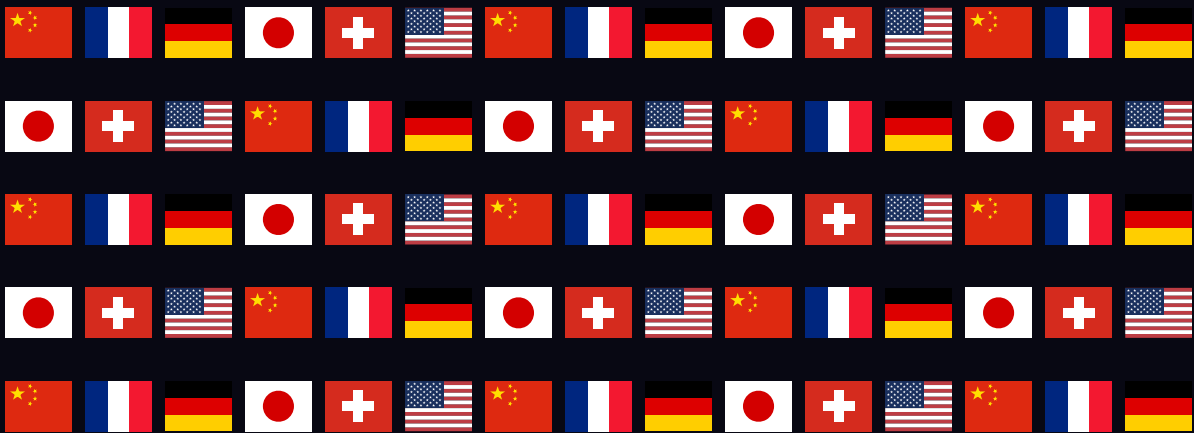


RISK & COMPLIANCE MANAGEMENT

USA



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 06 April 2023

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. © Copyright 2006 - 2023 Law Business Research

Table of contents

LEGAL AND REGULATORY FRAMEWORK

Legal role

Laws and regulations

Types of undertaking

Regulatory and enforcement bodies

Definitions

Processes

Standards and guidelines

Obligations

LIABILITY

Liability of undertakings

Liability of governing bodies and senior management

CORPORATE COMPLIANCE

Corporate compliance defence

Recent cases

Government obligations

DIGITAL TRANSFORMATION

Framework covering digital transformation

UPDATE AND TRENDS

Key developments of the past year

Contributors

USA



Mahnu V Davar
mahnu.davar@arnoldporter.com
Arnold & Porter



Jonathan E Green
jonathan.green@arnoldporter.com
Arnold & Porter



Annie Blackman
annie.blackman@arnoldporter.com
Arnold & Porter



Ryan D White
ryan.white@arnoldporter.com
Arnold & Porter

Arnold & Porter

LEGAL AND REGULATORY FRAMEWORK

Legal role

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

Regulators and enforcement authorities in the United States expect companies – particularly those in highly regulated industries – to maintain ‘effective’ compliance programmes. Effective programmes are those that effectively serve to prevent or detect and correct violations of law relative to the size, type, and risks of an organisation. Various government agency documents identify hallmarks of an effective compliance programme. Some state and federal regulators require regulated companies to maintain compliance programmes as a matter of law. For example, healthcare providers or healthcare entities that enrol in direct contracts with Medicare are expected to provide specific training to employees and contractors on fraud, waste, and abuse laws, and also to maintain certain programmatic elements to help identify and report in a timely manner healthcare law violations. In the financial services industry, broker-dealers and investment advisors are generally required to establish, maintain, and enforce written policies and procedures reasonably designed to achieve compliance with relevant laws and regulations. Certain industries are also subject to self-disclosure programmes that create strong regulatory incentives to proactively identify and report violations, such as overpayments under government contracts and the banking industry’s affirmative obligation to file ‘suspicious activity reports.’ Moreover, long-standing prosecutorial guidance holds that timely self-reporting misconduct to law enforcement and maintaining an effective compliance programme can significantly mitigate – if not altogether avoid – criminal charges (or, in some cases, civil or administrative actions) against a corporate defendant. That guidance also influences the calculation of fines and penalties under certain laws. The extraterritorial reach of certain laws, such as the US Foreign Corrupt Practices Act, means that these considerations apply to corporations that choose to do business in the United States or trade on US exchanges, even if the majority of their corporate presence or business is outside the United States. In general, companies that maintain effective compliance programmes are better situated in the event of a regulatory inspection, enforcement action, or prosecution.

Law stated - 28 March 2023

Laws and regulations

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

A primary source addressing compliance expectations is the US Federal Sentencing Guidelines, as set forth in Chapter 8, Part B, Subpart 2.1 thereof. The Sentencing Guidelines have been modified over time to reflect the evolution of compliance expectations. The Guidelines are promulgated by the US Sentencing Commission, an independent agency of the federal judiciary, and address how to calculate fines, penalties and prison sentences for a wide variety of offences committed by organisations as well as individuals. In general, they provide a formula for each offence that is then adjusted based on the underlying facts surrounding the conduct and defendant in question, taking into account certain aggravating and mitigating factors. One of the mitigating factors recognised for organisations is the existence of a compliance programme. The Guidelines set out basic elements of an effective compliance programme, which may lead to reduced sentences, including reduced fines and penalties.

These Guidelines are used not only by judges but also by a variety of government agencies to guide their own regulatory and enforcement efforts. Some US states have required certain companies, such as those operating in the pharmaceutical industry, to maintain compliance programmes as a condition of doing business in the relevant state. In addition, the public statements and priorities of regulatory agencies have a significant impact on the regulatory and compliance landscape. There is also caselaw interpreting these guidelines as well as other important laws, such as Delaware corporate law (eg, *In re Caremark*), which establishes ‘duty of care’ norms for corporate officers and directors.

Types of undertaking

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

All organisations, companies, corporations, and other entities are covered, regardless of form. There is some recognition in the Sentencing Guidelines and other pronouncements that small companies should be evaluated differently from larger ones. Nevertheless, the governing authorities and high-level personnel of corporate entities are expected to ensure that a corporate compliance programme is effective. Some US case law in the healthcare and pharmaceutical context has virtually created a 'duty of care' for such individuals. Securities and banking laws also create certain obligations of directors and officers to ensure adequate oversight over corporate compliance activities. Listed companies have the further obligation of compliance with Exchange rules.

Law stated - 28 March 2023

Regulatory and enforcement bodies

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

There is no one 'compliance regulator' in the United States, per se. The existence or lack of a compliance programme, however, is often an important factor in federal and state government enforcement actions, including criminal prosecutions. For example, the US Department of Justice (DOJ) has published guidance titled 'Evaluation of Corporate Compliance Programs,' which sets forth factors that federal prosecutors should consider when investigating, bringing criminal charges against, and resolving criminal charges against companies.

Some regulators have given more detailed guidance on their expectations for particular types of entities than others. For example, the Securities and Exchange Commission (SEC), the Environmental Protection Agency, the Department of Health and Human Services Office of Inspector General (HHS-OIG), the Office of Foreign Asset Control and various state and federal insurance and banking regulators, just to name a few key players, all have set forth specific guidance for the industries they regulate. All these agencies may impose requirements relating to industry-specific compliance standards on organisations as part of the resolution of an investigation in cooperation with state or federal prosecutors.

The DOJ is unlikely to bring causes of action against corporations solely on the basis of a perceived failure to implement an effective compliance programme. However, the presence or absence of a compliance programme is an important factor that the DOJ considers in the resolution of many matters. The DOJ often requires compliance programme enhancements as part of a corporate settlement. The DOJ may also enforce the terms of its settlements and, therefore, has ongoing oversight of how well a compliance programme is being implemented and maintained. In some instances, as a condition of settlement, DOJ may require that an independent compliance monitor – paid for by the company – oversee a company's compliance programme for a fixed period of time.

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. Increasingly, the states of California, Texas, Illinois, Massachusetts and New York are playing a more active role in applying consumer

protection laws to punish and deter regulatory violations. As a consequence, the Attorneys General of these states, and even attorneys representing major cities or counties, have become more familiar with corporate compliance programme requirements and concepts.

Law stated - 28 March 2023

Definitions

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

The elements of an effective compliance programme are set out in the Sentencing Guidelines and incorporated into regulations and guidance put forth by individual US regulatory bodies, such as the SEC, HHS-OIG, and others. In addition, these elements are widely recognised in agency guidelines, such as DOJ's guidelines for Evaluation of Corporate Compliance Programs, and various pronouncements by the SEC. Moreover, settlements entered into by organisations with the US government often define compliance programme requirements. In general, risk management principles are recognised as part of an effective compliance programme and are described as part of the process to prevent, detect and respond to wrongdoing.

Law stated - 28 March 2023

Processes

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

The Sentencing Guidelines set forth processes involved in an effective compliance programme. In June 2020, DOJ's Criminal Division released the most recent version of its guidance on the 'Evaluation of Corporate Compliance Programs.' This guidance

is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations). The document focuses on three main questions: (1) Is the corporation's compliance program well designed? (2) Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively? (3) Does the corporation's compliance program work in practice? The guidance then sets forth 50 topics to help prosecutors answer those fundamental questions. DOJ also publishes and continually updates the Justice Manual (formerly known as the United States Attorneys' Manual), which contains DOJ policies and procedures, including with respect to 'Principles of Federal Prosecution of Business Organizations.' The Justice Manual contains the DOJ's FCPA Corporate Enforcement Policy. This policy strongly incentivises companies to voluntarily disclose potential misconduct, fully cooperate with the government's investigation, and remediate the alleged misconduct, including through an effective compliance programme and disgorgement of improper gains. If a company satisfies these three criteria, then, in the absence of aggravating circumstances, it will be entitled to a presumption that the DOJ will decline to prosecute the company. In addition, DOJ's recent additions to their Corporate Enforcement Policy, referred to as the Monaco memorandum, establish a stronger, department-wide focus on corporate compliance and individual accountability in criminal corporate enforcement. In addition, the DOJ Criminal Division and SEC Enforcement Division have published detailed information regarding their expectations for anti-corruption compliance programmes. This information can be found in 'A Resource Guide to the US Foreign Corrupt Practices Act,' originally published in 2012 and updated in 2020. Moreover, 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 HHS-OIG Compliance Programme 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 HHS 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. In addition, the SEC has promulgated a detailed and elaborate set of compliance criteria and routinely conducts inspections of entities it regulates in order to ensure that compliance systems are functioning effectively. In 2001, the SEC issued a report (often referred to as the 'Seaboard Report') explaining how it considers, among other things, the effectiveness of corporate compliance programmes in 'determining whether, and how much, to credit self-policing, self-reporting, remediation and cooperation – from the extraordinary step of taking no enforcement action to bringing reduced charges, seeking lighter sanctions, or including mitigating language in documents [used] to announce and resolve enforcement actions.' In particular, the SEC will consider 'what compliance procedures were in place to prevent the misconduct now uncovered' and 'why did those procedures fail to stop or inhibit the wrongful conduct.' (provision referencing compliance programme).

Law stated - 28 March 2023

Standards and guidelines

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

The main standards and guidelines are generally based on the Sentencing Guidelines and have been further developed through implementation of the Guidelines, other guidance issued by various agencies, and the resolution of enforcement actions. These standards are generally described as follows.

Support and commitment from senior management of the organisation

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. Although 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.

High-level personnel in 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.

Typically, a dedicated compliance infrastructure, with one or more senior corporate officers responsible for compliance, is expected. 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

As a best practice, an organisation should use reasonable efforts not to employ any person – particularly a member of management – 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. For companies with international business, there has been increased attention on compliance with trade sanctions, export control requirements, foreign agent registration, and other rules. As a result, risk-based due diligence of prospective employees, current employees, business partners, and customers has become increasingly important and failures to timely screen sanctioned parties can lead to significant penalties for organisations and individuals. Certain industries often are expected to follow specific and technically detailed exclusion/debarment regulations, such as healthcare providers or medical product developers whose products are subject to reimbursement by the Medicare and Medicaid programmes in the United States.

Training and communication

Organisations should take reasonable steps to communicate standards, procedures, and other aspects of the compliance programme periodically and in a practical manner, by conducting effective training programmes and otherwise disseminating information about compliance responsibilities. Members of the governing authority, high-level personnel, substantial authority personnel, organisation employees and, as appropriate, an organisation's agents all should receive compliance training. A compliance programme cannot be effective without adequate communication and training. Although 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 be limited to formal settings. Although the nature of communication may vary based on the organisation and its business, it is often expected that compliance messages be disseminated through such methods as email reminders, internal newsletters and pamphlets, postings on bulletin boards, and a separate space on the organisation's intranet. Messages should include examples of good practices of ethical conduct, 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 publicize 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. Often, there are no set rules 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. Lack of monitoring or auditing resources is a common area of attention for litigants or prosecutors alleging that a company's compliance programme is ineffective.

Incentives and discipline

The compliance programme should be promoted and enforced consistently throughout an organisation through appropriate incentives to perform in accordance with it and appropriate disciplinary measures for engaging in misconduct and for failing to take reasonable steps to prevent or detect misconduct. Organisations should reward their employees for good behaviour, and they should 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, 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.

Incentives are important, but 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. Good compliance programs also include mechanisms for anonymous reporting and protect 'whistle-blowers' from retaliation – which is strictly forbidden by several US laws. If misconduct has been detected, an organisation should take reasonable steps to respond appropriately, to determine the root cause of the misconduct, and to prevent further misconduct, including making any necessary modifications to the compliance programme. Often, it is necessary for a company to engage independent outside counsel to investigate potential legal or policy violations, particularly when there is a need for the organisation to avail itself of the secrecy afforded by the attorney-client privilege, or to ensure a degree of independence from in-house counsel.

Risk assessment and periodic reviews

In implementing the elements of discussed above, an organisation should periodically assess the risk of criminal conduct and should take appropriate steps to design, implement, or modify the elements to reduce the risk of criminal conduct identified through those processes. Periodic reviews and assessments of a compliance programme are

viewed as essential since 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. Organisations also may conduct audits to assess whether controls have been implemented effectively. In the United States, companies generally favour conducting sensitive risk assessment activities under attorney–client privilege to allow the corporation an ability to fully understand potential weaknesses and opportunities and receive advice from expert counsel prior to taking a particular action.

Law stated - 28 March 2023

Obligations

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.

Law stated - 28 March 2023

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

Organisations are expected to implement, maintain, and enforce an effective compliance programme.

Law stated - 28 March 2023

LIABILITY

Liability of undertakings

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, 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 their words 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 oral communications including at meetings, by email, and through one-on-one interactions where employees are encouraged to conduct business ethically and in accordance with applicable laws and organisation policies.

In addition, certain 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. Case law in certain areas, such as pharmaceutical and medical device regulation, suggests that senior managers can be held vicariously accountable for regulatory violations committed through acts or omissions of junior employees or the corporation as a whole. Certifications that are knowingly false can also result in liability.

Law stated - 28 March 2023

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

Organisations that breach compliance obligations under law face potential civil liability through government enforcement actions. This liability could include fines, disgorgement of gains, restitution, and debarment from participating in government programme. Liability of this nature typically would result from a violation of applicable law or regulation, as opposed to a violation of a purely internal compliance programme requirement.

Organisations may also face the risk of civil liability from private litigants who may claim that the organisation failed to fulfil a contractual or other obligation to manage risk through a compliance programme. For example, an investor may claim a loss of value that would not have been experienced if the programme had been managed effectively. These private legal actions may result in added defence costs, judgments or settlements, and reputational harm, depending on the facts of the underlying matter.

Law stated - 28 March 2023

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 on 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. If an organisation has settled an enforcement action, compliance obligations may be required as part of the settlement agreements. Failure to meet the 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, courts have interpreted certain laws as authorising sanctions if senior management fails to prevent violations, since the senior managers are presumed to have known about the violations by virtue of their position in an organisation. US public health laws, such as the Federal Food, Drug and Cosmetic Act, and environmental laws, such as the Clean Water Act, are examples of laws that have been applied broadly in such circumstances.

Law stated - 28 March 2023

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

As a general matter, a company can be held criminally liable for the illegal acts of its directors, officers, employees, and agents. Various laws also specifically provide for corporate criminal liability. Examples of such laws include the Foreign Corrupt Practices Act, which prohibits the payment of bribes to non-US government officials to obtain an improper advantage, and the Anti-Kickback Statute, which prohibits domestic bribery in the healthcare sector where federal healthcare programme dollars are involved. Organisations face criminal liability based on the underlying law rather than a general failure to maintain an effective compliance programme.

Law stated - 28 March 2023

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?

Those who participate in the underlying misconduct run the risk of civil liability. As a general matter, the more active the involvement of the individual in the misconduct, the greater the risk of personal liability. However, the relevant standards for civil liability can vary, depending on the law in question. Members of the governing bodies and management of publicly traded companies are often indemnified pursuant to the corporation's bylaws, but that indemnity has limits, and it is possible that officers and directors could face liability from private litigants under securities laws, for example. Personal liability may also flow from a government-negotiated settlement, if management's conduct is considered egregious or if management makes representations that were known to be false at the time they were made.

Law stated - 28 March 2023

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

In general, members of governing bodies and senior management face only limited administrative or regulatory consequences for ordinary compliance programme failures. However, such members are at risk if they participate in the underlying misconduct or undertake specific obligations regarding compliance as part of a government settlement and fail to fulfil those obligations. Members of governing bodies may face more significant liability for the failure to implement an effective compliance programme if that failure was done for the specific purpose of enabling misconduct.

Law stated - 28 March 2023

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

Liability may result if members of governing bodies and senior management participate in the underlying criminal misconduct. Absent such activity, the risk of criminal liability to board members and senior management for failing to implement compliance programme obligations are low, unless it can be proved that such failure was part of a deliberate plan to engage in illegal activity. However, knowingly false statements about the existence or efficacy of the compliance programme may result in liability.

Law stated - 28 March 2023

CORPORATE COMPLIANCE

Corporate compliance defence

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

There is no complete corporate compliance defence in the United States. As previously noted, however, the US Sentencing Guidelines and guidance from various government agencies take corporate compliance programmes into

consideration. Under DOJ policy, prosecutors must consider the state of a compliance programme at both the time of the alleged misconduct and at the time of a charging or sentencing decision. Thus, an effective compliance programme may result in more lenient treatment, including reduced criminal penalties or even the avoidance of prosecution altogether based on the discretion of the prosecutor. An effective compliance programme can also help to counter allegations of corrupt or improper intent. Moreover, under the policy of the DOJ and many other regulators (such as the SEC), companies generally receive significant 'cooperation credit' if they voluntarily self-disclose a violation discovered through the exercise of an effective internal compliance programme.

Law stated - 28 March 2023

Recent cases

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

Allegations of compliance programme failures continue to play a prominent role in US governmental investigations. In previous versions of this chapter, we have listed a number of notable settlements, including to note the extraterritorial reach of certain statutes, such as the Foreign Corrupt Practices Act (FCPA), over the activities of employees and executives involved in allegedly corrupt payments in connection with recent national corruption scandals.

The US government brought numerous FCPA enforcement actions in 2022, with billions of dollars in criminal penalties assessed against corporate entities. In one such action, Swiss-based Glencore International AG pled guilty to violations of the FCPA and agreed to pay US\$1.1 billion to resolve charges that it engaged in a conspiracy to pay US\$100 million in bribes to government officials in Africa and South America. The DOJ's decision to impose significant penalties on Glencore resulted from several factors: the involvement of high-level employees in the bribery scheme, the failure of the company to voluntarily and timely disclose the conduct, the state of the compliance programme and progress of remediation, and the company's cooperation with the DOJ's investigation. DOJ indicated that Glencore did not receive full credit for cooperation because it did not demonstrate full cooperation at all times, it delayed producing relevant evidence, and it did not timely remediate. DOJ also noted that, while Glencore had taken remedial measures, some of its compliance enhancements were not fully developed. Thus, DOJ said they would impose an independent compliance monitor on Glencore for three years and require a Chief Compliance Officer certification, in addition to CEO certification, as part of the company's compliance process—the first DOJ settlement to include such a requirement. In another case from 2022, Swiss-based technology company ABB Ltd. agreed to pay US\$315 million to resolve the government's investigation of FCPA violations stemming from the bribery of high-ranking officials in South Africa's state-owned energy industry. The DOJ agreed to forego criminal prosecution in favour of a three year deferred prosecution agreement despite ABB's criminal history. Due in part to ABB's 'extraordinary' cooperation with DOJ, ABB's penalty reflects a 25 per cent reduction from the middle to higher end of Sentencing Guidelines.

In the past few years, DOJ has demonstrated an increased focus on corporate cooperation in criminal investigations, and broadened pathways for corporations to receive credit for that cooperation. Given this focus, the DOJ is quick to point out notable instances of positive outcomes for companies subject to potential criminal enforcement for issues relating to compliance where those entities have pursued voluntary self-disclosure and received corporate resolutions from the agency. In 2022, DOJ issued a letter of declination of criminal prosecution in which it informed Safran S.A. of its decision to decline to prosecute the company for violations of the FCPA. Although DOJ found that employees at Safran had conducted bribe payments over a period of 16 years, DOJ noted that the company's decision to make a full disclosure of the bribery payments, engage in remediation, and disgorge ill-gotten gains factored into their decision to decline to pursue prosecution. In contrast, in the 2020 Bank of Nova Scotia spoofing case, the bank's compliance programme was alleged to be so inadequate that DOJ said it contributed to the misconduct at hand, emphasising the importance of a well-functioning compliance programme to mitigate serious corporate criminal liability.

Significant and aggressive prosecutions of corporate entities, senior executives and, in some cases, customers, were a theme of recent investigations and settlements in the healthcare industry. The Avanir case involved an investigation into allegations that the company – through several sales and marketing employees – conspired with a number of doctors to use sham consulting agreements, meals, and other alleged kickback payments to increase the adopting and prescribing of a prescription behavioural drug. As part of the resolution of that case, Avanir agreed to significant compliance enhancement requirements through the terms of a deferred criminal prosecution agreement, as well as a corporate integrity agreement with the Department of Health and Human Services. Two doctor-customers and at least two former company employees were criminally charged for their roles, and many other individuals, including senior managers and executives, were named by the government in its filings. Notably, the criminal case used evidence from text messages on systems such as Kik and WhatsApp to show that consulting and other payments were not legitimate but rather intended to be kickbacks. In 2022, DOJ entered into a deferred prosecution agreement, including US\$1.31 million in civil penalties (also imposed against the company's CEO), with Solera Specialty Pharmacy over allegations that the company submitted fraudulent claims to Medicare for Evzio, a high-priced drug used to reverse opioid overdoses. DOJ explained that pharmacies, like all other Medicare providers, must submit accurate claims and emphasized that the agency would pursue False Claims actions against entities at every level of health care delivery.

In 2022, the Securities and Exchange Commission (SEC) brought charges against 16 Wall Street firms regarding their failure to maintain and preserve electronic communications. The penalties ranged from US\$10 million to US\$125 million, largely depending on the size of the firm. In aggregate, the SEC's combined penalties amounted to US\$1.1 billion against companies for violating recordkeeping provisions of US securities law in which, according to the SEC's order, employees of the firms – including high-level supervisors responsible for implementing compliance policies – communicated about securities issues on personal devices, using text messaging applications. They did not, according to the SEC, preserve the majority of these communications. In addition to civil penalties, the companies agreed to take steps to reenforce their compliance procedures for electronic communications, such as retaining compliance consultants to review company policies and procedures. SEC chair Gary Gensler signalled that the SEC will continue to apply recordkeeping requirements to developing technologies in methods of communication.

In recent years, DOJ has also pursued enforcement action against telemedicine companies and medical practitioners for violations of anti-kickback statutes and other federal criminal laws related to the inappropriate prescription of products and services reimbursable by federal health care programmes in the United States. Since 2019, DOJ has brought multiple cases against medical practitioners for their roles in telemedicine fraud schemes. A notable example of this enforcement trend includes several national joint-agency takedown operations, dubbed collectively as Operation 'Happy Clickers,' of marketers and owners of durable medical equipment supply companies and genetic testing laboratories. Other actions include a 2022 case brought by DOJ, in which a nurse practitioner was convicted of Health Care Fraud, false statements related to health care, and aggravated identity theft for facilitating the orders of more than 3,000 orthotic braces with fraudulently generated patient data. Using the information of patients that she had never met or spoken to, the nurse practitioner defendant generated US\$3 million in excessive charges to Medicare. This increase in cases related to telehealth correspond to a Special Fraud Alert issued by OIG in 2022, in which OIG urged medical practitioners and telemedicine companies to thoroughly examine their compliance programmes to avoid scrutiny.

Law stated - 28 March 2023

Government obligations

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

There are generally applicable obligations for government entities or agencies regarding implementing or maintaining compliance programmes, although many government agencies have internal policies and procedures, as well as an Inspector General who is charged with policing misconduct within the agency. Government employees, like private sector employees who engage in misconduct, may be charged under applicable law.

Law stated - 28 March 2023

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).

In the United States, 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 that obtain patient-identifiable information in the healthcare context, such as gene sequencing companies or companies who operate health software platforms. The Securities and Exchange Commission (SEC) has also been very active in policing digital assets that, in the SEC's view, constitute securities under US law. The SEC has brought cases alleging that the unregistered offering of digital assets – such as cryptocurrencies – violates US securities laws as well as cases alleging that those selling digital assets have fraudulently misrepresented features of the asset, the use of funds solicited, and other material matters.

California has been a leader in regulating digital technologies, in part because of the large number of digital asset companies located there. It has passed its own set of state-specific laws governing privacy and consumer protection that must be followed in addition to federal laws. For example, the California Consumer Privacy Act has been likened by some commentators to a 'mini GDPR' in that it imposes significant and broad privacy control requirements on entities doing business in California, one of the most important markets for retail and e-commerce companies. The law also impacts medical products and digital health companies in new ways that require a rethink of old healthcare privacy-focused compliance programmes and systems.

Other technologies, such as artificial intelligence, robotics and blockchain, have been subject to certain regulatory agencies' working groups and public-private workshops intended to help define the parameters of these technologies and educate regulators on technological advances. The Food and Drug Administration (FDA) and other healthcare regulators have recently put out several key guidance documents setting forth the parameters of their intended jurisdiction over digital technologies in the healthcare space.

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 that 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 the 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, etc.

Where regulated as medical devices, such technologies must comply with significant regulatory, quality and compliance requirements set forth by the FDA and other Department of Health and Human Services agencies, including to follow the guidance mentioned earlier about maintaining effective compliance programmes to mitigate the risk of false or fraudulent claim submission to Medicare and Medicaid.

Law stated - 28 March 2023

UPDATE AND TRENDS

Key developments of the past year

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

In the United States, the emphasis on risk assessment by corporations has continued. DOJ and other authorities remain active in policing bribery, kickbacks, and inappropriate marketing, manufacturing, and import practices in sectors such as healthcare and pharmaceuticals. In the last year, DOJ has announced significant changes in compliance enforcement that place a stronger emphasis on individual accountability and corporate cooperation in corporate criminal enforcement.

On 15 September 2022, Deputy Attorney General Lisa Monaco issued a memorandum, 'Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group.' The memorandum, referred to as the Monaco Memo, announced major revisions to DOJ's approach to investigations of corporations and corporate officials. This new guidance impacts how DOJ evaluates a company's cooperation and voluntary self-disclosures of wrongdoing, company policies on personal devices and third-party messaging applications, and a company's history of misconduct. Most notably, DAG Monaco stressed that the DOJ's 'first priority' in criminal corporate enforcement going forward will be to hold accountable individual corporate officials who are responsible for and/or are benefitting from corporate crime.

DOJ's new policies reward corporations with strong compliance systems and give credit to those that voluntarily disclose wrongdoing in a timely manner and fully cooperate with government investigations. For the first time, DOJ requires every division that prosecutes corporate crime to have a documented internal policy on the benefits of self-disclosure, including two principles that DAG Monaco said should apply to all self-disclosure programmes: that companies would not be required to plead guilty for conduct they voluntarily self-disclose, and that the imposition of independent compliance monitors would not be required when a company demonstrates that it has an effective compliance programme. The Memo also promotes an increased focus on compliance programmes for personal devices and third-party messaging applications used to conduct professional business. Although policy is evolving in this rapidly changing area, and DAG Monaco suggested that DOJ would continue to study best practices for personal devices and third-party applications, companies should evaluate compliance policies as they apply to these devices and applications – and particularly how they pertain to ephemeral messaging applications.

Changes in enforcement also affect CEO and CCO certification of corporate compliance plans. In remarks on the Monaco memo, DOJ officials indicated that they would continue to seek Corporate Compliance Officer (CCO) certifications for criminal corporate resolutions, saying that the certifications are a tool for CCOs to address internal compliance issues. In addition, in December 2022, the SEC voted to adopt amendments to Rule 10b5-1 for parties that frequently have access to non-public information. Changes to the rule include: a cooling-off period for directors, officers, and persons other than issuers, requiring certification by directors and officers that they are not aware of non-public information and have adopted trading plans in good faith, a prohibition on overlapping trading plans, and limiting single-trade plans to one trading plan per year.







In a January 2023 update to the Corporate Enforcement Policy, Assistant Attorney General Kenneth A Polite announced further revisions that give prosecutors additional discretion to decline criminal enforcement when a company has

voluntarily self-disclosed offending conduct or else fully cooperated with a DOJ criminal investigation. In his remarks on these revisions, AAG Polite noted that well-functioning compliance programmes best position companies to identify issues and decide whether to pursue voluntary self-disclosure. This update, according to AAG Polite, incentivises compliance by corporate actors through policies that allow prosecutors to grant declination if, among other things, a company has an effective compliance programme.

In addition to policy changes within DOJ and the SEC, in July 2022 the Office of the Inspector General (OIG) issued a Special Fraud Alert for practitioners who enter into arrangements with telehealth medicine companies. With the growing acceptance and use of telehealth following the covid-19 pandemic, OIG's alert explains that the agency has conducted dozens of investigations into fraud schemes by companies that purport to provide telehealth services. Although these fraud schemes varied in design and operation, OIG identified that kickbacks to recruit and reward medical practitioners formed a common element in its investigations. In many of these arrangements, telehealth companies paid medical practitioners to order items and services for patients with whom they had a limited relationship and without regard to medical necessity. Because these arrangements have the potential to cause significant harm to federal health programmes in the United States, such as Medicare and Medicaid, OIG encourages medical practitioners to 'exercise caution and use heightened scrutiny when entering into arrangements with Telemedicine Companies' that could potentially violate federal laws, such as the anti-kickback statute, the criminal healthcare fraud statute and the False Claims Act.

Law stated - 28 March 2023

Jurisdictions

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