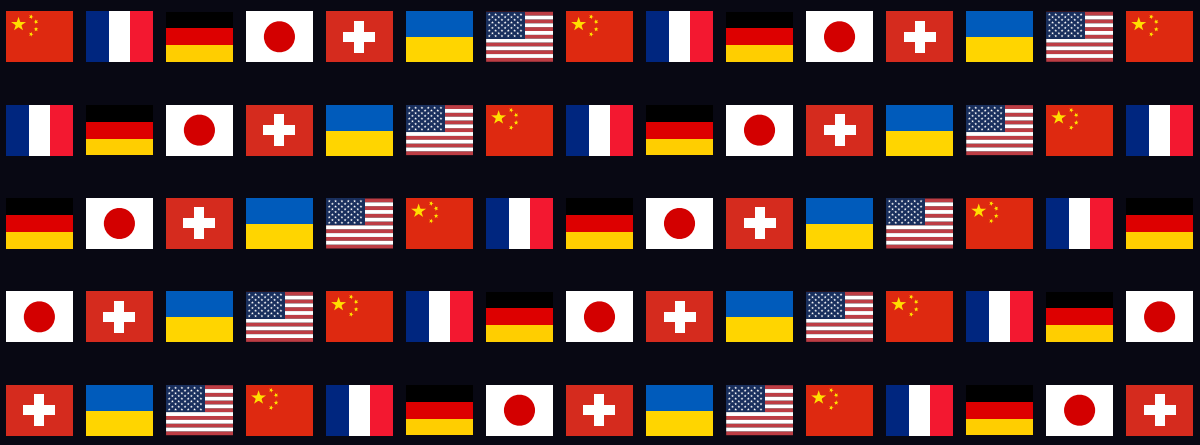
RISK & COMPLIANCE MANAGEMENT

China



LEXOLOGY
Getting The Deal Through

Consulting editor
LALIVE

Risk & Compliance Management

Consulting editors

Daniel Lucien Bühr

LALIVE

Quick reference guide containing side-by-side comparison of local insights into Risk & Compliance Management, including laws and regulations; principal regulatory and enforcement bodies; definitions, processes, standards and guidelines; civil, administrative, regulatory and criminal liabilities (for undertakings, governing bodies and senior management); corporate compliance defence; recent leading cases; risk and compliance framework covering digital transformation; and recent trends.

Generated 04 April 2022

Table of contents

Contributors

China

Alan Zhou
alanzhou@glo.com.cn
Global Law Office

Jacky Li
jackyli@glo.com.cn
Global Law Office

Jenny Chen
jennychen@glo.com.cn
Global Law Office

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

Corporate risk and compliance management is recognised as the foundation for sustainable development of undertakings. In a social system governed by the rule of law, legal and compliance is surely among the basic prerequisites for undertakings to achieve long-term growth. As is reiterated by President Xi Jinping, it is crucial to regulate corporate investment and business practices, and to ensure compliance operation and management, so as to fulfil social responsibility.

Law stated - 12 July 2021

Laws and regulations

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

Corporate risks could be divided into two levels, criminal risks and administrative risks. Criminal risks are regulated by the Criminal Law and its corresponding judicial interpretations. For criminal risks, among the 469 crimes prescribed by the Criminal Law, there are approximately 150 unit crimes for which an undertaking itself could be deemed the perpetrator. As for administrative risks, they are derived from the respective administrative laws and regulations, such as the Company Law, the Anti-unfair Competition Law, the Anti-Monopoly Law and the Advertisement Law, the Cybersecurity Law, the Personal Information Protection Law, the Data Security Law covering violations such as commercial bribery, monopoly, company illegal operation, illegal advertising personal information protection and data security.

Compliance management is also an integral element of the above laws and regulation. In addition, there are specified regulations and guidelines published for various types of undertakings, such as the Measures on Compliance Management of Insurance Companies, the Guidelines for Comprehensive Risk Management of Centrally Governed Enterprises, the Guidelines for Centrally-Governed Enterprises on Compliance Management (for Trial Implementation), the Guidelines for Compliance Risk Management of Commercial Banks, the Measures for the Compliance Management of Securities Companies and Securities Investment Fund Management Companies and the Anti-monopoly Compliance Guidelines for Business Operators.

Law stated - 12 July 2021

Types of undertaking

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

Generally, undertakings attached to national security, people's livelihood, social public interests and state assets will be of highest priority for risk and compliance management. For example, undertakings in key industries such as financial and telecommunications would usually be required to spend more efforts in risk and compliance management.

As for listed companies, a recent trend is to classify the listed companies into different risk level and subject to differentiated supervision based on the classification results. The listed companies are divided into four classes, namely highest risk, second highest risk, concern and normal, in accordance with the different degrees of risk and supervision priority.

Law stated - 12 July 2021

Regulatory and enforcement bodies

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

From a criminal perspective, authorities with criminal enforcement power mainly include:

- public security bureaus (PSBs), responsible for investigations, criminal detentions, the execution of arrests and preliminary inquiries in criminal cases;
- the people's procuratorates (procuratorates), responsible for prosecutions, the approval of arrests and conducting investigations on criminal violations;
- supervisory commissions, which supervise all public officials, investigate duty-related illegal activities and offences, and carry out anti-corruption work; and
- national security authorities, which investigate and handle cases of crimes that compromise national security, performing the same functions and powers as PSBs.

From an administrative perspective, authorities with enforcement power mainly include:

- the State Administration for Market Regulation, which oversees market regulation, food safety, healthcare compliance, advertisement violations, competition violations, commercial bribery, antimonopoly; and its subsidiary bureaus, including the administrations for market regulations at the provincial, municipal and county levels;
- the National Development and Reform Commission and its subsidiary bureaus, responsible for overall planning and control of the national economy, and investigating price-related violations;
- the China Securities Regulatory Commission and its subsidiary bureaus, responsible for the administration of securities and investigating securities fraud;
- the China Banking and Insurance Regulatory Commission, responsible for unified supervision and management of the banking and insurance industry in accordance with laws and regulations, maintaining the legal and sound operation of the banking and insurance industry, prevent and resolve financial risks, protecting the legitimate rights and interests of financial consumers, and maintaining financial stability;
- the People's Bank of China and its subsidiaries, responsible for carrying out monetary policy and regulation of financial institutions in mainland China, and regulating money laundering activities;
- the Cyberspace Administration of China (CAC), responsible for the overall planning and co-ordination of network security and relevant supervision and administration; and
- other administrative authorities, such as the State Taxation Administration, the Customs and the Environmental Protection Bureaus, etc.

Law stated - 12 July 2021

Definitions

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

'Risk management' and 'compliance management' are defined in various regulations and guidelines. For example, 'risk management' is defined by the Guidelines for Comprehensive Risk Management of Centrally Governed Enterprises as the process and methods of providing reasonable assurance to achieve the overall goal of risk management by

implementing the basic process of risk management in all aspects of enterprise management and operation, fostering a good risk management culture, and establishing a sound comprehensive risk management system, including a risk management strategy, risk management financial measures, organisational and functional system of risk management, risk management information system and internal control system.

'Compliance management' is defined by the Measures on Compliance Management of Insurance Companies as the act of preventing, identifying, evaluating, reporting and responding to compliance risks by establishing compliance management mechanisms, formulating and implementing compliance policies, conducting compliance audits, compliance inspections, compliance risk monitoring, compliance assessments and compliance training.

Law stated - 12 July 2021

Processes

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

Risk and compliance management processes are set out in various regulations and guidelines such as the Guidelines for Compliance Risk Management of Commercial Banks, the Guidelines for Comprehensive Risk Management of Centrally Governed Company, the Guidelines for Enterprise Legal Risk Management and the Guidelines for Enterprises on the Compliance Management of Overseas Operations.

Law stated - 12 July 2021

Standards and guidelines

Give details of the main standards and guidelines regarding risk and compliance management processes in your jurisdiction.

The main processes for risk and compliance management stipulated in various regulations and guidelines are by large similar, with certain variance for the specifics.

For instance, the Guidelines for Compliance Risk Management of Commercial Banks provides the basic elements, as follows:

- compliance policies;
- organisation structure and resources of the compliance management department;
- compliance risk management plan;
- identification of compliance risks and the management procedures; and
- compliance training and educational system.

The Guidelines for Enterprises on the Compliance Management of Overseas Operations provides that such processes include the following steps:

- setting up compliance management structure (such as compliance committee, compliance officer, etc);
- establishing compliance management system (such as internal policies);
- designing and implementing compliance management operation mechanism (such as compliance training, compliance reporting);
- risk identification, assessment and disposal;
- compliance monitoring, audit, review and improvement; and
- compliance culture development.

Law stated - 12 July 2021

Obligations

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

The newly promulgated Data Security Law (effective since 1 September 2021) and Personal Information Protection Law (effective since 1 November 2021) stipulates the requirement for all companies in China to establish data compliance management systems and related compliance obligations.

In addition, certain types of entities in mainland China are subject to specific compliance governance obligations according to relevant laws, regulations and guidelines.

For instance, the Measures on Compliance Management of Insurance Companies provides that insurance companies shall appoint a chief compliance officer and set up a compliance management department, which are entitled to the rights of information access, investigation, reporting and their independence from other departments shall also be ensured. Similar governance obligations are imposed on commercial banks and centrally governed state-owned enterprises.

For other types of companies, it would be deemed as recommended and best practices to have independent compliance professionals and department responsible for compliance management, rather than compulsory legal obligations.

Law stated - 12 July 2021

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

Key elements for risk and compliance management generally include:

- setting up compliance management structure (such as compliance committee, compliance officer);
- establishing compliance management system (such as code of conduct and internal policies);
- providing adequate training to the employees and third parties;
- establishing and maintaining effective reporting channels;
- establishing comprehensive compliance accountability system;
- compliance monitoring, audit, review and improvement; and
- compliance culture development.

Law stated - 12 July 2021

LIABILITY

Liability of undertakings

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

For board of directors, their main compliance management responsibilities include:

- approving the strategic planning, basic system and annual report of corporate compliance management;
- promoting the improvement of the compliance management system;

- deciding on the appointment and dismissal of the person in charge of compliance management;
- deciding on the setup and functions of the compliance management department;
- studying and deciding on the major issues related to compliance management; and
- determining the handling of violations according to the authority.

For senior management, the main compliance management responsibilities include:

- establishing and improving the organisational structure of compliance management according to the decision of the board of directors;
- approving the specific system requirements for compliance management;
- approving the compliance management plan and taking measures to ensure the effective implementation of the compliance system;
- identifying compliance management processes to ensure that compliance requirements are integrated into the business area;
- promptly stopping and correcting non-compliance with business operations, and conducting accountability or proposing suggestions for handling violations according to the authority; and
- other matters authorised by the board of directors.

Law stated - 12 July 2021

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

Deficiencies in risk and compliance management will not necessarily occasion civil liability to undertakings. Nevertheless, if such deficiencies lead to any conduct that infringes the legitimate rights and interests of other parties, undertakings may face civil liability for such infringement.

For instance, due to inadequate compliance management, if a company commits commercial bribery to obtain an improper advantage against its competitors, those competitors may bring civil actions against the company for the unfair competition, seeking for compensation.

From an internal perspective, if any deficiency infringes the rights of its own employees, such as leaking the personal information of the employees, those employees may also sue the company and claim for damages.

Law stated - 12 July 2021

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

Deficiencies in risk and compliance management will occasion administrative or regulatory consequences if such deficiencies directly or indirectly lead to any administrative violations committed by undertakings.

For instance, in 2020, one Chinese local bank was fined for more than 10 times for administrative violations related to loaning mismanagement, violation of the prudent operation rules and other types of non-compliant business operation. Particularly for prudent operation rules, pursuant to the Law on Banking Regulation, they shall include risk management, internal control, capital adequacy ratio, quality of assets, reserves for losses, risk concentration, affiliated transactions or liquidity of assets. And violation of the prudent operation rules, including deficiencies in risk management and internal control, would be subject to fine, suspension of business and revocation of business licence (under serious circumstances).

Law stated - 12 July 2021

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

Among the 469 crimes prescribed by the Criminal Law, there are approximately 150 unit crimes for which a company could be qualified as the perpetrator, and for these unit crimes, a company will be held criminally liable if:

- a collective decision has been made by the management of the company, or an individual decision by the relevant responsible personnel on behalf of the company, such as the legal representative; and
- the crime is committed in the name of the company and the illegal proceeds go to the company.

Deficiencies in risk and compliance management will occasion criminal liability if such deficiencies directly or indirectly lead to any criminal violations committed by undertakings. Conversely, if a company is subject to criminal liability, it is likely that there are deficiencies in risk and compliance management for the company's business operation.

Law stated - 12 July 2021

Liability of governing bodies and senior management

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

If breach of risk and compliance management obligations leads to any conduct that infringes the legitimate rights and interests of other parties, undertakings may face civil liability for such infringement. Under these circumstances, a director, supervisor or senior management may be held liable for compensate the loss to the company if he or she violates laws, administrative regulations or the company's articles of association during the performance of duties in accordance with the Company Law.

Law stated - 12 July 2021

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

Breach of risk and compliance management obligations may occasion administrative or regulatory consequences to directors and senior management if such breach leads to any administrative violations.

For instance, in 2020, some senior management in banking industry were fined, given warnings and prohibited from engaging in banking due to those banks' non-compliance with the prudent operation rules (which includes risk management) as prescribed by the Law on Banking Regulation. Another example is for data compliance, person directly in charge may be subject to fine and administrative custody if a company fails to fulfil those mandatory data compliance obligations imposed by the Cybersecurity Law and the Data Security Law.

Law stated - 12 July 2021

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

The Criminal Law adopts a dual punishment system for unit crime, which means both the company and the responsible persons are subject to the criminal liabilities with only a few exceptions otherwise prescribed in the Criminal Law. Therefore, breach of risk and compliance management obligations may occasion criminal liability to directors and senior management if such breach leads to any crimes committed by the company, and the following elements need to be satisfied simultaneously:

- the crime is expressly stipulated in the Criminal Law that 'the persons who are directly in charge and the other persons who are directly responsible for the crime' shall be penalised, such as production and sale of fake or substandard goods, tax evasion, bribery and illegal business operation;
- the crime is committed in the name and under the control of the will of the company; and
- directors and senior management act as the persons who are directly in charge or who are directly responsible for the crime, playing the role of determining, approving, inspiring, conniving or directing in the crime committed by the company.

Law stated - 12 July 2021

CORPORATE COMPLIANCE

Corporate compliance defence

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

Corporate compliance may serve as a defence from the following perspectives.

On a criminal level, one type of defence strategy that commonly adopted by companies is using corporate compliance as part of the evidence to prove the alleged criminal conduct is committed by employees as an individual crime, rather than a unit crime. There are no clear standards or requirements for such defence, and the court would usually consider the elements such as the design, implementation and effectiveness of the corporate compliance programme.

Taking commercial bribery as an example, the bribery acts of an employee of a company could be deemed as either an individual crime, or a unit crime, depending on various considerations including the company's involvement in the bribery act (such as whether it is the company's decision to conduct the bribery), the possession of the illegal gains, and whether the bribes are offered in the name of the company or the individual employee. If the charge is raised against the individual employee, then the company would not be held accountable for the crime. One representative case is that in 2016, one local pharmaceutical company was charged for the crime of bribery committed by a unit. In its defence, the company used the evidence that the code of conduct and other internal policies explicitly prohibit gift-giving and any other types of bribery, together with the other evidence to support its defence that the bribery was committed by one senior executive for the benefit of him or herself, rather than the company. The court eventually ruled for the company in this case.

In addition, since March 2020, the Supreme People's Procuratorate has been promoting pilot programs on corporate compliance reforms, including 'non-arrest based on compliance', 'non-prosecution based on compliance', and 'leniency application based on pleading guilty'. In the pilot regions, the People's Procuratorates can conduct compliance visits to the companies involved in the case, reach compliance supervision agreements with the companies, request the companies to establish or improve their compliance systems within a certain period of time, and review and evaluate the results. Based on the circumstances of the case and the review results, the People's Procuratorates would determine whether to arrest, prosecute or propose a lighter punishment.

On an administrative level, in accordance with the Anti-Unfair Competition Law amended in 2017, the acts of bribery committed by the employee of a company shall be deemed as the conducts of the company, unless it has evidence to prove that such acts of the employee are irrelevant to seeking for transaction opportunities or competitive advantages for the company. However, no specified regulations or judicial interpretations regarding what evidence would be most

valid have been made available. Some local regulations (such as the Shanghai Anti-Unfair Competition Regulations) contain provisions encouraging companies to establish compliance management system of anti-bribery and anti-unfair competition and in practice, some multinational and local companies have already implemented compliance projects and preventative measures such as providing regular compliance training and requiring employees' written compliance commitment letters in preparation for any potential legal liability concerns. Furthermore, it has been suggested by the former State Administration for Industry and Commerce in a press conference in November 2017, that if the business operator has set up measures that are legitimate, in compliance and reasonable, and has adopted effective inspection on the implementation, the company could be relieved from the legal liabilities.

Additionally, the newly revised Administrative Penalty Law provides that where a party concerned has sufficient evidence to prove that the party has no subjective fault, no administrative penalty shall be imposed on the party. Although there is no official interpretation on the standard of proof for no subjective fault, it is commonly believed that compliance measures would be an important element in corporate defence.

Law stated - 28 January 2022

Recent cases

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

In November 2021, the former chairman, general manager, and other 11 senior executives of a local listed pharmaceutical enterprise were criminally sentenced and fined for committing financial frauds including manipulating securities market, illegally disclosing or not disclosing material information and commercial bribery. In addition, the stakeholders of the company were held civilly liable for misrepresentation with a compensation totalling 2.459 billion yuan to 52,037 investors. This is a typical example reflecting corporate risk and compliance management failure in terms of white-collar crime and financial fraud.

Law stated - 28 January 2022

Government obligations

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

Risk and compliance management related obligations for government and government agencies are mostly obligations to supervise. For instance, the China Banking and Insurance Regulatory Commission is responsible for supervising, inspecting and assessing the effectiveness of the risk and compliance management of the commercial banks. The State-owned Assets Supervision and Administration Commission of the State Council is responsible for actively promoting the compliance management of the centrally governed state-owned enterprises.

As for state-owned enterprises, mainly centrally governed state-owned enterprises, their key risk and compliance management obligations include:

- establishing compliance management system (such as code of conduct and internal policies);
- establishing a compliance risk identification and early warning mechanism;
- strengthening compliance risk response;
- establishing and improving the compliance review mechanism;
- strengthening the accountability for violations;
- strengthening the compliance assessment and evaluation;

- strengthening the development of compliance management information;
- establish a specialist and high-quality compliance management team;
- providing adequate training to the employees and third parties;
- establishing and maintaining effective reporting channels; and
- cultivating compliance culture and awareness.

Law stated - 28 January 2022

DIGITAL TRANSFORMATION

Framework covering digital transformation

Please provide an overview on the risk and compliance governance and management framework covering the digital transformation (machine learning, artificial intelligence, robots, blockchain, etc).

Digital transformation is in principle governed by the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, along with the corresponding implementation rules. While there are no specific rules for the risk and compliance governance and management framework, the general requirements on cybersecurity and data protection include:

- multi-level protection scheme;
- personal information protection and important data protection;
- critical information infrastructure protection; and
- network information content control.

In addition, the general requirements for data security include:

- a data security management system;
- data security training;
- data security risk monitoring and reporting of data security incidents;
- protecting important data and core data; and
- restricting data provided to foreign judicial and law enforcement agencies.

More specifically, the requirements for personal information protection include:

- an internal management system and operating procedures;
- category-based management of personal information;
- technical security measures such as encryption and de-identification;
- access control on personal information processing and training; and
- an emergency response plan for personal information security incidents.

For blockchain, a high-level regulation, the Management Regulation for Blockchain Information Services was promulgated in January 2019 and took effect in February 2019, which stipulates some general requirements for record filing and security. In January 2021, the draft for a national standard, the Blockchain Information Services Security Specifications, was released for public comments, which provides more specified technical requirements covering the

collection, processing, publishing, transfer, storage and disposal of data in blockchain information services.

For artificial intelligence (including machine learning and robots (AI)), the National Professional Committee on Governance of New Generation Artificial Intelligence released the Principles of Governance of New Generation Artificial Intelligence – Developing Responsible Artificial Intelligence in June 2019, which establishes the framework and action guidelines for AI governance. And recently, a Cybersecurity Standards Practice Guidance – the Artificial Intelligence Ethical Security Risk Prevention Guidelines – was released in January 2021 by the National Information Security Standardisation Technical Committee, which identifies the ethical security risks related to artificial intelligence and the preventative measures for risk management.

Law stated - 01 November 2021

UPDATE AND TRENDS

Key developments of the past year

What were the key cases, decisions, judgments and policy and legislative developments of the past year?

From a legislation perspective, key developments cover multiple areas including antitrust, general corporate governance, data security and personal information protection, etc.

With respect to antitrust, the draft amendment to the Anti-monopoly Law was released for public comments in October 2021, which intends to introduce several new governance mechanisms with more stringent penalty regimes. In addition, the Notice of the State Administration for Market Regulation on Promulgation of the Guidelines for Overseas Anti-monopoly Compliance of Enterprises was promulgated by the State Administration for Market Regulation in November 2021 for the purpose of encouraging enterprises to cultivate a compliance culture of fair competition, establish and strengthen an overseas antimonopoly compliance management system, prevent overseas antimonopoly legal risks, and ensure sustainable and sound development of enterprises.

With respect to data security and personal information protection, two important pieces of legislation, the Data Security Law and the Personal Information Protection Law both came into effect in 2021. The Data Security Law intends to set up the data security system, impose data security obligations on individuals and entities for data related activities. And the Personal Information Protection Law focuses on personal information protection, with more specified requirements on protecting sensitive personal information, cross-border data transfer, as well as more clarity on the legal obligations and consequences.

With respect to anti-money laundering, the draft revision to the Anti-money Laundering Law was released for public comments in June 2021, which proposes to expand the definition of anti-money laundering and money laundering behaviours, include more parties under regulation and broaden the investigation authorities, etc. Furthermore, the draft intends to encourage relevant parties to prevent anti-money laundering risks and strengthen the governance by clarifying the obligations of each regulated party.

From a law enforcement perspective, the key enforcement areas include anti-bribery, antitrust, securities fraud, anti-money laundering and data protection.

Law stated - 01 November 2021

Jurisdictions

China	Global Law Office
France	De Gaulle Fleurance & Associés
Germany	Pohlmann & Company
Japan	Mori Hamada & Matsumoto
Switzerland	LALIVE
Ukraine	Sayenko Kharenko
USA	Arnold & Porter