-blowing on top of specific provisions already contained in the Financial Act, the Banking Act and the Anti-Money Laundering Act.

As mentioned, banks and insurance companies are required to implement risk management and compliance functions aimed at carrying out risk and compliance management pursuant to mandatory law and regulatory provisions. In relation to banks, on 26 September 2017, the European Banking Authority published its guidelines on

internal governance (including internal control systems) under Directive 2013/36/UE (EBA/GL/2017/11). In particular, these guidelines provide that a bank's risk management function should be established and should:

- be actively involved in elaborating an institution's risk strategy and in ensuring that the bank has effective risk management process in place;
- be involved in the evaluation of the impact of such changes on the bank's overall risk, before decisions on material changes or exceptional transactions are taken; and
- ensure that all risks are identified, assessed, measured, monitored, managed and reported on by the relevant units in the institution.

In addition, these guidelines recommend that institutions establish a permanent and effective compliance function to manage compliance risk.

Compliance function should:

- advise the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards;
- verify that new products and new procedures comply with the current legal framework; and
- ensure that the compliance policy is observed.

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

Italian subsidiaries or branches of foreign legal entities are fully subject to Legislative Decree 231/2001 on criminal responsibilities of legal entities for offences committed by their directors, managers, agents or employees. To exculpate from those criminal responsibilities, Italian subsidiaries and branches of foreign entities must comply with the same requirements as all other undertakings incorporated or operating in Italy. Those requirements include the adoption and implementation of an effective set of internal rules and procedures and the appointment of an independent supervisory body, adequately budgeted and with direct reporting to the board of directors.

Italian branches of EU banks and of Canadian, Japanese, Swiss and US banks shall not apply Italian regulatory provisions to internal control systems (including the risk and compliance process). However, the legal representative of such branches shall attest compliance by the relevant branch with the applicable Italian laws and regulations.

EU banks operating on a cross-border basis are not required to comply with said provisions owing to the circumstance that they shall already comply with their EU home member state regulations (equivalent to Italian provisions).

Italian branches of non-EU banks (different from those referred to above) shall comply with the same regulatory provisions on internal control systems (including the risk and compliance process) applicable to Italian banks. Non-EU banks operating on a cross-border basis are not required to comply with said provisions (however they shall obtain authorisation from the Bank of Italy assessing the equivalence of provisions applicable to non-EU banks, pursuant to their local law).

EU insurances companies operating in Italy through a branch or on a cross-border basis shall comply with Solvency II provisions on risk and compliance management (equivalent to Italian regulations).

Italian branches of non-EU insurance companies shall comply with Italian regulatory provisions on internal control systems (including risk management and compliance). Non-EU insurance companies cannot carry out insurance activities in Italy on a cross-border basis.

The GDPR 679/2016 applies to any processing of data within the context of the activities of the EU establishment of a data controller or data processor, even if the processing is carried out outside of the EU. In many important instances the GDPR also applies to data controllers or processors not established in the EU.

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

Violation of compliance rules may expose undertakings to actions for civil damages, administrative fines and, in more than one case, to criminal responsibilities. With respect to Legislative Decree 231/2001, in addition to monetary sanctions, courts may order the publication of the judgment on the press, disqualify the undertaking from contracting with public administrations, inhibit the business of the undertaking (or specific lines of business) and even appoint trustees or commissioners that replace the managing bodies of the undertakings. Conditions to go exempt from criminal responsibilities are explained in question 7.

Banks should adopt adequate measures and procedures in order to ensure the proper and sound management of their business. In particular, banks should establish:

- a second-level control function:
  - a comprehensive risk management function, which would have sufficient authority, stature, and resources taking into account the proportionality criteria, to implement risk policies and the risk management framework within the relevant bank. The risk management function, inter alia, should be actively involved at an early stage in elaborating the bank's risk strategy and in ensuring that the same bank has effective risk management processes in place; and
  - a permanent and effective compliance function to manage its compliance risk, which should be able to report directly, where appropriate, to the management body in its supervisory function. The compliance function should be independent of the business lines and internal units it controls and have sufficiently authority, stature and resources to carry out its tasks;
- a third-level control function:
  - an independent and effective internal audit function, in charge of reviewing control activities carried out by the relevant business line and by risk management and compliance functions. Internal audit function should be independent and ensure that the monitoring tools and risk analysis methods are in adequacy with the bank's size, locations and the nature, scale and complexity of the risks associated with the bank's model and business activities and risk culture and risk appetite.

It is worth mentioning that the internal governance arrangements and processes mentioned above should apply, mutatis mutandis, to insurance companies. In this regard, insurance companies should establish, in addition to the above, the actuarial function, which shall, inter alia:

- coordinate the calculation of technical provisions;
- ensure the appropriateness of the methodologies and underlying models used as well as the assumptions underlying the calculation of technical provisions; and
- assess the sufficiency and quality of the data used in the calculation of technical provisions.

The GDPR 679/2016 dictates a number of assessments, actions and controls aimed at the protection of personal data. Violations can generate very high fines and may also trigger inhibitions.

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

In principle, CEOs and executive directors have the duty to give and maintain an adequate set-up of the company's structure, including as regards compliance. Moreover, in many instances, CEOs may be indicted of crimes committed by officers down the management chain because of the CEO's position as top-executive officer with a duty to be informed and supervise on the management of the company. Only in specific cases can CEOs demonstrate that they have effectively delegated a function to a lower officer and be exempt from responsibility. In no case will CEOs be exempted for negligence or reckless disregard in supervising. Non-executive directors may similarly suffer severe consequences if they do not supervise the CEOs or do not intervene to eliminate or at least reduce compliance violations.

Although legal entities do not have a strict regulatory obligation to prepare and implement a 231 compliance shield (see question 7), pursuant to case law, directors have a fiduciary duty to minimise risks of crime commission and so, effectively, they are bound to adopt and implement a 231 compliance shield as part of their fiduciary duties.

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

Companies are bound to compensate damages suffered by third parties as a direct result of illegal or illicit actions or omissions attributable to the company (or its directors, managers or employees) as a result of wilful misconduct or simple negligence. In certain cases (eg, data protection laws) a stricter liability regime applies. In any case, damages

Update and trends

With respect to data protection, on 25 May 2018 the GDPR will commence being directly applicable in Italy. The Italian government plan to enact a Legislative Decree in May 2018 to coordinate Italian legislation on data protection with the GDPR. The Italian privacy code will be repealed, while certain resolutions, general orders and instructions issued by the Italian data protection authority will survive.

As regards Legislative Decree 231, the EU Directive 2017/1371 of 5 July 2017 should be transposed into Italian law by July 2019, which will entail that certain tax crimes (VAT fraud) will commence to trigger companies' responsibilities (on top of criminal responsibilities of the individual offender) when such tax crimes are committed by directors, managers, employees and agents in the interest or to the benefit of the company.

must have been suffered as a direct and immediate result of the compliance violation (that is, there must be an ordinary causal nexus between the violation and the production of the prejudice whose redress is requested) and the plaintiff has the burden of proof as to the existence and amount of the damage.

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

Legal entities are jointly liable for payment of fines levied against their representatives or employees for conducts or omissions related to their office or work.

On top of that, Legislative Decree 231 provides for the following administrative sanctions that can be levied directly against a legal entity:

- pecuniary penalties;
- disqualifications, such as disqualification from exercise of the whole business, suspension or revocation of authorisations, licences or concessions, prohibition to trade with the public administrations, exclusion from grants, loans or subsidies, prohibition to advertise goods or services;
- confiscations; and
- publication of the court's decision in one or more newspapers at the entity's expense.

In broad terms, banks deemed liable for breaches of rules regarding internal control system and governance – also for those established by the Bank of Italy – are punished with an administrative pecuniary sanction from €30,000 to 10 per cent of their turnover.

Insurance companies deemed liable for breaches of rules regarding internal control systems and governance – also for those established by IVASS – are punished with an administrative pecuniary sanction from €5,000 to €50,000.

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

Even if the adoption of a 231 compliance shield is not considered compulsory by the law (see question 10), failure to adopt or adoption of a non-effective 231 compliance shield prevents the legal entity from utilising the compliance defence. In fact, the legal entity, in that case, will not be allowed to be exonerated from criminal responsibilities, although it can still apply for a reduction of the sanction if the legal entity implements a solid 231 compliance shield before the first discussion hearing of the criminal trial commences.

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

Directors and general managers may be liable for breach of their duties towards their company, the company creditors, single shareholders or single third parties.

Responsibility towards creditors subsists if compliance rules safeguarding the integrity of the company's net assets have been breached and the net assets are consequently insufficient to satisfy the creditors (in practice, when the company has become insolvent). That can take place, for example, when directors illicitly distribute reserves or act in conflict against their company.

Responsibility to single shareholders and single third parties can arise only when they have been directly and specifically damaged (eg, a damage that is personal to them and is not the mere implication of a damage that affects the earnings of all the shareholders or the rights of all stakeholders).

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

Legal entities that, in their capacity as joint obligors, have paid fines levied against their directors and employees generally have recourse to them.

Directors and senior management can receive fines for a broad variety of compliance crimes, including corporate compliance, breaches of data protection rules, insider trading and market abuse, environmental and health and safety violations.

In broad terms, members of administrative, direction and control bodies as well as personnel of banks, are punished with an administrative pecuniary sanction from €5,000 to €5,000,000 for breaches of the rules regarding internal control system and governance – also for those established by the Bank of Italy – to the extent that their conducts have contributed to the relevant infringements.

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

The Italian civil code and the legislation on insolvency and quasi-insolvency of companies provide for a wide range of corporate crimes, including false financial statements, illicit obstacles to mandatory audits and controls, illicit distribution of equity, illicit operations on treasury shares, extraordinary transactions in prejudice of creditors, conflict of interest, corruption, insider trading and market abuse, procuring or facilitating insolvency, etc.

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

With respect to crimes committed by directors and senior management, in order to avoid (or at least reduce) the 231 sanctions, the legal entity must prove that:

- it has adopted and continuously implemented an effective 231 compliance shield (see question 7);
- a special compliance supervisory office (independent, autonomous, adequately budgeted and professional) has been set up;
- the executive has committed the crime by 'fraudulently evading or escaping' the company's compliance programmes and controls; and
- there has been no omission or negligence imputable to the above said supervisor.

The above involves a first phase of shaping the 231 compliance shield through a risk assessment or gap analysis exercise, a second phase of compilation or collection of punctual compliance rules and procedures (not merely paperwork), the appointment of a supervisory body and the approval and implementation of a disciplinary code.

For crimes committed by employees, the legal entity will be held liable if the commission of the crime was determined by the breach of the supervisory obligations on employees by senior managers.

As to the relationships with third parties under the influence of the company (small suppliers, agents, etc), it is advisable to include specific contractual clauses to entitle the company to terminate the agreement, and to apply penalties in case of commission of a crime or investigations over the third party or service provider.

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

One of the most critical points concerning compliance risks and failures is the parent company's responsibility for breaches imputable to the subsidiary. On that point, the Criminal Supreme Court restated in 2016 (Decision 52316) that the parent and the group companies can be criminally liable pursuant to Legislative Decree 231/2001 if the crime

was committed with their help or with the involvement of an individual acting on their behalf. The Court also reiterated that the mere adoption of a 231 compliance shield is insufficient for the company to avail itself of the compliance defence – the appointment of a specific supervisory body, vested with independent and effective powers, being crucial.

In a 2017 judgment (Decision 49056), the Criminal Supreme Court also stated that the responsibility of a company for a bribe paid to governmental officers can be assessed (and sanctions may be levied) even if the corrupted governmental officers have not been identified (provided that the proof of a bribe has been reached) and even if the governmental officers are not indicted in the same judicial proceedings as the one pending against the company (in the specific case, those officers had settled their responsibilities in a separate judgment). The court also reaffirmed that sole-shareholder companies are also subject to Legislative Decree 231/2001 and continue to be imputable regardless of whether they are solvent or insolvent.

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

The anti-corruption legislation requires the public authorities to adopt an anti-corruption strategy and an action plan that should provide a valuation of the exposure level to corruption risks within the public offices, and the organisational measures to prevent such risks. In particular, the anti-corruption plan should, inter alia:

- identify the areas that present material corruption risk;
- provide training activities and control measures to prevent corruption risks; and
- provide communication flows towards the anticorruption supervisor, who is required to monitor and control the functioning and effectiveness of the anti-corruption plan.

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

Legislative Decree 231/2001 and the anti-corruption legislation have different scopes of application, although both are aimed at preventing the commission of crimes and exempting from liability the legal entity if the measures adopted are effective. In such respect, as to the crimes to be prevented, Legislative Decree 231 regards crimes committed in the interest or to the advantage of the legal entity; the anti-corruption legislation also addresses the commission of crimes committed against the legal entity. Furthermore, the latter makes reference to a broader concept of corruption, including not only all crimes against public authorities, but also all cases of 'bad administration'.

Andrea Fedi **afedi@legance.it**
Marco Penna **mpenna@legance.it**

Via Dante, 7
20123 Milan
Italy
Tel: +39 02 89 63 071
Fax: +39 02 896 307 810

Via di San Nicola da Tolentino, 67
00187 Rome
Italy
Tel: +39 06 93 18 271
Fax: +39 06 931 827 403

www.legance.it

Japan

Hiroyuki Nezu, Masataka Hayakawa, Kumpei Ohashi, Teruhisa Toyama and Tadashi Yuzawa

Atsumi & Sakai

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Japan seems to have a particular problem with corporate scandals, such as false accounting (false statements on annual securities reports, etc) and insider trading. These scandals can impair corporate values, harm the social credibility of the affected company and, in some cases, jeopardise its survival. Scandals in the securities market, such as false statements submitted by listed companies, may not only ruin the credibility of the relevant company, but also bring the market into disrepute. Risk and compliance management are of the utmost importance to all companies in order to avoid scandals and achieve sustainable growth.

Although the importance of compliance has been increasing in light of scandals and poor governance, no extensive body of law or practice on the subject exists. Compliance is not a discrete field of law or regulation, and there is no legally binding general definition of the concept in Japan. 'Compliance' is only loosely defined and is not readily distinguished from 'corporate governance', 'internal control', or 'corporate social responsibility'. That said, some provisions of Japanese law are related to loosely defined compliance matters, so it could be said that there is a general concept of compliance under Japanese law. Outside of regulated and finance-related sectors, such as banking, insurance and financial services, compliance in Japan is more of a reactive function than a proactive one.

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

As mentioned in question 1, there are no laws that directly impose obligations of risk and compliance management and it is therefore not possible to make a general statement about the fields of law that businesses must cover with their compliance management activities, and management remains responsible for adhering to all laws. That said, the areas of law that companies primarily focus on for specific compliance risks (as opposed to general obligations to manage a company properly) are antitrust, anti-corruption, money laundering, data protection and employment. Antitrust, anti-corruption and money laundering are of particular importance given the potential for significant penalties and reputational damage from non-compliance.

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

All companies, regardless of the nature of their business, are subject to the Companies Act and other laws of general application that impose compliance obligations directly or by implication. All directors of companies are subject to duties of care (see question 10). Listed companies and companies in regulated industries are subject to specific compliance management requirements.

It cannot be said that specific types of undertakings are targeted regarding their imposition of compliance management obligations.

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

There are no regulatory or enforcement bodies with responsibility for corporate compliance. It is for directors of companies to determine how best to comply with their and the company's compliance obligations.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

As noted in question 1, there are no specific laws and regulations that define 'risk management' and 'compliance management'.

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

No. It is for directors of companies to determine how best to comply with their and the company's compliance obligations.

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

There are none. It is for directors of companies to determine how best to comply with their and the company's obligations.

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

Companies incorporated in Japan under the Companies Act are, as a basic rule, subject to the Companies Act and other general legislation governing their activities (eg, antitrust laws and banking regulation). Foreign companies listed on a stock exchange in Japan are subject to the rules of the exchange and related requirements of the Financial Instruments and Exchange Act (FIEA). Japanese corporate and administrative law, and the Criminal Code generally only apply to acts that are carried out in Japan.

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

The Companies Act requires that directors or the board of directors of a large company, or a company with committees, establish systems that ensure that directors and executive officers comply with laws, regulations, the company's articles of incorporation and other applicable requirements during the execution of their duties. Although these provisions are generally not understood as imposing a corporate (as opposed to an individual's) duty to develop such a system, court precedents have implied a corporate duty to develop an internal control system that is closely related to the risk and compliance management obligation arising from a director's duty of care of a prudent manager owed to the company (see question 10).

The FIEA requires that listed companies file an 'internal control report'. This report evaluates the management structures and procedures the company has in place to ensure the appropriateness of its financial statements, accounting and other information concerning the company and the corporate group to which it belongs. Listed companies are also required to submit a letter with their annual and quarterly securities reports, confirming that the statements contained in those reports are appropriate under the FIEA and related regulations. The internal control report requires an audit certification by a certified public accountant or audit firm in order to assure that it is fair and proper.

The listing regulations of the Tokyo Stock Exchange (TSE) require all domestic companies listed on the exchange to develop a system necessary to ensure the appropriateness of their business, and to put in place management structures and procedures as required under the Companies Act (as mentioned above), and operate them appropriately.

TSE listing regulations also require listed companies to respect the TSE's Principles of Corporate Governance for Listed Companies, as well as to make efforts to enhance their corporate governance.

Ministries may, from time to time, issue guidance, among other things, on the establishment of internal control and risk management systems for the industries and bodies they regulate. While these do not have the force of law, the affected entities do habitually comply with them (and it would be imprudent for them not to do so).

In addition to legal and regulatory compliance requirements, there are also 'soft compliance' requirements. For example, the Keidanren, a federation of companies, industrial associations and regional economic organisations, publishes a non-binding Charter of Corporate Behaviour, which states that companies should maintain high ethical standards and go above and beyond mere compliance with laws and regulations regarding their social responsibilities. Various trade associations have similar principles.

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

The Companies Act imposes an obligation on directors to exercise the duty of care of a prudent manager (also known as a 'fiduciary duty') in the management of their company, which requires that directors act with the level of care that is normally expected to be taken by a person in the same position and, if relevant, with the same expertise as the director – the duty is owed to the company. The duty of care could be interpreted to include a (compliance) duty to organise the managed business (including its controlled subsidiaries) in such a way so as to ensure adherence to all applicable laws so far as is reasonably possible. In order to comply with these duties, directors should familiarise themselves with background information, such as the company's size and business type, and the occurrence of previous scandals, etc, and the occurrence of misconduct or violations by other companies in the same business.

The relationship between a company and its managers (persons other than directors exercising management functions and with authority to bind the company) is one of entrustment and employment, the managers therefore owing a duty of care to the company. The liability of officers is almost the same as that of directors (see above), though managers are usually appointed as the head of an office or branch office, and their powers and liability are limited to such office.

If a director, officer or manager suspects that an employee has engaged in an unlawful activity, he or she must take action to prevent the offence, and to prevent similar cases of non-compliance from occurring in the future by testing the effectiveness of the existing compliance programme, and adopt adequate improvement measures and controls if required. It is the responsibility of management to determine what constitutes an adequate and effective compliance programme. It was noted in a judgment that 'what should be included in the development of a risk management system is a matter of business judgment, and it should be noted that directors are given broad discretion thereover for their expertise in company management.' The board of directors must continuously review whether or not an existing internal control system is still appropriate and operating properly, and any deficiencies must be corrected in a timely manner. Establishment of an internal audit department, on-site audits and a whistle-blower system, and monitoring of reporting of unfair acts are some of the means to determine whether or not an internal control system is functioning properly.

Senior employees are also obligated to monitor internal control systems, but are not liable for any failure to develop appropriate internal control systems.

Although the Companies Act does not clearly specify the duties owed by directors of parent companies with respect to management of subsidiaries, there are provisions in the Banking Act based on the assumption that bank holding companies are authorised and obligated to manage and control their subsidiary banks.

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

An undertaking would only face civil liability for a risk or compliance management deficiency if the deficiency gave rise to a claim under another head, for example, tort.

A company may be liable under civil law for compliance violations resulting from torts committed by its employees or persons acting in its name. Essentially, a company is liable for the acts of its employees and directors while they are acting in the course of their employment or performance of their duties. A company is also liable for the acts of its agents when they are acting within the scope of their authority unless the company or its directors exercised reasonable care in appointing the agent or in supervising the business, or if the damages could not have been avoided even if the company or its directors had exercised such reasonable care.

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

Although Japan does not have a separate body of administrative law as is found in some civil law European jurisdictions, administrative actions may be taken pursuant to the specific law to which the breached compliance obligation relates.

Where an activity of a company is subject to regulatory oversight, and the applicable law provides regulators with enforcement powers, the relevant authority is often entitled to impose sanctions, including fines.

Where a company listed on the TSE has made false statements in securities reports or other sources, or where auditors, etc, of the company express, for example, an adverse opinion in audit reports and the TSE deems that 'improvement of the internal management system, etc, of such listed company is highly necessary', then the TSE may designate the listed stock as a security on alert. If the internal management system is not improved within the prescribed period, or the TSE deems that improvement is not expected (ie, no steps are taken for fact-finding, no policies considering preventative steps are disclosed, or the proposed policies lack practicability), then the company will be delisted.

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

Corporate criminal law does not exist in the Japanese legal system, as only natural persons may be subject to criminal prosecution under the Penal Code. A company can, however, be subject to criminal fines under a number of other statutes, for example, the Anti-monopoly Act, the Companies Act and the Labor Law.

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

The Companies Act stipulates that if a director, accounting advisor, company auditor, executive officer or accounting auditor of a company neglects their duties (such as their implied duty to develop and monitor internal compliance systems), they shall be liable to the company (but not its shareholders) for any resulting damages. And if a director knowingly breaches their duties, or is grossly negligent in performing them, they shall be liable to any third party (including shareholders in the company) suffering loss as a result. A director (but not the other officeholders mentioned above) may be released, in whole or in part, from their liability to the company (but not to third parties) for breach of duty on a case-by-case basis, the basis of this release depending on whether the director acted with wilful misconduct or was grossly negligent. If the director acted with wilful misconduct or was grossly negligent, shareholders' unanimous approval is needed for such a release; otherwise, a partial limitation of liability may be available under the company's articles and the Companies Act, though there is a minimum liability in some cases.

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

No specific or 'catch all' administrative liability exists for directors, officers or managers of a company that fail to supervise a subordinate, or to put adequate supervisory processes in place. However, such failures may violate specific legislation, depending on the nature of the business and the act or failure in question, and could give rise to third-party claims.

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

Persons are criminally liable if they commit criminal offences themselves or if the criminal offence arises from their actions, for example, when they instruct others to commit a criminal act or otherwise contribute to it. A director's breach of the duty of care owed to their company (see question 10) does not, in itself, give rise to any criminal liability. As there is no catch-all risk and compliance management obligation at law, there is no related criminal liability.

Specific legislation may impose criminal sanctions for certain acts that are compliance-related; for example, the Anti-monopoly Act imposes criminal fines on representatives of companies who have failed to take necessary measures to prevent certain acts (such as not complying with regulatory orders), despite their knowledge of an intention to commit such acts, or who have failed to take necessary measures to rectify such acts despite their knowledge of them.

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

No, but in practice taking appropriate measures, such as implementing effective internal compliance management, may mitigate penalties for breach of statutory or regulatory obligations, or claims by third parties. For example, in a judgment in 2009 relating to the liability of a representative director for the acts of an employee in falsifying sales amounts, the Supreme Court held that the representative director had not violated their duty to develop an internal control system, on grounds that, among other things, the representative director had developed a management system that was sufficient to prevent unfair acts that could normally be expected (such as the false entries).

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

The most recently publicised case of corporate management failure is the ¥220 billion false accounting by Toshiba Corporation, one of the leading electronics manufacturers in Japan. According to a third-party committee's report on the case, the underlying cause of this false accounting was the company's top management's extreme pressure to pad the company's profits, and that the actions were not revealed by the company's internal controls. There have been many other cases of accounting fraud by listed companies in recent years, triggering claims for damages by shareholders, including institutional investors, or significant administrative monetary penalties. What underlies these accounting frauds is, in many cases, the failure of compliance management.

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

There are no legally binding risk and compliance management obligations for government, government agencies and state-owned enterprises, though any such entity that is a company would have to comply with the general management obligations and other obligations that a director of a private company would be subject to.

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

Risk management in the public sector is not a statutory obligation at this point in time, and it has been acknowledged that local governments have not made enough efforts to develop their internal control systems. Internal controls requirements of incorporated administrative agencies differ from those of private companies due to their businesses being stipulated by individual laws, the involvement of the government, etc, in the evaluation of performance and review of operations, and their budget being under strict management due to the institutional constraint that they are financially supported by the government. It has been suggested that these differences should be thoroughly examined to determine to what extent they are still appropriate.

Atsumi & Sakai

Hiroyuki Nezu **hioyuki.nezu@aplaw.jp**
Masataka Hayakawa **masataka.hayakawa@aplaw.jp**
Kumpei Ohashi **kumpei.ohashi@aplaw.jp**
Teruhisa Toyama **teruhisa.toyama@aplaw.jp**
Tadashi Yuzawa **tadashi.yuzawa@aplaw.jp**

Fukoku Seimei Building
2-2-2 Uchisaiwaicho
Chiyoda-ku
Tokyo 100-0011
Japan

Tel: +81 3 5501 2111
Fax: +81 3 5501 2211
www.aplaw.jp/en/

Mexico

Reynaldo Vizcarra, Jonathan Edward Adams and Lorena Castillo
Baker & McKenzie Abogados, SC

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Corporate risk and compliance management in Mexico has traditionally played a mostly commercial and business contingency role. Mexico has not had corporate criminal liability until recently, and does not have significant product liability or product recall actions. Although Mexico has had a class-action lawsuit mechanism since 2011, lawyers have not taken up the challenge of forming a class action bar such as exists in the United States and other jurisdictions. Mexico still shares a significant core of common culture, and litigiousness is clearly not one of its characteristics. Most Mexicans prefer to conserve the social fabric and community of which they are a part, and consider this to be of more value than short-term pecuniary personal gain. For this reason, tort litigation is almost unheard of in Mexico. Regulatory compliance has also not traditionally been a focus of serious risk and compliance management because many managers have relied on their abilities to bribe officials who threaten fines or closure for lack of regulatory compliance.

One of the few areas in which litigation is considered acceptable social behaviour is labour and employment. Termination of labour employment can only be for legislatively defined just cause, which is notoriously hard to prove. Therefore, Mexican employees expect generous severance payments when they are dismissed or laid off. If full severance is not paid to an employee, the employee will often sue to recover this amount, which may take several years. For this reason, corporate risk and compliance management in Mexico focuses significantly on labour and employment matters.

Recent years have seen a change of situation. The largest single factor driving this change is aggressive enforcement by the US Department of Justice (DOJ) and Securities and Exchange Commission (SEC) of the Foreign Corrupt Practices Act in Mexico. With regard to the number of enforcement actions settled by the DOJ and SEC, Mexico ranks fourth in the world with 48 actions, trailing only China, Nigeria and Iraq. Arguably, this ranking is not as negative as it might at first appear, given Mexico's status as the US's second-biggest trading partner. However, this activity is especially visible to US-based companies operating in Mexico, which take the threat of prosecution very seriously, especially in the past 10 years that have seen a significant uptick in enforcement actions.

More recently, Mexican lawmakers have become active in areas that drive risk and compliance management. The class action lawsuit mechanism that became law in 2011 have not yet become actively used, but development takes time: the modern US class action was born in 1966 with a renewal of the Federal Rules of Civil Procedure. The most likely reason for the lack of activity in the class action space in Mexico is the very limited provisions for litigation discovery. This deprives the plaintiffs of the opportunity to establish their case in many instances.

Perhaps of most importance for the evolution of risk and compliance management in Mexico is the recent advent of criminal liability for corporate entities. In December 2014, the Mexico City legislature enacted criminal liability for companies. Although this change was not widely reported at the time, and many practitioners did not become aware of the change until well after its enactment, word has begun to spread through the community. This is especially the case because of a few high-profile cases that have involved criminal liability for companies, owing to the significant fines levied on the companies. Where Mexican criminal law traditionally has been based on a defined number of multiples of the federally mandated minimum wage (currently around US$5 per day) and designed to punish individuals who can be incarcerated, fines have been somewhat low. For example, top fines for such crimes as bribery under federal law are approximately US$5,000. Mexico City's law defines its monetary penalties based on not the daily wage of the worker, but on the average daily profits of the company, and equates a year of incarceration to a penalty of 920 days of average daily profits.

The Mexico City criminal law should drive risk and compliance management because, for lower level employees, one of the elements of the crime is that the company did not exercise proper control over the activities of the employees who were the active participants in the crime.

Federal criminal law (the Federal Criminal Code and the National Code of Criminal Procedure) was modified in June 2016 to impose criminal liability on companies for most types of white-collar crimes. This law also includes the element of lack of proper controls, so it should also drive compliance and risk management in Mexican companies.

Finally, the General Law of Administrative Responsibilities establishes administrative penalties for various corruption-related offences. Enacted in July 2016, it entered into force fully in July 2017. It establishes a much more detailed set of standards that a company must meet to avoid liability. As discussed below, under the General Law of Administrative Responsibilities, having a compliance programme can act in essence as an affirmative defence. Failure to have a compliance programme or an adequate integrity policy can be a significant factor in determining corporate criminal liability and expose corporate entities to sanctions, which can be as high as US$6.5 million, plus damages and disgorgement.

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

Specifically, the new General Law of Administrative Responsibilities sets out the characteristics needed for an integrity policy or compliance programme. In addition, the Model Program for Corporation Integrity published by the Ministry of Public Administration provides recommendations for compliance programmes or integrity policies.

Highly regulated industries, such as finance, insurance and healthcare industries, have specific legal regimes to manage the types of risk and compliance that are specific to each industry. For companies in general, the laws and regulations that specifically address risk and compliance management and are of the highest priority are the corporate law, consumers' protection law, commercial law, labour law, administrative law and criminal law.

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

Under the General Law of Administrative Responsibilities all companies are regulated regardless of the form of the entity.

Limited companies are the least regulated types of company unless they engage in one of the more regulated industries or activities discussed below. These entities must follow laws that protect their shareholders (corporate laws), employees (labour laws), commercial counterparts (commercial laws) and consumers (consumers' protection laws), as well as civil society as a whole (environmental laws, competition laws, land use laws, criminal laws, etc).

Publicly traded or listed companies are also subject to laws regarding periodic financial reporting and disclosure, and avoidance of self-dealing and insider trading.

Financial institutions are subject to additional laws regarding their fiduciary duties toward the parties whose assets they hold. These differ depending on whether they are banks, investment funds, insurance companies or other types of financial institutions.

Healthcare companies are another type of undertaking subject to special rules related to risk and compliance management. Specifically, treatments provided to patients, clinical studies, medications, medical devices and the claims and promotional programmes made in relation to the foregoing are more highly regulated than other types of corporate activity.

Other industries that are highly regulated include power generation and transmission, mining, aviation and transportation. Each has its own set of standards that drive risk and compliance management.

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

For all federal crimes, the General Prosecutor of the Republic heads both the investigation and prosecution, through the federal prosecutor's office. For laws that apply to specific industries or activities, Mexican law has created special administrative enforcement entities that may assist the federal prosecutors in their work. Each of the 31 states and the City of Mexico have their own state prosecutors.

The principal powers of the General Prosecutor of the Republic are investigating and prosecuting federal crimes through the police, gathering evidence, carrying out actions to protect victims or the public, requesting arrest and search warrants from the federal courts, and deciding whether or not to prosecute.

The main agency involved in investigating crimes, including bribery, is the Attorney General, who investigates crimes at the federal level (General Prosecutor of the Republic) and at the state level (eg, Judicial Attorney General).

The agency's most recent report from 2017 contains a section on crimes committed by public servants and against the administration of justice. This section includes statistics and data as to the efficacy of the agency's investigations, and also refers to the Special Unit for the Investigation of Crimes Committed by Public Servants and against the Administration of Justice, and its mission to combat corruption and impunity of public servants.

Each Mexican government agency has the authority to enforce the General Law of Administrative Responsibilities.

Under the General Law of Administrative Responsibilities, internal control bodies of each government agency are responsible for investigating, substantiating, determining and imposing sanctions for minor administrative offences by public officials. In cases of serious offences by either public officials or private entities, the Superior Federal Court of Administrative Justice has jurisdiction to impose sanctions.

The Federal Court of Administrative Justice (now split from the fiscal court) resolves matters appealed from the internal control bodies for government employees, and all matters for private citizens.

For regulatory matters, Mexican law has created special entities to investigate and resolve administrative matters, which may later be appealed to the courts. For instance, the Federal Commission for Protection Against Sanitary Risks is assigned to investigate and determine administrative liability for healthcare regulations. It has investigatory powers, including inspections. In financial industry matters, the National Banking and Securities Commission has investigatory and inspection faculties.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

Mexican law defines risk management and compliance management for various industries, such as the healthcare, mining and financial industries. These definitions focus on technical aspects of each discipline. Federal and state criminal laws require 'proper internal controls' to avoid liability for criminal acts carried out for their benefit or on their behalf. However, it is the General Law of Administrative Responsibilities that has the clearest definition of risk management under Mexican law. The existence of an adequate integrity policy or compliance programme can be a significant factor in determining corporate criminal liability for reducing sanctions as long as it meets the following characteristics set out in the General Law of Administrative Responsibilities:

- a clear and complete organisational and procedural manual that clearly defines the functions and responsibilities of each part of the company, and specifies clearly the chains of command and leadership for each corporate structure;
- a code of conduct that is duly published and made known to every person in the organisation and that has systems and mechanisms for effective implementation;
- adequate and effective controls, monitoring and auditing systems that ensure compliance on a continuous and periodic basis throughout the organisation;
- adequate whistle-blowing systems for internal reports also allowing for reporting to authorities, as well as disciplinary processes with clear and specific consequences for those who act contrary to internal company policies or to Mexican legislation;
- adequate systems and processes for training on ethics standards;
- human resources policies to avoid hiring employees who could be a risk to the integrity of the company. These policies cannot enable discrimination on the basis of ethnicity, nationality, gender, age, disabilities, social status, health status, religion, political opinion, sexual orientation, marital status, or any other ground that compromises human dignity or curtails human rights and liberties; and
- mechanisms to ensure transparency and disclosure of interests (avoiding conflicts of interest) at all times.

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

The characteristics of a compliance programme or integrity policy have been defined for the first time in the new General Law of Administrative Responsibilities, which entered into force in July 2017. Additionally, in June 2017, the Ministry of Public Administration published the Model Program for Corporate Integrity, which provides the following recommendations for compliance programmes or integrity policies:

- include measures to promote internal norms and accountability within the company, in accordance with national and international commitments;
- 'tone at the top' commitment from board of directors and general manager;
- third parties and distributors are obligated to adhere to the company's compliance policies;
- the Code of Conduct must be adequately published and communicated to company personnel. Reference to the Confederation of Employers of the Mexican Republic is recommended;
- apply the Code of Conduct in practice and promote reports of suspicious activities. If a company has multiple divisions, implementation can take place on an area-by-area basis;
- the anti-corruption policy must take into account the degrees of risk for the country, industry, transaction, commercial opportunity and commercial association. For these purposes, rely on the Model for International Internal Controls;
- for financial organisations, refer to these three guidelines:
  - the Sole Memorandum for Banks;
  - the Sole Memorandum for Stock Exchange; and
  - the Sarbanes Oxley Act;
- special attention is to be paid to the following areas of the company: sales, contracts, human resources and government contacts. The guide also recommends observance of the guide for the UK Bribery Act;
- systems for self-reporting and training must be adequate and efficient; and
- human resources must employ policies to avoid the employment of individuals who could generate a risk to the integrity of the company.

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

The General Law of Administrative Responsibilities sets out the main standards for risk management in anti-corruption matters. The law has no regulations at this time. However, the Model Program for Corporate Integrity provides recommendations for compliance programmes or integrity policies, as discussed above.

Other industry-specific laws set out processes in various regulations and Mexican official standards (NOM). For example, NOM-220-SSA1-2012 sets out the plan that healthcare companies must establish for pharmacovigilance. Similar standards for other industries would be too numerous to list, and require specific subject-matter expertise to interpret.

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

As discussed above, risk and compliance governance obligations apply to operations in Mexico of various undertakings, regardless of the form of the entity. With the exception of a relatively few provisions of Mexican law, such as criminalisation of foreign corrupt practices of Mexican companies, Mexican law is territorial in its application. Whether an entity is domiciled or not in Mexico, its operations in Mexico will be subject to Mexican law, including risk and compliance governance obligations.

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

While it is not mandatory, undertakings are expected to implement and maintain an adequate integrity policy or compliance programme as discussed in questions 6 and 7 above.

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

Members of the board of directors and administration have a duty of care and of loyalty toward the company. As part of this duty, they must disclose conflicts of interest and recuse themselves from participating in decisions in which they have a conflict of interest. If they fail to do so, they are liable to the company for any damages caused. Directors and administrators are liable for the value of the capital contributions made by shareholders, for dividends, for accounting, control, files and other information required by law, and for the fulfilment of shareholder resolutions. They must also report any breaches of duty of care or loyalty to the auditors or be jointly liable with the directors at fault. If shareholders representing 25 per cent or more of the corporate capital of the company agree, they may sue the directors in the name of the company.

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

Yes. When companies fail to comply with legally established regulations, they can be civilly liable for any damages caused to third parties owing to their lack of compliance. For example, if a mining company does not follow safety standards (NOM-032-STPS-2008, NOM-023-STPS-2012) it may be liable pursuant to the federal or state civil code for any harm suffered by third parties or employees. In another example, a company that does not maintain proper risk and compliance management of the performance of its employees will be unable to demonstrate just cause for termination and, therefore, be liable for severance payments that would otherwise not be due.

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

Yes. As discussed above, as of July 2017, under the General Law of Administrative Responsibilities, legal entities may be subject to corporate administrative liability when acts related to serious administrative offences are committed by individuals – either employees or third-party representatives – acting on behalf of the entity. Sanctions for corporate entities include double disgorgement or, even if there was no proven tangible benefit, sanctions can include fines of up to the equivalent of US$6.5 million. Corporate entities can be sanctioned by up to 10 years' debarment from participating in public procurement, suspension of the entity's activities or even dissolution of the corporate entity. Because the General Law of Administrative Responsibilities was recently fully implemented, there is no track record yet on the criteria that the administrative courts may use to evaluate compliance programmes or integrity policies nor guidance by the enforcement authorities on how they may use evidence of compliance programmes in decisions on whether or not to bring enforcement actions.

Update and trends

In June 2017, the Ministry of Public Administration published its Model Program for Corporate Integrity to provide interpretation of the provisions of the General Law of Administrative Responsibilities. This Model Program provides guidance on corporate compliance programmes and integrity policies.

Lack of risk and compliance management in relation to regulations for specific industries will expose companies to liability for fines and other sanctions.

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

Yes. As discussed above, under Mexico City and the Federal Criminal Code, when a person commits a crime for the benefit, account, in the name of, or using means provided by the company, and the company has not implemented 'proper controls', the company will be liable for the crime, along with any individuals who may be liable. The concept of proper controls is not defined by the law, nor is it clear how judges have been or will interpret the requirement that their absence be proven as an element of the criminal liability for companies. Although criminal proceedings are now open to the public under the 2011 criminal procedure provisions, the files are only available to victims and defendants, so legal professionals only have access to rulings on an anecdotal basis.

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

Not unless they have breached their duty of care or loyalty.

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

Not directly unless they have breached their duty of care or loyalty.

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

The Mexico City Criminal Code divides criminal liability in companies between high-ranking officials, for which there is strict liability for the company, and lower-ranking employees, for whom the prosecutor must prove a lack of proper controls. For the strict liability cases, it is almost inevitable that at least one of the administrators will have committed acts sufficiently related to the criminal liability that the administrator will be liable criminally as well. This liability would not be for breach of risk and compliance management obligations. It would be for independent criminal acts. However, in the second case, where proper controls are not established, the law does not establish criminal liability for directors or senior managers in the absence of mens rea of their own.

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

As discussed above, it appears that a lack of 'proper controls' is a required element of the crime itself. However, it is not clear how strict judges are being in interpreting this requirement. They may, in practice, be considering that if a crime is committed for the benefit of the company or using its resources, the lack of proper controls is a given. If this is the case, a defendant company that is able to show proper controls will likely be treated as having presented an affirmative defence. There are no specific requirements. However, it is likely that the elements of an integrity policy or compliance programme, as discussed in question 5, would be persuasive in showing proper controls.

For administrative liability, while there is no affirmative defence for adequate procedures to negate corporate administrative liability in Mexico, the existence of an adequate integrity policy or compliance programme is a significant factor in determining liability, which must be proven beyond a reasonable doubt, a standard usually reserved for the criminal context. The requirements for an effective integrity policy are listed in question 5 above.

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

Since its enactment in 2012, the Federal Law for the Protection of Personal Data in Possession of Private Parties has been strictly enforced by the National Institute for Access to Information (INAI). During the past five years, the INAI has levied fines totalling approximately US$19 million to companies for data protection violations, most of them in the financial and insurance sector.

From 2014 to 2017, the Mexican antitrust watchdog, the Federal Economic Competition Commission, levied fines totalling approximately US$224 million for antitrust violations committed by seven competing maritime shipping companies, four financial and investment fund management firms, and Pemex Transformación Industrial, among others.

In August of 2015, Gas Express Nieto, a local natural gas company, paid approximately US$4 million in settlement of criminal charges for failure to follow regulatory safety obligations in relation to natural gas delivery. An explosion in January of that year near a children's hospital in the outskirts of Mexico City caused the deaths of five persons and injuries to over 70 others.

In November of 2011, HSBC Mexico agreed to pay nearly US$30 million to the Mexican National Banking and Securities Commission, admitting to over 800 compliance failures identified in 2007 and 2008 in relation to money laundering. This case led HSBC Mexico to launch an internal project to implement significant improvements and a complete overhaul of its compliance department.

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

Yes. The Organic Law of Federal Public Administration requires that all government agencies and government in general conduct their business according to policies. Specifically regulated areas include public safety, crime prevention, prevention of unlawful discrimination, sale of public property, elimination of poverty, social inclusion, environmental protection, trade, industry, transportation, communication, anti-corruption, public health and population centres.

The new General Law of Administrative Responsibilities substitutes the Federal Law of Administrative Responsibilities of Public Servants with its own provisions, which are now not limited primarily to government officials.

State-owned enterprises also have obligations on risk management and compliance. For example, the board of directors of the largest state-owned enterprise, Petróleos Mexicanos, has the obligation to establish policies in many areas, including environmental, health and safety compliance, employment practices and third-party contracting. To implement the third-party contracting policies, there is a Committee on Acquisitions, Leasing, Works and Services, which must identify and evaluate risks in the implementation of its policies. Pemex also has an Audit Committee, with its own policies.

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

In general, the public sector has been and continues to be far more highly regulated than the private sector, including in matters of risk and compliance management. From a legal perspective, public sector entities are limited in their activities to those that are specifically mandated by law. Private sector entities are free to act, as long as it is not prohibited by law. Although healthcare, worker protection, consumers' protection, market competition and financial services have been regulated for many years in relation to risk and compliance management, only recently has the law introduced general provisions on risk management, such as those of the Federal Criminal Code or the General Law of Administrative Responsibilities.

Baker McKenzie.

Reynaldo Vizcarra **reynaldo.vizcarra-mendez@bakermckenzie.com**
Jonathan Edward Adams **jonathan.adams@bakermckenzie.com**
Lorena Castillo **lorena.castillo-lopez@bakermckenzie.com**

Edificio Virreyes
Pedregal 24, 12th floor
Lomas Virreyes / Col Molino del Rey
11040 Mexico City
Mexico
Tel: +52 55 5279 2900
Fax: +52 55 5279 2999

Oficinas en el Parque
Torre Baker McKenzie, 10th floor
Blvd Antonio L Rodríguez 1884 Pte
Monterrey, NL 64650
Mexico
Tel: +52 81 8399 1300
Fax: +52 81 8399 1399

bakermckenzie.com

Nigeria

Babajide Ogundipe, Olatunde Ogundipe and Olajumoke Omotade

Sofunde Osakwe Ogundipe & Belgore

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Corporate risk and compliance management are routine elements to which attention must be paid in corporate governance in Nigeria. However, it is not presently recognised as a distinct field of law in Nigeria. Prior to the 2007 banking crisis, the amount of attention paid to corporate risk management was significantly less than that placed on compliance. An example of the emphasis placed on compliance is the provision in section 295 of the Companies and Allied Matters Act (CAMA) Cap C20, Laws of the Federation of Nigeria 2004, which is an amendment to the CAMA enacted in 1990. The 2004 amendment requires publicly traded companies to appoint a company secretary with specialised knowledge (eg, a legal practitioner, chartered accountant or chartered secretary). The company secretary is responsible for ensuring compliance with legislation and regulations. However, the 2007 crisis in the banking sector led to financial sector reforms, which put risk and compliance on the legislative front lines. An example of this was the enactment of the Investment and Securities Act 2007. This legislation required all organisations involved in the Nigerian capital market to appoint a compliance officer.

In most major corporate bodies in Nigeria, other than those involved in the capital market, corporate risk and compliance tend to be the responsibility of general counsel or in-house legal departments and it would appear that only the largest corporate bodies have a specific compliance department. This is notwithstanding provisions in the Investment and Securities Act that require registered organisations to appoint a compliance officer.

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

As indicated above, corporate risk and compliance management is yet to be viewed as a distinct practice area in Nigeria. There are, however, a number of laws and regulations to which attention needs to be paid when considering these matters. The laws and regulations that address corporate risk and compliance, which tend to be in respect of specific commercial activities, include the following:

Legislation

- The Companies and Allied Matters Act 2004;
- the Investment and Securities Act 2007;
- the Anti-Money Laundering Act 2011;
- the Banking and Other Financial Institutions Act 2004;
- the Financial Reporting Council of Nigeria Act 2011;
- the International Financial Reporting Standards;
- the Central Bank of Nigeria (Establishment) Act 2007; and
- the National Deposit Insurance Corporation Act 2006.

Regulations

- The Codes of Corporate Governance for Banks in Nigeria and Discount Houses, issued by the Central Bank of Nigeria (CBN);
- the Guidelines for Risk Management Framework for Licensed Pension Operators, issued by the National Pension Commission;
- the Code of Good Corporate Governance for the Insurance Industry in Nigeria, issued by the National Insurance Commission;
- the Nigerian Stock Exchange Listing Requirements;
- the Securities and Exchange Commission (SEC) Rules and Regulations;
- the SEC Code of Corporate Governance;
- the SEC Code of Conduct for Shareholders' Associations;
- the Nigerian Communications Commission Code of Corporate Governance for telecommunication companies; and
- Credit Bureau Regulations issued by the CBN.

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

The primary target of rules related to risk and compliance management are banks and other financial institutions, companies listed on stock exchanges and other, non-listed, public companies.

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

There are numerous regulatory and enforcement bodies with responsibilities for corporate compliance in Nigeria, with the principal ones including the following:

- The CBN is vested with the overall control and administration of monetary and financial sector policies of the federal government. It is empowered to carry out routine examinations of banks and other financial institutions and to demand and receive information in respect of their operations. It also has extensive powers to sanction banks and other financial institutions.
- The Corporate Affairs Commission (CAC) is responsible for the administration of the CAMA. The functions of the Commission are to administer the CAMA, in particular, the regulation and supervision of the formation, incorporation, registration, management and winding-up of companies; the establishment and maintenance of a company's registry with suitably and adequately equipped offices in all the states of the federation to discharge its functions under the CAMA or any other law in respect of which it is charged with responsibility; and to arrange or conduct investigations into the affairs of companies where the interests of shareholders and the public demand.
- The functions of the Financial Reporting Council of Nigeria (FRCN), as stated in the Financial Reporting Council of Nigeria Act 2011, include the enforcement and approval of the 'compliance with accounting, auditing, corporate governance and financial reporting standards in Nigeria'. In the performance of these functions, it has been given widely stated powers that have been the source of some controversy, such as, for example, the extent of its powers to regulate the manner in which audit firms present reports of private companies.
- The National Deposit Insurance Corporation was established to insure all deposit liabilities of licensed banks and other deposit-taking institutions operating in Nigeria. It is mandatory for licensed financial institutions to insure their deposits with the Corporation.
- The Department of Petroleum Resources is an agency of the Ministry of Petroleum, established to supervise and regulate the petroleum industry in Nigeria. It enforces safety and environmental regulations and ensures that those operations conform to national and international industry practices and standards. It processes all applications for petroleum sector-related licences so as to ensure

compliance with laid-down guidelines before making recommendations to the Minister of Petroleum Resources.
- The Economic and Financial Crimes Commission was established under the Economic and Financial Crimes Commission (Establishment) Act 2004. Under the Anti-Money Laundering Act, the commission receives suspicious transaction notifications from financial institutions.
- The SEC was created under the Investment and Securities Act 2007. The Commission regulates and develops the Nigerian Capital Market. The commission also scrutinises the capital market with the mandate of ensuring orderly and equitable dealings in securities and protecting the market against insider trading abuses.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

As indicated above, there are no specific laws and regulations that define 'risk management' or 'compliance management'. The definitions relied on are based on a combination of corporate governance legislation and regulatory bodies' codes and regulations.

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

They are set out, to a somewhat limited extent, in various regulations and laws as general provisions by which relevant organisations are bound.

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

As discussed above, there is no uniform set of risk and compliance standards applicable to all Nigerian companies. By legislation passed in 2011, the National Assembly created the FRCN. The functions of the FRCN under the statute include:
- developing and publishing accounting and financial reporting standards to be observed in the preparation of financial statements of public interest entities;
- reviewing, promoting and enforcing compliance with the accounting and financial reporting standards adopted;
- receiving notices of non-compliance with approved standards;
- receiving copies of annual reports and financial statements of public interest entities from preparers;
- advising the federal government on matters relating to accounting and financial reporting standards;
- maintaining a register of professional accountants and other professionals engaged in the financial reporting process;
- monitoring compliance with the reporting requirements specified in the adopted code of corporate governance;
- promoting compliance with the adopted standards issued by the International Federation of Accountants and the International Accounting Standards Board;
- monitoring and promoting education, research and training in the fields of accounting, auditing, financial reporting and corporate governance;
- conducting practice reviews of registered professionals;
- reviewing financial statements and reports of public interest entities;
- enforcing compliance with the legislation and the rules of the FRCN on registered professionals and the affected public interest entities;
- receiving, in advance of publication, copies of all qualified reports, together with detailed explanations for such qualifications, from auditors of the financial statements, along with the power to prevent publication of the financial statements until all accounting issues relating to the reports are resolved by the FRCN;
- adopting and keeping up-to-date accounting and financial reporting standards, and ensuring consistency between standards issued and the International Financial Reporting Standards;
- specifying, in the accounting and financial reporting standards, the minimum requirements for recognition, measurement, presentation and disclosure in annual financial statements, group annual financial statements, or other financial reports by all public interest entities, in the preparation of financial statements and reports; and
- developing or adopting and keeping up-to-date auditing standards issued by relevant professional bodies and ensuring consistency between the standards issued and the auditing standards and pronouncements of the International Auditing and Assurance Standards Board.

The granting of such wide functions and powers on such a body, not unexpectedly, created tensions between the FRCN and auditors, the Institute of Chartered Accountants of Nigeria, the Association of National Accountants of Nigeria, public companies, large private companies, public interest entities (defined in the legislation as 'governments, government organisations, quoted and unquoted companies and all other organisations that are required by law to file returns with regulatory authorities and this excludes private companies that routinely file returns only with the Corporate Affairs Commission and the Federal Inland Revenue Service'), and numerous other bodies.

In addition to these tensions, there was also widespread dissatisfaction with the provisions in the legislation that enabled the FRCN to impose levies on registered professionals (publicly quoted companies) based on market capitalisation, and on public interest entities based on turnover.

After skirmishes in 2014–2016 between the FRCN and auditors of banks, directors of banks that the FRCN purported to suspend or remove from office, and a former governor of the CBN, the executive secretary of the FRCN was dismissed in January 2017. A new executive secretary was appointed, along with a chairman. The three Corporate Governance Codes, for the private, public and not-for-profit sectors, issued in October 2016 were suspended. A committee was established in January 2018 to review the suspended codes and to develop and recommend the revised Code(s). The issue as to what is the lawful extent of the powers of the FRCN remains unaddressed.

In the interim, the various other regulatory bodies have retained a certain level of freedom to impose their own guidelines. These tend to be strongly influenced by international standards. Common to virtually all bodies is a requirement for a compliance officer to be appointed and for there to be a risk management committee.

The general nature of the main standards and guidelines regarding risk and compliance management processes can be seen from regulations issued by the CBN in respect of banks and other financial institutions, which is probably the most regulated sector in Nigeria. The CBN regularly issues regulations and guidelines that set standards that undertakings regulated by it must follow. These include updating qualification requirements of chief compliance officers and specifying standards required for risk management procedures.

The guidelines that come from the CBN are largely influenced by international agreements and independent advisory bodies such as the Financial Action Task Force. Currently, CBN guidelines require banks and other financial institutions to adhere to the following:
- there must be a chief compliance officer (CCO). Initially, it was required that there be one for each branch, but this was relaxed to allow one to serve clusters of branches;
- the CCO must report directly to the board and must have the status of at least a general manager;
- the CCO must in addition to a minimum education requirement have training in an international standard;
- there must be a risk management committee;
- with regard to the finance industry, there are different standards that banks may use in their risk management procedures; these are based on international standards and there is an implication that, with preapproval from the CBN, there is flexibility in acceptable standards;
- there are different risk management standards prescribed by the CBN for different kinds of transactions and actions such as accepting new customers, providing credit services for individuals and providing credit services for companies;
- additionally, the CBN issues extensive manuals detailing procedures required for compliance with legislation; and
- every financial institution is required to have a comprehensive anti-money laundering/combating financial terrorism (AML/CFT) compliance programme to guide its compliance efforts and to ensure the diligent implementation of the CBN manual.

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

Generally, there is a requirement for the appointment of a compliance officer who reports directly to the board. However, the specifics vary

from industry to industry as no uniform set of rules and regulations currently exist. Nevertheless, it would appear that the general requirements are that the compliance officers have specialised knowledge, independence from management and report directly to the board of directors.

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

As addressed above, Nigeria does not have a singular set of risk and compliance management obligations. Financial institutions are regulated by the CBN, which has issued numerous regulations. The only obligation that applied to all corporations whether public, private, financial or non-financial, is the requirement for the appointment of a compliance or risk management committee/officer to oversee the compliance protocols of the organisation. Frequently, such officers are required to be part of senior management and to have direct reporting lines to the board of directors. Other obligations are sector-specific.

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

As mentioned above, obligations vary from industry to industry. As the banking industry is the most developed this answer will focus on that. Obligations for the banking industry include:

- AML/CFT compliance is ultimately the responsibility of the board/senior management;
- an AML/CFT compliance manual must be formulated by the management and presented to the board for consideration and formal approval;
- senior management approval is required before establishing business relationships with politically-exposed persons;
- where a customer has been accepted or has an ongoing relationship with the financial institution, and the customer or beneficial owner is subsequently found to be, or becomes, a politically-exposed person, the financial institution is required to obtain senior management approval in order to continue the business relationship;
- in relation to cross-border and correspondent banking and other similar relationships, in addition to performing the normal customer due diligence measures, financial institutions must obtain approval from senior management;
- an employee training programme under the guidance of the compliance officer in collaboration with senior management is required;
- the board and senior management may be investigated for their roles in contravention of the provisions of the AML/CFT manual produced by the CBN; and
- on the second contravention of the CBN's AML/CFT manual, responsible parties including but not limited to members of the board and senior management will be blacklisted from working in the financial services industry, and the officers penalised shall be reflected in the institution's financial statements and published in the newspapers.

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

In circumstances where there are deficiencies in risk and compliance management, and such deficiencies occasion loss or injury to third parties, undertakings responsible for causing such loss or injury will have civil liability to the affected third parties.

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

Failure to observe laws and regulations normally result in either administrative or penal consequences for deficient undertakings. The consequences are dependent upon the legislation and regulations involved. In some circumstances, the consequences are entirely administrative and in others, they are penal and require formal prosecution and conviction before they can be applied. Examples of administrative sanctions include the imposition of administrative fines where companies fail to file requisite returns with the CAC within stipulated time frames. The failure of financial institutions to maintain minimum capital ratios at all times carries administrative penalties including, but not limited to, the prohibition of the institution from advertising for, or accepting, new deposits, and the revocation of the institution's operating licence. The SEC has the power to prohibit an organisation from trading in particular securities if it deems that action to be necessary for the protection of persons buying and selling the particular securities.

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

Criminal liability is imposed by some statutory provisions for risk and compliance management deficiencies. Examples include criminal sanctions to risk and compliance regulators or other bodies indicated in the legislation under the Anti-Money Laundry Act for failure to provide information, or for the provision of inaccurate information. The Banks and Other Financial Institutions Act also provides criminal sanctions, fines, and terms of imprisonment for certain management.

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

Civil liability for governing bodies in breach of compliance management obligations exists in relation to certain specific statutory offences. For example, section 85 of the Investment and Securities Act 2007 allows all persons who suffer damages as a result of subscribing for shares or debentures after relying on a prospectus that contains untrue misleading information, to seek damages from any director of the company at the time of the issue of the prospectus or any person who consented to be named and is named in the prospectus as a director. The act also extends this liability to employees of the company who participate in or facilitated the production of the prospectus.

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

In certain circumstances, members of governing bodies and senior management may be sanctioned for regulatory deficiencies of their organisations. An example of this is section 16(4) of the Anti-Money Laundering Act that provides that if there is a serious oversight or flaw in its internal control procedures owing to a financial institution's or the compliance officer at management level's failure, the disciplinary authority responsible for the financial institution or the person's professional body may take disciplinary action against the financial institution and the responsible individuals. Administrative consequences vary from dismissal to a complete ban from operating within that industry. Section 16(1)–(3) of the Anti-Money Laundering Act holds that a director or employee of a financial institution, who destroys or removes a register or record required to be kept, may be banned indefinitely, or for a period of five years, from practising the profession that provided the opportunity for the offence to be committed.

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

Individuals may face criminal liability for the breach of risk and compliance management obligations. Examples of such liability can be found in the CAMA, the Banks and Other Financial Institutions Act, the Food and Drugs Act, and several other statutes.

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

At present, there are no provisions in any statutes or regulations that enable the existence of compliance regimes to exculpate undertakings or individuals.

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

In October 2017, the SEC ordered the Nigerian Stock Exchange (NSE) to suspend trading of the stock of Oando plc. The suspension was as a result of complaints from two shareholders, who held over 70 per cent of the company's issued equity. It was alleged that the chairman of the company's board had mismanaged the company and the complaint sought his removal and the postponing of the company's annual

general meeting until after an examination of the company's activities. The SEC investigated the activities of the company and concluded that the company was in breach of a number of risk and compliance regulations, including rules against related party transactions and insider trading. On 9 April 2018, there were reports in the media that the SEC had directed that the suspension be lifted. Trading resumed on 12 April, following a statement by the SEC that said 'the SEC directed NSE to lift technical suspension and allow market determination of the share price'. A forensic audit is ongoing.

The FRCN imposed a fine of 1 billion naira (approximately US$5 million) against Stanbic IBTC, the Nigerian affiliate of the South African Bank, Standard Bank. In addition, the FRCN announced the suspension of several senior officials of the bank, including its chairman. These sanctions were imposed as a result of alleged misstatements in the bank's 2015 financial report. The sanctions were eventually lifted, following a private agreement between the bank and the FRCN, under which the bank was able to publish its 2015 financial report at the end of 2016.

MTN, Nigeria's largest mobile telephone operator, announced on 26 October 2015, that it had been fined 1.04 trillion naira (approximately US$5.2 billion) by the Nigerian Communication Commission (NCC) for failure to ensure that active SIM cards on its network were registered. Nigerian regulations require that every active SIM card on a Nigerian telephone network is registered to an individual, whose photograph and fingerprints are recorded against the SIM. MTN allegedly failed to disconnect unregistered SIMs, some of which the NCC claimed were being used by criminal groups such as the Boko Haram insurgents. Following negotiations, it was announced on 10 June 2016, that MTN was permitted to pay a reduced fine of 330 billion naira. In addition, MTN was required to make a public apology to the Nigerian government and the people of Nigeria. The NCC stated that it was necessary to impose a fine high enough to signal to MTN and other mobile telephone operators that it would not be 'business as usual' for the mobile service provider that was required to pay such a fine.

First Bank of Nigeria, United Bank for Africa and Skye Bank were fined 1.9 billion naira, 2.9 billion naira and 4 billion naira, respectively. The fines were announced via CBN circulars on 26 October 2015 for First Bank and United Bank for Africa, with the announcement of Skye Bank's fine coming on 9 November 2015. These fines were for delays in transferring government funds to the Treasury Single Account with the Central Bank of Nigeria as required by regulations introduced in 2012 by the Goodluck Jonathan administration. These regulations had only been partially implemented prior to President Buhari taking office in May 2015 and one of the first administrative steps taken by the Buhari administration was the full implementation of the policy.

Guinness Nigeria, an affiliate of Diageo plc, was fined 1 billion naira by the National Agency for Food and Drug Administration and Control (NAFDAC) on 9 November 2015 'as administrative charges for various clandestine violations of NAFDAC rules, regulations and enactments over a long period of time'. Guinness was also accused by the agency of revalidating expired products without authorisation and supervision by NAFDAC, as well as failing to secure the gate of its warehouse, allowing raw materials used in the production of beer and non-alcoholic beverages by the firm to be permanently open to intrusion and exposure to the elements and rodents, which would 'invariably affect the integrity of the raw materials'. Ultimately it was announced on 11 March 2016 that the issue had been settled out of court. As part of the resolution, NAFDAC would be present during the destruction of the expired raw materials in its rented warehouse and both parties agreed that this would be the procedure for the exercise in future. Guinness Nigeria also agreed to pay administrative and service charges to NAFDAC to cover the cost of the investigative inspection of raw materials carried out by the Agency, as well as for the supervision by NAFDAC of the destruction of the raw materials that would be carried out by Guinness Nigeria.

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

Some government agencies have risk and compliance obligations. An example of such can be found in the legislation relating to the Asset Management Corporation of Nigeria (AMCON), a government agency established in the wake of bank failures with the specific remit of removing non-performing loan assets from the balance sheets of banks in Nigeria. Under section 7 of AMCON's establishment act (Asset Management Corporation of Nigeria Act 2011) the agency is required to keep books of all transactions in compliance with CBN rules. While the AMCON legislation makes no provisions for sanctions, the application of CBN rules would appear to subject AMCON to the same rules, obligations and sanctions that apply to financial institutions.

Part 15 of the Investment and Securities Act applies to government agencies seeking to raise finance on the capital market. Such bodies, when seeking to raise finance on the market, have the same disclosure obligations as other entities seeking the same and would appear to be subject to the same governance, and sanctions, regime.

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

There do not appear to be any key compliance differences between public sector and private sector compliance management obligations.

Sofunde Osakwe Ogundipe & Belgore
legal practitioners

Babajide Ogundipe **boogundipe@sooblaw.com**
Olatunde Ogundipe **oaogundipe@sooblaw.com**
Olajumoke Omotade **ooomotade@sooblaw.com**

7th Floor
St Nicholas House
Catholic Mission Street
PO Box 80367
Lafiaji Lagos
Nigeria

Tel: +234 1 4622502
Fax: +234 1 4622501
www.sooblaw.com

Russia

Alexey Borodak and Sergey Avakyan
Norton Rose Fulbright (Central Europe) LLP

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Together with the growth and complicated nature of the Russian economy, businesses in Russia essentially need to create effective models of managing the risks related to compliance, using applicable laws and regulations. It is believed that the concept of compliance started to develop in Russia in the early 2000s, and has obtained particular legal meaning in Russia only during recent years.

Nonetheless, the reasons for establishing corporate risks and compliance management systems within Russian organisations vary and still do not relate altogether to the obligatory statutory requirements.

The main spheres that are commonly subject to compliance management in Russia are anticorruption; antitrust; combating money laundering and terrorism financing; and personal data protection. Compliance itself is a broad concept and needs to be clarified and narrowed for the purposes of this overview.

Since Russian legislation and regulations provide extremely limited guidance on requirements for implementing risk management and compliance measures within the abovementioned spheres, this chapter shall selectively deliberate over these spheres.

In general, risk and compliance management in Russia remains more integrated with the financial public sectors, and with those corporations that are dealing with international markets, rather than with purely local market players.

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

There are only few acts in Russia that provide risk and compliance-related requirements, or guidelines describing a basis for building up respective management systems within entities in Russia. Among them are the following main specialised statutes, that impose obligations on performing risk and compliance management within the entities:

- Federal Law No. 273-FZ On Combating Corruption, dated 25 December 2008 (article 13.3);
- Federal Law No. 115-FZ On Combating Money Laundering and the Financing of Terrorism, dated 7 August 2001;
- Federal Law No. 39-FZ On Securities Market, dated 22 April 1996 (article 10.1);
- Federal Law No. 414-FZ On Central Depositary dated 7 December 2011 (article 8); and
- at the same time, lots of rules of law that indirectly form a framework of risk and compliance management activity in Russia are represented by administrative, criminal or other sanctions and are set down in the Code of Administrative Offences or the Criminal Code of the Russian Federation.

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

Russian legislation has not yet ventured deeply into regulation of the undertakings that may be referred to risk and compliance management. This particularly relates to entities such as limited liability companies.

Meanwhile, joint stock companies have comparatively more guidance with respect to risk management and compliance, compared to limited liability companies. This has been the case since the adoption of the model Corporate Governance Code – a document introduced by the Central Bank of Russia in 2014 that is aimed at building up the general compliance principles within joint stock companies and listed companies.

Regarding risk and compliance management frameworks, the most heavily regulated sphere is still the financial sector. Thus, risk and compliance management regulations within credit organisations are constantly being adopted by the Central Bank of Russia (eg, the regulations on internal control in credit organisations and bank groups issued by the Central Bank of Russia on 16 December 2003).

In 2013, the Central Bank of Russia introduced the Basel III principles that provide governance for the capital adequacy calculations of Russian banks and require implementation of risk management procedures. The principles are aimed at improving the financial standing of Russian credit organisations and bringing Russian banking regulation closer to internationally recognised standards.

In 2016, the Central Bank announced its initiatives in active development regarding the institution of compliance practices (abiding by the code of corporate ethics; combating money laundering and financing of terrorism; regulating conflicts of interest; confidentiality compliance; the policies of Chinese walls; etc) for national financial institutes.

In December 2017, the Central Bank introduced an informational letter on applying a risk-oriented approach when combating money laundering and financing of terrorism, which suggests guidelines to all financial institutions with respect to risk and compliance control in order to comply with Financial Action Task Force recommendations.

Among common undertakings mentioned within Russian legislation, or often voluntarily undertaken by Russian organisations, are the following:

- designation of departments, structural units and officers responsible for the prevention of bribery and related offences;
- adoption of protocols on cooperating with law enforcement authorities;
- development and implementation of policies and procedures designed to ensure ethical business conduct;
- adoption of a code of ethics and professional conduct for the employees; and
- creating policies for identifying, preventing and resolving conflicts of interest.

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

Since there are almost no pure and complex compliance obligations imposed by Russian legislation, along with the compliance framework that leads to specific liability of the non-complying entities, most of the regulatory and enforcement bodies that may be related to corporate compliance control have a common scope of powers that varies depending on the nature of each body and its purpose.

Said powers typically consist of administrative discretions (powers of providing obligatory instructions, controlling and supervisory powers, powers of withdrawing licence or suspending the activity of particular entity, initiating cases on administrative offences, etc) or criminal ones (these fully belong to investigative authorities such as the investigative committee, Ministry of Internal Affairs, etc).

Bearing in mind the aforementioned scope of legislation that can be directly or indirectly related to corporate compliance, the following main regulatory and enforcement bodies can be mentioned:

- the Central Bank of Russia;
- the Public Prosecutors Office of the Russian Federation;
- the Federal Antimonopoly Service;
- the Federal Financial Monitoring Service (Rosfinmonitoring); and
- the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor).

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

Compliance itself is not yet legally defined in Russia. In the meantime, there are certain statutory provisions that show their influence on risk and compliance management activity within the entities.

Anti-corruption compliance

A comparably new article 13.3 to the Federal Law No. 273-FZ On Combatting Corruption dated 25 December 2008 requires all companies in Russia to develop and adopt measures aimed at preventing corruption. Although article 13.3 lists six broadly defined measures that companies may develop and adopt, it does not describe the steps companies should take to implement those measures, neither the law does explain whether the above measures are either mandatory or exclusive.

The 'all possible measures' provision, contained in article 13.3, can be interpreted to extend the requirements of Federal Law No. 273-FZ On Combating Corruption, to go even beyond the common requirements of the Foreign Corrupt Practices Act or the UK Bribery Act.

Anti-money laundering compliance

Federal Law No. 115-FZ On Combating Money Laundering and the Financing of Terrorism was enacted on 7 August 2001 in compliance with the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, signed in Strasbourg, France, which was ratified by Federal Law No. 62-FZ, dated 28 May 2001.

Said statute contains criteria for the volume of operations subject to mandatory control, lists those operations and determines the organisations conducting operations with money or other property that should inform an authorised agency about these operations, which, among others, mainly include credit organisations.

As a main aim, the law requires credit organisations to take all reasonable and available measures to identify the beneficial owners of their clients. However, this law does not provide the list of particular measures or guidelines that the credit organisations must follow regarding the identification process of the beneficial owner of the client. A non-exhaustive list of such measures is set out in the clarifications issued by Rosfinmonitoring and the Central Bank

Antitrust compliance

In Russia, discussion of the concept of antitrust compliance started around 2011, and by 2013 the Federal Antimonopoly Service had included antitrust compliance into their strategy and into the independent direction of further work. It has been declared as a priority development aim of the antitrust legislation and law enforcement practice due to its preventive function.

The Federal Antimonopoly Service recently developed a draft law aimed at implementation of special compliance measures within entities, that shall possibility lead to mitigating liability that arises out of antitrust violations.

Data protection compliance

Federal Law No. 152-FZ On Personal Data dated 27 July 2006 regulates all personal data that is processed by data operators or third parties in Russia. Personal data under the said law is represented by any information (directly or indirectly) related to an identified or identifiable individual (data subject).

Data protection laws apply to all data operators, and third parties acting under the authorisation of data operators. A data operator can be represented by a legal entity or individual that both:

- organises or carries out (alone or jointly with other persons) the processing of personal data; and
- determines the purposes of personal data processing, the content of personal data and the actions (operations) related to personal data.

The main obligations imposed on data operators to ensure the personal data is processed properly are the following:

- defining the categories of personal data, the purposes of data processing and the duration of processing;
- obtaining the data subject's consent (unless otherwise provided by the law);
- appointing a data protection officer, adopting the data protection policy (and other required documents) and taking other appropriate security (especially technical and organisational) measures to prevent unauthorised or unlawful data processing and a breach of the data protection legislation; and
- notifying Roskomnadzor of various circumstances for the purposes of registration (unless otherwise provided by the law).

According to the described statute, since 1 September 2015 all personal data operators shall be required to keep personal data of Russian citizens in Russia. Namely, it requires that databases that store personal data should be kept on servers on Russian territory. This requirement has quickly become an element of internal compliance of probably most of the businesses in Russia.

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

In general, risk and compliance management processes are usually not set out within the Russian legal framework. At the same time, the financial and public sectors may be the exception to said conclusion.

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

Unfortunately, there is no single legal source containing requirements, guidelines or recommendations on performance of risk and compliance management by entities in Russia.

The Corporate Governance Code could be mentioned in addition to the specialised legislation given in question 2.

The Central Bank of the Russian Federation approved the new version of the Corporate Governance Code on 21 March 2014. The Corporate Governance Code represents a set of voluntary principles and recommendations on corporate governance for joint-stock companies – primarily those that are subject to listing.

Although compliance with the Corporate Governance Code is not mandatory, a company that wishes to list on a stock exchange shall usually need to comply with the Corporate Governance Code.

Notwithstanding the fact that the Corporate Governance Code is primarily recommended for application within the joint stock companies and listed companies, all types of entities are free to refer to this document as a means of guidance.

The Corporate Governance Code regulates the following spheres:

- shareholder rights and the fair treatment of shareholders;
- the board of directors;
- the corporate secretary;
- incentive arrangements (remunerations and payments to directors, the CEO and key management);
- risk management and internal controls;
- disclosure of information; and
- certain important corporate actions, for example, material transactions, reorganisations, mergers and acquisitions, the listing and delisting of shares and increases of share capital.

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

Many entities incorporated in Russia that have a foreign participation in their charter capital tend to satisfy the compliance-related requirements of the foreign jurisdictions. Such situations often result in Russian entities adopting compliance policies and other related measures that are similarly complex and effective such as, for example, those in the United States, the European Union or the United Kingdom.

Notwithstanding the fact that the Russian legislation in general does not prescribe the obligatory rules for adopting such measures and standards of the latter, their voluntary implementation positively

affects the business activity of such entities and provides chances for exemption from liability, or at least mitigating it.

At the same time, no forms of entities are deprived from the option to establish certain internal corporate policies or regulations that impose obligations regarding compliance governance within such an entity. Compliance governance may therefore become one of the functional obligations (or even the primary one) of the board member(s) or other corporate bodies of the legal entity. Obligatory division of the compliance governance obligations within legal entities is, however, not yet prescribed by the existing legislation.

Meanwhile, if compliance obligations are not directly delegated to certain persons within the legal entity (board members or employees), under the general rule the liability for violating the compliance obligations would mainly lie with the entities' CEO.

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

As mentioned in question 3, in general, there are no pure risk and compliance management-related obligations established in Russia; however, those that are recommended and effectively accepted by the businesses are as follows:

- designation of departments, structural units and officers responsible for the prevention of bribery and related offences;
- adoption of protocols on cooperating with law enforcement authorities;
- development and implementation of policies and procedures designed to ensure ethical business conduct;
- adoption of a code of ethics and professional conduct for the employees; and
- creating policies for identifying, preventing and resolving conflicts of interest.

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

A member of the entity's management shall ensure that the company fully complies with its public law obligations. Therefore, for instance, if the entity breaches its legal obligations due to its CEO's bad faith or unreasonable actions or omissions that resulted in company losses, such losses may be recovered from the CEO. The company will be restricted from indemnifying the CEO for his or her actions or omissions that result from the company's breach of its public law obligations.

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

Entities or individuals may, in general, be held liable for the violation of civil law obligations that consist of compliance requirements arising out of the contracts or existing under law.

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

Anti-corruption compliance

The administrative liability of legal entities for corruption offences has been introduced to the Code of Administrative Offences by Federal Law No. 280-FZ of 25 December 2008 in view of ratification of the United Nations Convention against corruption (UNCAC) of 31 October 2003, the Criminal Law Convention on corruption (Strasbourg, 27 January 1999) and the adoption of the Federal Law On Counteracting Corruption.

Article 19.28 of the Code of Administrative Offences provides for the liability for illegal transfer, proposal or promise of property valuables to a domestic official or an authorised representative of a commercial or any other entity, as well as to an official of a public international organisation on behalf or in the interests of a legal entity, and unlawful rendering thereto of monetised services. The article provides for two qualifying elements: large-scale and extra-large-scale with regard to committed actions (equivalent to illegal gratification in the amount of 1 million roubles and 20 million roubles respectively). In 2016, article 2.6 of the Code of Administrative Offences was added with a new part, determining that a foreign legal entity that committed, outside the Russian Federation, an administrative offence provided for by article 19.28 of the Code of Administrative Offences, which was aimed against the interests of the Russian Federation, is subject to administrative liability on a common basis. The limitation period for liability for the offence provided by article 19.28 of the Code of Administrative Offences is equal to one of the maximum periods established by the Code of Administrative Offences – six years after the committed offence.

Currently, the minimal amounts of liability (1 million roubles, 20 million roubles and 100 million roubles) are provided for transfer, proposal or promise of illegal gratification on behalf or in the interests of a legal entity. Furthermore, article 19.28 provides for obligatory confiscation of money, securities, other property or cost of monetised services and other property rights constituting the subject of gratification.

Application of article 19.28 of the Code of Administrative Offences interprets an offence committed in the interest of a legal entity as an action by result of which a legal entity attains any business goals; satisfies its current or potential needs; achieves any benefits or advantages; or relief (mitigation) of liability or obligations. A Russian law enforcer therefore has a wide range of instruments for demonstrating the involvement of a legal entity in corruption offence.

Despite the fact that voluntary actions undertaken by a company to prevent corruption actions by its employees are not always taken into consideration by the law-enforcing bodies, due implementation of such measures may be one of the few defences of a legal entity in court. Legislative initiatives aimed at reforming of the practice of use of article 19.28 of the Code of Administrative Offences testify to the fact that the main condition for mitigation of or relief from liability may be active cooperation with the law enforcement authorities aimed at efficient investigation of the corruption offence.

Nevertheless, it is important that the company and its structural subdivisions are responsible when fulfilling their duties as envisaged by article 13.3 of Federal Law No. 273-FZ On Counteracting Corruption, aimed at development and application of anticorruption measures. An integrated approach is required for the organisation of internal control and creation of an efficient system for prevention of corruption, for example, by introducing compliance programmes as well as readiness for a prompt legal defence of one's interests if the law enforcement authorities bring any charges.

Antitrust compliance

A main financial sanction that may be imposed by Federal Antimonopoly Service in Russia is an administrative fine. The amount of such fine may range from 1 per cent to 15 per cent of a company's annual turnover in the affected market (0.3 per cent to 3 per cent for price-regulated markets and 'mono-product' companies), and in case of collusion relating to public tenders, 10 per cent to 50 per cent of the starting price of the affected tender. One common feature of all such fines is that they are issued pursuant to the Code of Administrative Offences, and the Code expressly provides that administrative liability is fault-based. This means that a company may be held administratively liable – and be ordered to pay a fine – only if the unlawful conduct (anticompetitive behaviour in this instance) was the fault of the company.

Personal data protection compliance

Breach of the established legal order for the collection, storage, use or distribution of personal data may entail the following administrative sanctions:

- warning or administrative fine, 300–500 roubles (for individuals);
- warning or administrative fine, 500–1,000 roubles (for officials); or
- warning or administrative fine, 5,000–10,000 roubles (for legal entities).

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

For the purposes of this question, it should be borne in mind that, according to the Criminal Code of the Russian Federation, only individuals may be subject to criminal liability.

Anti-corruption compliance

Anti-corruption related criminal offences set out in the Criminal Code of Russia include:

- receiving a bribe (article 290);
- bribing an official (article 291); and
- completing commercial bribery (article 204).

These articles were clarified and detailed in the summer of 2016.

Antitrust compliance
Article 178 of the Criminal Code of the Russian Federation establishes criminal liability for cartel activities that prevent, restrict or eliminate competition.

Personal data protection compliance
Under article 137 of the Criminal Code of the Russian Federation, unauthorised and illegal collection or distribution of personal data or privacy data may lead to the following criminal sanctions:

- a criminal fine of up to 200,000 roubles;
- salary amount for the period of 18 months;
- forced labour for 360 hours;
- correctional works for 12 months;
- compulsory works for two years, with or without disablement for three years;
- arrest for four months; or
- imprisonment for up to two years.

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

In 2013, the Supreme Arbitrazh Court of the Russian Federation issued Decree No 62 on losses recovery from management bodies of a legal entity directly allowing the possibility to recover from a company's management losses that became a result of that management's abuse of its power.

Generally, board members and CEOs in Russia are directly liable to the company and indirectly liable to shareholders for actions performed in bad faith or unreasonably against the interests of the entity. CEOs and board members are, by default, not liable to third parties. Management must prove that their actions and decisions were made in good faith and in the company's best interest.

Additionally, the CEO bears subsidiary liability for company debts in case of its insolvency if:

- he or she fails to submit the petition when the company becomes insolvent; or
- his or her acts or omissions cause the company's insolvency.

The aforementioned causes of insolvency may as well be connected to the failures on risk and compliance management of the respective entity.

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

Yes, the CEO and responsible members of management also bear personal administrative liability for a sufficient number of administrative offences. Personal administrative liability of the entity's management may, in general, entail fines, dismissal or disqualification.

Under the Code of Administrative Offences, the management of the entity (whose duties include responsibility for compliance procedures of the company) may incur personal administrative liability for each violation of the statutory regulations, performed by the entity.

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

Under the Criminal Code of the Russian Federation, any person who is governing the activity of the entity (including the CEO and members of the management board who are responsible for compliance issues) can be held criminally liable for any violation of statutory provisions that constitute a criminal offence. Criminal sanctions in such cases may include a fine, community service or imprisonment.

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

Unfortunately, there are still no provisions of the Russian legislation that establish compliance as the universal means of defence for any type of liability (however, the opposite initiatives are being actively discussed in the sphere of antitrust compliance).

In the meantime, most applicable legal sources of sanctions contain provisions that lead the investigating authority to consider the compliance measures performed by the entity or by the certain individuals as the mitigating circumstances (article 4.2 of the Code of Administrative Offences of the Russian Federation and article 61 of the Criminal Code of the Russian Federation).

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

It appears that most demonstrative cases of liability that follow failures within an organisation and its performance of risk and compliance management relate to the sphere of recent supervising activity of the Central Bank of Russia, and to the application of article 19.28 of the Code of Administrative Offences described above.

Thus, a poor system of compliance and internal control within a credit organisation has appeared as one of the substantive grounds for withdrawing the bank licence of JSC Regional Commercial Bank in September of 2016 (see Order of the Central Bank of Russia dated 19 September 2016 No. OD-3139).

In a meantime, failure to prove that a bribe was not given by the employee for the benefit of his employer, and absence of any compliance procedures within the respective legal entity, did not set the grounds for applying mitigating circumstances by the public prosecutor office in case of CJSC Grinn under article 19.28 of the Code of Administrative Offences in 2012. This resulted in a fine of approximately US$1.1 million together with the confiscation of a bribe of around US$700,000.

NORTON ROSE FULBRIGHT

Alexey Borodak **alexey.borodak@nortonrosefulbright.com**
Sergey Avakyan **sergey.avakyan@nortonrosefulbright.com**

White Square Office Center
Butyrsky Val str 10, Bldg A
Moscow 125047
Russia

Tel: +7 499 924 5101
Fax: +7 499 924 5102
www.nortonrosefulbright.com

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

Usually, with the participation of the state, entities tend to establish a variety of internal compliance management procedures and policies as prescribed by the statutes governing the activity of such entities (see Rosatom, Rosavtodor, Rostekh and others).

At the same time, broad incorporation of such measures also relates to the financial sector and the Central Bank of Russia (see the Risk Management Policy of the Central Bank of Russia).

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

The main difference is that the rules prescribing the necessity to establish compliance and internal control in the public sector are binding for the entities, and involve state participation. At the same time, adoption of such measures in the private sector has not yet become obligatory (except for credit organisations and related entities).

Spain

Helena Prieto González, Beatriz Bustamante Zorrilla, Marta Sánchez Martín and Alejandro Ayala González

Garrigues

1 What legal role does corporate risk and compliance management play in your jurisdiction?

The legal role that corporate risk and compliance management plays in the Spanish jurisdiction is defined by article 31-bis Spanish Criminal Code (CC). It is noteworthy that the legal framework for corporate risk and compliance management is laid down in a criminal law, but the two amendments to the CC (Organic Law 5/2010 and Organic Law 1/2015) introducing the criminal liability of legal entities are the main milestones in the jurisdictional handling of both corporate risk and compliance management.

Although the CC adopts a 'comply or explain' approach, in fact, any legal entity – no matter its size or if it is listed or not – that wishes to invoke the exoneration of corporate liability or a mitigating circumstance if a crime is committed by one of its managers or employees must have a corporate compliance system in place that meets the requirements laid down by article 31-bis CC.

Moreover, Law 31/2014 of 3 December, on the change of Corporate Enterprises for the improvement of corporate governance, imposes on directors a specific duty of corporate risk control, so that directors may be held liable, as guarantors, for the offences committed by the employees, on the basis of commission by omission.

In addition to this, listed companies are also affected by the Good Governance Code of Listed Companies (2015) that states the basic principles of the corporate compliance systems, also using a 'comply or explain' approach. Unlike the CC, the Good Governance Code of Listed Companies is considered as 'soft law'.

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

The following laws and regulations address corporate risk and compliance management:

- article 31-bis of the Spanish Criminal Code;
- Law 10/2010 of 28 April on prevention of money laundering and terrorist financing, and Royal Decree 304/2014 of 5 May on the regulation on the prevention of money laundering and terrorist financing;
- article 193.2 of the Stock Market Act, and Circular 1/ 2014 of the National Stock Exchange Commission (CNMV) for investment services companies; and
- Good Governance Code of Listed Companies issued by CNMV.

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

The following are the primary types of undertakings:

- under CC: every legal entity regarding criminal offences that may be committed in Spain or is committed outside Spanish territory can be prosecuted in Spain according to the law. The legal regimen is less demanding for small businesses (those that, pursuant to the applicable legislation, are authorised to submit an abbreviated profit and loss statement);
- under the Good Governance Code: every listed company; and
- under the Stock Market Act: investment services companies (financial institutions included).

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

The main enforcement bodies are as follows:

- Prosecution Office: enforcement of the Criminal Code under Circular 1/2016 of the Attorney General's office;
- SEPBLAC: Law 10/2010 of 28 April on prevention on money laundering and terrorist financing, and Royal Decree 304/2014 of 5 May on the regulation on the prevention of money laundering and terrorist financing;
- CNMV: enforcement of the Good Governance Code of listed companies; and
- CNMV and Bank of Spain: enforcement of sector-specific regulation for investment services companies and financial institutions.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

No. There are no definitions of these concepts but the requirements of a criminal compliance programme are defined under article 31-bis 5 CC, as explained below (see question 7).

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

Risk management and compliance management are defined by criminal, administrative and commercial laws and regulations.

From a criminal law perspective, the CC does not establish the obligation to have a compliance programme or specific compliance processes, although the due implementation of this type of programme or process has been configured in Spanish criminal law as an exonerating or mitigating circumstance.

In order to be able to appreciate this circumstance, compliance programmes must comply with conditions and requirements as explained below (see questions 7 and 17).

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

Requirements applying to organisational and management models are defined under article 31-bis 5 CC:

- the requirement to identify activities within the scope of which the crimes to be prevented may be committed – the 'criminal risk map';
- the requirement to establish protocols or procedures setting out the process by which the legal person reaches consensus, takes decisions and implements those decisions by reference to those protocols or procedures (code of conduct, compliance policy, organisational model, internal compliance system, etc);
- the requirement to have appropriate models for the management of financial resources in order to impede the commission of the crimes to be prevented;
- the requirement to impose an obligation to report possible risks and breaches to the body charged with overseeing the functioning of, and compliance with, the prevention model (an internal complaints channel);
- the requirement to establish a disciplinary system that appropriately penalises breaches of the measures established by the model

(infringements of the compliance system and the associated penalties); and
- the requirement to conduct a periodic review of the model and to amend it in the event of significant breaches or changes in the organisation, control structure or business pursued (internal or external audits; 'ongoing improvement').

Other standards and guidelines related to management processes are:
- ISO 31000 (2009): with regard to risk management, it states principles and guidelines and provides principles, frameworks and a process for managing risks;
- ISO 19600 (2014): concerning compliance management, it provides guidance for establishing an effective and responsive compliance management system within an organisation;
- ISO 37001 (2016): regarding anti-bribery management systems, it specifies requirements and provides guidance for establishing an anti-bribery management system; and
- UNE 19601 (2017): concerns criminal compliance management systems based on the CC.

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

In accordance with article 23 of the Organic Law of the Judiciary, Spanish courts will be competent to prosecute the crimes committed in the Spanish territory, regardless of the nationality of the originator. Therefore, undertakings domiciled or operating in Spain could be investigated or prosecuted by the Spanish courts, and the risk and compliance governance obligations will be the same as those established for Spanish undertakings.

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

The CC establishes a closed list of criminal offences that can be committed by legal entities. These specific criminal offences are:
- trafficking in, and the unlawful transplantation of, human organs (156-bis CC);
- trafficking in human beings (177-bis CC);
- prostitution and corruption of minors (189-bis CC);
- discovery and disclosure of secrets (197-quinquies CC);
- fraud (251-bis CC);
- criminal insolvency (258-ter and 261-bis CC);
- IT damage (264-quarter CC);
- crimes relating to intellectual and industrial property (270–272 CC and 273–277 CC);
- crimes relating to the markets and consumers (270–280, 281, 282, 282-bis, 283, 284, 285, 286 and 288 CC);
- corruption in business dealings (286-bis and 286-quarter CC);
- money laundering (302 CC);
- unlawful funding of political parties (304-bis CC);
- crimes against the public finance and social security authorities (310-bis CC);
- crimes against the rights of foreign citizens: unlawful trafficking or people smuggling (318 CC);
- planning crimes (319 CC);
- crimes against natural resources and the environment (325 CC);
- catastrophe hazard crimes (343 and 348 CC);
- crimes against public health (369-bis CC);
- forgery of credit cards, debit cards or travellers checks (386 and 399-bis CC);
- bribery (427 CC);
- misuse of public office (430 CC);
- incitement to commit acts of discrimination, hate or violence against groups (510 CC);
- terrorist financing (576-bis CC); and
- goods smuggling (the Anti-Smuggling Organic Law).

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

Regarding the risk and compliance management obligations of members of governing bodies and senior management, from the criminal law perspective, these bodies have three different obligations:
- periodic verification of the effectiveness and compliance of the compliance programmes and processes;
- supervision and control of the effective implementation of the compliance programmes and processes; and
- reception and investigation of the complaints formalised as a consequence of the violation of the crime prevention and control measures.

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

The imposition of criminal liability on undertakings is compatible with any civil liability for the loss and damage that the offence may have caused, and any other type of civil or administrative liability that may be imposed on the corporate entity or the individual. When convicted, undertakings face civil direct liability jointly with the individual for the crime committed.

This civil action, improperly said to derive from the crime, does not emanate from the crime, but rather from illicit acts or omissions (not necessarily criminal) that produce unjust negative consequences or damages. That is, the civil liability for which one responds in the criminal proceedings is the ordinary extra contractual civil liability resulting from acts or omissions that cause prejudicial results. Thus, both case law and commentary in Spain have unanimously recognised that the possible joint exercise of the criminal and civil actions must not lead us to forget that both have distinct characteristics and that the civil action derived from the crime (or to be rigorous, the damages caused by the crime) is governed by rules and principles of its own.

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

The Good Governance Code of listed companies approved by the board of the CNMV on 22 May 2006, and updated on 18 February 2015, does not regulate the application of administrative or regulatory sanctions if the recommendations are not followed. However, the 'comply or explain' principle became part of statute law under article 116 of Law 26/2003 by introducing a duty to publish an annual corporate governance statement reporting on the degree of compliance with corporate governance recommendations and, where appropriate, explaining any departure from such recommendations.

Under provisions of Law 10/2014 of 26 June 2014 on the regulation, supervision and solvency of credit institutions (Title IV, additional provision 14th and transitional provision 1st), the Bank of Spain may impose sanctions in relation to serious or very serious infringements for lack of compliance including regulated corporate governance procedures. The disciplinary and sanctioning system covers institutions and their directors or administrators.

Spanish regulations on money laundering (Law 10/2010 of 28 April on prevention on money laundering and terrorist financing, and Royal Decree 304/2014 of 5 May on the regulation on the prevention of money laundering and terrorist financing) establish the obligation for subject parties (article 2 of the Law) to have adequate prevention procedures and bodies. Article 26 of Law 10/2010 sets out which internal control obligations should be implemented. Sepblac (Spain's financial intelligence unit and anti-money laundering supervisory authority) is legally empowered to require information and documentation from all reporting entities. Failure to comply with these legal obligations constitutes an administrative offence under Chapter VII, articles 50–62 of Law 10/2010 without prejudice to those laid down as crimes in the CC.

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

In the cases provided for in the CC, legal persons shall be criminally liable (article 31-bis 1):
- for crimes committed in their name or their behalf, and to their direct or indirect benefit, by their legal representatives or by parties who, acting individually or as members of a body of the legal person, are authorised to take decisions in the name of the legal person or hold powers of organisation or control within said legal person; and
- for crimes committed in the course of corporate business, and for their account and to their direct or indirect benefit, by parties who, while subject to the authority of the natural persons referred to in

the preceding paragraph, were able to commit the acts as those natural persons seriously breached the duties of supervision, oversight and control of their activities, having regard to the specific circumstances of the case.

Whenever an undertaking is convicted for deficiencies of risk and compliance management, they face a mandatory penalty of a fine at a stipulated rate or on a proportional basis. Additionally, courts may impose optional penalties such as:

- winding up of the undertaking;
- suspension of the business (up to five years);
- closure of premises and establishments (up to five years);
- ban on engaging in any of the business activities in which the crime was committed, prompted or concealed (temporary up to 15 years or permanent);
- disqualification from obtaining public aid and subsidies, from entering into public sector contracts and from taking tax or social security benefits or incentives (up to 15 years); or
- court supervision to safeguard the rights of employees or creditors for as long as is deemed necessary, which may not exceed five years.

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

As explained in question 11, within a criminal proceedings civil actions can be exercised against the individual or the company responsible for the offence committed. Moreover, Capital Companies Law imposes, among other things, duties of diligent management on directors. This means that, generally speaking, directors' liability (civil law in nature from the shareholders or directors as regards damages) arises when the directors, having infringed the law, the bylaws or the duties inherent in their office have caused economic damage, provided that there is causation between the infringement committed by the directors and the damage caused to the company.

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

As explained above, under provisions of Law 10/2014 of 26 June 2014 on the regulation, supervision and solvency of credit institutions (Title IV, additional provision 14th and transitional provision 1st), the Bank of Spain may impose sanctions in relation to serious or very serious infringements for the lack of compliance with the obligations on corporate governance procedures regulated. The disciplinary and sanctioning system covers institutions and their directors or administrators (de facto or de iure).

Also, under article 54 of Law 10/2010 of 28 April, on prevention on money laundering and terrorist financing, in addition to the liability corresponding to the obliged person even by way of simple failure to comply, those holding administrative or management positions in the latter, whether sole administrators or collegiate bodies, shall be liable for any breach should this be attributable to the latter's wilful misconduct or negligence.

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

Yes, they do if they participate directly in the crime committed by the legal person as explained in question 13.

Moreover, the involvement of the person in the criminal act on which the attribution of criminal liability is based on must be interpreted broadly and encompasses both active forms of involvement (through an action in the strict sense) and passive forms (through passivity or the failure to do something required). According to article 31-bis 1b), CC governing bodies and senior management can transfer liability to undertakings when their subordinates commit criminal offences when carrying out their corporate activities and on their account and to their direct or indirect benefit, because the duties of supervision, surveillance and control of their activities were gravely breached by them. So members of governing bodies and senior managements may face criminal liability for breach of risk and compliance management, but this requires not only the breach of risk and compliance management but also that the manager can be found liable on the basis of commission by omission, according to article 11 CC.

In other words, they may be held liable if they failed to prevent offences from being committed by employees or officers within the company, being in a position of guarantor, when the requirements of omission to action are met and their omission is thus equivalent to an action. As laid down in Law 31/2014 of 3 December on the change of corporate enterprises for the improvement of corporate governance, they now have a specific legal duty of control of the company's activities and its risks (duty of corporate control). This results in a position of guarantor in terms of preventing crimes from being committed within the company. Both the CC and this law should be interpreted jointly to make an assessment of criminal liability of governing bodies and managers.

The delegation of duties by directors to third parties, including the compliance officer, should not mean that directors become fully exonerated in favour of the delegated party. Moreover, if the members of governing bodies and senior management fail to prevent offences from being committed because of poor performance of their duty of corporate control, the exoneration of corporate liability cannot be invoked by the company.

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

Article 31-bis 2 CC, establishes the grounds for a legal person to be exempted from liability when the crime is committed by those indicated in subparagraph a) of section 1 of article 31-bis CC, that is, by those that make decisions in the name of the legal person or hold powers of organisation or control within said legal person (ie, sole director, directors acting severally, joint directors, board of directors, executive committee and managing directors). This means that, if all the conditions contained in this article are fulfilled, the legal person shall be exempt from criminal liability.

These requirements are (article 31-bis 2 CC):

- the managing body must have actually adopted and implemented, prior to the commission of the crime, an organisational and management model incorporating suitable measures of oversight and control to prevent crimes of the same nature or to significantly reduce the risk of such crimes being committed;
- perpetrators must have committed the crime by fraudulently evading such models;
- supervision of the functioning of, and compliance with, the prevention model in place must be entrusted to a body within the legal entity that has standalone powers of initiative and control or on which statute has conferred the function of supervising the effectiveness of the internal controls of the legal entity; and
- there must not have been any omission or defective discharge of the functions of supervision, oversight and control of the body referred to.

The partial accreditation of these conditions could be considered as a mitigating circumstance.

When the criminal offence were perpetrated by those subject to the authority of those indicated in subparagraph a) of section 1 of article 31-bis CC, that is, by subordinated employees, the legal person shall be exempted from liability if, before the perpetration of the criminal offence, it has adopted and effectively implemented an organisational and management body to prevent criminal offences of the nature of the one perpetrated or to reduce in a significant way the risk of the perpetration thereof.

Additionally, there are certain circumstances when criminal liability of legal persons can be mitigated after the commission of the criminal persons. For this mitigating circumstance to be applicable, the legal person, through its legal representatives, should carry out the following activities:

- confess the criminal offences to the authorities before having knowledge of the initiation of judicial proceedings;
- collaborate with the investigation of the facts once the judicial proceedings have been initiated providing decisive evidences; and
- prior to the trial itself, endeavour to repair or decrease the damaged caused, or establish measures to prevent and discover the commission of criminal crimes by the company in the future.

This corporate compliance defence only applies for the company itself, and not for the employees. Therefore, the proceedings may continue to investigate or judge the individual's criminal responsibility.

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

Firstly, there have not been enough sentences regarding corporate risk and compliance management by companies in Spain. This is basically because, even if the introduction of legal entities criminal responsibility occurred in 2010, Spain's judicial procedure is very slow and most of the cases are still under investigation; only a few of them have been tried. That being said, and while some provincial courts have issued sentences concerning this matter, the leading case law comes from cases that the Supreme Court have reached.

So far, the Supreme Court has only issued a few sentences. The most important would be the following:

- The first one, dictated on 2 September 2015, was related to a fraud crime and concerned the criminal responsibility of companies. It indicated that any conviction of a company must comply with the basic principles of criminal law. Hence, the importance of this judgment is that it considers that companies are subject to the application of the principles of criminal law within a criminal proceeding where an individual is affected. However, the failure risk and compliance management was not assessed.
- On 29 February 2016, the Supreme Court dictated a sentence that, in relation to a drugs offence case where there were no compliance measures, states that constitutional rights and guarantees also apply to legal persons. Moreover, it indicates that the nature of criminal liability of companies is of self-responsibility meaning that, unlike the state prosecutor's criteria, which understand that a compliance system is configured as an absolutory excuse, the presence of appropriate mechanisms of control implies the very inexistence of the crime. The judgment also considers that the accusing parties should prove that there were not any instruments of compliance to avoid the commission of the crime and, additionally, that liability has to be established on the basis of the analysis of whether the offence committed by the individual under the wing of the legal entity (body corporate or legal person) has been facilitated by the absence of a 'culture of respect for law', which should be demonstrated in concrete ways (tangible manifestations or forms) of surveillance and control.
- According to another acquittal sentence dictated on 16 March 2016, the public prosecutor should make the same prosecutor effort for legal persons as for individuals, as they are subject to two different prosecutions, each being liable for their own offence. Even if the system is vicarious, that does not mean that criminal principles become secondary – all of the guarantees must be fulfilled.
- On 13 June 2016, another sentence from the Supreme Court rejected an appeal against an acquittal because, at the time when the offences were committed, article 31-bis had not been signed. There was no criminal liability allocated to the legal person from the prosecuting parties. It also states that an accusation against the legal person does not exclude the liability of the individual acting as its representative where there are elements of participation of the individual. The legislator has chosen a vicarious system, responding each of them separately.
- Another illuminating sentence was the one issued on 21 June 2017. Although it was not the case or even a key point of the resolution, the Supreme Court highlighted that, in order to convict a legal person, the crime must have been committed not only in the course of corporate business and for its account but also to its direct or indirect benefit. Therefore, the legal person cannot be held criminally liable if it was aggrieved and adversely affected by the crime, even when it was committed in the course of corporate business and for its account.
- The sentence issued on 19 July 2017 has not been seen as being as important as those previously mentioned. However, it sheds a light on different issues. It rules about a legal person's domicile, standing that its scope is the one stipulated by article 554.4 of the Criminal Procedure Act, whether or not the legal person is being investigated by a court. The sentence also implies that mitigating circumstance consisting of undue delays might be applied to legal persons (a question which had not been clear for commentary). Moreover, the resolution points out that in order to set aside the legal persons' right to presumption of innocence it is necessary to prove beyond a reasonable doubt three items:
  - the crime has been committed on its behalf by:
    - (i) their legal representatives;
    - (ii) by parties who, acting individually or as members of a body of the legal person, are authorised to take decisions in the name of the legal person or hold powers of organisation or control within said legal person; or
    - (iii) by parties subject to the authority of natural person referred to in (i) and (ii);
  - the crime has been committed to their direct or indirect benefit; and
  - the legal person has not implemented organisational and management models according to conditions established under article 31-bis 5 CC (see question 7).

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

According to article 31-quinquies CC, criminal liability of legal persons cannot be applied to territorial and institutional Public Administrations, to the Regulatory Bodies, to Public Agencies and Corporate Entities, to international organisations under Public Law, or to others that exercise public powers of sovereignty or administration. Additionally, this article states that in the case of state mercantile companies that implement public policies or provide services of general economic interest, they can only be subject to fine penalties or judicial intervention. If the legal form was established in order to elude criminal liability, the investigating court or judge can consider that the limitation is not applicable.

GARRIGUES

Helena Prieto González **helena.prieto@garrigues.com**
Beatriz Bustamante Zorrilla **beatriz.bustamante@garrigues.com**
Marta Sánchez Martín **marta.sanchez.martin@garrigues.com**
Alejandro Ayala González **alejandro.ayala@garrigues.com**

Hermosilla, 3
28001 Madrid
Spain

Tel: +34 91 514 52 00
Fax: +34 91 399 24 08
www.garrigues.com

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

As a consequence of the details given in question 19, those government bodies or agencies or stated-owned enterprises not included in the list of article 31-quinquies face the same risk and compliance management obligations as all private legal persons. For instance, political parties and trade unions were initially excluded from being criminally liable until 2012 when the CC was modified in order to include their potential liability.

Some public bodies, such as the Spanish Federation of Municipalities and Provinces, have developed internal good practice standards even if they are not potentially liable for criminal responsibility. This is an example of integrity compliance and ethical practices beyond the bounds of legislation.

Switzerland

Daniel Lucien Bühr and Marc Henzelin

Lalive

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Since the onset 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, disregarding conflicts of interest or ignoring anti-money laundering compliance, or manufacturers doing business in a manner that distorts the level playing field. These cases have triggered an endless stream of new regulations in Switzerland over the past decade. Many new regulations address integrity, governance, risk or compliance management challenges, directly or indirectly. And, of course, Switzerland, with its small domestic market surrounded by the European Union, must align its legislation with EU rules and international standards that have also become broader and more detailed. As a result of these national and international legal developments, guaranteeing that an organisation meets its compliance obligations has become a challenging task for which responsibility ultimately lies with the board of directors.

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's responsibility for compliance with the law throughout the entire company. in addition, article 102 of the Swiss Criminal Code (SCC) requires 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, together with their related ordinances, stipulate a range of 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 government's Financial Market Supervisory Authority (FINMA) regularly publishes non-binding circulars. For instance, in connection with risk and compliance management measures, FINMA explained corporate governance for banks and insurance companies and how banks should manage liquidity risks. The latter circular clarifies what the Liquidity Ordinance states regarding the minimum qualitative requirements for the way banks handle liquidity risk.

Other legally non-binding recommendations concerning internal controls, risk and compliance management were issued in 2014 by economiesuisse, the Swiss Business Federation, in its policy paper 'Fundamentals of effective compliance management'. This is the reference document on 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 with legal forms other than a public limited company) in practice follow the guidance given by the Swiss Code.

In October 2016, the Corporate Responsibility Initiative was handed in to the Federal Chancellery. The initiative, a request for a direct democracy vote by citizens, aims to ensure that companies with registered offices, headquarters or a main place of business in Switzerland, and their boards, are held accountable for any violation of human rights and environmental standards in Switzerland or abroad. The initiative is encountering criticism from multinationals, but ultimately Swiss voters will decide whether it is adopted.

Technological developments have also led to new compliance requirements, for instance for initial coin offerings and the issuing of cryptocurrencies. FINMA has taken a first step and in February 2018 it published a regulatory framework for initial coin offerings.

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 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 as yet not 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 all major legal risks to FINMA. FINMA issues ordinances and circulars and regularly publishes decisions and guidance on legal requirements for financial institutions, in particular the standard of professional diligence and best practice risk and compliance management.

The OAG, cantonal prosecutors and criminal courts enforce article 102 SCC, under which a company may be held criminally liable for failing to take all necessary and reasonable organisational (compliance) measures to prevent certain key crimes, such as bribery and money laundering. It is important to bear in mind that under the SCC a company may be fined up to 5 million Swiss francs, and have illicit profits confiscated. The cantonal and federal prosecutors play an increasingly significant role as enforcers of adequate corporate compliance. With its landmark case against Alstom in November 2011, the OAG developed its practice of effectively prosecuting companies that violate article 102 SCC for 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 2.5 million Swiss francs, was obliged to disgorge profits of 36.4 million Swiss francs.

On 1 January 2016, a memorandum of understanding on cooperation between FINMA and the OAG came into force, based on article 38 of the Federal Act on the Swiss Financial Market Supervisory Authority (FINMASA). This memorandum highlights the growing importance for Swiss enforcement agencies to exchange information and cooperate to combat corruption. FINMA's main task is the prudential supervision of institutions it has authorised to engage in financial market activities. The OAG, on the other hand, is the federal agency competent for prosecuting criminal acts with an inter-cantonal or cross-border dimension.

The federal and cantonal prosecutors are responsible for conducting criminal investigations and bringing charges for money laundering. Financial intermediaries and traders that suspect assets stem from a felony or misdemeanour or belong to a criminal organisation must notify the money laundering reporting office which may, in turn, notify the criminal prosecutor, which actually happens in about 70 per cent of cases. The OAG has recently opened a number of criminal investigations against Swiss banks for violating anti-money laundering and anti-bribery statutes.

With regard to COMCO, businesses are sanctioned (under administrative law) if they engage in cartels or illicit vertical restraints, abuse a dominant market position, or 'gun jump' to bypass merger control regulations. For example, one of COMCO's most recent high-profile probes concerned around 20 international banks for fixing the LIBOR, TIBOR and EURIBOR interest rates, with the banks ultimately fined a total of approximately 100 million Swiss francs in December 2016. Other recent COMCO activities include fining one of Switzerland's largest telecommunications companies, Swisscom, in connection with 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 Swiss legislation. However, international standards are increasingly being 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 its benchmarks should a company raise the compliance defence against a sanction.

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

Swiss legislation does not describe risk and compliance management processes specifically. There are, however, certain provisions that stipulate the precautions to be taken in that regard. For instance, article 728a CO states that the external auditor must examine whether an internal control system exists and must take it into account when determining the scope of the audit and during the audit procedure. Furthermore, the external auditor must ensure that the internal control system includes an adequate risk management 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 Organizations 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 (which, taken together, constitute the risk assessment process) and risk treatment. ISO Standard 19600 sets out the compliance responsibilities at all levels of an organisation, together with the procedure for 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, businesses 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 businesses domiciled in Switzerland as well as to any businesses operating in Switzerland if they have legal or compliance employees located in Switzerland. In both cases, the company is liable for its global business conduct.

Swiss law also sets out the duties that are specific to the board and inalienable. Under article 716a CO, the board's inalienable duties are the ultimate leadership and oversight of the company, including compliance with applicable laws.

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 company in the exercise of its business and in accordance with its purpose, the felony or misdemeanour is attributed to the company if it is not possible to attribute this act to any specific natural person as a result of inadequate (compliance) organisation by the company. In case of serious felonies (such as bribery), the company is criminally liable irrespective of the liability of any natural person, if the company has failed to take all necessary and reasonable organisational measures required to prevent such an offence.

In the banking sector, articles 3f and 3g BankA and 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 728b CO).

Under articles 717 and 754 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 requires the members of the board of directors or of the executive board to 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 companies if the damage has been caused by employees or other auxiliaries who were not diligently selected, instructed and supervised or if the company does not prove that the employer took all necessary precautions to prevent 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?

One example of administrative consequences for risk and compliance management deficiencies is the sanctions set out in article 49a of the CartA. In case of infringements against the CartA, companies can raise the compliance defence, in other words they can produce evidence that the infringement occurred despite the company'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 (eg, ISO 19600 and Organisation for Economic Cooperation and Development and International Chamber of Commerce guidelines). If a company successfully raises the compliance defence, it will not suffer sanctions.

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
- revoking of licences and compulsory liquidation.

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

Update and trends

Corporate Switzerland is facing a series of crises owing to increasing regulation and tighter controls by the authorities. A number of first-tier companies and public entities have recently been confronted with governance and compliance failures. By way of example, in February 2018, the public transport subsidiary of Swiss Post (PostAuto Schweiz AG) was accused of accounts and records violations from 2007 to 2015, with the intention of illegally obtaining at least 90 million Swiss francs in public subsidies for the operation of its regional transportation services.

The major investigative trend is that Swiss and foreign companies in all sectors are now more often targeted by criminal investigations on the basis of suspected organisational failure to prevent bribery and money laundering. In addition, employees at all levels who have either actively committed or passively turned a blind eye to fraud, mismanagement, corruption and money laundering are now systematically investigated. International cooperation has also been stepped up in 2017, notably with Brazil, France, Germany, Greece, Italy, the Netherlands, Spain and the United States.

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

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

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

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 any intentional or negligent breach of their duties of diligence. One of their key statutory responsibilities is to ensure compliance with the law by all employees. It is important to note that it is 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) that can be held liable, but also factual members of governing bodies who have not been formally appointed, yet exercise significant influence over 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 and regulatory consequences should they fail in their duty of diligence. FINMA can take administrative or regulatory measures against managers, such as disqualifying a director, adding a manager to a watchlist and issuing a business conduct letter. FINMA can enter an individual's information in a database known as the watchlist if the individual's business conduct is questionable or does not meet the legal requirements. The watchlist is used for assessing relevant information for compliance prerequisites, namely personal details; excerpts from commercial, debt enforcement and bankruptcy registers; criminal, civil and administrative court decisions; and reports by auditors and third-parties appointed by FINMA. Furthermore, under specific circumstances, FINMA can send a business conduct letter to those registered in the watchlist. A business conduct letter does not qualify as a decision; it merely states that FINMA reserves the right to review compliance with the diligence requirements should the manager change position. In the event of a disqualification, FINMA may ban individual directors 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 are criminally liable if they fail to implement effective risk and compliance management and turn a blind eye to mismanagement (article 158 SCC), embezzlement (article 138 SCC), money laundering (article 305-bis SCC) or bribery (article 322-ter et seq SCC), and so on. Failure to prevent serious criminal offences, such as bribery, is a corporate crime (see questions 9 and 13).

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

Under article 102(2) SCC, a company is criminally liable for certain felonies committed by its employees if it has not implemented the necessary and adequate (compliance) measures to prevent them. The burden of proof for the inadequacy of the compliance measures rests with the prosecutor or court. Nevertheless, the defendant company will want to establish that it has implemented all necessary and adequate compliance measures. To do this, the company will need to submit evidence regarding its compliance policy, its good compliance governance, the overall compliance management system, the procedures involved in the compliance management system, the measurement of the system's effectiveness, regular reporting to senior management, and continual improvement.

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

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

In August 2015, the OAG opened criminal proceedings against two former officials at 1MDB and against unknown persons based on the suspicion of bribing foreign public officials (article 322-septies SCC), misconduct in public office (article 314 SCC), money laundering (article 305-bis SCC) and criminal mismanagement (article 158 SCC). In April 2016, the investigation was extended to two former officials who had been in charge of Abu Dhabi sovereign funds. They are suspected of fraud (article 146 SCC), criminal mismanagement (article 158 SCC), misconduct in public office (article 314 SCC), document forgery (article 251 SCC), bribery of foreign public officials (article 322-septies SCC) and money laundering (article 305-bis SCC).

Further to the substantial number of *Petrobras/Lava Jato*-related investigations, the OAG convicted Brazilian company Odebrecht SA and its subsidiary Braskem in December 2016 for organisational failure to prevent the bribery of foreign officials and money laundering under article 102(2) SCC. The OAG stated that Odebrecht SA had created slush funds throughout the world to pay bribes to government officials, representatives and political parties in a bid to obtain business and projects from state-owned companies. As a result, Odebrecht SA was fined 4.5 million Swiss francs and was obliged to disgorge profits of more than 200 million Swiss francs. A number of banks have been affected by the *Petrobras/Lava Jato* investigations and filed suspicious-activity reports. This led to follow-up investigations in 2017 against individuals, such as a banker in Brazil.

The year 2017 saw the first settlement in a case of self-reporting to the OAG of suspected failure to prevent bribery of foreign officials. The reporting company was fined a symbolic amount of one Swiss franc in consideration of its timely self-reporting, full cooperation in the investigation and its substantial remediation. The OAG also set a compensatory claim of 35 million Swiss francs (disgorgement of illicit profits). The investigation took 13 months and illustrates the benefits of self-reporting.

Another notable example is the first conviction in the World Football's governing body, FIFA investigation, in which a former Swiss banker was convicted of failing to file mandatory money-laundering reports, and the opening of a new FIFA-related bribery investigation against the former secretary-general of FIFA and the CEO of a media group in connection with the granting of World Cup media rights for events up to 2030.

Other key cases are the ongoing investigation of a pharmaceuticals company for alleged bribery in Greece, investigations into a major Swiss bank for its alleged involvement in a Venezuelan bribery scandal and its recruitment practices in Asia, and in October 2017 FINMA opened an investigation into the Raiffeisen Group and its former CEO for suspected corporate governance and conflict of interest issues.

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

When it comes to corporate criminal liability, the SCC does not differentiate between private and public companies. Within the meaning of article 102(4) SCC, the German term *Unternehmen* includes entities under both private and public law. Swiss state-owned companies such as cantonal banks, hospitals, telecommunications providers, energy suppliers, 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 in the event of employee misconduct.

The government and all government agencies are obliged to conduct themselves in accordance with the statutes under which they are established and governed. These statutes all require the government and government bodies to meet 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 in both the private and public sector. All organisations must introduce and maintain best practice (legal) risk management systems and compliance management systems. The main difference between private sector and public sector obligations is the overall purpose, which for public sector organisations covers the smooth running of government and the maintenance of citizens' trust, and for private sector companies covers such items as the protection of employees, shareholders and creditors.

LALIVE

Daniel Lucien Bühr **dbuhr@lalive.ch**
Marc Henzelin **mhenzelin@lalive.ch**

Stampfenbachplatz 4
PO Box 212
8042 Zurich
Switzerland
Tel: +41 58 105 2100
Fax: +41 58 105 2160

Rue de la Mairie 35
PO Box 6569
1211 Geneva 6
Switzerland
Tel: +41 58 105 2000
Fax: +41 58 105 2060

www.lalive.ch

Turkey

Ümit Hergüner and Zeynep Ahu Sazcı Uzun
Hergüner Bilgen Özeke Attorney Partnership

1 What legal role does corporate risk and compliance management play in your jurisdiction?

In parallel with the global trend, corporate risk management and legal compliance have become an area of significant importance in Turkey.

Legislative developments in regulated industries have laid the foundation for the legal framework of risk and compliance management issues. The financial sector has always had a direct impact on risk and compliance management in terms of the economy, where ensuring stability in the management of sector players and minimising management risks are two primary goals. Along with close supervision of the regulatory authorities, the first regulations on risk management and legal compliance were adopted at the sector level. In recent years, Basel III criteria has become increasingly important and various new banking regulations have been adopted in an attempt to harmonise the Turkish legal framework with the European standard of risk management for capital adequacy, liquidity coverage ratios, mitigating credit risks, risk assessment models and measurement of market risk.

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

Since corporate risk and compliance management matters are not organised under a single source of law, the rules and principles can be found scattered across various pieces of legislation that set general standards and touch upon both civil and criminal liabilities arising from risk and compliance management failures for corporations and individuals.

Privately held companies

The Turkish Commercial Code (TCC), published in 2012, is the general set of rules applicable to all companies, listed and privately held alike, which rests on four main principles: transparency, equality, accountability and responsibility. It governs board duties and accountability, introduces a clear cut distribution of liability, requires the formation of early risk detection committees and allows a more transparent system for the benefit of all stakeholders through mandating annual activity reports, company websites and electronic shareholders' meetings.

Failure to comply with these rules can lead to civil liabilities for the board of directors and the management of a privately held company. As further detailed below, compliance failures could also lead to criminal liability on the part of the board of directors (as the governing body) or the management of a privately held company. White collar crimes such as bribery, fraud, money-laundering of criminal proceeds and embezzlement are the main white collar corruption offences that would trigger criminal liability as per the Turkish Criminal Code (the Criminal Code), applicable to all individuals within companies regardless of whether they are privately held, listed or regulated.

Listed companies

For listed companies, the main source of law is Corporate Governance Principles Communique No. II. 17-1 (the Corporate Governance Communique) issued by the Capital Markets Board (CMB). The Corporate Governance Communique aims to enhance corporate governance mechanisms and risk and compliance management systems for listed companies. The communique provides 20 mandatory corporate governance principles that listed companies must abide by, making an exception for small groups that remain below certain thresholds in terms of overall market value and the market value of floating shares. The mandatory principles mainly focus on maintaining efficient disclosure mechanisms and transparency, appointing independent directors, and forming committees including those monitoring risk and corporate governance compliance within the board of directors.

Owing to their inherent nature, listed companies benefit from a higher level of scrutiny by regulatory authorities as opposed to privately held companies not active in a regulated sector. Therefore, any failure to comply with these principles would be more easily detected in terms of civil or criminal liability.

For listed companies, in addition to the offences exemplified above for privately held companies, the Capital Markets Code also names certain white collar crimes leading to criminal liability, including insider trading and market manipulation, that are specifically applicable to listed companies.

Banks

For banks and other actors in the financial services sector, the main piece of legislation is Banking Code No. 5411 (the Banking Code). The Banking Code sets forth the principles and procedures to establish confidence and stability in financial markets, effective functioning of the credit system, and the protection of the rights and interests of depositors. The regulatory authority, the Banking Regulation and Supervision Agency (BRSA), is entitled to deliver secondary legislation for these issues. For compliance and risk management, the Regulation on Banks' Internal Systems sets forth the rules for establishing internal control, internal audit and risk management systems for banks by specifying various types of risks and how to mitigate and process such risks.

Insurance companies

Insurance Code No. 26551 (the Insurance Code) requires insurance and reinsurance companies to establish an effective internal control system, covering internal audit and risk management, in order to monitor compliance with the legislation, internal directives, management strategy and policies, and to prevent fraudulent acts and irregularities in all transactions.

As data protection is one of the current trending topics in Turkey, duties of the board of directors and senior management to ensure the protection of customer and employee personal data are of increasing importance. The laws on personal data are governed by the Code on the Protection of Personal Data. The Code allows companies to retain and process customer and employee personal data only after obtaining explicit consent (save for specific exceptions).

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

While Turkish legislation does not make a distinction between different types of undertakings in terms of risk and compliance management rules and principles, regulated entities (eg, listed companies, banks, insurance companies and other financial institutions) have a stricter list of obligations.

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

Privately held companies

Privately held companies that are not active in a regulated sector and therefore do not enjoy the close scrutiny of a regulatory authority are usually monitored by their shareholders, board of directors, management, creditors or customers. Compliance issues can be raised by these constituents and may lead to civil or criminal liability by reference to courts depending on the nature of the problem.

For market competition matters, the Turkish Competition Authority is the main authority that oversees compliance with Turkish competition regulations. It can, among other things, conduct investigations, issue administrative fines for non-compliance and review merger and acquisition transactions for approval.

Also, there are authorities focused on other fields of compliance. For instance, the Board of Protection of Personal Data is authorised to oversee the protection and legal processing of individual personal data.

Listed companies

The CMB is the regulatory and supervisory authority for listed companies, intermediary institutions, portfolio management companies and other capital markets institutions. For both listed companies and capital markets institutions, the CMB issues secondary legislation (ie, CMB communiques) that govern areas of law varying from corporate governance rules to financial reporting. In order to enhance enforcement mechanisms for listed companies in terms of compliance, the CMB is equipped with broad intervention powers. For example, in the case of a compliance violation, the CMB is authorised to issue administrative fines, seek judicial orders to invalidate non-compliant transactions where the company failed to comply with mandatory principles, seek injunctive relief, withdraw activity permits and signatory authorities, replace board members, order to restore compliance or ban trading.

Banks

The BRSA is the regulatory body focused on banks and banking activities. In the case of non-compliance with banking regulations, the BRSA is authorised to initiate criminal investigations by filing with the public prosecutor, issuing administrative fines, forcing non-compliant institutions to cease activity, or issuing and cancelling permits that are required to carry out banking activities.

For Criminal Code violations, legal proceedings are carried out by the Turkish criminal courts where public prosecutors act ex officio. In relation to crimes that are governed by specific pieces of legislation (eg, crimes listed under the Banking Code), public prosecutors initiate criminal proceedings by filing with the relevant authority (eg, BRSA for banking crimes listed under the Banking Code).

For the prevention of money laundering and financing of terrorism, the Financial Crimes Investigation Board (MASAK) is the regulatory body established in 1997 that has the authority to monitor financial institutions that are active in capital markets, insurance, banking and other financial services sectors. The relevant legislation provides a list of individuals and entities from different occupational groups that are obliged to conduct know-your-customer tests and inform MASAK of suspicious transactions. The list includes, among other entities, banks, insurance and pension companies, sports clubs, public notaries and certified accountants. Accordingly, MASAK is authorised to examine suspicious transaction reports and any documents and records of a company to ensure compliance with the Code on Prevention of Money Laundering. In the existence of concrete evidence indicative of money laundering activities, MASAK can also initiate criminal investigations through filing with the public prosecutor.

Insurance companies

For insurance and reinsurance companies, the regulatory body is the Undersecretariat of the Turkish Treasury (the Undersecretariat). The Undersecretariat is authorised to issue and cancel activity permits if the company fails to comply with certain requirements.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

Turkish legislation does not set forth an explicit definition for the terms 'risk management' and 'compliance management'. However, the pieces of legislation mentioned in question 2 seem to collectively recognise risk and compliance management principles as a means of running effective and transparent operations within a company and emphasise institutions such as risk detection committees, activity reports and board liability rules.

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

In general, the laws and regulations set out major requirements for risk and compliance management processes (eg, formation of risk detection committees, publishing corporate governance compliance reports), but the details are left for the company to tailor. However, in line with the global trend, more comprehensive rules and procedures have been introduced particularly in the financial services sector as explained in question 7 below.

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

Privately held companies

The TCC introduced the concept of 'early risk detection' as a measure to be taken by an early risk detection committee to foresee and mitigate risks. Privately held companies exceeding certain thresholds and, therefore, subject to independent audit requirements, may be required to immediately form a committee upon written request from an independent auditor if considered necessary. This committee is obliged to issue their first risk determination report within one month of formation.

Privately held companies are also free to adopt risk and compliance management processes inspired by those available at listed or regulated companies (detailed below).

Listed companies

For listed companies, compliance with corporate governance principles stands out as an important requirement of the CMB. As per the comply-or-explain principle, listed companies are required to prepare annual corporate governance compliance reports, annexed to the annual activity reports, and to disclose to what extent they comply with the CMB's corporate governance principles. These principles deal with a large range of topics including risk management.

Under the TCC, companies listed on the stock exchange are obliged to establish a specialised committee for the early detection of risks or threats jeopardising the existence, development and continuation of the company. These committees must also implement any measures necessary to manage these risks.

Under the Corporate Governance Principles Communique, listed companies, excluding banks, are obliged to establish early risk detection committees. Formation of these committees is not obligatory for banks since internal control mechanisms (explained below) cover this function. Early risk detection committees report to the board of directors once every two months and alert the directors of any potential risks or threats that the company may face in order to allow directors to take any necessary precautions. Under the Corporate Governance Communique, corporate governance and early risk detection committees are the entities that are expected to oversee listed company's compliance and risk management practices, and are each composed of a minimum of two members. The board of directors and early risk detection committees must review the effectiveness of the risk management and internal control systems annually.

Banks

The risk and compliance management process for banks is regulated in a stricter manner. Accordingly, the board of directors of a bank is obliged to establish efficient and effective internal systems for risk tracking, covering all activities of domestic and foreign branches and consolidated subsidiaries of banks operating in Turkey. Internal systems consist of internal audit, internal control and risk management systems run by the relevant units under the board of directors' supervision. The duties and responsibilities related to overseeing internal

systems may be delegated to a non-executive board member, a committee consisting of non-executive members, or to the audit committee. All of these systems target compliance and risk management issues of the bank.

Internal control units inform the audit committee of information provided by internal control personnel and personnel carrying out operations in intervals no longer than three months.

The internal audit unit focuses on the sufficiency and effectiveness of internal control and risk management systems. Internal audit unit activities will be reported to the audit committee by the relevant manager in three-month intervals. The report is reviewed by the manager and audit committee, and the audit committee then presents the report to the board of directors within 10 days.

The risk management unit deals with the establishment of a risk management system, the design, selection and implementation of risk measurement models and compliance monitoring concerning risk management policies specifically tailored for different types of risks (such as interest rate risk, treasury risk, credit risk, indirect country risk, etc) by the board of directors. These risk types are specified and detailed under the banking regulations.

Insurance companies

Insurance company regulations create an obligation of sufficient and active internal systems within the corporate organisation. Accordingly, insurance companies are required to establish internal audit, internal control and risk management systems. Risk management activities are directly reported to the general manager.

In terms of corporate social responsibility, listed companies are encouraged to adopt universal standards in terms of human rights and moral standards regarding the environment, consumer rights and public health, and to combat against bribery. They must disclose in their annual report any social responsibility activities that have an environmental or social aspect. The importance of maintaining customer satisfaction as well as product and service quality is specifically emphasised for listed companies under the Corporate Governance Communique.

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

All undertakings domiciled or operating in Turkey are subject to the relevant risk and compliance obligations.

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

See question 7 for key risk and compliance management obligations.

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

Boards of directors are the main governing bodies in Turkish corporations, both privately held and listed. As a general principle, the board of directors is required to manage and represent the company by contemplating the long-term interests of the company with a rational and cautious approach to risk management, keeping the risk, growth and return balance of the company at an optimum level. Members of a board of directors owe a duty of loyalty and a duty of care to their company. The standard for the duty of care introduced by the TCC echoes the well-known 'business judgment rule'. The legislature, however, has left the scope of the Turkish business judgment rule unclear, and has deferred the interpretation surrounding the new standard to the Turkish courts. See question 14 for board liability matters.

The TCC clarifies the distinction between the representation and governance functions of boards of directors, which are both delegable. A board's governance power can be partially or wholly delegated to one or more management officers or third persons through an internal company bylaw to be prepared by the board, provided that the company's articles of association permits such delegation. If the governance power is delegated to management, then management officers would also be bound by the foregoing principles.

In addition to the foregoing, the TCC prohibits members of a board of directors from entering into any transactions with the company unless they are explicitly permitted to do so by the general assembly of shareholders. This is regardless of whether the board members act for themselves or on behalf of another person. If board members enter into such transactions with the company without shareholder authorisation, the company may choose to ratify the transaction or treat it as invalid. Furthermore, board members and their relatives who are not shareholders in the company must refrain from being indebted to the company by way of cash indebtedness. The company cannot provide sureties, guarantees or security interests to these persons. The creditors of the company are allowed direct recourse from persons acting in violation of this rule. The involvement by board members in activities competing with the company's business is also prohibited unless approved by the general assembly prior or subsequent to the transaction. In order to avoid conflicts of interest, board members are restricted from attending and voting at meetings where their or their relatives' interests will be discussed. Board members violating this restriction may be held personally liable for any losses suffered by the company in this connection.

For listed companies, the board of directors is also required to establish internal control systems, including risk management and information systems and processes. These internal control systems may ultimately reduce the effects of any risks that may influence the company's stakeholders or shareholders by taking into account the views of the board committees. Privately held companies may also adopt these methods to increase compliance oversight.

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

Yes, undertakings with risk and compliance management deficiencies may face civil liabilities. This liability could arise from the general principles of tort law or from provisions of specific legislation such as the TCC or the Banking Code.

Companies and employers can be held liable for the acts of their employees unless it is proven that the company was diligent in selecting, instructing and supervising the employee.

Under the TCC, parent companies are prohibited from using their control rights to the detriment of their subsidiaries. If they do, they would be obliged to compensate the affiliate's loss within the same year. If the parent company fails to do the foregoing, any shareholder of the subsidiary has the right to request compensation for damages of the subsidiary. The parent company's board of directors would then be held liable along with the parent company. Creditors of the subsidiary may also request payment of the company's loss to the subsidiary.

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

Yes, they do. Undertakings with risk and compliance management deficiencies may be subject to regulatory consequences or administrative fines imposed by the regulatory authorities referred to in question 4.

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

Under Turkish law, legal entities may not face criminal liability. However, for certain crimes specified under the Turkish Criminal Code or other legislation (such as bribery, embezzlement, money laundering, purposefully polluting the environment or breach of competition), security measures may be taken against the legal entity, such as the cancellation or confiscation of an operation licence, if it is active in a regulated sector.

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

Yes, they do. Board members and senior management will be held liable for damages to the company, its shareholders or creditors proportionate to the extent their fault has been proven for breach of obligations, including their risk and compliance management obligations. They are held responsible on a pro rata basis with respect to the proportion of fault found attributable to them.

The liability system of the TCC exposes board members and senior management to claims not only from shareholders but also from creditors and puts the burden of proof on the board members rather than the claimant who challenges the presumption that the directors have

acted in line with their duties. Board members and senior management are held exempt from liability for fraudulent acts that are beyond their control.

Under the TCC's liability principles, a company's internal bylaws set out guidelines for governance including the definition of the board members' and senior management's duties, delegation of powers with respect to specific fields, exchange of information and reporting systems within the board. This clear-cut delegation of governance power made by internal bylaws also provides guidance on the allocation of liability. If the governance powers of the board have been delegated through the company's internal bylaws, liability will attach to the delegated powers. As a result, board members and senior management who have delegated certain powers or duties will not be held liable for the actions or decisions of their delegates provided that they have acted with reasonable diligence (ie, unless proven to have acted with insufficient diligence) in delegation, instruction or supervision of such delegates. This 'differentiated liability' system has replaced the established liability system of the former TCC (abolished in 2012) where all directors sitting on the board were held jointly and severally liable for damages incurred by the company arising from the breach of duties and responsibilities.

Similarly, the senior management and auditors of banks can be held personally liable for the loss incurred by the bank itself owing to their action in breach of the banking regulations.

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

Yes, they do. The TCC stipulates various administrative monetary fines for breach of certain provisions, such as non-compliance with bookkeeping requirements or inaccurate statements on capital adequacy, to be imposed on the relevant individual (from the board or senior management) that fails to comply with the obligation in question. Board members may also be held personally liable for unpaid public debts such as taxes or social security payments to the extent that the company itself is unable to pay them.

The Capital Markets Code grants broad powers to the CMB on that matter. Accordingly, for breaches of the capital markets regulations, the CMB may adopt measures such as cancelling the signatory authorities, dismissing individuals from their duties, appointing temporary individuals to vacant positions or issuing administrative fines on the individual.

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

Yes, they do. Criminal liability is generally governed under the Turkish Criminal Code. Therefore, if the members of governing bodies or senior management act in a way that falls within the scope of a specific crime (eg, bribery, embezzlement, forgery), they may face criminal liability.

In addition to the general scope of the Turkish Criminal Code, there are other pieces of more specific legislation under which criminal liability may arise, such as insider trading and market manipulation under the Capital Markets Code or forgery of company books under the Tax Procedure Code, which can lead to imprisonment or judicial monetary fines.

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

As explained in question 14, if there is a delegation of powers, board members and senior management who have delegated their powers or duties will not be held liable for the actions or decisions of their delegates unless proven to have acted with insufficient diligence in the delegation, instruction or supervision of such delegates.

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

The sale of a Turkish regional airline company demonstrated a recent example of corporate risk management failure on the part of both the seller and the purchaser, which in the end led to criminal proceedings. The deal had a fast-track and cursory negotiation phase where the purchaser did not run a thorough and reasonable due diligence on the target airline company and the seller did not run the necessary reliability checks on the purchaser and both parties proceeded with a share transfer agreement that did not have sufficient liability or protection mechanisms to cover their risks. Following the closing, the purchaser alleged that the financial situation of the company was misrepresented and initiated criminal proceedings for fraud against the seller. The seller, on the other hand, was exposed to potential criminal liability by the purchaser who, as a deal party, could be more prudently selected. The protracted dispute is still ongoing before court.

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

Since the 2000s, legislation on risk and compliance management in the public sector has been an important part of the Turkish government's agenda. The Code on the Public Financial Administration and Control from 2003 introduced the 'internal control' and 'internal audit' concepts to the public sector for the first time. Although this code seems to be limited to the financial aspects of risk and compliance management, subsequent secondary legislation (ie, the Procedure and Principles Concerning Internal Control and Preliminary Financial Control) has detailed the processes and covers general compliance issues. This legislation further stipulates that public administrations are required to comply with internal control standards to be published by the Ministry of Finance for both financial and non-financial transactions.

Today, all public administrations and state-owned enterprises are compelled to establish an internal control system that requires internal audit and risk management to be carried out by internal auditors.

Hergüner Bilgen Özeke
Avukatlık Ortaklığı Attorney Partnership

Ümit Hergüner **uherguner@herguner.av.tr**
Zeynep Ahu Sazcı Uzun **zasazci@herguner.av.tr**

Büyükdere Caddesi 199
Levent 34394
Istanbul
Turkey

Tel: +90 212 310 18 00
Fax: +90 212 310 18 99
www.herguner.av.tr

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

All entities and organisations are required to observe the rule of law regardless if they are public or private. Therefore, compliance obligations are fundamental for all organisations, and all entities are expected to comply with the law and implement the best risk and compliance management practices possible.

It should be noted that the Turkish Criminal Code introduces certain crimes that can only be committed by a government official (such as a bribe – several exceptions are reserved), and in some cases, being a government official may be considered an aggravating circumstance with respect to sanctions.

United Kingdom

Dan Lavender, Matt McCahearty and Malcolm Walton
Macfarlanes LLP

1 What legal role does corporate risk and compliance management play in your jurisdiction?

There is a complex legal framework underpinning corporate risk and compliance management in the UK.

This chapter focuses on core corporate risk and compliance management issues in the context of the UK financial services regime. Separate and distinct regimes apply to sectors outside the financial services market (eg, the pharmaceutical and energy sectors), which are enforced by designated UK and international regulatory agencies. These regimes are outside the scope of this chapter.

The legal framework for the financial services regime in the UK is vast and complex and there are detailed rules relating to specific sectors of the market. Most of the corporate risk and compliance management requirements derive from EU directives and regulations, which have been implemented into English law in the form of legislation and detailed regulatory rules.

There is also a wealth of case law from a variety of judicial and administrative bodies, including the European Court of Justice, the English courts and the UK regulator, the Financial Conduct Authority (FCA).

There has been a constant evolution and expansion of the regulatory landscape, particularly since the financial crisis of 2007–2008. These developments have seen a shift from the traditional approach of outcome-focused and principle-based regulation to an increasingly prescriptive and rules-based approach.

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

The most important statute in this area for financial services firms (including firms that are considering if their services might entail regulated business in England) is the Financial Services and Markets Act 2000 (FSMA), in particular sections 19 and 21 FSMA, which set out two restrictive regulatory regimes.

Key delegated legislation under FSMA includes:

- FSMA 2000 (Regulated Activities) Order 2001;
- FSMA 2000 (Financial Promotion) Order 2005;
- EU regulations that have a direct effect on English law (for example the Market Abuse Regulation);
- rules made by the UK regulators (the Prudential Regulation Authority (PRA) and the FCA) under FSMA, which apply to firms that are authorised and regulated in the UK as well as, in some circumstances, European Economic Area firms that are licensed by other European Economic Area regulatory authorities but conduct business in the UK. The FCA rules can be found at www.handbook.fca.org.uk/handbook and PRA rules at www.prarulebook.co.uk. These rules implement many European Commission financial services sectoral Directives (which do not have direct effect in English law and require implementing measures in order to take effect);
- within the FCA and PRA rules, a number of sourcebooks and chapters contain detailed requirements on risk and compliance management. These include the FCA's Senior Management Systems and Controls Sourcebook and the PRA's General Organisational Requirements, although many risk-management requirements are also found elsewhere. For example, FCA rules for the management of the risks associated with holding client money and assets are not contained in the FCA Handbook but are set out instead in the Client Assets Sourcebook;
- the Money Laundering Regulations 2007; and
- the Bribery Act 2010 and the Terrorism Act 2000.

Key competition law legislation includes the Competition Act 1998 and the Enterprise Act 2002. These need to be read in conjunction with legislation specific to the financial services sector, notably FSMA.

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

Generally speaking, any legal person who conducts activities within the scope of the restrictive regimes in section 19 and 21 FSMA will be targeted by the requirements and, regardless of its legal form or corporate structure, will need to seek authorisation from the PRA or FCA and comply with the relevant regulatory requirements.

For example, a sole trader may need to seek authorisation (typically from the FCA) and put in place systems and controls to organise his or her business effectively – just as a high street bank, which is a listed company, must also do (seeking authorisation from the PRA as it is a bank). Other entities such as limited liability partnerships will also need to seek authorisation if they are conducting activities that fall within the scope of the FCA or PRA.

What is required of each entity will, however, vary depending on the sector, size, scale and nature of the business and regulated activities being carried on.

Notwithstanding the above, it should be noted that certain regulated activities can only be performed by legal persons of a particular corporate form. For example, a sole trader could not seek authorisation to conduct insurance activities.

Competition law targets all types of undertakings operating in the UK (whether or not they are domiciled in the UK), including those outside of the financial services sector. In terms of financial services firms, the FCA has concurrent competition law powers (see question 4), which extend to all financial services undertakings and not just those authorised by the FCA.

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

The UK's approach to financial regulation involves several bodies, each with their own responsibilities and remit.

The PRA is responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms. The PRA has powers in relation to failing firms and enforcement powers relating to breaches of the PRA's regulatory requirements.

The FCA is responsible for the conduct regulation of financial services firms in the UK and the prudential regulation of firms that are not regulated by the PRA. Firms that are regulated by both the FCA and the PRA are known as dual-regulated firms.

The FCA has three operational objectives:

- to protect consumers;
- to protect and enhance the integrity of the UK financial system; and
- to promote effective competition.

The FCA has wide-ranging powers to facilitate these objectives. These include powers relating to rule-making, authorisation of firms, market regulation and passporting. The FCA also has extensive disciplinary and enforcement powers, which include the power to bring civil and criminal, as well as regulatory, proceedings.

The Competition and Markets Authority (CMA) is responsible for investigating and penalising breaches of competition law. The FCA also has concurrent competition law powers in relation to financial services firms, which include unannounced inspections and mandatory information requests. The FCA can also send 'on notice' letters to firms, warning them of potentially infringing behaviour in circumstances where a full investigation is not warranted.

The Serious Fraud Office (SFO) is an agency operating within the UK criminal justice system, which investigates and prosecutes serious and complex fraud as well as bribery and corruption cases. The SFO also deals with requests from overseas courts and prosecutors for international assistance.

In recent years, there has been a continuing trend of growing cooperation between UK and overseas regulators and agencies as issues become increasingly multi-jurisdictional in nature.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

No – these are not defined terms across most financial services legislation.

However, there are detailed rules covering these areas that vary between sectors (banking, insurance, asset management, etc). Refer to question 7.

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

Yes, although legislation and rules do not generally prescribe a single approach or structure to risk and compliance management. Historically, the requirements have tended to be non-prescriptive, looking to outcomes rather than the form of the arrangements.

However, particularly since the financial crisis, there has been a tendency for new legislation and rules to adopt a more prescriptive approach. This reflects a corresponding trend in EU financial services legislation, for example the Solvency II Directive for insurers and Markets in Financial Instruments Directive (MIFID) II for investment firms.

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

Firms that are authorised and regulated in the UK will be subject to high-level standards relating to risk and compliance management under the FCA's Principles for Businesses (and in addition, may be subject to the PRA's Fundamental Rules, depending on whether the firm is authorised by the PRA rather than the FCA).

Principle 3 of the FCA's Principles for Businesses requires a firm to 'take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'.

PRA Fundamental Rules 5 and 6 also require a firm to 'have effective risk strategies and risk management systems' and to 'organise and control its affairs responsibly and effectively'.

More detailed standards and guidelines are contained in the legislation and rules referred to in question 2, and expand upon Principle 3 and Fundamental Rules 5 and 6. These more detailed requirements vary significantly depending on the financial services sector in which a firm operates and the regulated activities that it carries out. There is no 'one size fits all' approach.

Some provisions are also subject to proportionality requirements. What is expected of a large bank will not be the same as a small firm that has a deposit-taking permission for certain limited business it may be carrying out, or a firm that does no more than make occasional introductions of business to another regulated firm.

Depending on the status of the firm, examples of the types of standards and guidelines that may apply are set out below. This list is included by way of illustration only and is not an exhaustive list of requirements:

- the duty to have robust governance arrangements, which include:
  - a clear organisational structure with well-defined, transparent and consistent lines of responsibility;
  - effective processes to identify, manage, monitor and report the risks the firm is or might be exposed to;
  - internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems;
- the duty to have business continuity procedures and a compliance manual;
- the duty to categorise clients and enter into written agreements with clients;
- the duty to report information and data to clients, and to the FCA or PRA;
- the duty to have a separate risk assessment function;
- the requirement for 'four eyes' in the running or management of the firm. For example, an investment firm that is a limited company will generally need to have at least two executive directors;
- the requirement to establish a compliance function and to appoint a money laundering reporting officer;
- the duty not to delegate responsibility to a third party. Functions that are outsourced to a third party must be supervised or overseen;
- the duty to establish a remuneration committee;
- the duty to comply with detailed conduct of business obligations when providing services to clients. These include high-level obligations such as the duty to act in the best interests of the client and to treat customers fairly, as well as more detailed rules, for example, the duty to ensure that investment advice and discretionary management services are suitable for the customer concerned;
- the duty to have a conflict of interest policy and keep a register of conflicts and manage any conflict that may entail a material risk of damage to clients' interests; and
- detailed requirements on holding and handling client money and assets.

Many of the processes that are required are ultimately derived from European Commission sectoral legislation.

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

Yes. The extent of the firm's obligations will depend on the regulated status of the firm. For example, firms authorised by the FCA and PRA will be required to comply with FCA and PRA rules relating to risk and compliance management, in addition to the rules that apply more widely to firms operating in the UK. The FCA rules are very broad capturing capital, governance, conduct of business and other compliance, risk and system and control requirements including duties at board level and personal responsibilities for individuals in various controlled functions. The extent to which the requirements apply to firms in part depends on the size of the firm in question. As explained above, the extent of the firm's obligations will also depend on the specific sector within which the firm operates.

Following a recent review of the compliance function in wholesale banks, the FCA noted that the compliance function is moving towards a pure, independent second line of defence risk function with a higher profile within firms (with compliance representatives increasingly being added to boards and governance committees). The FCA emphasised the importance of ensuring that compliance functions balance their role as an adviser to the front office with their role of providing challenge.

Incoming EEA firms (particularly those establishing a branch in the UK) that are authorised and regulated by other EEA regulatory authorities will be subject to some more limited UK rules, which may require certain risk and compliance arrangements to be put in place. Again, what is required will depend on the type of firm and the type of passport it is using (services or branch). Generally speaking, this type of firm will not be subject to UK prudential requirements.

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

The key risk and compliance management obligations of FCA authorised firms are outlined in question 7.

In addition, FCA and PRA authorised firms are required to deal with the relevant regulator in an open and cooperative way and to notify the regulator of anything relating to the firm of which the regulator would reasonably expect notice. This duty to self-report is contained

in Principle 11 of the FCA's Principles for Business and Fundamental Rule 7 of the PRA's Fundamental Rules. The FCA or PRA may bring an enforcement action against a firm that has acted in breach of this duty. For example, in April 2015, the FCA fined Deutsche Bank £226 million in connection with a breach of Principle 11, among other breaches. A significant part of the fine related to Deutsche Bank's conduct in providing false and misleading information to the FCA.

There are also risk and compliance management obligations that apply more broadly to firms operating within the UK. For example, the anti-money laundering regime (in particular, the Money Laundering Regulations 2007) applies to businesses identified as most vulnerable to the risk of money laundering. This includes financial institutions and businesses within the regulated sector, such as law and accountancy firms. Firms must be able to demonstrate that their client due diligence measures, ongoing monitoring and internal policies and procedures are appropriate in light of the risk of money laundering to their business.

It is also a criminal offence under the Bribery Act 2010 if a commercial organisation fails to prevent bribery (the 'failure to prevent' offence). This legislation is not sector-specific and the 'failure to prevent' offence applies to all UK corporates and partnerships. It may also apply to companies that are incorporated and operate outside the UK if part of their business is within the jurisdiction. There is a defence if the organisation can show that it had adequate procedures in place to prevent bribery (see question 17).

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

In addition to the regulatory requirements that apply to FCA authorised firms, there is a regime that applies to individuals who perform certain activities within authorised firms (known as 'approved persons'). These activities are referred to as 'controlled functions' and examples include being a director of an authorised firm and overseeing the firm's systems and controls.

The FCA may only grant an application for approval to perform a controlled function if it considers that the individual is fit and proper to perform the relevant function.

Individuals who perform controlled functions are required to comply with certain standards of conduct set out in the FCA's rules. In particular, individuals must comply with the FCA's Statements of Principle and Codes of Practice for Approved Persons (APER), which set out high-level principles of behaviour, as well as specific rules for particular types of controlled function.

The FCA may bring disciplinary action against individuals who fail to meet the standards of conduct expected of them (see question 15).

Increasing individual accountability is a key priority for the FCA. In March 2016, the FCA introduced the 'Senior Managers and Certification Regime' (SM&CR), which is designed to assist the FCA in holding senior management to account. Among other things, the regime requires firms to set out detailed statements of responsibility, identifying which individuals within the firm have responsibility for specific issues. There are also detailed rules relating to the conduct of 'senior managers' as well as new Conduct Rules that apply to most employees of relevant firms, including those performing unregulated roles. The Conduct Rules reflect the FCA's core standards expected of employees of authorised firms.

The regime currently applies only to deposit-taking institutions and certain insurance firms. However, in 2018 the regime will be extended to cover almost all FCA authorised firms (and will replace the Approved Persons Regime described above). It is currently intended that the rules will apply to insurers in late 2018 and solo-regulated firms in mid-to-late 2019. The FCA has confirmed that it will publish its rules and approach to the transition in a statement in summer 2018.

As well as the risk and compliance management obligations owed by directors and senior managers of authorised firms, directors also have general duties that are set out in the Companies Act 2006, supplemented by common law. These duties apply to directors of companies outside the financial services sector.

Directors of UK listed companies (including companies outside of the financial services sector) are subject to additional obligations, for example in relation to corporate governance. These are outside the scope of this chapter.

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

Yes. FSMA contains a provision (section 138D FSMA) that allows private persons a right of action for damages in respect of loss suffered as a result of a breach of FSMA.

There are also provisions in FSMA that give a right of action for specific breaches, including misleading information in listing particulars and prospectuses (section 90 FSMA).

The current regulatory environment has seen an increase in civil actions against financial institutions (particularly banks) for the mis-selling of investments and other financial products. As well as claims arising under section 138D FSMA, claims may be based on:

- alleged breaches of contract relating to the bank's advisory duty;
- alleged breaches of the bank's tortious duty of care; or
- misrepresentation on the part of the bank.

Misrepresentation claims may arise under the Misrepresentation Act 1967, the bank's duty not to misstate the position negligently or (less commonly) fraudulent misrepresentation.

The Consumer Rights Act 2015 came into force in October 2015 and allows businesses and consumers in all sectors to bring class actions in respect of breaches of competition law. This could make it easier for claimants to bring US-style class actions (for example, in relation to benchmark manipulations such as foreign exchange and LIBOR).

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

Yes. The FCA has wide-ranging enforcement powers against firms for breaches of regulatory rules. Enforcement action for risk and compliance management deficiencies is likely to be based on Principle 3 of the FCA's Principles for Businesses, which states that the firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

The FCA may impose a variety of disciplinary sanctions on firms for regulatory failures. These include:

- public censure;
- a financial penalty;
- suspensions or restrictions in relation to the firm's permission to perform regulated activities; and
- variation or cancellation of the firm's permission.

In deciding whether to impose a public censure or a financial penalty, the FCA will take into account the circumstances of the case, including the nature, seriousness and impact of the breach and the previous disciplinary record of the firm.

The FCA has provided guidance on the approach it will follow to determine the level of a financial penalty. Among other things, the FCA will take into account any financial benefit derived directly from the breach and any adjustments that should be made in light of mitigating and aggravating factors. The FCA also has the power to increase the penalty if it considers that the figure is insufficient to achieve its objective of deterrence.

In recent years, the FCA has imposed substantial financial penalties against banks for benchmark manipulation and anti-money laundering (AML) controls failings. In May 2015, the FCA imposed a financial penalty of £284,432,000 on Barclays Bank for systems and controls failures in connection with foreign exchange manipulation. At the time of writing, this is the largest financial penalty ever imposed by the FCA. In January 2017, the FCA imposed a financial penalty of £163,076,224 on Deutsche Bank AG for failing to maintain an adequate AML control framework (see question 18). At the time of writing, this is the largest financial penalty for AML controls failings ever imposed by the FCA.

Firms in all sectors can also face lengthy investigations by the CMA, when they are suspected of failing to act in accordance with competition law. Financial services firms may also face competition law investigations by the FCA. These investigations can result in large-scale fines.

Update and trends

Brexit

On 29 March 2019, the UK is due to leave the European Union (Brexit). The UK government remains in negotiation with the EU for a number of matters including trade and access arrangements between the UK and the EU post-Brexit and a proposed transitional period. Until Brexit takes effect, EU law continues to apply to UK firms. The FCA stated on 24 June 2016 that 'firms must continue to abide by their obligations under UK law, including those derived from EU law and continue with implementation plans for legislation that is still to come into effect'.

At the time of writing, the UK is seeking a free trade deal that makes unique provision for the financial services market between the UK and the EU. However, it remains to be seen whether this type of agreement will be negotiated and if so, what shape the bespoke financial services provisions will take. While it may be the case that much regulation of EU-origin continues in place for the purposes of continuity and reciprocity, the extent to which domestic rules and regulation will be amended after Brexit is currently unclear.

Data protection

The EU's existing data protection framework is being replaced by the General Data Protection Regulation (GDPR) on 25 May 2018. The GDPR enhances a number of the existing standards and aims to harmonise much of the data protection legislation across the EU including the UK. Among other things, scope is widened and it will be more difficult to obtain and rely on the consent of data subjects to the processing of their personal data and some firms will be required to appoint a Data Protection Officer. Firms will need to review their existing processes and controls and ensure they are compliant with the GDPR.

Focus on individual accountability

As explained above, there is an increasing regulatory focus on individual accountability with the Yates Memo in the United States and the SM&CR in the UK. In mid-to-late 2019, the UK regime will be extended to cover all firms authorised under FSMA. It will also apply to branches of non-UK firms with permission to carry out regulated activities in the UK. The regulators' intention is to drive up standards of individual behaviour in financial services at all levels and to make it significantly easier for the regulators to hold senior managers to account for failures within their firms.

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

The UK government is currently consulting on the creation of new offences to make corporations liable for certain criminal activities.

For serious offences that do not impose strict liability, a corporation will only normally be liable for the criminal actions of an employee if the individual is sufficiently senior to be the 'directing mind and will' of the company (the identification doctrine). This is a highly fact-specific question, the complexity of which increases with the size of the company and the structure of its management. A company can only be criminally liable if it can be shown that the directing mind, namely, the board or senior management of the organisation, were involved in the commission of the offence. Successful prosecutions of companies on this basis are challenging and consequently rare.

In January 2017, the UK government published a Call for Evidence seeking views on the extension of the failure to prevent offence under the Bribery Act 2010 (see question 9), as well as four alternative options. If a new corporate failure to prevent offence proves to be the best option for reform, the government's starting position is that the offence should initially apply to the most serious economic crime offences, which may include:

- conspiracy to defraud;
- fraud;
- false accounting; and
- money laundering.

If implemented, the offence will apply to corporations in all sectors.

In January 2017, the UK government also published a Call for Evidence on the alternatives to the identification doctrine for corporate criminal liability. At the time of writing, the Government is analysing the feedback.

Deferred Prosecution Agreements (DPAs) are available to bodies corporate, partnerships and unincorporated associations facing criminal proceedings in the UK. In question 18, we discuss the £500 million DPA that Rolls-Royce recently agreed with the SFO.

There is no specific corporate criminal liability for competition law breaches.

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

As explained in question 11, section 138D FSMA provides a right of action for damages for a person who has suffered a loss as a result of a breach of an FCA rule. See also question 15.

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

Yes. The FCA may take disciplinary action against approved persons who act in a way that is inconsistent with the standards of conduct set out in the FCA rules.

The FCA's disciplinary powers include financial penalties and issuing a public statement about the misconduct. The FCA may also suspend, restrict or withdraw the individual's approval and impose a prohibition order preventing the individual from performing controlled functions.

Under the SM&CR, the government has introduced a new statutory 'duty of responsibility' for senior managers, which means that they are required to take reasonable steps to prevent a regulatory breach by the firm in their area of responsibility. The FCA and the PRA can take disciplinary action against a senior manager for a breach of this statutory duty.

Directors, managers and other officers can face director disqualification orders for failing to comply with competition law. This applies to individuals in all sectors.

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

There are certain criminal offences that could apply to directors and senior managers of financial institutions if the individuals were personally culpable. For example, under section 89 of the Financial Services Act 2012, it is an offence to make false or misleading statements or create false or misleading impressions with the intention of inducing (or being reckless as to whether it may induce) another person to enter into an agreement (eg, an agreement to sell or buy shares in a company).

For conduct occurring post-March 2016, there is a new criminal offence relating to decisions taken by senior managers of banks, building societies and major investment firms (section 36 of the Financial Services (Banking Reform) Act 2013). Senior managers may be criminally liable if they make a decision (or fail to take steps that could prevent a decision being taken) that causes a financial institution to fail. In order for the offence to be made out, the senior manager must have been aware (at the time the decision was taken) of the risk that the decision might cause the financial institution to fail. The individual's conduct must also fall 'far below' what could reasonably be expected of someone in their position. At the time of writing, the FCA has not brought any prosecutions for this offence.

Directors and managers in all sectors can be prosecuted by the CMA for committing a cartel offence, namely, agreeing with one or more other persons to make or implement, or cause to be made or

implemented, arrangements whereby at least two undertakings will engage in one or more prohibited cartel activities. For such agreements entered into from 1 April 2014 onwards there is no need to establish that the individual acted 'dishonestly'.

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

Corporate compliance defences exist in relation to certain, specific statutory offences. For example, under the Bribery Act 2010, a corporate will have a defence to the criminal failure to prevent offence if it can show that it had adequate procedures in place, designed to prevent persons committing bribery. There is no definition of 'adequate procedures'; however, guidance has been published that places an emphasis on taking a risk-based approach while implementing proportionate procedures.

There is also a corporate defence to the financial promotions offence if a firm can show that it took all reasonable precautions and exercised all due diligence to avoid committing the offence (section 25(2) FSMA).

There is no specific corporate compliance defence in relation to FCA enforcement proceedings. However, in determining the level of the financial penalty, the FCA will consider whether there are any mitigating factors, which may include that the firm corrected the deficiencies in its compliance and risk management framework as part of a remediation programme. This could lead to a lower fine being imposed against the firm.

While not strictly a defence, it is also possible for businesses to apply for leniency in relation to certain types of competition law infringement. This may result in avoiding or receiving a reduced fine.

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

Deutsche Bank FCA Final Notice

On 31 January 2017, the FCA fined Deutsche Bank £163,076,224 in connection with deficiencies in its AML control framework.

The FCA found, among other things, that between 2012 and 2015 Deutsche Bank:

- performed inadequate customer due diligence;
- had deficient anti-money laundering policies and procedures;
- had an inadequate anti-money laundering IT infrastructure; and
- provided insufficient oversight of trades booked in the UK by overseas traders.

The FCA found that there were 'serious and systemic weaknesses' in Deutsche Bank's AML systems and controls, which 'created a significant risk that financial crime would be facilitated, occasioned or otherwise occur'.

Deutsche Bank was also fined US$425 million by the New York Department of Financial Services in connection with the mirror trading scheme.

Rolls-Royce DPA

In January 2017, Rolls-Royce entered into a DPA with the SFO, which was approved by the English court. The DPA involved payments by Rolls-Royce of nearly £500 million plus interest and the SFO's costs (£13 million). It is the largest DPA of its kind in the UK. Rolls-Royce's conduct involved offences relating to bribery of foreign public officials, commercial bribery and false accounting of payments to intermediaries.

The case highlights the importance of engaging openly and fully with the SFO from an early stage of its investigations. The extent to which Rolls-Royce co-operated with the SFO was, in the SFO's own words, 'extraordinary' and this was a key factor in persuading the judge to approve the DPA. Another key consideration was that Rolls-Royce had taken steps to review and enhance its ethics and compliance procedures such that Rolls-Royce had become a 'dramatically changed organisation'.

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

The answer to this question depends on the status of a governmental body, or state-owned enterprise.

There are exclusions and exemptions from financial services regulation under FSMA for certain state bodies, for example local authorities.

The FCA and PRA are subject to statutory duties (such as the general duties and objectives set out in FSMA) and must act within the scope of their authority and comply with other requirements (such as the duty to consult or implement European Commission law requirements in their rules to ensure that the UK meets its European Commission law obligations).

The fact that a firm is state-owned or partly state-owned does not usually provide an exemption from regulation. For example, the Royal Bank of Scotland plc is currently a partly state-owned UK bank. Its regulatory obligations are essentially the same as other banks of its size and scale carrying on the same regulated activities.

Competition law extends to 'undertakings' (the European Union law concept) and 'enterprises' (the UK law concept) in all sectors. In broad terms, this includes all entities to which a turnover can be ascribed, whether or not the entity is run for profit.

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

Financial services regulation under section 19 FSMA and section 21 FSMA will not generally be directly relevant to governmental bodies, as explained above.

However, a large body of European Union sectoral legislation and FSMA will limit and, in some cases, remove the discretion of the UK regulators, the FCA and the PRA.

From a competition law perspective, once competition law attaches to a body, the risks are essentially the same.

MACFARLANES

Dan Lavender **dan.lavender@macfarlanes.com**
Matt McCahearty **matt.mccahearty@macfarlanes.com**
Malcolm Walton **malcolm.walton@macfarlanes.com**

20 Cursitor Street
London EC4A 1LT
United Kingdom

Tel: + 44 20 7831 9222
Fax: +44 20 7831 9607
www.macfarlanes.com

United States

Keith M Korenchuk
Arnold & Porter

1 What legal role does corporate risk and compliance management play in your jurisdiction?

Compliance programmes that prevent, detect and respond to potential wrongdoing or misconduct are part of the expectations of the US government for organisations regardless of whether they operate in the US or in other countries around the world. While there is generally no legal requirement that organisations establish and maintain an effective compliance programme, having an effective compliance programme in place may serve to reduce fines, penalties and other terms of the settlement of any government investigation, whether brought on the basis of civil or criminal law. In addition, having a compliance programme that is effective is recognised as assisting in protecting the reputation of the organisation.

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

The primary source addressing compliance expectations is the US Federal Sentencing Guidelines (www.ussc.gov/sites/default/files/pdf/guidelines-manual/2016/GLMFull.pdf), as set forth in Chapter 8, Part B, Subpart 2.1 of those Guidelines. The Guidelines have been modified over time to reflect the ongoing evolution of compliance expectations. These Guidelines are established by the US Department of Justice (DOJ) and address how to calculate fines, penalties and prison sentences for a wide variety of offences committed by corporations and individuals. The Guidelines provide a formula for each offence that is then adjusted based on the underlying facts surrounding the conduct in question for aggravating and mitigating factors. One of the mitigating factors recognised for organisations is the existence of a compliance programme. The Guidelines set out the elements needed for a compliance programme to receive credit for reducing fines and penalties that would otherwise be due. These Guidelines are used by a variety of government agencies to guide their own regulatory and enforcement efforts.

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

All organisations, companies, corporations or other entities regardless of form are covered.

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

The primary agency that considers the impact of compliance issues is the DOJ, which may bring criminal or civil enforcement actions under the laws of the United States. In general, the DOJ has wide authority to enforce the laws of the United States. Typically, this means that the DOJ uses a variety of laws to address misconduct. While there is no direct action that can be brought for failure to maintain a compliance programme on its own, the presence or absence of a compliance programme is an important factor that the DOJ considers in the resolution of many matters. The DOJ has authority to impose, as part of the resolution of any action, requirements to implement and maintain a compliance programme and often does so. The DOJ also may enforce the terms of any settlement, and therefore has ongoing oversight of how well a compliance programme is being implemented and maintained.

In addition, many other agencies may also impose compliance expectations or requirements on organisations, and often work in conjunction with the DOJ. The agencies include, among others, the Securities and Exchange Commission (SEC), the Environmental Protection Agency, the Department of Health and Human Services, the Federal Trade Commission, the Financial Industry Regulatory Authority and the Office of Foreign Assets Control (OFAC). All of the agencies may impose requirements relating to industry-specific compliance standards on organisations as part of the resolution of an investigation.

Finally, state governments and state agencies may also be involved in enforcement matters and may also require organisations to make compliance commitments as part of a settlement of an enforcement action.

5 Are 'risk management' and 'compliance management' defined by laws and regulations?

The elements of a compliance programme are set out in the Guidelines. In addition, these elements are widely recognised in guidelines or settlements entered into by organisations with the US government through various enforcement agencies. In general, risk management principles are recognised as part of an effective compliance programme, and are described as part of the process to control risks, and to prevent, detect and respond to wrongdoing.

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

The Guidelines set out the details regarding processes involved for an effective compliance programme. In addition, for bribery and corruption risks, detailed information has been published regarding compliance programme responsibilities. This information can be found in A Resource Guide to the US Foreign Corrupt Practices Act (FCPA), published in 2012 by the DOJ and the SEC (www.justice.gov/criminal-fraud/fcpa-guidance) and in the United States Attorneys Manual (www.justice.gov/usam/united-states-attorneys-manual). In February 2017 the Fraud Section of the DOJ published its Evaluation of Corporate Compliance Programs (www.justice.gov/criminal-fraud/page/file/937501/download). This guidance includes 11 key compliance programme evaluation topics, and includes a number of common questions that the DOJ considers relevant in evaluating compliance programmes as part of a criminal investigation. In addition, in November 2017, the DOJ announced that they would permanently include in the US Attorneys Manual (www.justice.gov/usam/usam-9-47000-foreign-corrupt-practices-act-1977) core principles of its previously announced FCPA Pilot Program, which was launched in April 2016. This permanent enforcement policy strongly incentivises companies to voluntarily disclose potential misconduct, fully cooperate with the government's investigation and remediate the alleged misconduct through an effective compliance programme and disgorgement of improper gains. If a company satisfies these three criteria, absent aggravating circumstances, it will be entitled to a presumption that the DOJ will decline to prosecute the company. In March 2018, the DOJ announced its intention to apply the principles of this FCPA enforcement policy to other white collar crimes.

In addition, in some sectors like the healthcare and pharmaceutical industries, specific guidelines have been developed that apply the

compliance standards set forth in the Guidelines to specific business practices. For example, the application of compliance requirements to the pharmaceutical industry has been set forth in the OIG Compliance Program Guidance for Pharmaceutical Manufacturers (www.gpo.gov/fdsys/granule/FR-2003-05-05/03-10949) issued in 2003, and the document entitled Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors issued jointly by the Office of Inspector General of the US Department of Health and Human Services and the American Health Lawyers Association in 2003 (https://oig.hhs.gov/compliance/compliance-guidance/compliance-resource-material.asp).

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

The main standards and guidelines are based on the Guidelines and have been further developed through implementation of the Guidelines by various agencies and resolution of enforcement actions. These standards are generally described as follows.

Support and commitment from the top

As a foundational matter, senior management and boards of directors should create a 'tone at the top' that promotes a culture of compliance. In evaluating an organisation's compliance programme, US authorities say they will consider whether senior management has clearly articulated expectations of conducting business in compliance with all laws and organisation standards, communicated these expectations in unambiguous terms, followed these standards themselves, and supported compliance with appropriate resources. While 'tone at the top' is necessary, a commitment to compliance must be reinforced by middle management and others throughout the organisation as compliance is the duty of individuals at all levels.

Clearly articulated and visible corporate policies

Organisations should have written policies, procedures and codes of conduct that prohibit improper conduct. The policies should cover key risk areas and provide clear standards of expected behaviour. Typically, a code of conduct is included as a key document that sets forth expectations on acceptable conduct.

Governance and oversight

The governing authority should be knowledgeable about the content and operation of the compliance programme and exercise reasonable oversight with respect to its implementation and effectiveness.

The high-level personnel of an organisation should ensure that an organisation has an effective compliance and ethics programme. Specific individuals within high-level personnel should be assigned overall responsibility for the compliance programme. In addition, specific individuals within an organisation should be delegated day-to-day operational responsibility for the compliance programme. Individuals with operational responsibility should report periodically to high-level personnel and, as appropriate, to the governing authority or an appropriate subgroup, on the effectiveness of the compliance programme. To carry out such operational responsibility, these individuals should be given adequate resources, appropriate authority and direct access to the governing authority, or an appropriate subgroup.

A dedicated compliance infrastructure, with one or more senior corporate officers responsible for compliance, is needed. US enforcement authorities will look at whether an organisation devoted adequate staffing and resources to the compliance programme given the size, structure and risk profile of the business. At a minimum, US authorities expect that lead compliance personnel will have direct access to an organisation's governing authority, such as the board of directors or an audit committee.

Excluded persons

An organisation should use reasonable efforts not to include within its substantial authority personnel any individual whom an organisation knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics programme. Practically, this means that an organisation should routinely check whether employees are debarred from doing business with the US government, usually through checking online exclusions databases.

Training and communication

Organisations should take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance programme, by conducting effective training programmes and otherwise disseminating information appropriate to the respective roles and responsibilities of those required to be trained. The individuals included for this training are the members of the governing authority, high-level personnel, substantial authority personnel, organisation employees, and, as appropriate, an organisation's agents. A compliance programme cannot be effective without adequate communication and training. While the nature and type of training given depends on the circumstances of the organisation and how it conducts business, the ultimate goal of training and communication is to make sure that individuals understand what is expected of them and are able to incorporate compliance guidelines in their everyday activities.

Moreover, it is expected that communication regarding compliance issues should not take place only in formal settings. While the nature of communication may vary based on the organisation and its business, in general it is expected that communication efforts could include such elements as internal newsletters for employees, a separate space on the intranet devoted to ethics, dissemination of examples of good practices of ethical conduct, posting of pamphlets and announcements on bulletin boards, presentation of positive results obtained from the implementation of the code of conduct and incorporation of the ethical and integrity principles and values in the organisation's mission and vision statements. An effective compliance programme must provide resources for an organisation's employees and relevant third parties to obtain compliance information. Specific organisation personnel should be designated to help answer questions.

Monitoring and auditing

Organisations are expected to take reasonable steps to ensure that the compliance programme is followed, including monitoring and auditing to detect criminal conduct, to evaluate periodically the effectiveness of the compliance programme and to have and publicise a system, which should include mechanisms that allow for anonymity or confidentiality, whereby organisation employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation. These mechanisms for reporting potential or actual misconduct typically include the institution of hotlines, ombudsmen or other anonymous reporting systems. Monitoring and auditing serve as the basis for determining if the policies and procedures are being implemented effectively. What activities to monitor and audit are a function of the nature of the business and the way in which an organisation operates. Accordingly, there is no set rule as to what activities should be reviewed, but it is essential for an organisation to be able to justify the efforts it undertakes in that regard.

Incentives and discipline

The compliance programme should be promoted and enforced consistently throughout an organisation through appropriate incentives to perform in accordance with the compliance programme and appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct. Organisations should reward their employees for good behaviour, and consider including the review of business ethics competencies in the appraisal and promotion of management and measuring the achievement of targets not only against financial indicators, but also against the way the targets have been met and specifically against compliance with the organisation's policies. Incorporating adherence to compliance as a significant metric for management's bonuses, recognising compliance professionals and internal audit staff, and making working in the compliance organisation a way to advance an employee's career are all ways to promote compliance. While incentives are important, so are disciplinary procedures to address violations. To evaluate the credibility of a compliance programme, US authorities will assess whether an organisation has appropriate and clear disciplinary procedures, whether those procedures are applied reliably and promptly and, when applied, whether they are commensurate with the violation and used consistently.

Response to incidents
An organisation's response to a report of potential misconduct is also critical. Organisations must have an infrastructure in place to respond to the report, conduct appropriate investigations and document the response process, in a consistent manner. After criminal conduct has been detected, an organisation should take reasonable steps to respond appropriately to the criminal conduct, to determine the root cause of the misconduct, and to prevent further similar criminal conduct, including making any necessary modifications to the compliance programme.

Risk assessment and periodic reviews
In implementing the requirements listed above, an organisation should periodically assess the risk of criminal conduct and should take appropriate steps to design, implement or modify each requirement set forth above to reduce the risk of criminal conduct identified through those processes. Periodic reviews and assessments of a compliance programme are viewed as essential, as a programme that remains static is likely to become ineffective as risks shift. For example, organisations may use employee surveys to measure their compliance culture and strength of internal controls, identify best practices and detect new risk areas, or may conduct audits to assess whether controls have been implemented effectively.

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

Any organisation, regardless of the form of the entity that operates in the United States or is subject to US law, is expected to meet these compliance obligations.

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

Organisations are expected to implement and maintain an effective compliance programme as described above.

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

Members of governing bodies and senior management have several responsibilities regarding risk and compliance. First, governing board members have responsibility for compliance programme oversight. This means that board members must ensure that the compliance programme is effective, that it is designed to mitigate compliance risks, and that it has sufficient resources to prevent, detect and respond to potential misconduct. Second, board members must hold senior management and those responsible for the compliance programme accountable to implement the programme. Board members also must establish a 'tone at the top' that demonstrates to employees and external parties that the organisation expects all who are associated with it to act properly and in accordance with applicable laws and regulations as well as organisation policies.

With regard to senior management, the expectation is similar to that of members of the governing body. Senior management should ensure that the compliance programme has the resources and capabilities to implement a programme that prevents, detects and responds to potential misconduct. Senior management also has an obligation to demonstrate support for compliance through 'tone at the top.' This requires management to show by verbal communication and their actions that they require all employees to act in a compliant way and that misconduct will not be tolerated. This tone can be demonstrated through written and verbal communication to employees by email, in other written communication, through presentations at meetings, and through one-on-one interactions where employees are encouraged to only conduct business ethically and in accordance with applicable laws and organisation policies.

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

Those organisations that engage in misconduct involving compliance obligations under law face potential civil liability, which could include fines, disgorgement of gains, restitution and debarment from participating in government programmes. Liability occurs from a violation of applicable law or regulation, as opposed to a violation of a compliance programme requirement. For example, civil liability could occur if an organisation fails to obtain a required permit, but civil liability would not occur if an organisation's employee failed to follow a policy requiring a permit to be obtained.

In addition, organisations may face the risk of civil liability from private litigants who may claim that the organisation failed to fulfil its obligation to manage risk through a compliance programme, resulting in loss of value to an investor who would not have experienced a loss if the programme had been managed effectively. These private legal actions may result in added defence costs as well as judgments or settlements, depending on the facts of the underlying matter.

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

Administrative or regulatory action may result in being debarred from conducting business with government entities, restrictions or suspension of a licence, or fines associated with the underlying conduct. The nature of the action that could be taken is a function of the requirements of the underlying administrative provisions or regulations that specify the consequences of the violation. In instances where an organisation has settled an enforcement action, compliance obligations may be required to be undertaken as part of the settlement agreements. Failure to meet those settlement obligations relating to compliance may result in fines or penalties. For example, an organisation may have committed as part of a settlement to conduct annual training on compliance topics. Failure to complete that training obligation may result in administrative or regulatory action, including fines or penalties.

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

Criminal liability may occur for violations of applicable law. This liability may occur, for example, if the conduct violates a law such as the FCPA, which prohibits the payment of bribes to non-US government officials to obtain an improper advantage. Payment of the bribe would result in criminal liability for the bribe payer. Organisations that face criminal liability, however, do so based on the underlying law, rather than the failure to maintain an effective compliance programme.

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

Those who participate in the underlying misconduct run the risk of civil liability. Generally, however, without the active involvement of governing body members or management in the misconduct, the risk of personal liability is low. Liability could occur, however, if private litigants establish that management failed in its oversight duties in a securities law action, or if as part of a government-negotiated settlement, management makes representations about the compliance programme that are later determined to be incorrect.

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

In general, members do not face the risk of administrative or regulatory consequences for compliance programme management issues. Risk could occur, however, if members participate in the underlying misconduct or undertake specific obligations regarding compliance as part of a government settlement and fail to fulfil those obligations.

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

If members of governing bodies and senior management participate in the underlying criminal misconduct, there may be liability. Without active involvement in the criminal misconduct, the risk of criminal liability to board members and senior management is low for failing to implement compliance programme obligations.

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

There is no corporate compliance defence. Having an effective compliance programme, however, may result in the reduction of fines, penalties and other adverse actions in the settlement of the enforcement action.

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

In 2017 and 2018, there were a number of settlements involving the failure of organisations to manage compliance risks. Notable settlements included:

- In September 2017, Telia Company AB agreed to pay US$965 million to resolve FCPA violations in Uzbekistan, with some of those payments being allocated to Dutch and Swedish authorities. Its Uzbek subsidiary, Coscom LLC, agreed to plead guilty to FCPA violations.
- In November 2017, SBM Offshore NV agreed to pay US$238 million to resolve FCPA offences in Brazil, Angola, Equatorial Guinea, Kazakhstan, and Iraq. SBM entered into a deferred prosecution agreement with the DOJ. One of its subsidiaries pleaded guilty to conspiracy to violate the anti-bribery provisions of the FCPA.
- In December 2017, Keppel Offshore & Marine Ltd and its subsidiaries agreed to pay penalties totalling more than US$422 million to authorities in the United States, Brazil and Singapore, of which US$105 million will paid to the US. The US company, Keppel Offshore & Marine USA Inc, pleaded guilty to conspiracy to violate the anti-bribery provisions of the FCPA.
- In February 2018, US Bancorp agreed to pay penalties, both civil and criminal, of US$613 million after being charged with having a defective anti-money laundering compliance programme and seeking to hide the weaknesses from federal regulators. The company, among other actions, had restricted its transaction monitoring systems to levels based upon staffing levels and available resources, rather than based on the risks present in the transactions.
- In February 2018, Rabobank National Association, a subsidiary of Dutch-based Rabobank, forfeited more than US$368 million, pleading guilty to defrauding the US and to obstructing an examination by the US Office of the Comptroller of the Currency. Prior to the plea, the former anti-money laundering investigations manager for the bank had pleaded guilty to aiding and abetting anti-money laundering violations.

In addition, several individuals were sentenced to prison for FCPA violations, and a number of individuals were charged or had pleaded guilty and are awaiting sentencing. For example:

- In July 2017, Dmitrij Harder, a Russian national living in Pennsylvania, was sentenced in federal court in Philadelphia to 60 months in prison for bribing an officer at the European Bank for Reconstruction and Development and ordered to forfeit US$1.9 million. He had previously pleaded guilty in 2016 to violating the FCPA.
- In September 2017, Amadeus Richers, a German citizen living in Brazil, was sentenced to time served plus three years of supervised release. He had previously pleaded guilty to conspiracy to violate the FCPA and admitted that from 2001 until 2004 he and his co-conspirators paid US$3 million in bribes to officials at Telecommunications D'Haiti.
- In September 2017, Frederic Pierucci, a French citizen, was sentenced to 30 months in prison for bribing officials in Indonesia. Pierucci was vice president of global sales for an Alstom SA subsidiary in Connecticut. He was also fined US$20,000 by the federal court in New Haven, Connecticut. He had previously pleaded guilty in 2013 to an FCPA conspiracy and a substantive FCPA offence.

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

There are no specific obligations for government entities or agencies regarding implementing or maintaining compliance programmes. Government employees, like private sector employees who engage in misconduct, may be charged under applicable law.

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

There are no specific compliance obligations of governments or government agencies.

Arnold & Porter

Keith M Korenchuk **keith.korenchuk@arnoldporter.com**

601 Massachusetts Ave, NW
Washington, DC 20001
United States

Tel: +1 202 942 5817
Fax: +1 202 942 5999
www.arnoldporter.com

Do DOJ policy and the ISO compliance standard overlap?

Daniel Lucien Bühr
Lalive

Overview

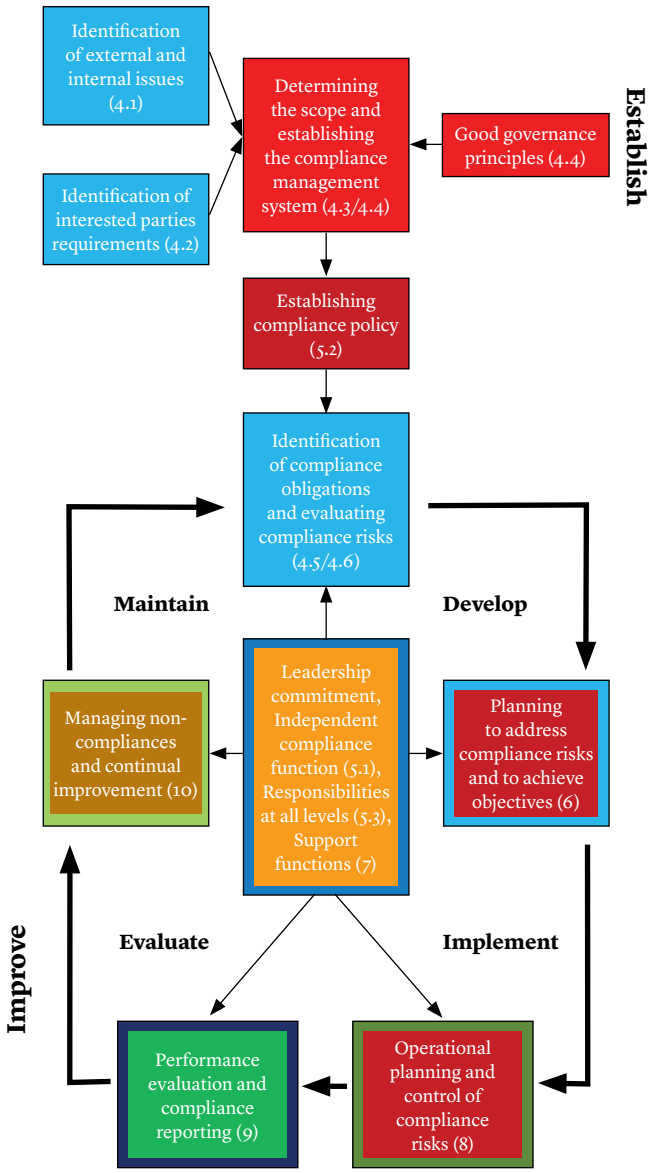
In February 2017, the Fraud Section of the United States Department of Justice's Criminal Division published a document entitled 'Evaluation of Corporate Compliance Programs',[1] its most recent communication of the DOJ's assessment criteria for effective corporate compliance programmes. The DOJ recognises that each company's risk profile and the solutions it adopts to reduce risks should be evaluated on their own merits. The DOJ therefore tailors its determination to each case. However, even tailored determinations raise many of the same questions. The DOJ document explains the questions the DOJ may ask about a corporate compliance programme. However, it gives no guidance on how companies can provide the right answers.

In December 2014, the International Organization for Standardization published ISO International Standard 19600 – Compliance management systems – Guidelines,[2] which helps organisations establish, develop, implement, evaluate, maintain and improve an effective and responsive compliance management system. It is the first international standard on state-of-the-art compliance management and provides the basis for other international standards, such as ISO 37001 – Anti-bribery management systems.

The DOJ document and ISO 19600 differ, yet they have a shared preventive goal. The following table shows that US policy and the Standard are largely compatible, and that ISO 19600 is an appropriate way to bring companies to a level of compliance management that allows them to provide the right answers to the DOJ's questions, should that be necessary. The table below illustrates the overlap between the DOJ and ISO guidance; the flowchart opposite illustrates the management system that the Standard advocates. The colour scheme of both graphics indicates the topical overlap.

No.	DOJ document topic	ISO 19600, sections	Overlap?
1	Analysis of underlying misconduct	Introduction; 10.1	Yes[3]
2	Senior and middle management	Introduction; 4.4; 5.1; 7.3.2.3	Yes
3	Autonomy and resources	4.4; 5.3; 5.3.4	Yes
4	Policies and procedures	5.1; 5.2; 5.2.1; 5.3.4; 6.2; 8.1; 8.2; 9; 9.1; 9.1.6	Yes
5	Risk assessment	4.6; 6.1	Yes
6	Training and communications	5.3.4; 7.2.2; 7.3.2.3; 9.1.6;	Yes
7	Confidential reporting and investigation	5.3.3; 9.1.7; 9.2; 10.1.2	Yes
8	Incentives and disciplinary measures	5.3.4; 7.3.2.2; 7.3.2.3; 10	Yes
9	Continuous improvement, testing and review	9.2, 9.3 and 10.2	Yes (principles)
10	Third-party management	8.3	Yes (principles)[4]
11	Mergers and acquisitions	N/A	N/A

Flowchart of an ISO 19600 – Compliance management system:[5]



The ISO Standard introduces a transparent management system that is auditable and cost-efficient. The Standard represents state-of-the-art compliance management and provides a basis for the legal presumption of diligent management.

In the following we reproduce in abridged form the DOJ's document going through the sample topics and questions section by section and highlighting the overlap with the ISO Standard:

1. Analysis and remediation of underlying misconduct

Root Cause Analysis – What is the company's root cause analysis of the misconduct at issue? What systemic issues were identified? Who in the company was involved in making the analysis?

Prior Indications – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations involving similar issues? What is the company's analysis of why such opportunities were missed?

Remediation – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

The Standard does not ask questions related to past conduct. However, its Introduction states that regulatory and judicial bodies can benefit from the Standard as a benchmark when considering an organisation's commitment to compliance through its management system.

In Section 10 – Improvement, the Standard lists actions an organisation should take if it detects non-compliance. These actions include the elimination of the root causes of non-compliance and the required remedial changes to the compliance management system.

2. Senior and middle management

Conduct at the Top – How have senior leaders, through their words and actions, encouraged or discouraged the type of misconduct in question? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How does the company monitor its senior leadership's behavior? How has senior leadership modelled proper behavior to subordinates?

Shared Commitment – What specific actions have senior leaders and other stakeholders . . . taken to demonstrate their commitment to compliance, including their remediation efforts? How is information shared among different components of the company?

Oversight – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

The ISO Standard recommends that the governing body (in companies, the board of directors) and top management demonstrate leadership of and commitment to the compliance management system by establishing and upholding the core values of the organisation and ensuring that the necessary resources are available, allocated and assigned (section 5.1. a, d). They should also ensure alignment between operational targets and compliance obligations (Section 5.1. i) and establish and maintain accountability mechanisms, including timely reporting on compliance matters, including non-compliance (Section 5.1. j).

Under Section 7.3.2.3 – Compliance culture, the development of a compliance culture requires the active, visible, consistent and sustained commitment of the governing body and management to a common, published standard of behaviour that is required throughout every area of the organisation.

The Standard requires direct access of the compliance function to the board and compliance training at all levels (Sections 4.4 and 7.2.2)

3. Autonomy and resources

Compliance Role – Was compliance involved in training and decisions relevant to the misconduct? Did the compliance or relevant control functions . . . ever raise a concern in the area where the misconduct occurred?

Stature – How has the compliance function compared with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? . . .

Experience and Qualifications – Have the compliance and control personnel had the appropriate experience and qualifications for their roles and responsibilities?

Autonomy – Have the compliance and relevant control functions had direct reporting lines to anyone on the board of directors? How often do they meet with the board of directors? Are members of the senior management present for these meetings? Who reviewed the performance of the compliance function and what was the review process? Who has determined compensation/bonuses/raises/hiring/termination of compliance officers? Do the compliance and relevant control personnel in the field have reporting lines to headquarters? . . .

Empowerment – Have there been specific instances where compliance raised concerns or objections in the area in which the wrongdoing occurred? How has the company responded to such compliance concerns? Have there been specific transactions or deals that were stopped, modified, or more closely examined as a result of compliance concerns?

Funding and Resources – How have decisions been made about the allocation of personnel and resources for the compliance and relevant control functions in light of the company's risk profile? Have there been times when requests for resources by the compliance and relevant control functions have been denied? If so, how have those decisions been made?

Outsourced Compliance Functions – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? What has been the rationale for doing so? Who has been involved in the decision to outsource? How has that process been managed (including who oversaw and/or liaised with the external firm/consultant)? What access level does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

Section 4.4 of the Standard mentions three principles of good compliance governance: the compliance function should (i) have direct access to the board, (ii) be independent (from line management) and (iii) have appropriate authority and adequate resources.

The compliance function and its tasks are defined in Section 5.3.4. The Standard provides a check-list of the compliance function's tasks ranging from identifying the organisation's compliance obligations to the implementing a compliance reporting and documenting system and the provision of objective compliance advice to the organisation.

Section 5.3.4 states that the compliance function should demonstrate integrity, effective communication skills and an ability and standing to command acceptance of its guidance and have the relevant competence.

Outsourced processes are addressed in Section 8.3. All outsourced processes (compliance-related or not) should be monitored for compliance and are subject to effective compliance due diligence to maintain the organisation's standards and commitment to compliance.

4. Policies and procedures

a. Design and Accessibility

Designing Compliance Policies and Procedures – What has been the company's process for designing and implementing new policies and procedures? Who has been involved in the design of policies and procedures? Have business units/divisions been consulted prior to rolling them out?

Applicable Policies and Procedures – Has the company had policies and procedures that prohibited the misconduct? How has the company assessed whether these policies and procedures have been effectively implemented? How have the functions that had ownership of these policies and procedures been held accountable for supervisory oversight?

Section 5.2 of the Standard holds that the organisation's compliance policy should (among other aspects) outline the scope of the compliance management system, the extent to which compliance will be integrated with other functions, and the degree to which compliance will be embedded into operational policies, procedures and processes. This policy should be available as documented information and be written in plain language so that all employees can easily understand the principles and intent.

Gatekeepers – Has there been clear guidance and/or training for the key gatekeepers (e.g., the persons who issue payments or review approvals) in the control processes relevant to the misconduct? What has been the process for them to raise concerns?

Key gatekeepers are not specifically addressed in the Standard. However, under Section 5.3, the responsibilities and authorities for all relevant roles (ie, governing body, senior management, compliance function, other management and employees) should be assigned and communicated within the organisation.

Accessibility – How has the company communicated the policies and procedures relevant to the misconduct to relevant employees and third parties? How has the company evaluated the usefulness of these policies and procedures?

Section 7.5.3 holds that documented information . . . should be controlled to ensure: a) it is available, accessible and suitable for use, where and when it is needed . . . . Section 8.2 – Establishing controls and procedures – recommends that clear, practical and easy to follow documented operating policies, procedures, processes and work instructions be established.

b. Operational Integration

Responsibility for Integration – Who has been responsible for integrating policies and procedures? With whom have they consulted . . .? How have they been rolled out . . .?

According to Section 5.3.4, the compliance function, working with management, should be responsible for integrating compliance obligations into existing operational policies and procedures.

Controls – What controls failed or were absent that would have detected or prevented the misconduct? Are they there now?

Payment Systems – How was the misconduct in question funded . . .? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

Approval/Certification Process – How have those with approval authority or certification responsibilities in the processes relevant to the misconduct known what to look for, and when and how to escalate concerns? What steps have been taken to remedy any failures identified in this process?

According to Section 8.1 – Operational planning and control, the organisation should plan, implement and control the processes needed to meet compliance obligations.

The Standard does not address the funding of misconduct. But Section 9.1.7 – Compliance reporting states that the governing body, management and the compliance function should ensure that they are effectively informed on the performance of the compliance management system, including all relevant non-compliance.

Section 9.1.7 recommends that there be sign-off on the accuracy of reports to the governing body, including by the compliance function.

Vendor Management – If vendors had been involved in the misconduct, what was the process for vendor selection and did the vendor in question go through that process?

Vendor management is not specifically addressed in the Standard, but Section 8.3 covers all outsourced processes and holds that organisations should consider compliance risks related to other third-party-related processes, such as supply of goods and services, and distribution of products, and put controls in place, as necessary.

5. Risk assessment

Risk Management Process – What methodology has the company used to identify, analyze, and address the particular risks it faced?

Information Gathering and Analysis – What information or metrics has the company collected and used to help detect the type of misconduct in question? How has the information or metrics informed the company's compliance program?

Manifested Risks – How has the company's risk assessment process accounted for manifested risks?

The Standard (see Section 4.6) is based on the methodology of ISO Standard 31000 – Risk management. However, the Standard also leaves room for alternative approaches and methods to identify, analyse and evaluate compliance risks, such as the COSO ERM framework.

The Standard states that a compliance risk assessment is the basis of any compliance management system and that a risk assessment process essentially consists in relating the compliance obligations (as defined in Section 3.16) to the activities, products and services of the organisation.

6. Training and communications

Risk-Based Training – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees that addressed the risks in the area where the misconduct occurred? What analysis has the company undertaken to determine who should be trained and on what subjects?

Form/Content/Effectiveness of Training – Has the training been offered in the form and language appropriate for the intended audience? How has the company measured the effectiveness of the training?

Communications about Misconduct – What has senior management done to let employees know the company's position on the misconduct that occurred? What communications have there been generally when an employee is terminated for failure to comply with the company's policies, procedures, and controls . . .?

Availability of Guidance – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

Section 7.2.2 of the Standard outlines training principles. Education and training of employees should be tailored to the obligations and compliance risks of employees, aligned with the corporate training programme and incorporated into annual training plans.

Training should be practical, readily understood and relevant to employees' day-to-day work. Education and training should be assessed for effectiveness and updated as required. Compliance performance should be measured by indicators such as the percentage of employees effectively trained, the frequency of contact by regulators, the usage of feedback mechanisms etc (Section 9.1.6 – Development of indicators).

Section 7.3.2.3 – Compliance culture – mentions ongoing communication on compliance issues and prompt and proportionate disciplining of wilful or negligent breaches of compliance obligations as examples of factors that will support the development of a compliance culture.

According to Section 5.3.4, the compliance function should provide employees with access to resources on compliance procedures and references and provide objective advice to the organisation on compliance-related matters. Inversely, employees should use available compliance resources and participate in training (Section 5.3.6 – Employee responsibility).

7. Confidential reporting and investigation

Effectiveness of the Reporting Mechanism – How has the company collected, analyzed, and used information from its reporting mechanisms? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

Properly Scoped Investigation by Qualified Personnel – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

Response to Investigations – Has the company's investigation been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

Section 10.1.2 of the Standard outlines the escalation process: an effective compliance management system should include a mechanism for employees and others to report suspected or actual misconduct, or violations of the organisation's compliance obligations, confidentially and without fear of retaliation.

Section 9.1.5 holds that information classification and management is critical. Information collected needs to be analysed and assessed to identify root causes.

According to Section 5.3.3, the organisation's governing body and top management should appoint a compliance function with access to all information needed to perform compliance tasks.

The compliance function can conduct audits as required (Section 9.2). The audit criteria and scope of each audit should be defined and auditors should be selected and audits be conducted to ensure objectivity and the impartiality of the audit process.

Top management should ensure that effective and timely systems of reporting are in place (Section 5.3.3). All non-compliance needs to be appropriately reported (Section 9.1.7).

8. Incentives and disciplinary measures

Accountability – What disciplinary actions did the company take in response to the misconduct and when did they occur? Were managers held accountable for misconduct that occurred under their supervision? Did the company's response consider disciplinary actions for supervisors' failure in oversight? What is the company's record (e.g., number and types of disciplinary actions) on employee discipline relating to the type(s) of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

Human Resources Process – Who participated in making disciplinary decisions for the type of misconduct at issue?

Consistent Application – Have the disciplinary actions and incentives been fairly and consistently applied across the organization?

Incentive System – How has the company incentivized compliance and ethical behavior? How has the company considered the potential negative compliance implications of its incentives and rewards? Have there been specific examples of actions taken (e.g., promotions or awards denied) as a result of compliance and ethics considerations?

Section 10 of the Standard holds that when non-compliance occurs, the organisation should take action to correct it, eliminate the root causes, implement any action needed and review the effectiveness of corrective action.

Section 7.3.2.3 underlines the need for prompt and proportionate disciplining in the case of wilful or negligent breaches of compliance obligations.

The compliance function should be responsible for promoting the inclusion of compliance responsibilities into job descriptions and employee performance management processes (Section 5.3.4).

Section 7.3.2.2 states that senior management has a key responsibility for ensuring that operational objectives and targets do not compromise compliant behaviour.

9. Continuous improvement, periodic testing and review

Internal Audit – What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?

Control Testing – Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?

Evolving Updates – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

Section 9.2 of the Standard holds that the organisation should conduct audits at least at planned intervals to provide information on whether the compliance management system conforms to the organisation's own criteria for its compliance management system and the recommendations of the Standard, and is effectively implemented and maintained. The audit results should also be reported to the management.

Section 9.3 holds that the organisation should retain documented information as evidence of the results of management reviews and provide copies to the governing body.

Section 10.2 recommends that the organisation should seek to continually improve the suitability, adequacy and effectiveness of the compliance management system. The information collected, analysed and evaluated accordingly, and included in compliance reports, should be used as the basis for identifying opportunities to improve the organisation's compliance performance.

10. Third-party management

Risk-Based and Integrated Processes – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

Appropriate Controls – What was the business rationale for the use of the third parties in question? What mechanisms have existed to ensure that the contract terms specifically described the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

Management of Relationships – How has the company considered and analyzed the third party's incentive model against compliance risks? How has the company monitored the third parties in question? How has the company trained the relationship managers about what the compliance risks are and how to manage them? How has the company incentivized compliance and ethical behavior by third parties?

Real Actions and Consequences – Were red flags identified from the due diligence of the third parties involved in the misconduct and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues? How has the company monitored these actions (e.g., ensuring that the vendor is not used again in case of termination)?

Section 8.3 of the Standard holds that the organisation should consider compliance risks related to third-party-related processes, such as supply of goods and services and distribution of products, and put controls in place.

The Standard also holds that outsourcing of operations usually does not relieve the organisation of its legal responsibilities or compliance obligations. If there is any outsourcing of activities, the organisation needs to undertake effective due diligence to maintain its standards and commitment to compliance.

ISO Standard 37001 on anti-bribery management systems, specifies in detail the requirements of best practice third-party due diligence, monitoring, auditing and the corrective actions that must be taken in case of non-compliance.

11. Mergers and acquisitions

Due Diligence Process – Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What has been the M&A due diligence process generally?

Integration in the M&A Process – How has the compliance function been integrated into the merger, acquisition, and integration process?

Process Connecting Due Diligence to Implementation – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures at new entities?

The Standard does not specifically address M&A-related due diligence and compliance risk management. But any acquisition is part of a company's business conduct and therefore subject to proper due diligence, particularly also post-acquisition.

Notes

1 See: https://www.justice.gov/criminal-fraud/strategy-policy-and-training-unit/compliance-initiative
2 See: https://www.iso.org/standard/62342.html
3 However, ISO 19600 is "forward looking" and general and not meant to provide answers to individual cases.
4 ISO Standard 37001 – Anti-bribery management systems is more detailed.
5 The Flowchart of a compliance management system taken from ISO 19600:2014 is reproduced with the permission of the International Organization for Standardization, ISO. The numbers in the chart cells refer to the relevant sections of the Standard, which can be obtained from any ISO member and from the website of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-78915-067-4