Risk & Compliance Management 2019

Contributing editor
Daniel Lucien Bühr
Lalive

LEXOLOGY
Getting The Deal Through

LALIVE

LALIVE

THE DISPUTES POWERHOUSE

Geneva Zurich London

lalive.law

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

Dan White
dan.white@gettingthedealthrough.com

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
Third edition
ISBN 978-1-83862-111-7

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

Risk & Compliance Management 2019

Contributing editor
Daniel Lucien Bühr
Lalive

Lexology Getting The Deal Through is delighted to publish the third edition of *Risk & Compliance Management*, which is available in print and online at www.lexology.com/gtdt.

Lexology 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 Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured.

Lexology 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.lexology.com/gtdt.

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.

Lexology 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.

LEXOLOGY®
Getting The Deal Through

London
April 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

Global overview

Daniel Lucien Bühr
Lalive

The third edition of *Risk & Compliance Management* of the Lexology Getting The Deal Through series reflects digital transformation. The questionnaire now also addresses risk and compliance management, specifically regarding new technologies and tools such as machine learning, artificial intelligence (AI), robots and blockchain.

It is surely too early for asking all the right risk and compliance questions regarding digital transformation, or even for providing the right answers. However, risk and compliance management experts around the globe understand the importance of asking governance, risk and compliance questions regarding digital technologies and searching for the right answers. At this early stage, it may be wiser to start by analysing the ethical and legal principles and due process rules when addressing the challenges of new tools and processes.

One of the key questions is always 'Who is accountable and liable for a specific action (or omission)?' If a bank client uses the bank's robo-adviser (ie, an online, automated portfolio management service that uses computer algorithms instead of human advice) and the client then loses money as a result of a material defect of the robot, can the bank then blame the robot and argue that as the robot is equipped with AI, is outside its scope of control and therefore the bank cannot be held liable? What if the robot was not defective but the advice followed a widely spread programming pattern, which created a systemic market risk and led to widespread losses of investors?

According to legal concepts in the civil law and common law systems, the liability for any action or omission falls to an individual or a legal entity. Therefore, individuals and entities will always remain liable for engaging in digital technological means. Accordingly, and ethically rightly so, whatever individual or entity employs digital means shall bear ultimate accountability and liability for damages caused by these means. The individuals and entities have a duty of care (ie, they must act diligently) and are liable for any simple fault.

Digital transformation does not change the principles of good governance or the methodology of effective risk and compliance management. However, we need to think about how the principles and methods are applied to the challenges ahead. What is the role of board members, in particular members of audit committees, when they exercise their role as ultimate leaders and supervisors? How can they spot risks and ask the right questions in order to avoid defects, fraud, mismanagement, anti-competitive behaviour, corruption or money laundering hidden in robots and 'intelligent' or 'self-learning' systems? Also, how can they promote and uphold an organisational culture of transparency, integrity and accountability in an increasingly virtual business reality?

The more we think of the beautiful new digital world, the more we will realise that risk sources, the uncertainty of events and developments, and the effects of the uncertainty on objectives will change. And given the rapid growth of data volumes and transactions, the risks will multiply or even grow exponentially. And with the changing and growing risks, legal risks will also change and grow. My prediction, therefore, is that in a few years we will experience not only the large-scale chances but also the large-scale risks of digital transformation. And we will see instances of large-scale non-compliance based on the new digital means.

To benefit from the chances and effectively manage the risks of digital transformation, both private and public organisations should consider ubiquitous ethical values, legal principles and fundamental human rights, and follow international best-management practices in their systematic and diligent risk and compliance management. The time to do so and 'get all men and women on deck' is right now.

I hope you enjoy the 2019 edition of *Risk & Compliance Management* and find it interesting and of value to your business.

Argentina

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

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

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

With regard to corruption risk management, the Argentine Anti-Corruption Law No. 27,401, in force since 1 March 2018, criminalises certain illegal interactions between legal entities and public officials or officials of public international organisations, such as bribery.

Law No. 27,401 also regulates anti-corruption integrity programmes. Such integrity programmes must meet certain requirements imposed by the law such as being appropriate to the specific risks, related to the legal entity's activities, and the size and economic capacity of the legal entity. Implementing risk-based integrity programmes is mandatory for legal entities engaging in certain major contracts with the federal government, but are voluntary for all other legal entities. In all cases, these programmes are key to seeking reductions and even exemptions from penalties under Law 27,401.

The Argentine Anti-Corruption Office enacted guidelines on the design and implementation of integrity programmes under Law No. 27,401, addressing a number of relevant issues such as risk analysis, tone from the top, periodic risk assessments, periodic monitoring, policies, the role of a compliance officer and others factors.

With regard to risk management in the anti-money laundering and anti-terrorist financing field, Law No. 25,246 sets forth that certain subjects, such as financial entities and foreign exchange agencies, must implement a compliance programme addressing such risks. The Financial Information Unit of Argentina issued a set of regulations to clarify the procedures to be followed by such subjects in order to fulfil the compliance provisions of Law 25,246. These regulations generally follow the global standards set forth by the Financial Action Task Force (FATF), such as the 'risk-based approach'.

Certain industry-specific regulations of regulating bodies also address risk and compliance management obligations. For example, Resolution 38,477 of the Federal Superintendence of Insurance addresses risk-based rules on policies, procedures and internal controls to combat fraud for insurance and reinsurance entities, Regulation 'A' 5,398 of the Central Bank of Argentina establishes a mandatory integral process for risk management for financial entities and other processes addressing companies offering securities.

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

In addition, certain industry associations (eg, the Chamber of Argentine Pharma Companies) have enacted ethics codes that provide guidelines on how their members can manage specific risks.

Laws and regulations

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 certain illegal interactions with public officials and officials of public international organisations;
- Resolution 27/2018 of the Argentine Anti-Corruption Office, which approves guidelines regarding the implementation of risk-based anti-corruption compliance programmes;
- Law No. 25,246, which sets forth the obligation for certain subjects to implement a compliance programme focused on risk management;
- Resolutions of the Financial Information Unit, which specifically adopts FATF's standards for the risk-based approach for financial entities and foreign exchange agencies (Resolution 30–E/2017), entities subject to the capital market's regime (Resolution 21/2018), and persons in the insurance sector (Resolution 28/2018);
- Resolution 134/2018 of the Financial Information Unit and its amendments, which set forth risk-based obligations for certain subjects in line with FATF's recommendations in the matter;
- Resolution 38,477 of the Federal 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 that body;
- Regulation 'A' 5,398 of the Central Bank of Argentina, which sets forth the obligation of financial entities to have integral risk management processes;
- Regulation 'A' 6,131/2016 of the Central Bank of Argentina, which establishes the Guidelines for the Settlement of Foreign Exchange Transactions, setting out risk management provisions for financial entities exposed to risks arising in these kind of transactions, between their negotiation and their conclusion; and
- General Resolution 606/2012 of the Argentine Securities Commission that approved the Corporate Governance Code for companies listed for a public offering.

Types of undertaking

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 – those with either local or foreign capital stock, with or without government participation – that engage in certain major contracts with the federal government. Other legal entities 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 cases of breaches of Law No. 27,401.

The anti-money laundering and anti-terrorist financing regulations apply to all legal entities and individuals. However, specific risk-based compliance provisions regarding, among others, the implementation of compliance programmes, 'know your customer' procedures and reporting obligations, apply only to a specific number of subjects, such as the following:

- financial entities;
- foreign exchange offices and foreign exchange agencies;
- undertakings in the gambling industry;
- 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, aircraft and vehicles;
- individuals and legal entities engaged in transactions related to works of art, antiques, sumptuary assets, jewels and precious stones;
- insurance companies;
- issuers of travellers cheques and credit and debit cards;
- companies providing armoured transportation services;
- mailing companies providing currency transfer services;
- public notaries;
- customs brokers; and
- regulatory agencies.

Industry-specific regulations apply to certain subjects such as financial entities and insurance companies. Entities issuing securities in regulated markets are also subject to compliance regulations.

Regulatory and enforcement bodies

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

The Argentine Anti-Corruption Law No. 27,401 is enforced by the criminal courts with the participation of prosecutors. In addition, the Argentine Anti-Corruption Office enforces administrative anti-corruption regulations. This office, which has powers to investigate and report cases to prosecuting authorities plays a key role in investigating corruption cases and closely follows up on developments of such cases with the courts.

The Financial Information Unit is entrusted with the analysis, investigation, treatment, reporting (eg, to prosecutors) and communication of information or suspicions regarding money laundering and terrorist financing. It is also authorised to apply sanctions on undertakings and report cases to criminal prosecutors.

The Central Bank of Argentina is the main regulatory and enforcement agency for financial institutions, having auditing and sanctioning powers.

The Argentine Securities Commission has regulatory and sanctioning powers over listed companies.

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

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

Definitions

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

In general terms, most of the regulations mentioned above define 'risk and compliance management' or, at least, provide some clarifications, recommendations and factors to be considered while performing risk and compliance management obligations. For example, Law No. 27,401 does not provide definitions of 'risk management' or 'compliance management' as such, but it establishes that integrity programmes shall be implemented or improved according to the results of proper anti-bribery and anti-corruption risk analysis.

The guidelines on integrity programmes of the Anti-Corruption Office establish additional provisions that thoroughly addressed 'risk management' and 'compliance management', giving details on the processes and the issues to be considered. A similar approach is taken by anti-money laundering and terrorism financing regulations.

Processes

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

The laws and regulations mentioned above usually 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 that Law. To help legal entities comply with the requirements of Law 27,401, as mentioned, the Argentine Anti-Corruption Office enacted guidelines on integrity programmes specifically addressing risk assessment, compliance programme assessment and the office's suggested procedures.

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

Standards and guidelines

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

Law No. 27,401, passed by Congress in 2017, establishes that integrity programmes must be appropriate to the specific risks related to the activities, size and economic capacity of a legal entity, in accordance with further regulations of this law to be enacted by the relevant authorities.

Additionally, the main standards and guidelines regarding anti-corruption and bribery, and risk and compliance management processes, are those enacted by the Argentine Anti-Corruption Office through Resolution 27/2018. The guidelines' main goal is to 'provide technical guidance for companies, civil society organisations, other legal entities, state agencies, members of the justice system and the professional community'. These guidelines also highlight that integrity programmes 'must be tailored to each legal entity taking into consideration its own needs, characteristics and culture, as well as the context in which it operates and its associated risks'.

Anti-money laundering and anti-terrorism financing standards and guidelines are provided in Law No. 25,246, passed by Congress in 2000, and its amendments, and the regulations issued by the Financial Information Unit. For example, Resolution 30–E/2017, issued by the Financial Information Unit, establishes a minimum standard for risk and compliance management processes, providing that the risk self-assessments must be appropriate to the nature and business capacity (considering all business units) of the entities subject to the regulation and take into account specific risk factors such as 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 regulation, based on its activities.

Regulation 'A' 5,398 of the Central Bank of Argentina provides that each financial entity must issue its own risk management strategies and policies according to the guidelines provided therein regarding, among others, credit risks, liquidity risks and market risks. Also, Regulation 'A' 6,131/2016 of the Central Bank establishes the Guidelines for the Settlement of Foreign Exchange Transactions addressing risk management applicable to financial entities.

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.

Obligations

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

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

Law No. 27,401 does not provide governance obligations on anti-corruption risks, although it provides guidelines on integrity programmes, including clear and affirmative support to the programme by the legal entity's top management. Also, the Anti-Corruption Office's guidelines on integrity programmes focus on the 'tone from the top' element, establishing a set of recommendations to achieve management's participation. Also, the guidelines recommend legal entities to appoint a compliance officer within the management hierarchy and ensures the officer has full access to the entity's top management.

Law No. 25,246 addresses anti-money laundering and counter-terrorism financing and sets forth the obligation for certain subjects to appoint a compliance officer, who must be a member of the governing body. The officer's personal information must be supplied to the Financial Information Unit.

Resolution 38,477, which applies to the insurance and reinsurance industry, specifically addresses the obligation to appoint a regular compliance officer, who must be of at least senior executive level.

Listed corporations are subject to compliance obligations. 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.

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

Broadly speaking, the general approach of the different regulations is to adopt proper compliance programmes in accordance with applicable laws and as a result of specific risk analysis.

Pursuant to Law No. 27,401, undertakings that implement an integrity programme shall conduct appropriate risk analysis as the basis for drafting and updating such programmes. According to the risks identified, the integrity programme may have different elements including, at least, a code of ethics or conduct or integrity policies, internal policies to prevent crimes during any interaction with the public sector, and periodic training. Other elements that may be necessary to implement are the appointment of a compliance officer, third-party due diligence procedures and whistle-blowing channels.

According to the anti-money laundering and anti-terrorism financing laws, certain key individuals and legal entities must implement compliance procedures, including anti-money laundering and anti-terrorism financing codes, that describe rules and procedures to be followed.

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, which must be periodically adjusted considering changes in the entity and the market.

Resolution 38,477 establishes, insurance and reinsurance entities' obligation to implement a fraud-related compliance policy following certain minimum legal requirements.

According to Resolution 606/2012 of the Argentine Securities Commission, a listed company's Corporate Governance Code may include, among others, an integral corporate risk management policy issued by the entity's top management and assessments of the policy's implementation.

LIABILITY

Liability of undertakings

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 set forth specific obligations applicable to members of governing bodies and senior management. However, the anti-corruption guidelines on integrity programmes address the relevance of members of governing bodies and senior management participating in training, approving the company's code of conduct, and generally supporting the compliance programme.

Most of the above-mentioned Financial Information Unit's resolutions specifically address obligations of members of governing bodies and senior management, such as approving the methodology and results of self-assessment of risks, appointing a compliance officer, and their role as members of the Committee to prevent money laundering and terrorism financing.

Pursuant to Regulation 'A' 5398 of the Central Bank, there are different obligations for members of governing bodies and the senior management of financial entities. The entity's board of directors is accountable for the adequateness of risk management policies and credit risks assumed by the entity and its management. Therefore, the board must, among other actions, approve and review credit policies and strategies, approve the entity's threshold of risk tolerance, and ensure senior management capabilities for managing credit transactions are met according to the entity's risk policies. Regarding senior management, the regulation establishes that they are in charge of implementing the risk management policies approved by the board of directors and setting forth written procedures to identify, assess, follow up, control and mitigate credit risks.

In any case, the governing bodies and senior management must also comply with the general fiduciary duties set forth in section 59 of the General Corporate Law, irrespective of whether the legal entities at which they perform duties have risk and compliance management obligations or not.

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

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 face administrative or regulatory consequences for risk and compliance management deficiencies only if laws and regulations specifically provide them.

In particular, there are no administrative or regulatory consequences for risk and compliance management deficiencies under Law No. 27,401, but there are administrative fines established in Law 25,246 for breach of anti-money laundering and anti-terrorism financing risk and compliance management obligations.

Also, other regulations issued by regulatory authorities establish consequences for risk and compliance management deficiencies shown by those individuals or entities subject to its powers. For example, non-compliance with regulations issued by the Central Bank of Argentina and the Argentine Securities Commission may cause financial entities and listed companies to face regulatory sanctions such as fines, suspensions and disqualifications from operating.

In a similar way, the National Superintendence of Insurance has the power to establish administrative sanctions on insurance and reinsurance entities in cases of breaches of regulations that were enacted by the regulator regarding, for example, failure to comply with risk and compliance management. Such administrative sanctions include fines, warnings and suspensions to operate.

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, in case of deficiencies in the integrity programme, legal entities may be affected as they may be ineligible for reductions or exemptions from penalties. The other relevant laws and regulations mentioned above do not establish criminal liability for risk and compliance management deficiencies alone. However, fines and regulatory sanctions may be imposed.

Liability of governing bodies and senior management

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 breaching compliance management obligations if they do not establish the proper risk and compliance management required according to relevant regulations applicable to the legal entity and act in a way that is considered a breach of their fiduciary duties of loyalty and care, which are established in section 59 of Argentine Corporate Law.

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

Yes. For example, the Central Bank of Argentina and the Financial Information Unit are entitled to impose administrative sanctions (eg, fines, suspensions and disqualifications) for breaches of established obligations on members of governing bodies and senior management performing functions within regulated entities.

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

There is no regulation that criminalises members of governing bodies and senior management for breaching 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 and compliance management may trigger breaches of administrative, civil, criminal and other regulations.

CORPORATE COMPLIANCE

Corporate compliance defence

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

Law No. 27,401 makes corporate compliance one of the elements that judges must consider when deciding on penalties to be imposed. Further, legal entities may be exempted from penalties and administrative responsibility if they:

- spontaneously self-report a crime set forth by this law as a consequence of internal detection and investigation;
- had established a proper integrity programme before the facts under investigation, which required an effort by the wrongdoers to breach it; and
- return the undue benefit obtained through the crime.

Also, legal entities may enter into effective collaboration agreements that establish as conditions that the legal entity must:

- pay 50 per cent of the minimum fine;
- return the things and profits obtained through the crime; and
- surrender those goods that presumably would be forfeited in case of conviction.

Additionally, such agreements may establish the condition that a compliance programme must be implemented or the current programme adjusted, among other requirements.

No 'actual defences' are established in anti-money laundering and anti-terrorism financing regulations, but certain factors for reduction in penalties are addressed, such as compliance with internal rules and procedures, omission of vigilance on the actions of wrongdoers, and the size, nature and economic capacity of the legal entity, and others.

Recent cases

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 with the courts, although administrative sanctions have been imposed.

Government obligations

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

In early 2018, through the Administrative Decision 85/2018, the government enacted guidelines on good governance for state-owned companies and those with government participation which addresses among others, risk and compliance management. In particular, it has a whole chapter about risk-based audits and controls and others addressing integrity and compliance programmes.

Additionally, some government agencies (eg, the Federal Tax Authority) have voluntarily implemented compliance management process and obligations (ie, code of conduct, and training) seeking transparency, ethics and compliance.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

There are no significant compliance regulations specifically addressing digital transformation. That being said, any companies involved in digital transformation would be subject to Anti-Corruption Law No. 27,401 and, depending on its activities and operations, it could be subject to other compliance-related regulations mentioned in the paragraphs above.

UPDATE AND TRENDS

Current developments and emerging trends

21 Are there any other current developments or emerging trends that should be noted?

While anti-money laundering and regulatory compliance are stable areas of the law, anti-corruption compliance and enforcement is showing major growth in Argentina in terms of laws and regulations, enforcement and interest from companies.

Pedro Serrano Espelta
pse@marval.com

Gustavo Morales Oliver
glo@marval.com

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

Brazil

Bruno De Luca Drago and Fabianna Vieira Barbosa Morselli
Demarest Advogados

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

Corporate risk and compliance management has 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 in 2014, which determine that the execution of an effective integrity programme can reduce penalties imposed on legal entities by up to 20 per cent.

Equally important is Law No. 12,850/13, enacted around the same time of the BCCA, which provides for criminal enforcement against '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. 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 pieces of legislation, and partially because of new interpretations of former legislations and burden of proof standards applied by the courts, several Brazilian companies have been dragged into the criminal investigation spotlight – particularly as a result of Operation Car Wash, which was reported on 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.

Laws and regulations

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.

Types of undertaking

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 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'. The law defines 'foreign public agents' as anyone who holds an office, is employed by a civil service, public entity, government entity or diplomatic representations abroad of their home country, such entities being controlled by a foreign government or an international public organisation.

It is important to note that the BCCA did not establish criminal liability of legal entities, but rather administrative and civil liability. Moreover, the law does not exclude the administrative and civil liability of an entity's directors or officers, who 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 succeeding entity 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 infringements perpetrated, with 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 similar perspectives 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.

Regulatory and enforcement bodies

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, when an 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 authority.

In cases 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 Tribunals (over issues of Improbity Law) and the Administrative Counsel of Economic Defence. They deal with competition issues involving bid rigging, among other things.

Definitions

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'.

Processes

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.

Standards and guidelines

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

In Brazil, standards and guidelines regarding risk and compliance management processes are based on legislation and general guidelines that discuss risk and compliance management processes.

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

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:

- the engagement of senior management of the company;
- the implementation of a code of ethics, a code of conduct, and compliance policies applicable to all employees and managers;
- the 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 being granted to a compliance officer;
- an open communication channel for reporting 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.

In addition, in September 2015 the General Comptrollers' Office (CGU), which is the office responsible for the internal monitoring of the Brazilian government, published a document containing general guidelines for private companies that wish to develop or enhance an integrity programme.

In a nutshell, the guidelines establish the five key pillars for an integrity programme:

- commitment and support from the high administration in order to promote a culture of ethics and compliance with the law;
- the necessity of the establishment of an autonomous, independent and impartial body responsible for managing the programme, as well as the adequate resources and personnel for these activities;
- profile and risk assessments in order to have better knowledge of a company's internal processes and the risks it is exposed to;
- structuring of policies and instruments, with frequent training sessions for employees to improve levels of compliance; and
- strategies for continuous monitoring and enhancement of the programme.

Finally, it is important to highlight that the guidelines emphasise that there is no specific formula for the development of an integrity programme, as such programmes need to be tailored to the operations and characteristics of individual company.

Non-governmental benchmarks, such as those resulting from private committees, such as the Corporate Responsibility and Anti-Corruption Committee of the International Chamber of Commerce ICC-Brazil, are also relevant guidelines for companies.

Obligations

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 and 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, that contain, 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 matters.

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 pieces 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 agreement 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 to 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 1.5 million 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. Certain obligations may apply in certain circumstances, such as for participating in the 'new market' of the Brazilian Stock Exchange where higher levels of governance apply.

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

Except for those cases reported 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 legislation.

In this regard, it is recommended that companies implement mechanisms and internal control proceedings against irregularities upon applying application of its conduct and ethics statutes. Such mechanisms, referred to as an 'integrity programme', must be suitable and updated according to the undertaking's activities and requirements. The existence of a well-structured integrity programme helps to diminish penalties in the event of an infringement of compliance or anti-corruption 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.

LIABILITY

Liability of undertakings

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 duties (an 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 administrative fines. As mentioned in question 12, generally companies in Brazil are not obliged to have a well-structured compliance programmes, but having such a programme reduces the probability of incurring compliance-related infringements and enhances the companies' image in the market, creating brand value and increasing its attraction to investors.

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

As stated 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. In addition, the Brazilian Competition Authority (CADE) has established that having a compliance programme or committing to one can be a mitigating factor leading to a reduction of penalties in the event of the conviction for anticompetitive practices.

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 held 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.

Liability of governing bodies and senior management

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 the liability of individuals.

Regarding 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 a freeze of assets, required to return money illegally obtained, or face fines of up to three times of the value obtained illegally, in addition to restoring 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 or cartel membership, 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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

The offenders may present a defence based on a 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.

Recent cases

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 Brazilian Federal Police Department's anti-corruption investigation – and its related operations. The companies targeted were discovered to be part of several corruption and cartel scandals in several different markets in which they are active, shedding light on the importance of a well-structured compliance programmes and regular monitoring. The settlement agreements executed – and these still under negotiation – are also serving to determine the structure of such mechanisms.

The uncovering of these scandals revealed that many relevant Brazilian corporations had a disregard for compliance issues. These scandals also exposed government authorities for being part of the fraudulent schemes and disrespecting the guidelines established in the Brazilian legislation, which led to the enforcement of stronger rules for entities of the public administration.

Government obligations

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).

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

In general, Brazil still has a long way to go concerning the development of risk and compliance governance regarding digital transformation. In fact, the Brazilian authorities rarely discuss themes such as machine learning, artificial intelligence and robots. Blockchain and cryptocurrencies have been discussed more openly, although a specific framework for this subject is still very preliminary. The main concern is how the increase in the use of cryptocurrencies may affect anti-corruption and anti-bribery regulation.

In this respect, the Brazilian authorities recently approved Law No. 13,709/2018 (Brazilian New Data Protection Law), which will bring some relevant changes to the framework of data protection in the next years. For that matter, the New Data Protection Law brings innovations to the current framework in order to match Brazil's scenario to other foreign countries. For example, there are relevant changes in the use of the obtained data, the necessity of written (or equivalent) consent for use of this type of data and the establishment of relevant fines for those who disrespect the legislation (such fines may be up to 2 per cent of the company's revenues in Brazil, limited to the maximum amount of 50 million reais).

The New Data Protection Law is scheduled to come into force in 2020. In practice, this means that companies have about one year to adapt to the legislation's provisions.

UPDATE AND TRENDS

Current developments and emerging trends

21 Are there any other current developments or emerging trends that should be noted?

Alongside the federal anti-corruption legislation, several states in Brazil are also creating specific laws concerning civil and administrative liability for companies that commit infringements against the public administration. In this respect, some states, including Alagoas, the Federal District, Goiás, Maranhão, Mato Grosso, Mato Grosso do Sul, Minas Gerais, Paraná, Rio Grande do Norte, Santa Catarina, São Paulo and Tocantins, already had specific laws concerning the civil and administrative liability in the state sphere. More recently, the states of Pernambuco, Rio Grande do Sul and Rio de Janeiro have also created laws with the same objective. This demonstrates the growing concern of Brazil's state and federal governments with the development of better and stricter controls over conduct that may harm the public administration, especially related to corruption practices.

In addition, we also highlight two new trends that have been growing in Brazil: third-party background checks and the Empresa Pró-Ética (Pro-Ethics Company) programme.

First, for the background checks, we notice that companies are increasingly concerned with secondary and joint liability for illegal behaviour of third parties. In this sense, companies are being more careful about the companies they choose to do business with, implementing strong compliance rules and scrutinising all potential business partners, from suppliers to customers.

The Empresa Pró-Ética programme grants a certificate to companies that meet several requirements regarding integrity, such as transparency, compliance programmes and other measures for detecting and preventing fraud and acts of corruption. This certificate is granted by the Federal Comptrollers' Office (CGU) after a comprehensive assessment and creates brand value and positive publicity for the company. The programme gained relevance in the recent years and went through a reformulation.

Several companies have demonstrated adherence to the programme in recent years. In 2017, it registered 375 applications – a 92 per cent increase from 2016 – but only 23 companies fulfilled the requirements and were recognised with an Empresa Pró-Ética 2017 award.

The main reasons the 352 remaining companies were disqualified were:

- a lack of evidence on the implementation and effectiveness of integrity policies;
- a lack of maturity in the compliance policies;
- inadequacy of the company's programme's structure versus the profile of the company;

- a lack of adaptation of the global programme to Brazil's legal framework; and
- a short time frame for the companies to implement the recommendations formulated in previous versions of the programme.

As from 2018, the certification cycle, from register to the granting of the certificate will occur every two years. This is justified due to the increasing numbers of companies seeking certification and a longer time required for the analysis. Furthermore, most companies were not able to fulfil the recommendations within a one-year time frame.

The submission form will also be simplified, with the aim of making it clearer and more objective, with a focus on evidence of the effectiveness of the company's compliance programme.

Bruno De Luca Drago
bdrago@demarest.com.br

Fabianna Vieira Barbosa Morselli
fmorselli@demarest.com.br

Av Pedroso de Moraes, 1201
Pinheiros
São Paulo 05419–001
Brazil
Tel: +55 11 3356 1800
Fax: +55 11 3356 1700
www.demarest.com.br

China

Gary Gao
Zhong Lun

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

The corporation is a fundamental unit of a society's economy, as well as a crucial civil and commercial subject. Therefore, various laws and regulations on the management and control of corporate risk and compliance management play irreplaceable roles in China's jurisdiction.

Laws and regulations

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

Managing and controlling corporate risk and compliance management is a relatively broad concept, involving all aspects of corporate operation and governance. The most common topics include: strategic risk, financial risk, market risks and operational risks. At present, China does not have a specialised law or regulation integrating the management and control of corporate risk and compliance management. These provisions are spread across laws and regulations governing various fields. Examples of such legislation are the:

- Company Law and Administrative Regulations on Company Registration, which outlines the general requirements for companies;
- Law on Enterprise Income Tax, Basic Rules for Enterprise Internal Control and Financial Rules for Financial Enterprises, which deal with finance risk management;
- Anti-Unfair Competition Law, Labor Contract Law and Interim Regulations on Prohibition of Commercial Bribery, which govern operation risk management; and
- Law on International Judicial Assistance in Criminal Matters, which improves anti-corruption repatriation and asset recovery, and strengthens international cooperation in combating transnational crimes.

Types of undertaking

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, they are all heavily regulated by laws and regulations. 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 internet financial institutions' management and control of risk, such as the management and control 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.

Regulatory and enforcement bodies

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 and the areas they are responsible for, include the:

- Administration for Market Supervision (previously known as the Administration for Industry and Commerce): market supervision and management and law enforcement administration;
- Tax Bureau: classifying taxpayers and administration of tax collection;
- General Administration of Customs: port management, bonded supervision, and management and customs inspection;
- Foreign Exchange Authority: supervising the foreign exchange market, and managing foreign exchange settlements and sales;
- China Securities Regulatory Commission (this mainly concerns listed companies): centralised and unified supervision and management of the securities and futures markets, and supervising listed companies and securities market activities performed by the shareholders of listed companies under their obligations stipulated by the laws and regulations;
- China Banking and Insurance Regulatory Commission (this mainly concerns 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; and inspecting banking financial institutions and insurance companies' business activities and their related risks;
- Public Security Bureau: maintains social order, protecting public and private property, and preventing and punishing delinquent activities and crime;
- Procuratorate: works on behalf of the state in accordance with law, to exercise the state organs' authority as procurators. The main duties are investigating criminal responsibility, raising public prosecution, and implementing legal supervision; and
- Supervisory Committee: this newly established institution is the political organ that enables the self-supervision of the Communist Party of China (the party) and the state. It supervises all civil servants who exercise public power on behalf of the party and the

state. It investigates illegal behaviour that is in breach of civil servants' duties.

Definitions

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

There are some definitions of 'management and control of risk' and 'compliance management and controlling' in the laws and regulations regarding financial institutions and listed undertakings. The laws and regulations include 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.

Processes

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 processes of management and control of risk and compliance management stipulated in various rules and regulations (such as those mentioned in question 5). However, in China, it is rare that rules are made that specify how companies or enterprises undertake specific processes involving the control and management of risk and compliance, unless the state is strengthening its supervision of a specific industry. If so, the state may issue specific risk compliance requests for companies in that specific industry.

In addition, owing to the special status of state-owned enterprises, the state may announce some principal regulations or guidelines in order to push a state-owned enterprise to manage and control risk and compliance. An example of this is the Opinion on the Overall Advancement of the Rule of Law Construction of Central Enterprises, which was announced by the State-owned Assets Supervision and Administration Commission of the State Council.

Standards and guidelines

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

Generally, the standards and guidelines concerning financial institutions' and listed companies' management and control of risk and compliance are based on laws and regulations. For example, the Guidelines on Comprehensive Risk Management for Banking Financial Institutions stipulate the standards and guidelines for banking financial institutions' risk systems 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; and
- internal controlling and audit systems.

Guidelines on Compliance Management for Central State-owned Enterprises (for Trial Implementation) accelerates the improvement of legal compliance management level and strives to forge 'central state-owned enterprise by the rule of law'. Guidelines on the Compliance Management of Enterprises' Overseas Operations promotes enterprises to enhance their awareness of compliance management in overseas operations and improves the level of compliance management of overseas operations.

Obligations

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 require a company to establish an internal reporting mechanism but, in practice, most large-scale enterprises will establish such a mechanism. Generally, the internal reporting mechanism will detail 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 (eg, the informant may not be demoted or fired, have their salary reduced, etc, because of their report).

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 the board of shareholders, the rule of procedure of the board of directors, and compliance with the company's equity structure and various policies, etc.

'Financial and tax compliance' includes compliance with revenue accounting, and compliance with tax payment, etc.

External operation

This mainly includes business compliance and third-party compliance.

'Business compliance' refers to compliance with a business model, contract signing procedure, etc.

'Third-party compliance' includes risk audits for transactions, internal audits and third-party audits, and regular assessments and rewards, punishments, etc.

LIABILITY

Liability of undertakings

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 a compliance policy by the management. The management's main obligations include:

- establishing a compliance controlling strategy;
- establishing a risk compliance system;
- cultivating risk consciousness in employees and a compliance culture in the company;
- supervising the company's compliance operations;

- bans on:
  - embezzling the company's property via taking advantage of a position;
  - taking bribes or committing bribery for the benefit of the company or an individual;
  - violating the obligation of prohibiting business competition; and
- confidentiality.

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

Yes. If the non-compliant activity infringes a third party, that third party may be able to sue the company.

and collect sensitive personal information without consumers' authorisation, a consumer may be able to bring civil litigation against the company in order to make the company compensate them for the infringement regarding right to reputation and right to privacy, etc.

Another example is if a company fires an employee who conducted non-compliant activity and does not state this as a reason for the employee's dismissal in its compliance governance documents, the employee may sue the company.

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

Yes. If a company's non-compliant activity violates related laws and regulations, the company may face a corresponding administrative punishment.

For example, if the company violates the Anti-Unfair Competition Law to bribe a trading party, the administrative organisation can, among other punishments, impose a penalty, confiscate illegal gains, revoke the company's business licence, and record the violation in the company's credit record.

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

Yes. If the company's non-compliant activity violates 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 financial penalty imposed on them that totals several times the size of the original payment amount.

Liability of governing bodies and senior management

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-compliant activity violates related laws and regulations, the legal representative of the company and the senior management involved in the non-compliant 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 or 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-compliant activity violates related laws and regulations, the company's legal representative and senior management involved in the non-compliant 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 expelled from the party or dismissed from office 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-compliant activity violates related laws and regulations and meets the standard of filing a criminal case, the senior management involved in the non-compliant 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, those directly in charge will be sentenced to fixed-term imprisonment (that is sentence to jail for a specified time period) or criminal detention (eg, held in a police station for questioning).

CORPORATE COMPLIANCE

Corporate compliance defence

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

According to the current laws and regulations in China, there is no generalised defence of 'compliance'. However, in judicial practice and law revision, there are some narrow 'compliance' defences.

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 non-compliant activity was individual behaviour conducted by an 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 an opportunities' transaction or competition advantage and an employee's non-compliant bribery, including that the employer has not gained any benefit due to the employee's non-compliant activity, the employer may not be punished.

Recent cases

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

On 6 January 2018, the National Internet Information Office Cyber Security Coordination Bureau interviewed the relevant personnel in charge of Alipay (China) Network Technology Co Ltd and Sesame Credit Management Co Ltd regarding the 2017 Alipay Annual Bill Scandal. The government coordinator pointed out that the collection and usage of personal data by Alipay and Sesame Credit did not comply with the National Standards for Personal Information Security and violated the commitment of the Personal Information Protection Initiative.

Alipay and Sesame Credit are required to strictly follow the requirements of Cyber Security Law, carry out special rectification, and take effective measures to prevent similar incidents from happening again.

On 15 July 2018, government inspectors discovered that Changchun Changsheng Biotechnology, China's second-largest maker of rabies vaccines, had forged reports and violated regulations while producing 250,000 doses of rabies vaccines for humans. This scandal led to a national outrage against lack of medical compliance. State and local Food and Drug Administrations revoked Changsheng's drug approval documents, issued a fine totalling 9.1 billion yuan, and 14 directly responsible personnel faced administerial and criminal prosecution.

Government obligations

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 list of prohibited actions, vigorously reducing administrative examination and approval of items, banning a disguised form for examination and approval, etc.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

The enactment of the Cyber Security Law and its matching regulations marks China's entry into the era of data compliance. The key aspects of this legislation include that companies must have:

- network information content management systems;
- network security level protection systems;
- key information infrastructure security protection systems;
- network security review, personal information and important data protection systems;
- data exit security assessment, network key equipment and network security special product security management systems; and
- network security incident response system, etc.

In addition, in January 2019, China enacted the Management Regulations for Block Chain Information Services. These Regulations aim to clarify the information security management responsibility of blockchain information service providers, thus helping to standardise and promote blockchain technology. It is worth noting that China has banned initial coin offerings and other events related to the financing of cryptocurrencies. According to the relevant government announcements, Bitcoin and the like are not currencies per se, and initial coin offerings are essentially unauthorised and illegal public offerings, and are suspected of being illegal fundraisings, financial frauds and pyramid schemes.

As for robots, machine learning, and artificial intelligence, China has publicised its Nationwide Industry Development Plan, in which risk and compliance matters related to these technologies are addressed on a strategic level.

中倫 ZHONG LUN

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

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

Corporate risk and compliance management is gaining 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 a ruling by Germany's Federal Court of Justice 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 board member's 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. Finally, 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 the attention of investors and the media in Germany and that of large companies, leading 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 medium-sized companies, particularly as 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 systems arise). This in turn may result in damage claims, criminal prosecution and administrative fines against them.

Laws and regulations

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 (eg, limited liability companies) are also legally responsible for ensuring that the represented company complies with laws.
- Risk management is the specific duty of the management boards of stock corporations, pursuant to section 91 paragraph 2 German Stock Corporation Act. The boards 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.
- In the case of a listed stock corporation, pursuant to section 317 paragraph 4 of the German Commercial Code, an annual audit has to include an assessment of whether the executive board has taken the appropriate measures, pursuant to section 91 paragraph 2 of the German Stock Corporation Act.
- 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 the organisational measures necessary to fulfil the compliance obligation open. Each individual company is left to decide on the concrete structure governing its compliance processes and systems and, subject to due examination and preparation, this decision lies within the entrepreneurial discretion of the board of directors.

Types of undertaking

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, and 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 by their companies.

Regulatory and enforcement bodies

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 their 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).

Definitions

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

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

The DCGK addresses listed companies and provides a definition of compliance in clause 4.1.3: 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 DCGK 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 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 an internal control system and internal auditing. The internal control system must 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.

Processes

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 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.

Standards and guidelines

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

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

In addition, the International Organization for Standardization has published ISO 19600, a standard regarding the use of compliance management systems. To prove compliance with ISO 19600, it is possible to have a compliance management system certified. However, it is of significance that ISO 19600 (at least in Germany) cannot be regarded as a generally accepted standard.

The DCGK applies to listed companies in Germany. It does not contain any basic rules for the methodical design of a compliance management system. However, Section 4.1.3 of the DCGK stipulates that the management board must ensure compliance with statutory provisions and internal company guidelines and work to ensure that these are observed by the group companies. This also typically requires the establishment of an adequate compliance management system and a whistleblower system. Section 3.4 DCGK provides that a company's management board has a duty to inform the supervisory board about compliance-relevant issues. According to section 5.3.2 DCGK, the supervisory board should also set up an audit committee with regard to compliance-relevant topics. The DCGK thus emphasises the importance of the topic of compliance for listed companies and lays down certain organisational requirements in this respect without commenting in more detail on the content of the system. In addition, the DCGK only applies to listed companies and its binding effect is limited (comply or explain principle).

One must note that all guidelines mentioned above are non-binding and that a board of directors has rather broad discretion in weighing the specific risks of the entity they represent and how to address them. Also, a frequent review of the compliance management system is strongly recommended.

Obligations

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

larger undertakings implement a risk and compliance structure that reflects adequate governance obligations. However, which rules that are implemented depends on each specific case. Depending on the individual situation, best practices comprise of the following (see also question 9):

- Typically, German companies have a management board and a separate supervisory board. This two-board structure is mandatory for a German stock corporation, and most European companies also use 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 the heads of risk and compliance management have direct access to the supervisory board. 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 for 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 DCGK. 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 DCGK 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 DCGK 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 DCGK recommends regular exchanges 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 judgement 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 for an individual analysis and the setting 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 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 of individual misconduct or the non-functioning of the systems; adequate reactions against lawbreakers and responsible supervisors.
- Proportionality, so that the system is 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:

- anti-corruption;
- anti-money laundering;
- antitrust;
- capital market issuer obligations (eg, ad hoc notices);
- data protection;
- employment;
- environmental protection;
- information technology;
- 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 (see question 6). Even though this framework is legally not binding, undertakings 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;
  - 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 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.

Compliance function

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.

Compliance officer and function staff

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 officer 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.

LIABILITY

Liability of undertakings

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 proper risk and compliance management. A group of companies' management board members 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 management 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', 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 is 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 be 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.

In a judgment dated 9 May 2017, the German Federal Court of Justice ruled that the existence of a compliance management system may lead to lower criminal fine, if the company had installed an efficient compliance management system aiming at preventing violations of the law and a compliance deficiency occurs.

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 its operating 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 on whether to introduce a criminal liability for undertakings. A major reason against introducing such liability is that administrative fines (see question 12) are considered sufficient.

Liability of governing bodies and senior management

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 did not properly supervise the delegated member and the compliance officer repeatedly reported compliance failures (eg, the Siemens corruption case).

In accordance with the jurisprudence of the Federal Court of Justice, 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 violations 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 MAN's commercial vehicle division ultimately admitted that he had not done enough to prevent bribery payments in Slovenia during 2004 to 2005, and was convicted for accessory to corruption by omission.

CORPORATE COMPLIANCE

Corporate compliance defence

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 a 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. The Federal Court of Justice has recognised such leniency for companies that have installed proper compliance management systems (see question 12 above). Furthermore, they will also credit the firm for correcting 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.

Recent cases

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

Volkswagen emissions scandal I – 'Dieselgate'

Public enforcement authorities and private plaintiffs worldwide are holding Volkswagen (VW) responsible for the use of illegal defeat devices in engine controls, the resulting false emission reports, and delaying providing capital market information. VW chief executive Martin Winterkorn. Winterkorn has resigned and VW has dismissed several top managers over the scandal.

Stock price damage claims in excess of €1 billion against VW are pending at German courts, for VW alleged violating its duty to publish ad hoc notices.

Even though the scandal has not been settled, it has become clear that there was a massive failure in VW's compliance system and culture, resulting in damages in excess of €28 billion (as of February 2019).

Volkswagen emissions scandal II – seizure of internal investigations material at a law firm

In the Volkswagen emissions scandal, public prosecutors are now able to access internal documents that VW's legal advisers, a global law firm with a corporate seat in the US, had gathered in the course of VW's internal investigations.

According to the decisions of the German Federal Constitutional Court (BVerfG) dated 27 June 2018, a US law firm is not entitled to constitutional rights in Germany and, therefore, cannot file a constitutional complaint. Only a legal entity whose head office is located in Germany or in another member state of the European Union may do so.

The court also rejected the motions of the respective German lawyers (working for the US law firm) which they had filed personally.

In the case at hand, even VW was not allowed to argue an infringement of constitutional rights because VW itself was not involved in the criminal proceedings, as Audi – a VW subsidiary – was the defendant.

Two conclusions can be taken from this. First, a wise choice of the legal adviser is very important. Secondly, before internal investigations start, the competent members of the management board should analyse the situation diligently, weighing advantages, disadvantages and structuring alternatives.

Truck cartel

In the summer of 2016, the European Commission fined four European manufacturers of trucks – DAF, Daimler, Iveco/Fiat and Volvo/Renault – for unlawful collusion on pricing. The firms had to pay nearly €3 billion, most of which was borne by Daimler, which had to pay nearly €1 billion. Scania has not accepted its fine. MAN remains unpunished, as it acted as a crown witness.

The 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 of a 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 is lowered by a higher court, the ruling demonstrates the willingness of the courts to answer non-compliance with high penalties.

Government obligations

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'.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

For the members of management boards, supervisory boards and compliance departments, the use of new technologies and digitalised business models creates opportunities and risks.

On one side, the advancing digitalisation offers, for example, improved possibilities to counter corruption or other forms of white-collar crime. Robot technology and artificial intelligence may help to handle effectively vast amounts of data and facilitate compliance management. On the other hand, new types of crime are also emerging, such as cyberespionage or attacks against networked production facilities.

However, in Germany discussions and lawmaking on governance and management framework covering digital transformation are only beginning. At the moment, as a principle, the current legal framework has to be applied, which, typically, has not yet been adapted to new technologies.

The compliant use of digital technologies may cause challenges regarding the EU General Data Protection Regulation. It leads to an increased documentation and proof of compliance in the context of data processing and complying with IT security.

UPDATE AND TRENDS

Current developments and emerging trends

21 | Are there any other current developments or emerging trends that should be noted?

Decrees and judgments

According to the Decree of Application of the Federal Ministry of Finance dated 23 May 2016, an internal control system serving to fulfil tax obligations can be an indication that a violation has not been committed with 'intent' or 'recklessness', resulting in an exclusion of an infringement or reducing the fine.

The aforementioned decree is in line with a judgment of Germany's Federal Court of Justice dated 9 May 2017 ruling that the existence of an effective compliance management system may lead to a lower criminal fine, if a compliance deficiency has occurred despite the company having installed such a system.

Following a decision of the German Federal Constitutional Court dated 27 June 2018, results of an internal investigation at a law firm may be seized under certain conditions (see question 18).

Cybercrime

Ultimately, an increasing number of cybercrime incidents in Germany have been reported. It is recommended that the management board, even in smaller enterprises or subsidiaries, decides on appropriate risk management measures aiming at strengthening the defence against such attacks (including technical and non-technical measures). There are examples of medium-sized companies that have suffered losses in

ROTTHEGE | WASSERMANN
LAWYERS • AUDITORS • TAX ADVISORS

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

the range of €40 million. If an incident has occurred, imminent action and support from competent advisors are required.

Transparency Register

Pursuant to the German Anti-Money-Laundring Law, since mid 2017 legal representatives of companies established under German private law, as well as incorporated partnerships, trustees and custodians are obligated, to immediately disclose their ultimate beneficial owners in the Transparency Register, unless such beneficial owners are already evident from another public register (eg, the German commercial register). In most cases, publicly listed companies are excluded from the notification obligation, but stock companies are typically within the scope of the obligation because their beneficial owners (major shareholders) are not registered in any public register.

Greece

Vicky Athanassoglou
VAP Law

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

The focus of the European Union 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 (OECD) 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 the role of corporate risk and compliance management is still being defined under the Greek legal framework. Following the world financial crisis in 2008, and as a result of the Greek recession, Greek enterprises are proving willing to incorporate best practices regarding risk and compliance management functions into their structures. For this purpose, new legislation has already adopted in the form of amendments to existing legislation and the incorporation of EU directives.

Laws and regulations

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. 3,016/2002 on Corporate Governance, Remuneration and Other Issues
As amended in force, this law provides the minimum corporate governance requirements for listed companies.

Law No. 4,548/2018
The 'SA Law', which amends and reforms Law No. 2,190/1920, the core piece of legislation for sociétés anonymes, entered into force on 1 January 2019.

As its predecessor, the SA Law applies to both non-listed and listed public limited liability companies (under the corporate form of sociétés anonymes), setting rules for:

- general meetings;
- roles of the board of directors;
- relationships between the members of the board of directors and the company; and
- rights of minority shareholders, etc.

The SA Law has not introduced major amendments in the corporate governance sectors and Law 3,016/2002 on corporate governance for listed companies will continue to apply and to be monitored by the Hellenic Capital Markets Commission in the context of its supervision competencies. Nevertheless, discussions have arisen regarding the need to amend Law 3,016/2002 in order to incorporate the new provisions of Law 4,548/2018.

Law No. 4,449/2017 On the Statutory Audit of the Annual and Consolidated Financial Statements, Public Oversight of the Audit Work
This law is referred to by every undertaking that is obliged to keep financial statements.

There is also specific legislation containing risk and compliance obligations applies to credit institutions (Law No. 4,261/2014) and insurance undertakings (Law No. 4,364/2016). Also, in addition to the obligations imposed by the above legislation a set of basic principles and best practices was introduced in the Hellenic Governance Code For Listed Companies, which was 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 aforementioned undertakings, but mainly credit institutions and, where relevant, financial institutions:

Supervisory framework for credit institutions

- Law No. 4,261/2014 (as mentioned above);
- Decision of the Governor of the Bank of Greece No. 2,577/2006; and
- Law No. 3,746/2009 On the Insurance of Investment and Deposits Fund.

Protection of bank secrecy and confidentiality
Legislative Decree 1,059/1971, as applicable, on the protection of bank deposits.

Protection of market abuse
Law No. 3,340/2005, as applicable, on insider dealing and market manipulation, in combination with Law No. 4,443/2016 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. 3,606/2007, as amended by Law No. 4,514/2018, transposing the MiFID II directive, regarding markets in financial instruments, and Law No. 3,556/2007, as applicable, on transparency regarding issuers whose shares are admitted to an organised financial market.

Money laundering

Law No. 3,691/2008, as applicable on the prevention and suppression of legalising income from criminal activities and financing of terrorist activities, was amended by Law No. 3,932/2011, 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. 4,389/2016, the said national authority aims to combat the legalisation of proceeds from criminal activities and terrorist financing, and assists the 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, the 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. 2,656/1998, 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. 2,472/1997, as applicable, on the protection of natural persons with regard to the processing of personal data;
- Law No. 3,471/2006, as applicable, on data protection in electronic communications: Decisions by the Data Protection Authority; and
- the EU General Data Protection Regulation (GDPR) 2,016/679, which has been in force since May 2018.

Consumer protection

- Law No. 2,251/1994, as applicable, on consumer protection;
- Law No. 3,862/2010, as applicable, on payment services in the internal market; and
- Decision of the Governor of the Bank of Greece No. 2,501/2002 on the informing of interested parties regarding credit transactions and relevant contract terms.

Protection of competition

Law No. 3,959/2011, 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.

Types of undertaking

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 aforementioned Law No. 3,016/2002, provisions regarding corporate governance in general, and thus, also including types of risk and compliance management, apply to companies that use the legal form of a société anonyme (defined and organised by Law No. 4,548/2018) which, additionally, are admitted in a regulated financial market (listed companies).

In addition, for specific categories of undertakings, such as financial, credit institutions and insurance undertakings, particular pieces of legislation apply, imposing tailored obligations on them. Specifically, for credit institutions, Law No. 4,261/2014, transposing EU Directive 2013/36, includes a set of corporate governance and specified risk management provisions. Moreover, for insurance undertakings, Law No. 4,364/2016, transposing Directive 2009/138, introduces detailed provisions on governance systems and risk management.

Regulatory and enforcement bodies

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 within the provisions of Law No. 3,016/2002 and Law No. 4,449/2017 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 antitrust 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. 4,099/2012), 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 to review certain procedures regarding risk management (eg, annual review of the cash flow plans of credit institutions according to Law No. 4,261/2014) 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 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 Authority's 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.

Definitions

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. 3,016/2002, 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. 4,364/2016 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.

Processes

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

The national legal framework, as mentioned above, is comprised of both statutory legislation and pieces of soft law (ie, codes of conduct) and provides a sufficient description of the processes followed for risk and management compliance.

Standards and guidelines

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 board of directors members of listed companies regarding corporate governance areas that are not covered by legislation, and thus to provide a complete best practices approach. It has to be noted that the Code is considered to be a set of basic principles, guidelines and suggestions, rather than a legally binding document.

In general, the standards introduced by the Code are divided into the general principles addressed to all sociétés anonymes 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 identifying the core risks faced by the company, and the main features of the internal control system applied, and the adoption of detailed policies regarding conflicts of interest of boards of directors' members. Following the reformation of law regarding sociétés anonymes in Greece, the corporate governance statement is an obligation of boards of directors, imposing criminal liability in case of misconduct.

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

Furthermore, according to the Decision of the Governor of the Bank of Greece No. 2,577/2006 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 regarding to compliance management for companies providing investment services. This Instruction contains clarifications about transposing European Securities and Markets Authority guidelines of 6 July 2012 (ESMA/2,012/388) into the Commission's supervisory practice. These guidelines are based on two axes: the competencies of regulatory compliance function (ie, risk assessment, supervisory programme, reports submission, etc) and the organisational requirements of the regulatory compliance function (ie, efficiency, independency, permanency of the function, etc).

Obligations

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

According to Law No. 4,449/2017 and Act No. 2,577/9.3.2006 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. 4,449/2017 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. 2,577/9.3.2006 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 audits performed by the home state supervising authority and external auditors concerning the branch's activities with regard to the related provisions (namely the prevention and suspension of money laundering, processes that ensure the transparency of transactions and provide sufficient information to 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. 3,016/2002 on corporate governance introduced the obligation for participation of non-executive and independent non-executive directors in the board of directors, with certain criteria determining when independence is indeed secured (article 4). Additionally, this law obliges listed companies to set an internal audit function characterised by autonomy from the other functions of the company and monitored by the board of directors' non-executive members, without any member of the board of directors being allowed to be also a member of the audit function. Duties of the audit function include the monitoring of the corporate and legal obligations of the company and the referral of cases of conflicts of interest to the board of directors. With regard to consequences of non-conformity with the said provisions, Law No. 3,016/2002 provides for an administrative fine issued by the Hellenic Capital Market Commission.

As mentioned above, Law 2,190/1920 on sociétés anonymes was recently replaced by Law 4,548/2018. The latter also applies to listed and non-listed companies limited by shares and it serves as the main piece of legislation for the functioning of the above undertakings. Hence, it provides a general framework for compliance and risk management issues, as discussed below.

Primarily, board of directors members are responsible for fulfilling the scope of company's management, managing the company's assets and the corporate object in general. They are also entrusted with a duty of loyalty, a duty of care, an obligation of non-competitive conduct, etc. article 96 constitutes a novelty in the Greek legislation for sociétés anonymes since it introduces a general clause regarding the general duties of their board of directors. In particular, members of a board of directors are required to:

- exercise their duties according to Law, the articles of association of the company and the resolutions of the general assembly;
- to manage the company's business in favour of company's interest;
- to oversee compliance with their decisions and the resolutions of the general assembly, and
- also to inform the other members of the board of directors for any company's business.

Furthermore, according to paragraph 2 of the above article, a board of directors is required to keep relevant records and books, to disclose and publish an annual financial statement, an annual management report and a corporate governance statement, where applicable, according to law. These obligations, in combination with the one that calls for carrying out an extraordinary 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 142 and 143). The annual management report (articles 150 and 151) should comply with the obligations of risk management and of the battle against corruption and bribery.

According to article 12, the appointment and the cessation for any reason whatsoever of the following persons are subject to publication: 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 87. 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 102, every board of directors member shall be liable for compensation towards the company for any act or omission constituting a breach of their duties. 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 information of an annual management report is specified according to the new article 150, and may differ depending on the size of the company and 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 the new article 152, regarding sociétés anonymes with transferable securities admitted to trading on a regulated market, specify 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. One of the introduced reformations is the provision about the criminal liability of the board in case of missing any of the required information in both the management report and the corporate governance statement (see question 16 below).

The duties of the 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. In case of conflict of interests, any board of director member dealing with the concerned conflict shall abstain from the relevant voting procedure, and should the necessary quorum be not achieved, the non-concerned board of directors members shall call for a general assembly, in order for the latter to resolve on the relevant matter.

Further to the above, the executive committee is a noticeable introduction in the SA Law. In particular, article 87 paragraphs 4 and 5 provide sociétés anonymes with the right to establish executive committees based on a relevant resolution of their boards of directors, or on a relevant provision in their articles of association. The said committee may be authorised to exercise some of the powers or duties of a board of directors.

As regards listed companies, they may appoint executive, non-executive and independent members, under the requirements and the consequences of Law 3,016/2002. These rights are granted also to non-listed companies, should there be such provision in their articles of association.

As far as listed companies are concerned, Articles 110-112 of the SA Law introduce an innovation in the remuneration policy of board of directors members, with the purpose to achieve harmonisation with EU Directive 2,017/828 amending Directive 2,007/36/EC as regards the encouragement of long-term shareholder engagement. Specifically, listed companies are required to establish a detailed remuneration policy for board of directors members and general directors, for a maximum period of four years. The said policy is subject to approval by the general assembly of shareholders, in which the shareholders who are also board of directors members or general directors are not allowed to vote and shall not be accounted for the fulfilment of quorum requirements. Hence, the principle of 'say on pay' is introduced, as prescribed in article 9 of the aforementioned directive. By virtue of the latter, shareholders shall have an opinion, on the basis of a binding or consulting vote, on the payments of the senior managerial members.

The Greek law adopted the option of the shareholders' binding vote. Furthermore, according to paragraph 6 of article 110, deviations from a company's approved remuneration policy are possible provided that they are necessary for the long-term benefit of the company. Moreover, the said deviations, as well as the relevant procedural details, must be specified. Additionally, the board of directors must introduce, as an agenda item in the general meeting of shareholders, the remuneration statements of the previous use, on which shareholders shall have a consulting vote. Thus, harmonisation with the directive's provisions on the disclosure of the remuneration policy is achieved. The remuneration statement must also be made available on the company's website for a minimum period of 10 years.

There is also a significant obligation for board of directors members regarding shareholder information. To be more specific, board of directors members 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 board 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).

Besides the above, the rights of information granted to minority shareholders by virtue of article 39 of the previous law, remain in force under the new Law 4,548/2018 (article 141). Additionally, the above-mentioned law introduces a new set of rights for individual shareholders of non-listed companies. Specifically, by virtue of paragraph 10 of article 141, a shareholder is able to request the following information from the board of directors:

- the company's capital;
- the categories of shares which have been issued;
- the number of shares owned by them; and
- a table of the company's shareholders.

Hence, the shareholder is always able to identify the shares' composition of the company.

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. 4,261/2014, which is 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 an efficient division of competencies, internal audit systems consisting of appropriate administrative and auditing processes, and 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. 4,261/2014), a risk management committee consisting of non-executive board of directors members 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. 4,364/2016 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. 4,364/2016, 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.

Public interest undertakings (listed, insurance, credit and financial undertakings)

Law No. 4,449/2017, 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 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).

LIABILITY

Liability of undertakings

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

The SA Law foresees, as mentioned above, a broad set of competencies for the board of directors of directors and for non-members exercising management duties delegated by the board of directors.

In a nutshell, the board is responsible for deciding upon any corporate issue regarding the management of corporate affairs, the company's assets and 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 are no conflict of interests. In this regard, article 97 paragraph 1b of the SA Law prescribes the obligation for board of directors members to disclose promptly and sufficiently to the company any conflicts of interest that might exist, not only in relation to themselves, but also in relation to persons connected to them.

Specifically for listed companies, according to Law No. 3,016/2002, board of directors 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 of directors.

Moreover, with regards to public interest entities, mainly listed companies, credit and insurance undertakings, subject to Law No. 4,449/2017, 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 of directors. That said, the board of directors 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 (among other things, 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. 4,364/2016) 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 of directors 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).

Liability of governing bodies and senior management

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 a société anonyme are liable against the company for any fault that occurred during the exercise of their competencies as managers of the corporate affairs (article 96, 97 and 102 of Law No. 4,548/2018). However, proving that they have acted as a prudent business person would exclude 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 board of directors members 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. 4,548/2018 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 of directors 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 of directors members of listed companies face administrative sanctions for non-compliance with a corporate governance obligations of Law No. 3,016/2002 and Law No. 4,449/2017. 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 of directors members (members of the audit committee might also be sanctioned according to Law No. 4,449/2007), 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, those entrusted with representing a company as well as the management of its corporate affairs are among the persons who face with criminal liability. Therefore, board of directors members of a société anonyme face criminal liability for breaches of their legal obligations, according to article 176-seq of Law No. 4,548/2018. Such breaches include, among other things, submission of false statements regarding the payment of corporate capital and the issuing of shares, omission of the annual balance sheet completion, and accusations of committing the crimes of articles 375 (embezzlement) and 390 (infidelity) of the Penal Code.

Further to that, as mentioned above, one of the reforms introduced by the SA Law is the provision about the criminal liability of the board of directors in cases where required information is missing in the management report or the corporate governance statement.

Criminal liability of responsible persons is also incurred for the breach of tax and social insurance law obligations, as well as for non-compliance with competition law.

One of the introduced reformations is the provision about the criminal liability of the board of directors when any of the required information in both the management report and the corporate governance statement is missing.

With regard to credit institutions, the relevant legislation (article 59 of Law No. 4,261/2014) foresees the criminal liability of the board of directors 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 the review of the company's practices by the Bank of Greece.

CORPORATE COMPLIANCE

Corporate compliance defence

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 why such actions were necessary. 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.

Recent cases

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

A major group active in jewellery and fashion

The present case concerns a group of companies in the industry of jewellery and fashion, which has been operating in Greece and is already active for years in the Asian market.

Recently it was the group has been publishing financial statements that did not depict the group's actual financial situation, while the founder-chairman and the chief executive of the mother company were

reportedly offering an unusually great number of shares of the mother company. Following that, the newly formed board of directors decided to file a lawsuit against the chairman, who had already resigned, the chairman of the daughter company in Asia and the financial manager, and raise a civil claim against them before the criminal court.

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. The Commission's 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 European Union. 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 by 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.

Government obligations

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 using the legal form of a société anonyme. Furthermore, 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 providing credit and insurance. That said, whether the ownership of the undertaking is private or public does not play a role in defining the obligations concerned.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

Although there is no established legal framework covering digital transformation in the field of risk and compliance governance and management as yet, companies are becoming familiar with artificial intelligence in practice, since the advantages for companies seem numerous.

The use of blockchain technology is making digital governance and e-voting more secure, as its encryption methods ensures it is harder to alter the result of voting procedures. Moreover, every act of corporate governance, transaction and logistic registration, as well as properties of companies, can be registered to a blockchain, thus ensuring audit procedures are more accurate and precise.

VAP LAW OFFICES
ATHENS | DÜSSELDORF

Vicky Athanassoglou
va@vaplaw.eu

Chrysa Mitka
chrysa.mitka@vaplaw.eu

Marios Petropoulos
mp@vaplaw.eu

Dimitra Savva
dimitra.savva@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

Italy

Andrea Fedi, Marco Penna and Lucio Scudiero
Legance – Avvocati Associati

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

In Italy, corporate risk and compliance management plays an increasingly key role.

Italy was one of the first countries to enact laws on legal entities' criminal liability for offences committed by their directors, representatives, executives, managers, agents and employees. Legislative Decree 231/2001 placed such responsibilities on legal entities more than 15 years ago, and embraces a wide variety of crimes that go far beyond anti-bribery and corruption, including, among others, health, safety and environmental (HSE) crimes. It is expected that certain VAT frauds will also become a '231 crime' during the course of 2019. On top of that, state-owned entities (including those incorporated as commercial companies) are also subject to a parallel anti-bribery legislation.

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 legal entities from liability 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'.

At the same time, data protection legislation has evolved as an effect of the European Union (EU) General Data Protection Regulation 679/2016 (GDPR) and the harmonisation Legislative Decree 101/2018, which has reshaped the Italian Privacy Code. The European Union NIS Directive 1148/2016 on cybersecurity has been transposed into Italian law by means of Legislative Decree 65/2018.

Naturally, sensitive legal sectors, such as banks, insurance companies and listed companies, are specifically regulated and deeply scrutinised (according to the Banking Act 385/1993, the Insurance Act 209/2005, and the Financial Act 58/1998).

Listed companies must publish an annual report on corporate governance and certain large companies are also subject to the obligation to publish an annual report on non-financial risks pursuant to Legislative Decree 254/2016 (recently amended by Law 145/2018) which has transposed EU Directive 95/2014 into Italian law.

Laws and regulations

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

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

Large undertakings are also subject to Legislative Decree 39/2010 (on the auditing of their accounts).

Listed companies

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 an annual basis, a report on corporate governance providing information on, among other things, 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 the adoption of an internal control and risk management system that consists 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 a listed company sets up a control and risk committee. This 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.

Banks

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.

Insurance companies

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 the current legislation.

Sanctions

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 liable 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 of, or to the benefit of, the legal entity. Legal entities may exculpate themselves from such criminal liability only when very strict conditions are satisfied. The list of crimes triggering criminal liability 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.

General Data Protection Regulation

From 25 May 2018, the GDPR directly applies in Italy.

Legislative Decree 101/2018 has harmonised Italian rules to the GDPR and reshaped the Italian Privacy Code. Data protection infringements trigger civil responsibility for damages, administrative fines and, in serious cases, criminal liability.

Cybersecurity gaps and failures may also trigger responsibility for essential facility operators and digital providers.

Types of undertaking

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.

Regulatory and enforcement bodies

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 responsible for supervising the Italian regulated financial markets and financial intermediaries. In particular, Consob has the power to enact regulations in order 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 Italy's stock exchange. Its main responsibilities include supervising the transactions carried out on the markets and defining the rules and procedures for the admission to listing of companies' financial instruments.

While the enforcement of Legislative Decree 231/2001 on legal entities' criminal liability 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.

Definitions

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.

Processes

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 setup of a corporation must 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, since 2016, state-owned companies are obliged 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 GDPR 679/2016 and the NIS Directive on cybersecurity (when applicable).

Standards and guidelines

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, among other things, 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 by the 'comply or explain' principle and the directors will be required to explain the reason it was not applied.

The association of entrepreneurs (Confindustria) has issued guidelines that provide a methodological approach to identify and address compliance risks, and draft compliance shields to provide exemptions from criminal liability pursuant to Legislative Decree 231/2001. Indeed, legal entities may be exempted from criminal liability 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 (a 231 compliance shield) and appoint a special supervisory body. The association of entrepreneurs' guidelines require, among other things:

- 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;
- training employees and executives;
- carrying out monitoring and inspections;
- regularly updating and upgrading the compliance rules and the functioning of the system; and
- establishing a whistle-blowing procedure.

In that respect, it is worth remembering that Italian Law 179/2017 has recently implemented a general regulation for whistleblowing, on top of specific provisions already contained in the Financial Act, the Banking Act, and anti-money laundering legislation. Certain provisions regarding the whistleblowing are also contained in the Privacy Code.

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 (EBA) 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 an 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 functions 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.

Obligations

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 liability of legal entities for offences committed by their directors, managers, agents or employees. To exculpate from those criminal liabilities, 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 that directly reports to the board of directors.

Italian branches of EU banks, Canadian, Japanese, Swiss and US banks need 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 must 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 applies to any processing of data in the context of the activities of an establishment of a data controller or a data processor in the EU, even if the processing is carried out outside of the EU. In many important instances the GDPR also applies to data controllers or data 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, criminal liabilities. With respect to Legislative Decree 231/2001, in addition to monetary sanctions, courts may order the publication of the judgment in 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. The conditions for exemption from criminal liability are explained in question 7.

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

- a second-level control function, which includes:
  - a comprehensive risk management function, which has sufficient authority, stature and resources taking into account the proportionality criteria, to implement risk policies and the risk management framework within the relevant bank; and
  - the risk management function, among other things, 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 sufficient authority, stature and resources to carry out its tasks; and
- a third-level control function, which includes:
  - 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; and
  - the internal audit function should be independent and ensure that the monitoring tools and risk analysis methods are adequate for the bank's size, locations, nature, scale and complexity of the risks associated with the bank's model, business activities, risk culture and risk appetite.

It is worth mentioning that the internal governance arrangements and processes mentioned above should apply, once necessary changes have been made, to insurance companies. In this regard, insurance companies should establish, in addition to the above, the actuarial function, which shall, among other things:

- 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 may lead to very heavy fines and may also trigger inhibitions. Pursuant to the Italian Privacy Code, criminal sanctions may be triggered as well. It is also worth mentioning that certain privacy violations may be construed as unfair commercial practices.

LIABILITY

Liability of undertakings

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

In principle, chief executives and executive directors have the duty to create and maintain an adequate setup of the company's structure, including as regards to compliance. Moreover, in many instances, chief executives may be indicted of crimes committed by officers down the management chain because of the chief executive's position as the top executive officer with a duty to be informed on and supervise the management of the company. Only in specific cases can chief executives demonstrate that they have effectively delegated a function to a lower officer, thus being exempted from liability. In no case will chief executives be exempted for negligence or reckless disregard in supervising. Non-executive directors may similarly suffer severe consequences if they do not supervise the chief executives 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. The same reasoning can be extended to other compliance systems (eg, privacy, health, safety and environment, etc).

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 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 from 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 of between €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 in law (see question 10), failing to adopt, or adopting an ineffective, 231 compliance shield prevents the legal entity from utilising the compliance defence. In fact, the legal entity, in that case, will not be exonerated from criminal liability, 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.

Liability of governing bodies and senior management

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 breaches of their duties towards their company, the company's 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, and health, safety and environmental 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 million 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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 (ie, one that is 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 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 (eg, 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.

As far as data protection is concerned, the Data Protection Authority has wide discretion in establishing a fine's amount and it is arguable that fines will be reduced if the legal entity can demonstrate it has strived to ensure compliance.

Recent cases

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 may 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.

Italian case law of the Supreme Court also reaffirms that ISO certifications are not the same as a proper 231 compliance shield, which needs to contain the specific analysis on the areas exposed to criminal risk, the disciplinary code, the appointment of the supervisory body, etc and must work in conjunction with code of ethics and training sessions to ensure awareness (Decision 41,768).

Government obligations

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

The anti-corruption legislation requires that public authorities 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, among other things:

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

Andrea Fedi
afedi@legance.it

Marco Penna
mpenna@legance.it

Lucio Scudiero
lscudiero@legance.it

Via Broletto, 20
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

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

With respect to governmental and quasi-governmental authorities and agencies it is worth noting that, pursuant to the reformed article 17 of the Code of the Digital Administration (Legislative Decree 82/2005), public administrations are obligated to appoint a responsible officer for digital transition, who shall be in charge of planning, coordinating and monitoring the path of the public administration towards the digitalisation of public services.

Blockchain, the common term for distributed ledger technologies, being 'technologies and IT protocols using a shared, distributed, replicable and simultaneously accessible ledger, decentralised and encrypted, which enables the registration, validation, updating and storage of data, whether encrypted or not, which cannot be modified or forged', are regulated by Law Decree No. 135/2018, which provides that the storing of an electronic document by means of a blockchain shall have the legal effect of an electronic timestamp, pursuant to Article 41 of EU Regulation No. 910/2014 (on electronic identification and trust services for electronic transactions in the internal market) and, hence, it can be used as evidence in legal proceedings. Blockchains must meet certain technical standards, which shall be set within 90 days from the entry into force of the legislation (14 May 2019) by the Agency for Digital Italy (AgID).

While the policymaking debate on new technologies is ongoing, the main sources of law on the risk and compliance governance covering digital transformation remain the ordinary liability regime for defective products, some rules of the Italian Civil Code and the GDPR.

According to the Consumers Code (Legislative Decree 206/2005) producers and/or distributors are liable towards consumers for damages caused by defective products. Therefore, insofar a robot, a robotic application or even the algorithm may be qualified as a 'product', producers and distributors will be liable for defects, at the terms and subject to the conditions set forth by the Consumers Code for products in general. Such liability may be triggered also if the algorithm, robot or robotic application has been programmed by an employee of the producer or a third-party programmer (article 2049 of the Italian Civil Code).

It is also significant to underline that, 'everyone is responsible for the damage caused by the things he has in custody, unless he proves that the damage was caused by force majeure' (article 2051 of the civil code). That provision may easily apply to owners of a robot or robotic application that causes damage to third parties. Furthermore, robotics may be considered as a business which is per se risky and, thus, subject to the stringent responsibility provided by article 2050 of the Italian Civil Code.

Lastly, we think it important to highlight that several provisions of the GDPR may be at odds with some of the key technologies driving digital transitions at this stage.

Blockchain applications are often in tension with the accountability principle set out by the GDPR, in that it is not always possible to single out data controllers and/or processors over public and permissionless blockchains. More, as blockchain implies that data, once written to the chain, cannot be changed, it may clash with the data subjects' rights to access, rectification and erasure. Lastly, smart contracts, which use blockchain technology, may in certain instances infringe upon the data subject's right not to be subject to a 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her' (article 22 GDPR). This last issue is shared by blockchain, robots and algorithms, as they all rely on the capability of an automated entity to autonomously make decisions, often based on personal data or by targeting individuals.

Japan

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

LEGAL AND REGULATORY FRAMEWORK

Legal role

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 value, 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.

Laws and regulations

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.

Types of undertaking

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.

Regulatory and enforcement bodies

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.

Definitions

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'.

Processes

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.

Standards and guidelines

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

There are no statutory regulations. It is for directors of companies to determine how best to comply with their and their company's obligations.

However, Japan Exchange Group (JPX) issued the Principles for Preventing Corporate Scandals (the Preventive Principles) in March 2018. The Preventive Principles are a set of principle-based guidelines that encourage every listed company to take creative approaches in implementing each principle and to establish effective measures that reflect the company's individual situation. According to JPX, a listed

company's failure to abide by the Preventive Principles alone will not constitute grounds for imposing adverse actions against it, as long as the company has not committed a breach of the Tokyo Stock Exchange Listing Regulations. Rather, the JPX expects that the Preventive Principles will be used as a guide for exercising self-discipline.

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 that a prudent manager owes to the company (see question 10).

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 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 requires that each domestic company listed on the exchange develops systems necessary to ensure the appropriateness of its business, and to put in place management structures and procedures as required under the Companies Act (as mentioned above) and operate them appropriately. Tokyo Stock Exchange listing regulations also require listed companies to respect the Tokyo Stock Exchange'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 Japan Business Federation, which is formed 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.

LIABILITY

Liability of undertakings

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, and 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 whistleblower 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 Tokyo Stock Exchange 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 Tokyo Stock Exchange deems that 'improvement of the internal management system, etc, of such listed company is highly necessary', then the Tokyo Stock Exchange may designate the listed stock as a security on alert. If the internal management system is not improved within the prescribed period, or the Tokyo Stock Exchange 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 Antimonopoly Act, the Companies Act, and the Labor Law.

Liability of governing bodies and senior management

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 a 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 a criminal offence arises from their actions, for example, when they instruct others to commit a criminal act or otherwise contribute to one. A director's breaching the duty of care they owe 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 in law, there is no related criminal liability.

Specific legislation may impose criminal sanctions for certain acts that are compliance-related. For example, the Antimonopoly 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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 an employee 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).

Recent cases

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.

Government obligations

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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

There are no specific regulations that govern digital transformation including machine learning, artificial intelligence, robots and blockchain. In relation to artificial intelligence (AI), in July 2017, the Draft AI R&D Guidelines for International Discussion was issued by the Conference Toward AI Network Society, which is managed by the Ministry of Internal Affairs and Communication. The purpose of issuance of the guidelines is described as having the 'aim at protecting the interests of users and deterring the spread of risks, thus achieving a human-centred "Wisdom Network Society" by way of increasing the benefits and mitigating the risks of AI systems through the sound progress of AI networks'. The guidelines contain nine AI research and development principles. Summaries of each of the principles follow:

- Principle of collaboration – developers should pay attention to the interconnectivity and interoperability of AI systems.
- Principle of transparency – developers should pay attention to the verifiability of inputs/outputs of AI systems and that their judgements can be explained and are transparent.
- Principle of controllability – developers should pay attention to the controllability of AI systems.
- Principle of safety – developers should take to ensure that AI systems will not harm the life, body, or property of users or third parties through actuators or other devices.
- Principle of security – developers should pay attention to the security of AI systems.
- Principle of privacy – developers should take into consideration that AI systems will not infringe the privacy of users or third parties.
- Principle of ethics – developers should respect human dignity and individual autonomy in researching and developing of AI systems.
- Principle of user assistance – developers should ensure AI systems will support users and give opportunities to stakeholders, including users of AI systems.
- Principle of accountability – developers should make efforts to fulfil their accountability to stakeholders, including to users of AI systems.

Hiroyuki Nezu
hiroyuki.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

Atsumi & Sakai
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

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

Corporate risk and compliance management in Mexico has traditionally played mostly commercial and business contingency roles. 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 that 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 11 years which 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 is not yet 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 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. 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$5.00 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 million, plus damages and disgorgement.

Laws and regulations

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

Specifically, the 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.

Types of undertaking

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.

Regulatory and enforcement bodies

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 2018 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 this law, 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 Federal Court of Administrative Justice has jurisdiction to impose sanctions.

This 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.

Definitions

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 whistleblowing 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.

Processes

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

The characteristics of a compliance programme or integrity policy are defined in the General Law of Administrative Responsibilities. 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 it is to rely on the Model for International Internal Controls;
- for financial organisations, it is to 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 UK Bribery Act guide;
- 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.

Standards and guidelines

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 published by the Ministry of Public Administration 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.

Obligations

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 5 and 6.

LIABILITY

Liability of undertakings

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 (eg, NOM–032–STPS–2008 and 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 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 of the recent implementation of the General Law of Administrative Responsibilities, 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.

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.

Liability of governing bodies and senior management

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.

CORPORATE COMPLIANCE

Corporate compliance defence

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, consider 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.

Recent cases

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$21 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 (COFECE), 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 2018, COFECE levied fines totalling approximately US$13 million for antitrust violations committed by companies, most of them in the manufacturing, financial, real estate and energy sectors.

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 more than 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.

Government obligations

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 General Law of Administrative Responsibilities substituted 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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

Mexico is currently in the process of promoting and implementing artificial intelligence initiatives and programmes, and creating the framework to innovate in public services toward creating a digital transformation, mainly through the use of blockchain technology and artificial intelligence.

To date, however, there have been relatively few legal developments that regulate new artificial intelligence and blockchain technologies. One of the few new technology laws is the Law that regulates financial technology institutions, commonly known as the FinTech Law, published in Mexico's Federal Official Gazette on 9 March 2018. This law establishes the general regulatory framework for financial services to be rendered through new technologies and IT platforms or tools to facilitate financial transactions, and the use of authorised cryptocurrencies as an alternate form of payment for financial transactions. It also regulates the organisation, operation and authorisation of Mexican corporations to operate as financial technology institutions.

On another front, the Mexican government has launched numerous policies and initiatives to innovate in digital transformation matters. The previous administration had already created the National Digital Strategy (NDS), as the digital action plan to build a 'Digital Mexico' over the next few years, in which the adoption and use of information and communication technologies and innovation would contribute to achieving the country's development goals.

According to the report 'Towards an AI Strategy in Mexico: Harnessing the AI Revolution', the NDS has resulted in the implementation of national policies in the areas of connectivity, interoperability, data, digital inclusion and digital skills, coupled with efforts to ensure the consistency of legislation regarding e-government. The five objectives of the NDS set forth in the National Development Plan 2013–2018 are:

- government transformation;
- digital economy;
- quality education;
- effective universal healthcare; and
- citizen participation and innovation.

These objectives were to be achieved through national policies covering connectivity, digital skills inclusion, digital interoperability and identity, legal framework, and open government data, which are currently in place. According to the 'Digital Mexico' platform, this strategy has an overall completion of 94 per cent thanks to numerous efforts by the Mexican government to increase the coverage of mobile data services and internet access by creating and implementing programmes to provide free internet public spaces and deliver 4G broadband connectivity; a single platform for citizens to access government information, services and open data; and programmes to encourage digital inclusion and the development of digital skills, among others.

Furthermore, in June 2018, Mexico became one of the first 10 countries in the world to design and delivering a national strategy for the development of artificial intelligence, which resulted in an update to the NDS guidelines in July 2018, and the publication of a wide cross-sector consultation process on recommendations for a National Policy on Artificial Intelligence. These principles are spelled out in more detail in the General Principles and Guidelines for the Use of Artificial Intelligence Systems in the Federal Public Administration. Starting in 2017, through the BlockchainHackMX initiative, the NDS and the Ministry of Public Administration have been working on laying out the foundation principles of a Mexico Blockchain Network to promote the use of blockchain technology in the public sector as a mean to increase confidence in public institutions and effectively fight against corruption. In August 2018, the initiative published the governance model for the blockchain network, so that this network can be used in public services including public tender processes, registration of property and education certificates. This model was a collaborative effort by several governmental agencies, public universities and representatives of Mexico's blockchain industry, as well as international blockchain experts. The network brings in representatives from both public and private sectors, universities and civil organisations. As part of this initiative, the Mexican government planned to conduct Mexico's very first public procurement procedure through the use of Smart Tenders, a project that evolved from the Talent Land Hackathon 2018, based on blockchain technology. However, the procedure has not yet taken place, so the project's status is unclear.

In recent years, Mexico's public and private sectors have developed and deployed artificial intelligence projects in diverse sectors such as tax, agriculture, public transportation, and public health. To enhance the mechanisms used to detect shell companies and fraudulent operations, for instance, the Tax Administration Service (SAT) has been testing artificial intelligence algorithms. In conformity with the aggressive anti-corruption enforcement actions taken by the current administration, we expect for these technologies to be further improved and deployed.

As remarkable as these efforts are, it is also important to note that the Superior Audit Office of the Federation (ASF) recently detected some deficiencies in the NDS information reported by the Presidential Office, mainly, because it does not provide reliable information to follow up the implemented actions under the NDS and its results and efficiency. Now, as the current administration of President Andrés Manuel López Obrador reaches its 100-day mark, it is still unclear whether a digital strategy will be a national top priority and whether it will continue the steps begun under the NDS or design a new strategy to address Mexico's current digital challenges.

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
bakermckenzie.com

UPDATE AND TRENDS

Current developments and emerging trends

21 Are there any other current developments or emerging trends that should be noted?

As of this writing, Mexico's current administration under President Andrés Manuel López Obrador is taking aggressive and very public actions against corruption in the public and private sectors. So far, 2019 has witnessed aggressive enforcement actions against fuel theft, money laundering, tax evasion and investigations into corruption allegations of the administration left by former President Enrique Peña Nieto.

Nigeria

Babajide Ogundipe, Olajumoke Omotade and Olatunde Ogundipe
Sofunde Osakwe Ogundipe & Belgore

LEGAL AND REGULATORY FRAMEWORK

Legal role

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) to be 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.

Laws and regulations

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 (Nigeria's central bank);
- 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 Nigerian 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;
- the Credit Bureau Regulations issued by Nigeria's central bank; and
- the Nigeria Data Protection Regulation by the National Information Technology Development Agency.

Types of undertaking

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.

Regulatory and enforcement bodies

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. The principal ones include the following:

Central Bank of Nigeria

Nigeria's central bank 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.

Corporate Affairs Commission

The Corporate Affairs Commission (CAC) is responsible for the administration of CAMA. The functions of the Commission are to administer 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 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.

Financial Reporting Council of Nigeria

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.

National Deposit Insurance Corporation

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.

Department of Petroleum Resources

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.

Economic and Financial Crimes Commission

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.

Securities and Exchange Commission

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.

Definitions

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.

Processes

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.

Standards and guidelines

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 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 adopted accounting and financial reporting standards;
- 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 (IFRS);
- 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 audit professionals, the Institute of Chartered Accountants of Nigeria, the Association of National Accountants of Nigeria, public companies, large private

companies, public interest entities (defined in 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 CAC 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 (and publicly quoted companies) based on market capitalisation, and on public interest entities based on turnover.

In January 2017, after discussions between the FRCN, auditors and directors of banks that the FRCN intended to suspend or remove from office, and a former governor of Nigeria's central bank in 2014–2016, the executive secretary of the FRCN was dismissed. A new executive secretary was appointed along with a new chairman. The three Corporate Governance Codes for the private, public and not-for-profit sectors issued in October 2016 were suspended. In January 2018, a committee was established to review the suspended codes and to develop and recommend revised codes.

A new draft Code was published on 15 June 2018. Unlike the codes suspended in 2016 the new draft does not purport to apply to not-for-profit entities and private companies generally. Instead, the new draft Code seeks to regulate the following entities:

- public companies (whether listed or not);
- private companies that are holding companies of public companies or other regulated entities;
- concession and/or privatised companies; and
- Regulated Private Companies (RPCs) – private companies that file returns to any regulatory authority, other than the Federal Inland Revenue Service and the CAC.

This Code remains a draft and a working tool. 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 in the regulations issued by Nigeria's central bank in respect of banks and other financial institutions, which is the most regulated sector in Nigeria. Nigeria's central bank regularly issues regulations and guidelines that set standards which 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 Nigeria's central bank are largely influenced by international agreements and independent advisory bodies such as the Financial Action Task Force. Currently, Nigeria's central bank guidelines require banks and other financial institutions to adhere to the following directions:

- There must be a chief compliance officer (CCO). Initially, it was required that there be a compliance officer for each branch, but this was relaxed to allow one to serve clusters of branches.
- The CCO must report directly to the board, must have the status of at least a general manager, and posses a minimum education requirement and training in an international standard.
- There must also 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 pre-approval from Nigeria's central bank, there is flexibility in acceptable standards.

There are different risk management standards prescribed by Nigeria's central bank for different kinds of transactions and actions, such as accepting new customers, providing credit services for individuals and providing credit services for companies. Additionally, Nigeria's central bank 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 Nigeria's central bank manual.

In recent times, the Nigeria's central bank has issued consultative circulars relating to draft guidelines on new areas of financial activity, such as 'mobile money'. (This is described by the central bank as 'any mobile money payment and solution in Nigeria'. Examples include electronic wallets and the like, and payment platforms provided by non-banking entities, such as financial technology companies.)

Obligations

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 Nigeria's central bank, 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 or 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.

LIABILITY

Liability of undertakings

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. The risk and compliance management obligations in the banking industry include the following:

- the board and senior management of the banks are ultimately responsible for AML/CFT compliance;
- the bank management must formulate and present an AML/CFT compliance manual and present it to the board for consideration and formal approval;
- the bank's senior management's approval is required before establishing business relationships with politically exposed persons (being persons, or their close friends or family, who have

been entrusted with prominent public function, and are viewed as high-risk individuals regarding money laundering and corruption);
- 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;
- financial institutions must obtain approval from senior management before engaging in cross-border and correspondent banking and other similar relationships in addition to performing the normal customer due diligence measures;
- an employee training programme under the guidance of the compliance officer in collaboration with senior management of the bank is required;
- the board and senior management of the bank may be investigated for their roles in contravention of the provisions of the AML/CFT manual produced by Nigeria's central bank; and
- on the second contravention of Nigeria's central bank's AML/CFT manual, responsible parties including, but not limited to, members of the board and senior management of the bank 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. However, it should be stated that civil actions based on such deficiencies are not common in Nigeria.

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.

Liability of governing bodies and senior 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 failure by the financial institution or the compliance officer at management level, 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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.

Recent cases

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

On 29 August 2018, Nigeria's central bank announced the imposition of sanctions against MTN Nigeria Communications Limited (MTNN) and four commercial banks for alleged violations of laws and regulations.

The central bank demanded that MTNN return to Nigeria US$8.13 billion, which the bank claimed had been improperly transferred out of the country as dividend payments to MTNN shareholders – the largest of which was MTNN's parent company, MTN Group Limited, a company listed on the Johannesburg Stock Exchange. Banks alleged to have been complicit in the alleged infractions were also sanctioned by the central bank.

The laws and regulations alleged to have been violated were the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act 1995 and the regulations issued periodically by the central bank and contained in its Foreign Exchange Manual.

The allegations against MTNN first surfaced in 2016, when a member of the Nigerian senate moved a motion in the senate demanding that the relevant senate committee investigate his allegation that MTNN had repatriated about US$12 billion from Nigeria over a ten year period. He accused the company of 'unscrupulous violation of the Foreign Exchange (Monitoring and Miscellaneous) Act', alleging that the amount moved by MTNN was about half of Nigeria's foreign currency reserves.

The senate committee's investigation resulted in a report issued in 2017, which exonerated both MTN Group Limited and MTNN and recommended that the central bank sanction one particular bank 'for improper documentation in respect of capital repatriation and loan repayments' on behalf of MTNN. The report caused outrage when presented on the floor of the senate, with some senators questioning why the report largely condemned the central bank and exonerated MTNN. The matter came to a head when the central bank issued its sanctions against MTNN, the bank that the senate committee had recommended be sanctioned, and three other banks.

MTNN is the largest telecommunications provider in Nigeria and across Africa, and within the MTN Group, which is, in turn, Africa's largest telecommunications operator, both in terms of revenue and subscribers. MTN Group is also the 11th largest mobile network operator in the world, with operations in more than 20 countries in Africa as well as in Afghanistan, Iran, Syria and Yemen.

MTNN responded to the CBN's sanctions with litigation, denying that it had violated any law or regulation and that the penalties imposed by Nigeria's central bank were, in any event, unlawful. In response, the central bank issued a counterclaim against MTNN, contending that MTNN's conduct had contributed to the depletion of Nigeria's foreign currency reserves, exacerbating shortages caused by reduced earnings from crude oil following the sharp decline in prices in 2016.

The dispute was reported to have been resolved in late December 2018, when both MTNN and the central bank issued statements announcing a settlement. MTNN's statement indicated that the CBN had, 'upon review of . . . additional documentation, concluded that MTN Nigeria is no longer required to reverse . . . dividend payments made to MTN Nigeria shareholders'. The statement went on to say that Nigeria's central bank 'had instructed MTNN to take steps that would cost it approximately 19.2 billion naira (US$52.6 million)'.

The central bank's statement did not mention any figures, but confirmed that an agreement that would lead to the 'amicable disposal' and 'final resolution' of the litigation had been reached with MTNN.

In January 2019 the Securities and Exchange Commission closed down a company in Kano, in the north of Nigeria, for operating without being properly registered by the SEC.

Sofunde Osakwe Ogundipe & Belgore
legal practitioners

Babajide Ogundipe
boogundipe@sooblaw.com

Olajumoke Omotade
ooomotade@sooblaw.com

Olatunde Ogundipe
oaogundipe@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

In recent times, evidence that the EFCC has secured improvements in the compliance with anti-money laundering and anti-terrorism financing regulations by licensed bureaux de change operators in Nigeria has come to light. There have been reports in the media of the EFCC arresting persons suspected of money laundering offences based on information received from bureaux de change operators.

The use of foreign currency (primarily US dollars) to evade regulations related to cash transactions remains prevalent, primarily due to the fact that large sums take up less volume than Nigerian currency. It appears that bureaux de change operators are reporting large transactions to law enforcement, which in turn acts against the persons identified by the BDC operators.

Government obligations

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 Nigeria's central bank rules. While the AMCON legislation makes no provisions for sanctions, the application of Nigeria's central bank 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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

Presently there is no legislation covering digital transformation in Nigeria. This may change soon as there is clear interest shown by National Information Technology Development Agency in bringing Nigerian regulations up to date and Nigerians have shown interest in the use of cryptocurrencies.

Russia

Alexey Borodak and Sergey Avakyan
Norton Rose Fulbright (Central Europe) LLP

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

Together with the growth and the 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, but has only obtained particular legal meaning in Russia in recent years.

Nonetheless, the reasons for establishing corporate risks and compliance management systems within Russian organisations vary and still do not altogether relate to obligatory statutory requirements.

The main spheres that are commonly subject to compliance management in Russia are anti-corruption, 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 above-mentioned 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.

Laws and regulations

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

There are only few pieces of legislation 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 specialised statutes, that impose obligations on performing risk and compliance management within legal 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); and
- Federal Law No. 414-FZ On Central Depositary dated 7 December 2011 (article 8).

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 and other sanctions, are set down in the Code of Administrative Offences and the Criminal Code of the Russian Federation.

Types of undertaking

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 as '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 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 a 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.

In early 2019, the Federal Anti-monopoly Service renewed the discussion on the necessity of implementing anti-monopoly compliance standards within state and municipal bodies. Since 2016, the Federal Anti-monopoly Service has been trying to enact a bill defining 'anti-monopoly compliance' and regulating obligatory compliance systems within Russian legal entities and entrepreneurs.

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.

Regulatory and enforcement bodies

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, nor is there a compliance framework that entities can be held specifically held liable for not following, most of the regulatory and enforcement bodies related to corporate compliance control have a common scope that varies depending on the nature of each body and its purpose.

Said powers of powers typically consist of administrative discretions (powers of providing obligatory instructions, controlling and supervisory powers, powers of withdrawing the 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 are the:

- Central Bank of Russia;
- Public Prosecutors Office of the Russian Federation;
- Federal Anti-monopoly Service;
- Federal Financial Monitoring Service (Rosfinmonitoring); and
- Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor).

Definitions

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 Combating 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 US 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.

The 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. An inexhaustive 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 Anti-monopoly 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 Anti-monopoly 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 this 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.

Processes

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.

Standards and guidelines

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, in addition to the specialised legislation given in question 2, is also applicable.

The Central Bank of Russia 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 will 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 chief executive officer 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.

Obligations

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 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' chief executive.

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 are 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.

LIABILITY

Liability of undertakings

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 chief executive's bad faith or unreasonable actions or omissions that resulted in company losses, such losses may be recovered from the chief executive. The company will be restricted from indemnifying the chief executive 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 the ratification of the United Nations Convention Against Corruption 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, a new part was added to 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 of, 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 interprets an offence committed in the interest of a legal entity as an action that results in a legal entity attaining 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 corrupt actions by its employees are not always taken into consideration by law-enforcement bodies, due implementation of such measures may be one of the few defences available to a legal entity in court. Legislative initiatives aimed at reforming the practice of the use of article 19.28 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 an efficient investigation of the corruption offence.

Nevertheless, it is important that the company and its structural subdivisions are responsible for fulfilling their duties as envisaged by article 13.3 of Federal Law No. 273-FZ On Counteracting Corruption, which is aimed at developing and applying anti-corruption measures. An organisation must use an integrated approach to organising internal controls and create an efficient system for prevention of corruption, for example, by introducing compliance programmes as well as a readiness to promptly defend one's interests if law-enforcement authorities bring any charges.

Antitrust compliance

The main financial sanction that may be imposed by Federal Antimonopoly Service 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.

A 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 kept in mind that, according to the Criminal Code of the Russian Federation, only individuals are subject to criminal liability.

Anti-corruption compliance

Anti-corruption 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.

Liability of governing bodies and senior management

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, which allows for losses to be directly recovered from a company's management, if the losses were the result of the management's abuse of power.

Generally, board members and chief executives 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. Chief executives 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 chief executive bears subsidiary liability for their company's 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 caused 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 chief executive and responsible members of management also bear personal administrative liability for a 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 chief executive 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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 a universal means of defence for any type of liability. However, the such provisions 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).

Recent cases

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 in question 12.

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 the 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. 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

Government obligations

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).

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

Following the boost in development of blockchain-related technologies (including rapid and increasing turnover of the cryptocurrencies) the Russian government and legislative bodies have proposed number of initiatives aiming at clarification of the digital economy's status. While the status of cryptocurrencies has fallen out of the scope of such initiatives, the existing bills create a potential for heavy regulation of commercial activity with usage of digital means (smart contracts, digital rights, etc). Some of the proposed amendments to the existing core legislation may require commercial entities to revise or establish new policies regarding the implementation of digital technologies in future.

Spain

Helena Prieto González, Beatriz Bustamante Zorrilla, Marta Sánchez Martín and Alejandro Ayala González

Garrigues

LEGAL AND REGULATORY FRAMEWORK

Legal role

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'.

Laws and regulations

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 the prevention of money laundering and terrorist financing, and Royal Decree 304/2014 of 5 May on the regulation of 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.

Types of undertaking

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).

Regulatory and enforcement bodies

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;
- Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (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.

Definitions

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).

Processes

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 an obligation to have a compliance programme or specific compliance processes, although due implementation of this type of programme or process is an exonerating or mitigating circumstance under Spanish law. In order to be able to take advantage of this, compliance programmes must comply with conditions and requirements as explained below (see questions 7 and 17).

Standards and guidelines

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

Requirements applying to organisational and management models under Spanish jurisdiction are defined under article 31–*bis* 5 CC. These include requirements:

- to identify activities within the scope of which the crimes to be prevented may be committed – the 'criminal risk map';
- 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);
- to have appropriate models for the management of financial resources in order to impede the commission of the crimes to be prevented;
- 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);
- 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
- 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 the following:

- 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;
- UNE 19601 (2017): concerns criminal compliance management systems based on the CC; and
- UNE 19692 (2019): relating to management systems on tax compliance.

Obligations

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–*qua*ter 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, article 285–*bis*, 285–*qua*ter, 286 and 288 CC);
- corruption in business dealings (286–*bis* and 286–*qua*ter 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);
- influence peddling (430 CC);
- embezzlement of public funds (435 CC);
- incitement to commit acts of discrimination, hate or violence against groups (510 CC);
- criminal organisation and terrorism (580–*bis*); and
- goods smuggling (the Anti-Smuggling Organic Law).

LIABILITY

Liability of undertakings

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 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 permanently);
- 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.

Liability of governing bodies and senior management

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 criminal proceeding 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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.

Recent cases

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

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 has reached.

So far, the Supreme Court has only issued a few sentences. The most important are the following.

Sentence No. 514/2015, 2 September 2015

The first ruling, 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.

Sentence No. 154/2016, 29 February 2016

On 29 February 2016, the Supreme Court issued 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 absolute 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.

Sentence date no. 221/2016, 16 March 2016

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.

Sentence date no. 516/2016, 13 June 2016

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.

Sentence date no. 445/2017, 21 June 2017

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.

Sentence No. 583/2017, 19 July 2017

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).

Sentence No. 316/2018, 28 June 2018

The Supreme Court rendered a sentence on 28 June 2018 which highlighted that directors and officers liability insurance can require the insured to implement a compliance program. With this ruling, the insurers guarantee the reduction of the risk of the duty to indemnify, by lowering the possibilities that the commission of a criminal offence. However, the key point of this resolution is that the Supreme Court demonstrated that it is aware of the growing importance of the compliance programs in the insurance sector and, in general terms, in mercantile traffic. It is the first resolution that refers to third parties compliance.

Sentence No. 489/2018, 23 October 2018

The judgment handed down on 23 October 2018 directly ruled on companies' faculty of control on their employees regarding the commission of criminal offenses. The sentence embraced the jurisprudential doctrine of the European Court of Human Rights on the control of electronic communications at work (the so-called Bărbulescu II doctrine).

The European resolution can be seen just as a crystallisation of the doctrine of Spanish Constitutional Court on the same issue. However, the latter only applies on labour jurisdiction while the former does not distinguish. Therefore, the importance of the commented sentence lies in the fact that criminal jurisdiction now counts with basic but clear criteria.

A lack of a reasonable expectation of privacy is the keystone of accessing to companies' electronic means used by employees. To sum up, in cases where the employee accepted and signed a company's internal policy, the content of which warned about the prohibition of the private use of professional assets, as well as the company's faculty of controlling the proper use of such assets, the employee would have no reasonable expectation of privacy when using the corporate assets (even when it contained private information).

Sentence No. 506/2018, 25 October 2018

Last but not least, the Supreme Court issued a sentence on 25 October 2018 that ruled that even if the conviction of the legal person does not require a previous conviction of an individual, corporate criminal liability is not completely detached from individual criminal liability. Thus, if the acts of the individual are not unlawful, no corporate criminality can be imposed.

Government obligations

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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

There is no specific regulation on the risk and compliance management covering digital transformation. No specific legal provisions have been passed at this regard. However, it does not mean that digital transformation is ruled out. Risk and compliance management regulation is wide enough to accommodate the inclusion of digital transformation.

Cybersecurity is one of the most important areas in the digital transformation of companies where compliance management plays a core role nowadays. Certainly, compliance officers or compliance bodies' members having knowledge on this matter is highly desirable. Additionally, the aforesaid Attorney General's office's Circular 1/2016 points out that digital tools are a key measure of any organisational and management models, especially in large corporations. Thus, legal entities are gradually using digital transformation tools in their compliance systems.

In this sense, some of the offences that can be committed by legal entities are related to digital transformation in some way. Discovery and disclosure of secrets using informatics tools (197–*bis* and 197–ter CC) or IT damage (264–*qua*ter CC), among others, directly refers to using means that are subject to digital transformation. Therefore, they should be part of compliance programmes if companies wanted to use the exonerating or mitigating circumstance. Indeed, CC provisions presuppose adequate measures at this regard. On the other hand, one of the fundamental principles of the European General Data Protection Regulation is that a company is accountable for the lack of records of processing activities or even for the lack of evidence for such processing. Companies must generate sufficient traceability of their diligence to verify that they actually comply with the regulations in force. The European General Data Protection Regulation has been embraced and developed at national level by the Law 2/2018 of 5 December.

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

Switzerland

Daniel Lucien Bühr and Marc Henzelin
Lalive

LEGAL AND REGULATORY FRAMEWORK

Legal role

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 failures of organisational governance, and risk and compliance management, 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 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 (EU), 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.

Laws and regulations

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 a board of directors at 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 (AMLA), 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. For instance, the FINMA circular on banks' corporate governance stipulates that banks must appoint a chief risk officer (CRO) as head of risk control. In systemically relevant institutions, the CRO shall be a member of the executive board. And the circular on banks' liquidity risks clarifies the statutory minimum qualitative requirements for the management of liquidity risks and the minimum quantitative financing quota requirements.

Other legally non-binding recommendations concerning internal controls, risk and compliance management were issued in 2014 by 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) 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.

Types of undertaking

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.

Regulatory and enforcement bodies

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 (eg, 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 its 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 of 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 'jump the gun' 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.

In 2018, the Federal Audit Oversight Authority (FAOA) investigated KPMG's professional conduct as statutory auditor of Swiss Post. FAOA found significant shortcomings in the audit practices of KPMG and subsequently reprimanded the firm. It also opened investigations into the professional conduct of two KPMG auditors. KPMG cooperated with FAOA and took corrective action, in particular with regard to the avoidance of conflicts of interests resulting audit and (tax) advisory mandates.

Definitions

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.

Processes

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.

Standards and guidelines

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, which are increasingly used by companies as benchmarks. Some (mainly larger international) corporations also follow the soft law enterprise risk management framework created by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) or the 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.

Obligations

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. In this context, FINMA identified a serious lack of supervision of the former executive committee, in particular the former chief executive, by the board of directors of Swiss banking group Raiffeisen (see question 18).

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 a 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.

LIABILITY

Liability of undertakings

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. This standard requires the members of the board of directors or of the executive board to implement effective risk and compliance management systems. Recently the environment changed and these supervisory obligations are increasingly monitored and top managers are held accountable by the companies themselves and regulators. The board of directors of Swiss Post and of Raiffeisen (see questions 8 and 18) are currently considering claiming damages from their former executive directors.

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 such as:

- 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.

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.

Liability of governing bodies and senior management

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 (for recent case law see the cases of *Swiss Post* and *Raiffeisen*, see questions 8, 10 and 18). 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.

In two cases however, the Swiss Federal Administrative Court lifted such bans imposed by FINMA. In connection with the *1MDB* case (see question 18) FINMA banned a former compliance executive of Falcon Private Bank from practicing his profession for a period of two years. However, the Swiss Federal Administrative Court decided that the former compliance executive had violated reporting obligations but had no decision-making authority and thus was only culpable of simple negligence which would render such a two-year ban disproportionate.

In a similar case, FINMA expressed temporary disqualifications against seven UBS employees based on a fine that was rendered against UBS for market manipulation. FINMA concluded from its final decision against the bank that the employees violated regulatory duties. However, the Swiss Federal Administrative Court decided that the individual responsibility cannot not be simply derived from a decision regarding the bank but must be established against the employees individually and specifically.

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).

Additionally, Articles 37 and 38 of the revised Anti-Money Laundering Act provide for strict provisions and stipulates high fines in case of a violation of the reporting duties and duties to verify as set out in article 9 and 15 AMLA, respectively.

CORPORATE COMPLIANCE

Corporate compliance defence

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.

Recent cases

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

There were a number of high-profile governance, risk and compliance cases in 2018.

Swiss Post and Postauto AG

A major case is the suspected subsidies and accounting fraud at the government-owned enterprise Swiss Post and its subsidiary Postauto AG.

In February 2018, the Federal Office of Transport filed a criminal complaint against Postauto AG for alleged subsidies fraud and false accounting. The Federal Office of the Police (Fedpol) initiated an investigation for possible violations of administrative criminal law, fraud and document fraud, as well as disloyal management committed by various bodies of Postauto AG.

It was alleged that Postauto AG had, for many years, transferred profits from subsidised businesses to non-subsidised businesses in order to keep its entitlement to federal and cantonal subsidies.

An internal investigation report brought serious organisational deficiencies to light. Subsequently, the board of directors of Swiss Post dismissed the entire executive board of Postauto AG and most executive managers of Swiss Post. Swiss Post subsequently refunded about 205 million Swiss francs to the Swiss government and Swiss cantons.

RUAG

In 2018, the OAG opened criminal proceedings against an employee of the federal defence group RUAG. The OAG is investigating possible violations of the War Materials Act which prohibits the sale of certain weapons to a number of countries, such as Russia. In the context of this investigation, the OAG conducted a dawn raid at RUAG's offices in Berne. Ruag self-reported the matter to the OAG.

Raiffeisen

In October 2017, FINMA had opened an investigation into Raiffeisen bank group and its former chief executive officer for suspected conflicts of interest. The investigation was concluded in June 2018. FINMA found that the bank had insufficiently managed conflict of interests. Additionally, the board of directors of the bank neglected the supervision of the former chief executive and thus at least potentially enabled him to achieve financial advantages to the detriment of Raiffeisen.

FINMA assessed the measures taken by Raiffeisen in the meantime to improve its corporate governance and ordered further measures to restore proper and diligent management. A later internal investigation confirmed FINMA's regulatory assessment.

The bank is currently assessing whether to claim damages from former board members and executive directors, in particular the former chief executive.

1MDB

OAG's investigation into the Malaysian sovereign fund 1MDB that was opened in August 2015 was still ongoing in 2018. Meanwhile, the OAG is investigating two former officials and 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).

The two former officials had been in charge of an Abu Dhabi sovereign wealth fund and two former employees of Petrosaudi, a Geneva-based oil company which is linked to 1MDB via a joint-venture.

The OAG is closely coordinating its investigations with the Malaysian authorities, which are (now) supporting the Swiss investigation.

Odebrecht SA and Braskem

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 OAG's taskforce has seized about 1 billion Swiss francs in more than 1,000 bank accounts and is currently dealing with more than 50 requests for mutual legal assistance as a result of the publicity following the conviction of Odebrecht SA.

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

25 Eastcheap
London
United Kingdom
EC3M 1DE
Tel: +44 20 3880 1540

www.lalive.ch

Government obligations

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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

There are no legal provisions which explicitly regulate risk and compliance aspects of the digital transformation. Rather, it remains to be tested whether the existing legal framework is adequate to deal with the new legal challenges. Using the example of bitcoin, the legal literature generally affirms that cryptocurrencies constitute assets and are therefore subject to the anti-money laundering framework. Accordingly, and by way of example, bitcoin or tokens/coins of any kind can be confiscated under article 70 SCC in case that are the proceeds of a crime.

If a supplier or dealer of bitcoin qualifies as a regulated person under Swiss law, the respective due diligence obligations are applicable.

This applies for example for the purchase or sale of bitcoin against official currencies, as this constitutes a regulated money exchange activity and requires compliance with the due diligence obligations applicable to money transfers and transfers of value under the Anti-Money Laundering Ordinance of FINMA (AMLO-FINMA). The same applies if a person is subject to the provisions of the BankA.

The Federal Council has recently started to react to the advancing digital transformation. For instance, small to medium-sized fintech companies can now obtain a banking licences as well. FINMA has also published a regulatory framework for ICOs (see question 2).

Turkey

Ümit Hergüner and Zeynep Ahu Sazcı Uzun
Hergüner Bilgen Özeke Attorney Partnership

LEGAL AND REGULATORY FRAMEWORK

Legal role

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 area of significant importance in Turkey.

Legislative developments in regulated industries have laid the foundation for a 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 have 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.

Laws and regulations

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, 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 Communiqué No. II. 17–1 (the Corporate Governance Communiqué) issued by the Capital Markets Board (CMB). The Corporate Governance Communiqué aims to enhance corporate governance mechanisms and risk and compliance management systems for listed companies. The communiqué 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).

Types of undertaking

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.

Regulatory and enforcement bodies

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.

The Turkish Competition Authority is the main body 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 communiqués) 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, it is equipped with broad intervention powers. For example, in the case of a compliance violation, it 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.

Definitions

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.

Processes

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.

Standards and guidelines

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 Communiqué, 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 Communiqué, 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 Communiqué.

Obligations

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.

LIABILITY

Liability of undertakings

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, a board of directors is required to manage and represent its 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 judgement 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 by-law 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.

Liability of governing bodies and senior management

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 by-laws 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 by-laws also provides guidance on the allocation of liability. If the governance powers of the board have been delegated through the company's internal by-laws, 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.

CORPORATE COMPLIANCE

Corporate compliance defence

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.

Recent cases

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

In 2018, Turkey underwent a phase of high currency volatility and a peak in inflation that drastically affected the markets. In this high-risk economic environment, companies' risk management abilities were tested. Many companies, even sector leaders that did not take the necessary measures against currency risks such as adjusting their reserves or adapting to these sudden changes, suffered financial meltdowns, some of which have declared bankruptcy or *concordato* (debt restructuring in line with a plan to be approved by the court).

Although the economy steadied during the first quarter of 2019, this period reminded market players of the importance of risk and compliance management, especially in developing countries.

Government obligations

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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

Through digital transformation, analysis of 'Big Data' and data management have become pivotal to Turkish corporations. This also includes the protection of personal data. In addition to the Law on the Protection of Personal Data, which came into force on 7 April 2016, there is also secondary legislation regulating sector-specific rules with respect to breach reporting and data collecting, such as energy companies' risk management or cybersecurity issues.

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

Regarding risk and compliance governance, the legislative framework has been adjusted to be stricter regarding the consequences of digital transformation for entities in certain sectors, if not all sectors. For instance, in the financial sector, in order for payment entities and electronic money entities to apply for an activity permit, they must obtain a specific report indicating whether the company has established the appropriate departments for its activities (eg, accounting, information, risk management, and reporting systems) and whether the company has implemented the necessary data security measures. Companies in the energy sector have an obligation to report to the Energy Market Regulatory Authority with respect to their inventory of industrial control systems used within the company. These systems are used for the monitoring and management of processes in the energy production sector using specific software operating systems.

The relevant regulations also imposes certain obligations on the senior management of these companies, such as adopting a risk management policy, a data security policy, and a data security management process. However, these obligations remain sector-specific and general at this stage, without being specifically tailored for digital transformation.

All entities and organisations are required to observe the rule of law, regardless of whether 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 bribery – 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

LEGAL AND REGULATORY FRAMEWORK

Legal role

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 United Kingdom.

This chapter focuses on core corporate risk and compliance management issues in the context of the UK's 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 European Union (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.

Laws and regulations

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 the FSMA 2000 (Regulated Activities) Order 2001 and the FSMA 2000 (Financial Promotion) Order 2005.

Other key rules and regulations include: the EU regulations that have a direct effect on English law (eg, the Market Abuse Regulation (MAR)); and rules made by the UK regulators (the Prudential Regulation Authority (PRA) and the FCA) under FSMA that apply to firms that are authorised and regulated in the UK as well as, in some circumstances, European Economic Area (EEA) firms that are licensed by other EEA regulatory authorities but conduct business in the UK.

The FCA rules can be found in the FCA Handbook section of the FCA's website and PRA rules on the PRA Rulebook Online website. 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.

There are also statutes containing corporate risk requirements which apply to firms carrying on a business in the UK, including 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.

Types of undertaking

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

Generally speaking, any legal person conducting 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 would be a listed company, must also do by 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 out.

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.

Regulatory and enforcement bodies

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 remits.

Prudential Regulation Authority

The PRA is responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms. It has powers in relation to failing firms and enforcement powers relating to breaches of the PRA's regulatory requirements. The PRA has three operational objectives:

- to promote the safety and soundness of the firms it regulates;
- to protect insurance policyholders; and
- to promote effective competition.

Financial Conduct Authority

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, including 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.

Competition and Markets Authority

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.

Serious Fraud Office

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.

Definitions

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). See question 7.

Processes

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 at 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.

Standards and guidelines

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. In addition, they 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; and
  - 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 (eg, 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, (ie, 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, including high-level obligations (eg, the duty to act in the best interests of the client and to treat customers fairly) and more detailed rules (eg, 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.

Obligations

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 partly 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, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 implementing the EU's Fourth Directive on Money Laundering) 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 adopt a risk-based approach towards anti-money laundering and 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 either in the UK or overseas (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, on the balance of probabilities, that it had adequate procedures in place to prevent bribery (see question 17).

LIABILITY

Liability of undertakings

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, 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 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 to deposit-taking institutions and, as of 10 December 2018, all insurance firms (subject to certain transitional arrangements). However, in 2019 the regime will be extended to cover all FCA-authorised firms (and will replace the Approved Persons

Regime described above). It is intended that the rules will apply to solo-regulated firms from 9 December 2019.

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 all UK companies, including those outside of 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 (broadly, individuals and other non-corporate 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). Two notable collective actions have been launched under the new legislation, including one in the financial sector. This was an action against MasterCard for damages arising from the European Commission's 2007 decision that MasterCard's multilateral interchange fees in the EEA were in breach of EU competition law. Both actions have so far failed to overcome the challenges of having their class actions certified by the UK's Competition Appeal Tribunal.

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 recent years, the FCA has expanded its use of non-pecuniary sanctions and has also made use of redress schemes as a way of compensating consumers who have suffered loss as a result of a firm's misconduct.

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 anti-money laundering control framework (see question 18).

More recently, the FCA has increased its focus on firms' digital defences and the extent to which firms have put in place effective systems and controls to prevent cyberattacks. In October 2018 the FCA levied a substantial fine (£16.4 million) against Tesco Personal Finance Plc for failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyberattack which had occurred in November 2016. The FCA found that Tesco had breached Principle 2 of the FCA's Principles for Businesses, which requires a firm to conduct its business with due skill, care and diligence.

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 fines.

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

At the time of writing, there are two key corporate criminal offences in respect of risk and compliance management deficiencies: the corporate offence of failure to prevent bribery under the Bribery Act 2010, and the corporate offence of failing to prevent the criminal facilitation of UK and foreign tax evasion under the Criminal Finances Act 2017.

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. At the time of writing, the government is still analysing the feedback from its call for evidence.

Save for the offences noted above, 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.

Deferred Prosecution Agreements (DPAs) are available to bodies corporate, partnerships and unincorporated associations facing criminal proceedings in the UK. There have been four fines issued in relation to DPAs since their introduction in early 2014. In question 18, we discuss the £500 million DPA that Rolls-Royce recently agreed with the SFO and the DPA which was agreed between Tesco Stores Ltd and the SFO.

There is no specific corporate criminal liability for competition law breaches.

Liability of governing bodies and senior management

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 (which, as noted in question 10, will cover FCA solo-regulated firms from 9 December 2019), 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. To determine a senior manager's area of responsibility, the regulator will consider the senior manager's statement of responsibilities and the firm's responsibilities map.

The FCA and the PRA can take disciplinary action against a senior manager for a breach of this statutory duty. Since the introduction of SM&CR, there has been an increase in enforcement activity against individuals and this is a trend which is likely to continue in the next few years.

Directors, managers and other officers can face director disqualification orders for failing to comply with competition law. This applies to individuals in all sectors. The CMA has increasingly been applying this regime and streamlined its guidance on director disqualification orders in February 2019.

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 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 UK 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'.

CORPORATE COMPLIANCE

Corporate compliance defence

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 offences if it can show that it had adequate procedures in place designed to prevent persons from 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 believed on reasonable grounds that the content of the communication was prepared/approved by an authorised person, or 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.

Recent cases

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 AML policies and procedures;

- had an inadequate AML information technology 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 cooperated 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'.

Santander UK Plc

The FCA's largest fine in 2018 was issued to Santander. The bank was fined more than £32 million for failings in its probate and bereavement process (which resulted in Santander failing to transfer funds owing to beneficiaries).

Although Santander was principally held to have breached Principle 3 (by failing to take reasonable care to organise and control its bereavement process effectively) and Principle 6 (for failing to treat its customers fairly), the bank was also held to have breached Principle 11 for not giving proper disclosure of the failings in its bereavement process to the FCA.

This case emphasises the importance of maintaining an open dialogue with the FCA and the consequences a firm may face if it provides information to the FCA on a selective basis.

Government obligations

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' (an EU law concept) and 'enterprises' (an 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.

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 EU sectoral legislation and FSMA will limit and, in some cases, remove the discretion of 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.

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

The FCA has not made any changes to regulations or the FCA Handbook to respond to the risk and compliance framework in respect of digital transformation. The FCA describes itself as a technology neutral regulator and has previously stated that it believes that its current rules are flexible enough to accommodate technological advancement.

However more recently there has been significant progress in the assessment and development of risk, compliance and regulatory frameworks for innovative financial products and services in the UK. In October 2018 the UK Cryptoassets Taskforce (consisting of HM Treasury, the FCA and the Bank of England) published an overview report of the cryptocurrency market. The report indicates that subject to the outcome of relevant consultation processes, the government stands ready to legislate to redefine and extend the regulatory perimeter if necessary, to ensure that digital transformation is adequately and appropriately covered.

Additionally, the FCA has maintained active involvement in digital transformation, reviewing its framework regularly in light of advancements in the market. Its business plan for 2018/19 highlights the intention to continue to focus on this. The FCA's work in this area includes:

- publishing a consultation paper in December 2017 in relation to the use of distributed ledger technologies (eg, blockchain), in which the FCA highlighted what it perceives to be the risks of digital transformation and highlighted its intention to keep its rules and guidance under review vis-à-vis the developments in this market;
- operating the 'Regulatory Sandbox' which enables firms to test financial technology products and enables the FCA to determine whether regulation is sufficient to cover the digital transformation. Most recently, in early 2019, the FCA (in cooperation with other international financial services regulators) developed a 'Global Regulatory Sandbox' to allow firms to test innovative products on a cross-border basis and so as to facilitate international cooperation with the aim of increasing financial integrity, consumer wellbeing and financial protection;
- undertaking a review in May 2018 of firms that utilised automated investment services, such as automated online discretionary investment management as well as those firms providing auto-advice. This review highlighted that certain firms were inadequately applying FCA rules when undertaking automated investment services, for example by failing to gather enough information to properly assess suitability. To mitigate risk, the FCA provided firms with feedback letters, as a result of which several firms altered their policies to become compliant;

- publishing a 'Dear CEO Letter' to banks in June 2018, setting out what the FCA believes to be good practice in respect of managing the risks that are associated with cryptocurrency, in particular in relation to financial crime; and
- publishing a consultation paper in January 2019 setting out the FCA's views on the regulatory status of different types of cryptoassets under the current regulatory framework.

As explained above, the outcome of the consultation papers may result in HM Treasury legislating further to widen the scope of the FCA regulatory perimeter in order to adequately cover the digital transformation.

There has been considerable commentary about whether and to what extent competition law needs to be updated to take account of such digital transformation. However, for the time being, existing competition law is being deployed to address such issues. From a compliance perspective, this means that companies should take steps to minimise the risk of any digital tools being used to breach competition law. For example, if a company is using artificial intelligence, its operational parameters should include compliance with competition law.

UPDATE AND TRENDS

Current developments and emerging trends

21 | Are there any other current developments or emerging trends that should be noted?

Brexit

At the time of writing, it is uncertain whether or not, and on what timetable, the UK will leave the EU. 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'.

Currently, 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 agreed and if so, what shape the bespoke financial services provisions will take. There has been speculation that there will be 'equivalence' between the UK and EU markets in respect of financial services, which would allow access to markets by treating the UK's regulatory system as equivalent to that of the EU, but no concrete agreement has as yet been reached.

Additionally, the FCA has confirmed that it has agreed memoranda of understanding (MoUs) with the European Securities and Marketing Authority and EU regulators in the event of a no-deal Brexit. The MoUs will facilitate supervisory cooperation, enforcement and exchange between the FCA and the national competent authorities of EU countries in the event of the UK leaving the EU without agreeing to an exit agreement. 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.

Furthermore, the FCA has introduced the Temporary Permissions Regime (TPR), which enables those firms that currently rely on EU passports to perform regulated activities in the UK to continue to do so for up to three years after Brexit while preparing an application for full UK authorisation. Firms that benefit from the TPR will be deemed to possess the equivalent permissions required in order to perform those activities within the UK. FCA-regulated firms that enter the TPR will be given a 'landing slot' of three months, during which they will be able to submit an application for full UK authorisation. If they do not within the landing slot, they will no longer be able to benefit from the TPR.

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

Focus on individual accountability

As explained above, there is an increasing regulatory focus on individual accountability with the Yates Memo in the US and the SM&CR 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.

In May 2018, the FCA and the PRA published their joint decision in the first case brought under the SM&CR. The regulators fined the chief executive of Barclays Group (Mr James Staley) £642,430 for failing to act with due skill, care and diligence in relation to a whistleblowing report received by the bank in June 2016. The case demonstrates the high standard of conduct expected of senior managers and in particular, individuals carrying out chief executive functions.

We expect to see an increasing number of fines issued to senior managers over the next few years.

Market abuse

Market abuse and capital market disclosure issues are currently high on the FCA's enforcement agenda.

In December 2017, the FCA issued a fine to Tejoori Limited for failing to inform the market of inside information in breach of MAR. This is the first fine the FCA has imposed on a company listed on the Alternative Investment Market for breaching MAR in connection with late disclosure.

Insider dealing is also a key enforcement priority for the FCA and it has been particularly focused on securing criminal convictions against individuals involved in insider dealing rings. In December 2018, the FCA published new guidance on financial crime systems and controls relating to insider dealing and market manipulation. This includes guidance on: governance, risk assessment, policies and procedures, and ongoing monitoring. The FCA will expect firms to review the guidance and to make any appropriate enhancements to their systems and controls infrastructure.

United States

Mahnu Davar
Arnold & Porter

LEGAL AND REGULATORY FRAMEWORK

Legal role

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 US government's expectations for organisations, regardless of whether they operate in the US or in other countries. While there is generally no legal requirement for an organisation to 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 an effective compliance programme is recognised as assisting in protecting the reputation of the organisation.

Laws and regulations

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

The primary source addressing compliance expectations is the US Federal Sentencing Guidelines, as set forth in Chapter 8, Part B, Subpart 2.1 of those Guidelines. The Guidelines have been modified over time to reflect the 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.

Types of undertaking

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.

Regulatory and enforcement bodies

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 and serves as the federal government's lawyer in court. 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 (DHHS), the Food and Drug Administration, the Federal Trade Commission, the Financial Industry Regulatory Authority, and the Office of Foreign Assets Control. 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.

Definitions

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.

Processes

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

The Guidelines set out the details regarding processes involved in an effective compliance programme. In addition, detailed information has been published regarding compliance programme responsibilities regarding bribery and corruption risks. This information can be found in A Resource Guide to the US Foreign Corrupt Practices Act, published in 2012 by the DOJ and the SEC and in the United States Attorneys Manual. In February 2017 the Fraud Section of the DOJ published its Evaluation of Corporate Compliance Programs. 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 it would permanently include the principles of its Foreign Corrupt Practices Act (FCPA) Pilot Program, which was launched in April 2016, in the US Attorneys Manual. This 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, such as 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 various guidelines such as the OIG Compliance Program Guidance for Pharmaceutical Manufacturers 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 DHHS and the American Health Lawyers Association in 2003. For companies that seek to do business with the US government (such as selling goods or services to a government agency), an additional layer of regulations is set forth in the Federal Acquisition Regulations and relevant guidance must be followed. These, like the OIG guidance mentioned, seek to ensure that a regulated firm is trustworthy and can demonstrate responsibility to control the activities of its employees and contractors through the exercise of an effective compliance programme.

Standards and guidelines

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 the 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 its standards and procedures, and other aspects of the compliance programme periodically and in a practical manner, 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. Often it is necessary for a company to engage independent outside counsel to conduct an investigation into potential legal or policy violations, particularly when there is a need for the organisation to consider the investigation findings under attorney-client privilege.

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.

Obligations

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.

LIABILITY

Liability of undertakings

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, 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 both 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.

Additionally, certain sector-specific laws may set forth compliance obligations for members of senior management, such as certifications of accountability or certifications of the accuracy of required government filings.

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. In some heavily regulated industries in the United States, courts have interpreted certain laws as authorising sanctions if senior management fails to prevent violations they are presumed to have known about by virtue of their position in an organisation. US public health laws, such as the Federal Food and Drug Cosmetic Act, and environmental laws, such as the Clean Water Act, are examples of laws that have been applied broadly in such circumstances.

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.

Liability of governing bodies and senior management

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 criminal misconduct, the risk of criminal liability to board members and senior management is low for failing to implement compliance programme obligations.

CORPORATE COMPLIANCE

Corporate compliance defence

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.

Recent cases

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 be 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.

Government obligations

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.

Arnold & Porter

Mahnu Davar
mahnu.davar@arnoldporter.com

601 Massachusetts Ave, NW
Washington, DC 20001
United States
Tel: +1 202 942 6172
www.arnoldporter.com

DIGITAL TRANSFORMATION

Framework covering digital transformation

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

In the US, there is no single source of regulatory requirements for digital products. Rather, companies must carefully consider which sector and subject matter-specific laws apply to their products. For example, state and federal privacy laws set forth basic expectations regarding the solicitation, storage and use of consumer information. There is heightened scrutiny under these laws for companies who obtain patient-identifiable information in the healthcare context – such as gene sequencing companies or companies who operate health software platforms.

The state of California has been a leader in regulating digital technologies, in part because of the large number of companies working in this area based in that state. It has passed its own set of state jurisdiction-specific laws governing privacy and consumer protection that must be followed in addition to federal laws.

Other technologies, such as artificial intelligence, robotics, and blockchain have been the subject to specific regulatory agency's working groups and public-private workshops intended to help define the parameters of these technologies and educate regulators on technological advances.

From a compliance programme standpoint, US companies must apply a risk-based approach to developing controls around these new technologies. For example, the use of machine learning or artificial intelligence systems to manage customer service interactions (eg, customer service bots) can lead to reputational or legal risks if consumers feel like their rights have been violated or if they are provided deceptive, false, or misleading information about goods or services. For companies that pursue the use of such systems, the compliance department must work closely with technological experts to ensure that such systems are validated not only for their business purpose but also contain safeguards to allow for corrections and overrides when necessary to comply with consumer protection laws, for example.

Do DOJ policy and the ISO compliance standard overlap?

Daniel Lucien Bühr
Lalive

Overview

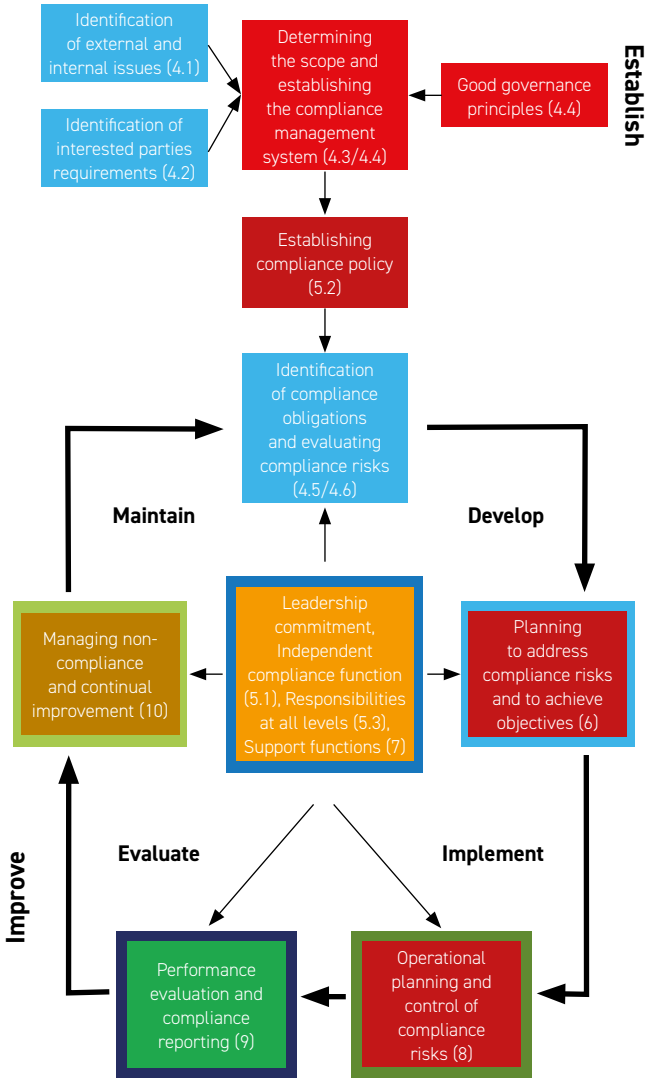
In February 2017, the Fraud Section of the United States Department of Justice's Criminal Division published a document entitled 'Evaluation of Corporate Compliance Programs',[1] its most recent communication of the DOJ's assessment criteria for effective corporate compliance programmes. The DOJ recognises 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. In 2018, ISO 19600 was confirmed, and it is currently advanced to a requirements standard (ISO 37301), which is planned to be published in 2020. ISO 19600 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]



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 globally recognised 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 top 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 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 (eg, 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, top 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 methods to identify, analyse and evaluate compliance risks, such for instance 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 (eg, 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 (eg, 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 top 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 (eg, 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.

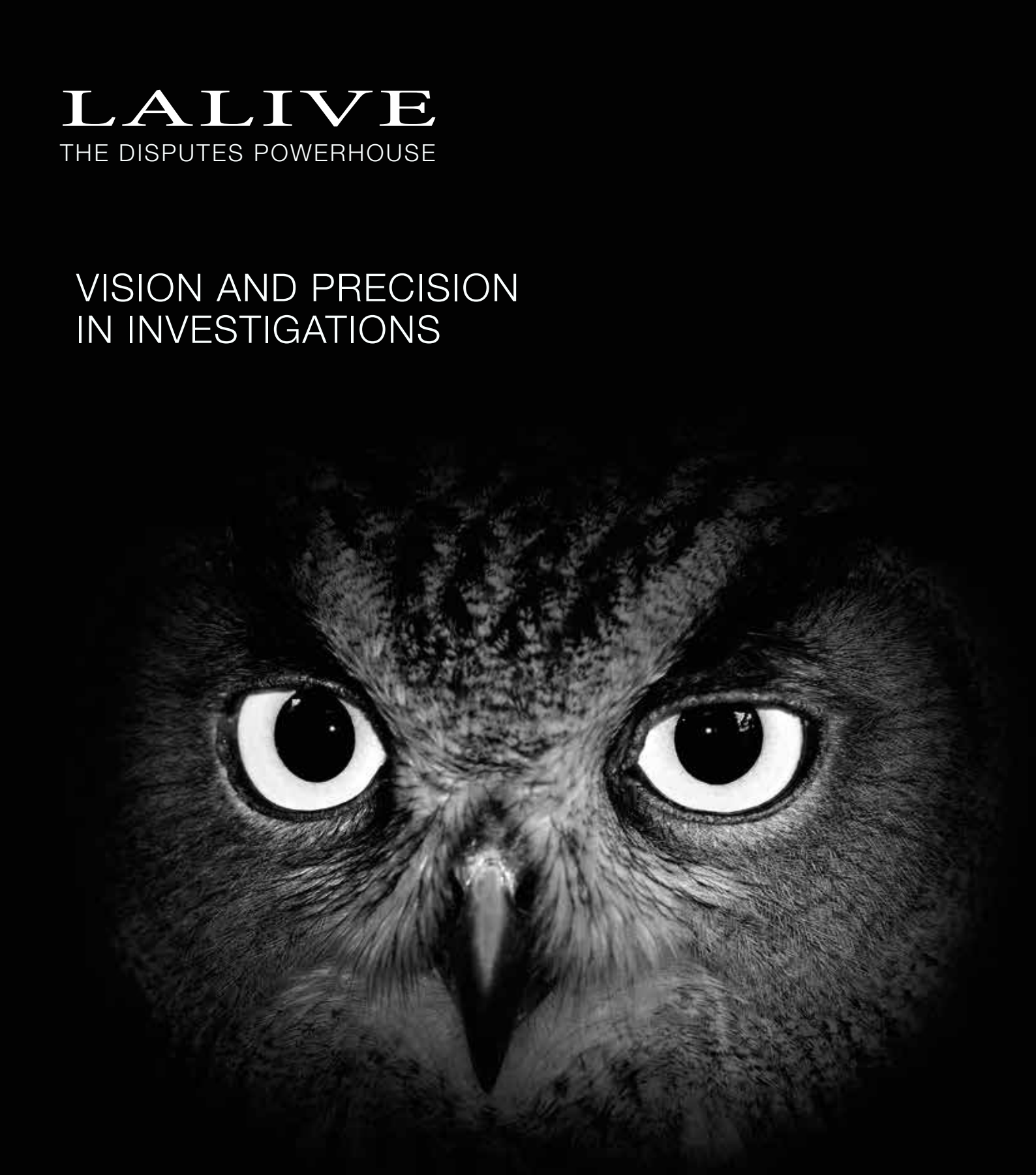
4 ISO Standard 37001 – Anti-bribery management systems is more detailed.

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.

LALIVE

THE DISPUTES POWERHOUSE

VISION AND PRECISION IN INVESTIGATIONS



Geneva Zurich London

lalive.law

Other titles available in this series

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
Defence & Security Procurement
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
Gaming
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
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
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 Procurement
Public-Private Partnerships
Rail Transport
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
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-111-7