Risk & Compliance Management

Contributing editor
Daniel Lucien Bühr

LALIVE

2018

GETTING THE DEAL THROUGH

Do DOJ policy and the ISO compliance standard overlap?

Daniel Lucien Bühr
Lalive

Overview

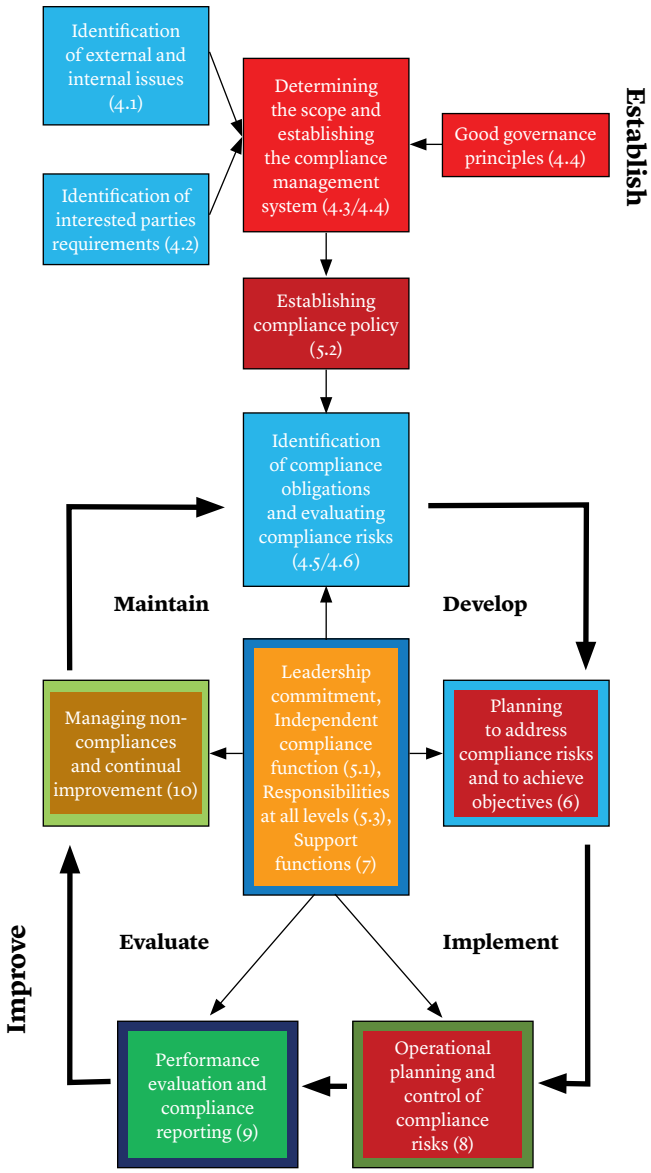
In February 2017, the Fraud Section of the United States Department of Justice's Criminal Division published a document entitled 'Evaluation of Corporate Compliance Programs',[1] its most recent communication of the DOJ's assessment criteria for effective corporate compliance programmes. The DOJ recognises that each company's risk profile and the solutions it adopts to reduce risks should be evaluated on their own merits. The DOJ therefore tailors its determination to each case. However, even tailored determinations raise many of the same questions. The DOJ document explains the questions the DOJ may ask about a corporate compliance programme. However, it gives no guidance on how companies can provide the right answers.

In December 2014, the International Organization for Standardization published ISO International Standard 19600 – Compliance management systems – Guidelines,[2] which helps organisations establish, develop, implement, evaluate, maintain and improve an effective and responsive compliance management system. It is the first international standard on state-of-the-art compliance management and provides the basis for other international standards, such as ISO 37001 – Anti-bribery management systems.

The DOJ document and ISO 19600 differ, yet they have a shared preventive goal. The following table shows that US policy and the Standard are largely compatible, and that ISO 19600 is an appropriate way to bring companies to a level of compliance management that allows them to provide the right answers to the DOJ's questions, should that be necessary. The table below illustrates the overlap between the DOJ and ISO guidance; the flowchart opposite illustrates the management system that the Standard advocates. The colour scheme of both graphics indicates the topical overlap.

No.	DOJ document topic	ISO 19600, sections	Overlap?
1	Analysis of underlying misconduct	Introduction; 10.1	Yes[3]
2	Senior and middle management	Introduction; 4.4; 5.1; 7.3.2.3	Yes
3	Autonomy and resources	4.4; 5.3; 5.3.4	Yes
4	Policies and procedures	5.1; 5.2; 5.2.1; 5.3.4; 6.2; 8.1; 8.2; 9; 9.1; 9.1.6	Yes
5	Risk assessment	4.6; 6.1	Yes
6	Training and communications	5.3.4; 7.2.2; 7.3.2.3; 9.1.6;	Yes
7	Confidential reporting and investigation	5.3.3; 9.1.7; 9.2; 10.1.2	Yes
8	Incentives and disciplinary measures	5.3.4; 7.3.2.2; 7.3.2.3; 10	Yes
9	Continuous improvement, testing and review	9.2, 9.3 and 10.2	Yes (principles)
10	Third-party management	8.3	Yes (principles)[4]
11	Mergers and acquisitions	N/A	N/A

Flowchart of an ISO 19600 – Compliance management system:[5]



The ISO Standard introduces a transparent management system that is auditable and cost-efficient. The Standard represents state-of-the-art compliance management and provides a basis for the legal presumption of diligent management.

In the following we reproduce in abridged form the DOJ's document going through the sample topics and questions section by section and highlighting the overlap with the ISO Standard:

1. Analysis and remediation of underlying misconduct

Root Cause Analysis – What is the company's root cause analysis of the misconduct at issue? What systemic issues were identified? Who in the company was involved in making the analysis?

Prior Indications – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations involving similar issues? What is the company's analysis of why such opportunities were missed?

Remediation – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

The Standard does not ask questions related to past conduct. However, its Introduction states that regulatory and judicial bodies can benefit from the Standard as a benchmark when considering an organisation's commitment to compliance through its management system.

In Section 10 – Improvement, the Standard lists actions an organisation should take if it detects non-compliance. These actions include the elimination of the root causes of non-compliance and the required remedial changes to the compliance management system.

2. Senior and middle management

Conduct at the Top – How have senior leaders, through their words and actions, encouraged or discouraged the type of misconduct in question? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How does the company monitor its senior leadership's behavior? How has senior leadership modelled proper behavior to subordinates?

Shared Commitment – What specific actions have senior leaders and other stakeholders . . . taken to demonstrate their commitment to compliance, including their remediation efforts? How is information shared among different components of the company?

Oversight – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

The ISO Standard recommends that the governing body (in companies, the board of directors) and top management demonstrate leadership of and commitment to the compliance management system by establishing and upholding the core values of the organisation and ensuring that the necessary resources are available, allocated and assigned (section 5.1. a, d). They should also ensure alignment between operational targets and compliance obligations (Section 5.1. i) and establish and maintain accountability mechanisms, including timely reporting on compliance matters, including non-compliance (Section 5.1. j).

Under Section 7.3.2.3 – Compliance culture, the development of a compliance culture requires the active, visible, consistent and sustained commitment of the governing body and management to a common, published standard of behaviour that is required throughout every area of the organisation.

The Standard requires direct access of the compliance function to the board and compliance training at all levels (Sections 4.4 and 7.2.2)

3. Autonomy and resources

Compliance Role – Was compliance involved in training and decisions relevant to the misconduct? Did the compliance or relevant control functions . . . ever raise a concern in the area where the misconduct occurred?

Stature – How has the compliance function compared with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? . . .

Experience and Qualifications – Have the compliance and control personnel had the appropriate experience and qualifications for their roles and responsibilities?

Autonomy – Have the compliance and relevant control functions had direct reporting lines to anyone on the board of directors? How often do they meet with the board of directors? Are members of the senior management present for these meetings? Who reviewed the performance of the compliance function and what was the review process? Who has determined compensation/bonuses/raises/hiring/termination of compliance officers? Do the compliance and relevant control personnel in the field have reporting lines to headquarters? . . .

Empowerment – Have there been specific instances where compliance raised concerns or objections in the area in which the wrongdoing occurred? How has the company responded to such compliance concerns? Have there been specific transactions or deals that were stopped, modified, or more closely examined as a result of compliance concerns?

Funding and Resources – How have decisions been made about the allocation of personnel and resources for the compliance and relevant control functions in light of the company's risk profile? Have there been times when requests for resources by the compliance and relevant control functions have been denied? If so, how have those decisions been made?

Outsourced Compliance Functions – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? What has been the rationale for doing so? Who has been involved in the decision to outsource? How has that process been managed (including who oversaw and/or liaised with the external firm/consultant)? What access level does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

Section 4.4 of the Standard mentions three principles of good compliance governance: the compliance function should (i) have direct access to the board, (ii) be independent (from line management) and (iii) have appropriate authority and adequate resources.

The compliance function and its tasks are defined in Section 5.3.4. The Standard provides a check-list of the compliance function's tasks ranging from identifying the organisation's compliance obligations to the implementing a compliance reporting and documenting system and the provision of objective compliance advice to the organisation.

Section 5.3.4 states that the compliance function should demonstrate integrity, effective communication skills and an ability and standing to command acceptance of its guidance and have the relevant competence.

Outsourced processes are addressed in Section 8.3. All outsourced processes (compliance-related or not) should be monitored for compliance and are subject to effective compliance due diligence to maintain the organisation's standards and commitment to compliance.

4. Policies and procedures

a. Design and Accessibility

Designing Compliance Policies and Procedures – What has been the company's process for designing and implementing new policies and procedures? Who has been involved in the design of policies and procedures? Have business units/divisions been consulted prior to rolling them out?

Applicable Policies and Procedures – Has the company had policies and procedures that prohibited the misconduct? How has the company assessed whether these policies and procedures have been effectively implemented? How have the functions that had ownership of these policies and procedures been held accountable for supervisory oversight?

Section 5.2 of the Standard holds that the organisation's compliance policy should (among other aspects) outline the scope of the compliance management system, the extent to which compliance will be integrated with other functions, and the degree to which compliance will be embedded into operational policies, procedures and processes. This policy should be available as documented information and be written in plain language so that all employees can easily understand the principles and intent.

Gatekeepers – Has there been clear guidance and/or training for the key gatekeepers (e.g., the persons who issue payments or review approvals) in the control processes relevant to the misconduct? What has been the process for them to raise concerns?

Key gatekeepers are not specifically addressed in the Standard. However, under Section 5.3, the responsibilities and authorities for all relevant roles (ie, governing body, senior management, compliance function, other management and employees) should be assigned and communicated within the organisation.

Accessibility – How has the company communicated the policies and procedures relevant to the misconduct to relevant employees and third parties? How has the company evaluated the usefulness of these policies and procedures?

Section 7.5.3 holds that documented information . . . should be controlled to ensure: a) it is available, accessible and suitable for use, where and when it is needed . . . . Section 8.2 – Establishing controls and procedures – recommends that clear, practical and easy to follow documented operating policies, procedures, processes and work instructions be established.

b. Operational Integration

Responsibility for Integration – Who has been responsible for integrating policies and procedures? With whom have they consulted . . .? How have they been rolled out . . .?

According to Section 5.3.4, the compliance function, working with management, should be responsible for integrating compliance obligations into existing operational policies and procedures.

Controls – What controls failed or were absent that would have detected or prevented the misconduct? Are they there now?

Payment Systems – How was the misconduct in question funded . . .? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

Approval/Certification Process – How have those with approval authority or certification responsibilities in the processes relevant to the misconduct known what to look for, and when and how to escalate concerns? What steps have been taken to remedy any failures identified in this process?

According to Section 8.1 – Operational planning and control, the organisation should plan, implement and control the processes needed to meet compliance obligations.

The Standard does not address the funding of misconduct. But Section 9.1.7 – Compliance reporting states that the governing body, management and the compliance function should ensure that they are effectively informed on the performance of the compliance management system, including all relevant non-compliance.

Section 9.1.7 recommends that there be sign-off on the accuracy of reports to the governing body, including by the compliance function.

Vendor Management – If vendors had been involved in the misconduct, what was the process for vendor selection and did the vendor in question go through that process?

Vendor management is not specifically addressed in the Standard, but Section 8.3 covers all outsourced processes and holds that organisations should consider compliance risks related to other third-party-related processes, such as supply of goods and services, and distribution of products, and put controls in place, as necessary.

5. Risk assessment

Risk Management Process – What methodology has the company used to identify, analyze, and address the particular risks it faced?

Information Gathering and Analysis – What information or metrics has the company collected and used to help detect the type of misconduct in question? How has the information or metrics informed the company's compliance program?

Manifested Risks – How has the company's risk assessment process accounted for manifested risks?

The Standard (see Section 4.6) is based on the methodology of ISO Standard 31000 – Risk management. However, the Standard also leaves room for alternative approaches and methods to identify, analyse and evaluate compliance risks, such as the COSO ERM framework.

The Standard states that a compliance risk assessment is the basis of any compliance management system and that a risk assessment process essentially consists in relating the compliance obligations (as defined in Section 3.16) to the activities, products and services of the organisation.

6. Training and communications

Risk-Based Training – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees that addressed the risks in the area where the misconduct occurred? What analysis has the company undertaken to determine who should be trained and on what subjects?

Form/Content/Effectiveness of Training – Has the training been offered in the form and language appropriate for the intended audience? How has the company measured the effectiveness of the training?

Communications about Misconduct – What has senior management done to let employees know the company's position on the misconduct that occurred? What communications have there been generally when an employee is terminated for failure to comply with the company's policies, procedures, and controls . . .?

Availability of Guidance – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

Section 7.2.2 of the Standard outlines training principles. Education and training of employees should be tailored to the obligations and compliance risks of employees, aligned with the corporate training programme and incorporated into annual training plans.

Training should be practical, readily understood and relevant to employees' day-to-day work. Education and training should be assessed for effectiveness and updated as required. Compliance performance should be measured by indicators such as the percentage of employees effectively trained, the frequency of contact by regulators, the usage of feedback mechanisms etc (Section 9.1.6 – Development of indicators).

Section 7.3.2.3 – Compliance culture – mentions ongoing communication on compliance issues and prompt and proportionate disciplining of wilful or negligent breaches of compliance obligations as examples of factors that will support the development of a compliance culture.

According to Section 5.3.4, the compliance function should provide employees with access to resources on compliance procedures and references and provide objective advice to the organisation on compliance-related matters. Inversely, employees should use available compliance resources and participate in training (Section 5.3.6 – Employee responsibility).

7. Confidential reporting and investigation

Effectiveness of the Reporting Mechanism – How has the company collected, analyzed, and used information from its reporting mechanisms? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

Properly Scoped Investigation by Qualified Personnel – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

Response to Investigations – Has the company's investigation been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

Section 10.1.2 of the Standard outlines the escalation process: an effective compliance management system should include a mechanism for employees and others to report suspected or actual misconduct, or violations of the organisation's compliance obligations, confidentially and without fear of retaliation.

Section 9.1.5 holds that information classification and management is critical. Information collected needs to be analysed and assessed to identify root causes.

According to Section 5.3.3, the organisation's governing body and top management should appoint a compliance function with access to all information needed to perform compliance tasks.

The compliance function can conduct audits as required (Section 9.2). The audit criteria and scope of each audit should be defined and auditors should be selected and audits be conducted to ensure objectivity and the impartiality of the audit process.

Top management should ensure that effective and timely systems of reporting are in place (Section 5.3.3). All non-compliance needs to be appropriately reported (Section 9.1.7).

8. Incentives and disciplinary measures

Accountability – What disciplinary actions did the company take in response to the misconduct and when did they occur? Were managers held accountable for misconduct that occurred under their supervision? Did the company's response consider disciplinary actions for supervisors' failure in oversight? What is the company's record (e.g., number and types of disciplinary actions) on employee discipline relating to the type(s) of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

Human Resources Process – Who participated in making disciplinary decisions for the type of misconduct at issue?

Consistent Application – Have the disciplinary actions and incentives been fairly and consistently applied across the organization?

Incentive System – How has the company incentivized compliance and ethical behavior? How has the company considered the potential negative compliance implications of its incentives and rewards? Have there been specific examples of actions taken (e.g., promotions or awards denied) as a result of compliance and ethics considerations?

Section 10 of the Standard holds that when non-compliance occurs, the organisation should take action to correct it, eliminate the root causes, implement any action needed and review the effectiveness of corrective action.

Section 7.3.2.3 underlines the need for prompt and proportionate disciplining in the case of wilful or negligent breaches of compliance obligations.

The compliance function should be responsible for promoting the inclusion of compliance responsibilities into job descriptions and employee performance management processes (Section 5.3.4).

Section 7.3.2.2 states that senior management has a key responsibility for ensuring that operational objectives and targets do not compromise compliant behaviour.

9. Continuous improvement, periodic testing and review

Internal Audit – What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?

Control Testing – Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?

Evolving Updates – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

Section 9.2 of the Standard holds that the organisation should conduct audits at least at planned intervals to provide information on whether the compliance management system conforms to the organisation's own criteria for its compliance management system and the recommendations of the Standard, and is effectively implemented and maintained. The audit results should also be reported to the management.

Section 9.3 holds that the organisation should retain documented information as evidence of the results of management reviews and provide copies to the governing body.

Section 10.2 recommends that the organisation should seek to continually improve the suitability, adequacy and effectiveness of the compliance management system. The information collected, analysed and evaluated accordingly, and included in compliance reports, should be used as the basis for identifying opportunities to improve the organisation's compliance performance.

10. Third-party management

Risk-Based and Integrated Processes – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

Appropriate Controls – What was the business rationale for the use of the third parties in question? What mechanisms have existed to ensure that the contract terms specifically described the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

Management of Relationships – How has the company considered and analyzed the third party's incentive model against compliance risks? How has the company monitored the third parties in question? How has the company trained the relationship managers about what the compliance risks are and how to manage them? How has the company incentivized compliance and ethical behavior by third parties?

Real Actions and Consequences – Were red flags identified from the due diligence of the third parties involved in the misconduct and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues? How has the company monitored these actions (e.g., ensuring that the vendor is not used again in case of termination)?

Section 8.3 of the Standard holds that the organisation should consider compliance risks related to third-party-related processes, such as supply of goods and services and distribution of products, and put controls in place.

The Standard also holds that outsourcing of operations usually does not relieve the organisation of its legal responsibilities or compliance obligations. If there is any outsourcing of activities, the organisation needs to undertake effective due diligence to maintain its standards and commitment to compliance.

ISO Standard 37001 on anti-bribery management systems, specifies in detail the requirements of best practice third-party due diligence, monitoring, auditing and the corrective actions that must be taken in case of non-compliance.

11. Mergers and acquisitions

Due Diligence Process – Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What has been the M&A due diligence process generally?

Integration in the M&A Process – How has the compliance function been integrated into the merger, acquisition, and integration process?

Process Connecting Due Diligence to Implementation – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures at new entities?

The Standard does not specifically address M&A-related due diligence and compliance risk management. But any acquisition is part of a company's business conduct and therefore subject to proper due diligence, particularly also post-acquisition.

Notes

1 See: https://www.justice.gov/criminal-fraud/strategy-policy-and-training-unit/compliance-initiative
2 See: https://www.iso.org/standard/62342.html
3 However, ISO 19600 is "forward looking" and general and not meant to provide answers to individual cases.
4 ISO Standard 37001 – Anti-bribery management systems is more detailed.
5 The Flowchart of a compliance management system taken from ISO 19600:2014 is reproduced with the permission of the International Organization for Standardization, ISO. The numbers in the chart cells refer to the relevant sections of the Standard, which can be obtained from any ISO member and from the website of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts Competition
Compliance
Complex Commercial Litigation Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management Securities Finance
Securities Litigation
Shareholder Activism & Engagement Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation Tax Controversy
Tax on Inbound Investment Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com