BIBLIOGRAPHY

Albrecht & Albrecht 2009
W.S. Albrecht & Albrecht, *Fraud Examination & Prevention,* Independence KY: South-Western Cengage learning 2009

Albrecht 2014
W.S. Albrecht, 'The Compromise Triangle', *The Wheatley Institution* 2014-May.

Bleker-van Eyk 1995
S.C Bleker-van Eyk, *The OECD Declaration and Decisions concerning Multinational Enterprises,* Nijmegen: Ars Aequi Libri 1995.

Bleker-van Eyk 2013
S.C Bleker-van Eyk, 'De Compliance Officer 2.0', *MAB* 2013-10.

Borak et al. 2016
D. Borak et al., 'New Rules Curbing Wall Street Pay Proposed, *Wall Street Journal* 2016-April.

Cressey 1953
D.R. Cressey, *Other People's Money,* New York: The Free Press 1953.

Van Dijk 1987
P. van Dijk, 'Normative Force and effectiveness of International Norms', *GYIL* 1987-30.

Gude 2015
R. Gude, *Het Agoramodel: de wereld is eenvoudiger dan je denkt,* Leusden: ISVW uitgevers 2015.

Mendoza et al. 2016
J.P. Mendoza et al., 'Can too much Auditing Backfire: A cross-country analysis of Auditing and Tax Compliance', *Journal of Public Economics* 2016-June.

Mendoza et al. 2015
J.P. Mendoza et al., 'Only the Carrot, Not the Stick: Incorporation Trust into the Enforcement of Regulation', *PLOS ONE* 2015-february.

Wells 1997
J.T. Wells, *Occupational Fraud and Abuse: how to prevent and detect asset misappropriation, corruption and fraudulent statements,* London: Obsidian Publishing Company 1997.

3. Compliance Management[1]

Prof. S.C. Bleker-van Eyk

3.1 THE COMPLIANCE FUNCTION

During the 1990s, the importance of compliance increased. The amount of both national and international legislation grew rapidly. At the beginning of this century, after some important ethical breaches within corporate enterprises, the legislature followed by creating a deluge of laws and regulations, mostly aimed at governance risk and compliance. After 9/11, corporate enterprises were confronted with increased and complex regulations on sanctions and export controls. After Enron and WorldCom, the Sarbanes-Oxley Act was introduced. In 1977, the Foreign Corrupt Practices Act (FCPA) came into force. However, the prosecution of foreign multinationals has only truly been enforced since the beginning of this century, mostly due to the entry into force of the Anti-Bribery Convention of the OECD. In addition, the United Kingdom Bribery Act became effective in 2011.[2]

In this chapter, the requirements of the compliance framework will be discussed, as well as the skills necessary to become an accomplished compliance officer. Both national and international examples will be given of required or recommended compliance frameworks, from the United Nations Global Compact to the ISO 19600 guideline.

3.2 INSTITUTIONALIZATION OF COMPLIANCE

Since the mid-1990s, compliance has gradually carved out a place for itself in financial institutions, growing from a Friday afternoon role for managers on the verge of retirement to full-fledged departments, some of them with a staff of several hundred. Compliance was slower to establish itself in non-financial companies, at least under that name. It started with the companies that were heavily regulated, for example the

1. Parts of this chapter was previously published in Dutch in Bleker-van Eyk 2013, pp. 402–411.
2. Both the FCPA and the UKBA will be discussed in more detail in Part IV *infra.*

pharmaceutical industry and the aircraft industry, which had been subject to strict airworthiness rules since the 1950s. Only in the course of this current century have non-financial companies gradually become aware of the importance of creating a compliance role, mainly because of the increase in regulations and enforcement in the medical industry, the military industry and other industries increasingly faced with enforcement of all sorts of rules (e.g. on exports and imports, food safety and other types of safety). The extraterritorial application of the American export rules is still the driving force behind the creation of many compliance roles in the industrial world.[3]

In recent years, we have seen increasing attention to compliance in the non-financial sector, owing to growing awareness of the extraterritorial application of anti-corruption legislation. Since 1997, the OECD Anti-Bribery Convention has enabled the US to enforce its legislation more effectively in other countries, as the States Parties – not only the OECD Member States – meet the requirement of dual criminality once they have ratified it. However, true awareness in boardrooms of the extraterritorial application of foreign legislation only seems to have developed after the passing of the UKBA.[4] Undoubtedly, Great Britain is not so far away that directors can sleep at night. Most of them slept fine with the American Foreign Corrupt Practices Act, which presented – and still presents – a far greater danger. Competition cases have also created a good deal of turmoil in recent years, though they are rarely regarded as compliance matters, and are usually still dealt with by legal departments. The question is whether this is correct. Competition cases fall under national and international legislation and can entail substantial risks. The purpose of compliance is to promote the observance of national and international laws and regulations, as well as internal rules and standards, to protect the integrity of the organization and its directors and staff. The aim is to control the risks of non-compliance with laws, regulations and standards and to prevent the damage that could result.[5] In short, compliance in effect ensures desirable, agreed upon conduct, as laws and regulations can either be breached by action or omission. This does not by definition apply to all laws and regulations, but it does, particularly, to laws and regulations related to achieving the company's key objectives. One could say that compliance derives its *raison d'être* from a company's license to operate. Compliance risks are risks that can pull the proverbial rug from under the company, or at least cause major material and reputational damage.

3.3 THE COMPLIANCE LANDSCAPE

When setting up a compliance function it is important to take into account the necessary requirements from the point of view of both governance and requirements

3. *Cf.* the United States: Directorate of Defense and Trade Controls (DDTC) http://www.pmddtc.state.gov/compliance/index.html; Bureau of Industry and Security (BIS) http://www.bis.doc.gov/complianceandenforcement/emcp.htm; OFAC http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.
4. Bleker 2012.
5. Sylvie C. Bleker-van Eyk's definition as used in the Postdoctoral Course in Compliance & Integrity Management at the VU.

set by the appropriate supervisory authorities that supervise the actions of a particular company.

The landscape of compliance is directly related to the scope of compliance. The scope of compliance cannot encompass 'the observance of external (international and national) laws and regulations' as such. This would lead to a tsunami of rules and regulations that would be better dealt with by other departments within the company that are directly linked to the behavior targeted by that particular field of legislation. The scope of compliance should be linked to the key objectives of the organization and hence to the laws and regulations that can affect the organizations' license to operate. Numerous supervisory authorities exist, including a wide area of laws and regulations that are not directly linked to key objectives and where compliance is better left to other departments. For instance, legislation with regard to food safety in canteens should fall outside of the scope of compliance. This might be taken care of by other departments, for example the facility department. However, if the organization is a consultancy company advising large organizations on how to set up canteens within their organization, from a point of view of possible reputational damage it would be wise to make food safety regulations an essential part of compliance.

Note that compliance can also require cooperation with other organizational departments such as legal or human resources. Within the institutionalization of compliance, cooperation with other departments may best be served through an interdepartmental body coordinating the efforts and preventing overlap, or worse, conflicting internal procedures.

3.3.1 Compliance Charter

Corporate governance is defined as an internal system encompassing policies, processes and people, which serves the needs of shareholders and other stakeholders by directing and controlling management activities with good business savvy, objectivity, accountability and integrity. Sound corporate governance is reliant on external marketplace commitment and legislation, as well as a healthy board culture that safeguards policies and processes.[6]

Corporate governance encompasses governance issues, risk management and compliance activities. Key elements of good corporate governance principles include honesty, trust and integrity, openness, performance orientation, responsibility and accountability, mutual respect, and commitment to the organization. Of importance is how directors and management develop a model of governance that aligns the various values of the corporate participants and evaluate this model periodically. In particular, senior executives should conduct themselves honestly and ethically, especially concerning actual or apparent conflicts of interest, and disclosure in financial reports.[7]

Good corporate governance practices, according to COSO,[8] will lead to an internal control system as a process, effected by an entity's board of directors, management and other personnel, designed to manage the 'key risks' and provide

6. Compliance Charter Fokker Technologies B.V.
7. Ibid.
8. See the Risk chapters Part II *infra*.

'reasonable assurance' regarding the achievement of objectives in the following categories:[9]

- achieving the strategic objectives and targets;
- effectiveness and efficiency of operations;
- reliability of financial reporting; and
- compliance with applicable laws and regulations.

Within an organization's governance structure, the Compliance Charter is the 'constitution' of compliance that directly links compliance to the key objectives of the organization and its license to operate. The Compliance Charter contains the basic principles of compliance and integrity management. It should entail the organization's vision on compliance, as well as the scope of compliance and the institutional set up of the compliance framework.

The Charter describes the activities of compliance, including the reporting lines and the goal of compliance and integrity management within the organization. The Charter is the main governance document linking compliance principles to the compliance framework.

A Compliance Charter should contain:

- the vision on compliance, in which the organization underlines the importance it attaches to conducting its business activities in compliance with existing laws and regulations;
- the definition of compliance;
- the scope of compliance;
- the objective of compliance: the main objectives of compliance should be determined from the point of view of:
  i. supporting the effective control environment,
  ii. creating a transparent compliance structure,
  iii. identifying, reporting and monitoring risks,
  iv. communicating on compliance issues,
  v. complying with all relevant laws and regulations;
- the importance of maintaining constant awareness of compliance;
- the compliance structure and functioning;
- the responsibilities for compliance throughout all levels of the organization;
- reporting on compliance;
- the budget for compliance.

3.3.2 Compliance Program

The Compliance Program contains a more extensive vision on compliance for a set period of time. In general, most compliance programs are set for a period of five years. While the Compliance Charter entails the more general principles, the Compliance Program contains a more specified program, including:

- the compliance cycle;

9. Compliance Charter Fokker Technologies B.V.

- the distribution of tasks between the different lines of defense against non-compliance;
- awareness programs;
- the distribution of tasks and responsibilities of the existing compliance officers within the organization;
- the implementation of compliance throughout the organization.

The primary responsibility for compliance lies within the business (the first line of defense) and, as a result, the final responsibility lies with the Chief Executive Officer (in a one-tier board) or the Chief Executive Officer together with the Chairman of the Supervisory Board (in a two-tier board). At first sight it may seem obvious that the business holds the primary responsibility for compliance. Compliance is directly related to the key objectives and business activities are the responsibility of the first line of defense. However, recent history has shown that this is not as obvious as it seems. Compliance is actually situated in the second line of defense and its function is to assist the business on matters of compliance. In practice, it has become a habit for business to 'outsource' compliance matters *and* the related decisions to the second line (compliance). In the decision-making process, the first line refers to the second line by stating that compliance has approved it, so the decision is in accordance with the requirements set by compliance. As a result, the business tries to shift its responsibilities away towards the second line. This is incorrect! The first line knows all the circumstances and the business requirements. It may ask for assistance, but it never tries to absolve itself of the responsibility for compliance. Also, shifting business decisions to compliance increases the burden on the compliance department, thereby creating an environment where compliance has to take decisions without an in-depth business perspective. Together with the existing excessive legislative burden, replacing compliance decision in the business by decision-making in the second line of defense creates an environment where the compliance function is increasingly pressed into a 'tick-the-box' mode, which will create more additional compliance risks. Also, relaying decision-making to the second line of defense is contrary to the 'Three Lines of Defense' model, according to which 'the board delegates to the CEO and senior management *primary ownership* and *responsibility* for *operating risk management and control* [including compliance risks]. It is management's job to provide leadership and direction to the employees in respect of risk management, and to control the organization's overall risk-taking activities in relation to the agreed level of risk appetite'.[10]

'To ensure the effectiveness of an organization's risk management framework, the board and senior management need to be able to rely on adequate line functions – including monitoring and assurance functions – within the organization.'[11] This model explains the relations between the three functions and serves as a guide to how responsibilities should be divided:

1. the first line *owns* and *manages* risk;
2. the second line oversees or specializes in risk (compliance); and
3. the third line provides independent assurance (internal audit).

10. https://www.iia.org.uk/threelines (emphasis added).
11. Ibid.

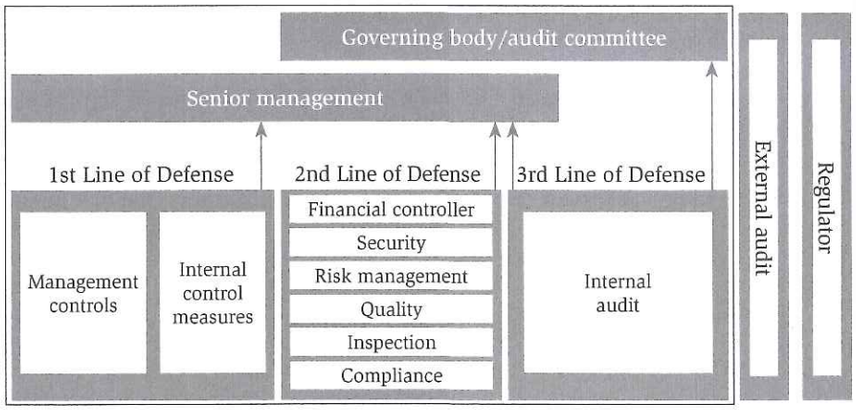


Figure 1: ECIIA/FERMA Guidance on the 8th EU Company Law Directive, Article 41

When assembling the 'Three Lines of Defense' model with the compliance structure discussed in the compliance program, the following compliance building arises.

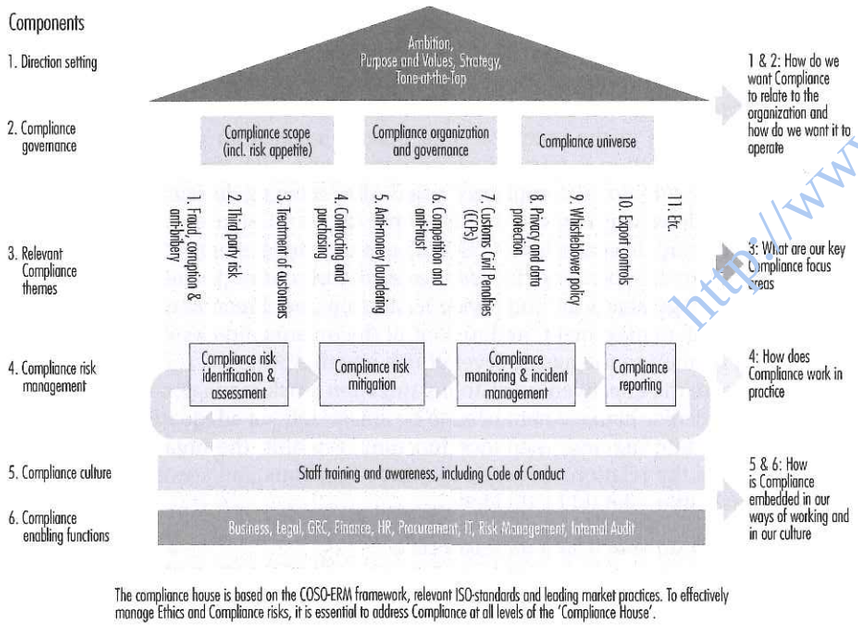


Figure 2: The Compliance House PwC 2017

3.3.3 Structure of the compliance function

3.3.3.1 *The final responsibility for compliance*

In this chapter's paragraph on countervailing power *infra*, the issue concerning the independence of the compliance officer is discussed as it relates to skills. Within the compliance structure of an organization it is of particular importance to pay attention to the positioning of compliance within the chain of command of the organization and to ascertain that the highest ranking officer in direct command of the compliance function is sufficiently empowered to perform his duties and assure that compliance is regarded as the conscience of the organization.

As discussed *supra*, compliance is the responsibility of the business. As a result, the Executive Board bears the final responsibility for compliance. In practice, many flavors exist as to the chief ranking officer responsible for compliance. In some organizations, the Chief Executive Officer (CEO) bears the final responsibility for compliance. However, organizations often designate the Chief Financial Officer (CFO) as responsible for compliance. Also, sometime the Chief Operating Officer (COO) is in charge of compliance. Both the CFO and COO seem an appropriate choice, because the final responsibility rests within the Executive Board. However, their primary responsibility is not compliance, and compliance requirements may be set aside more easily because they conflict with the Officer's primary responsibility. CFOs or COOs may be more tempted to set aside compliance requirements. Recently, Executive Boards have been supplemented with a CRO. Compliance and integrity contain imminent risks for the organization, and the CRO seems to be well equipped to take on the task of Chief Compliance Officer (CCO). However, it is important that the CRO understands the importance of compliance and integrity risks and the effect they may have on the entire organization.

Yet, too often compliance is covered on a lower level instead of by the highest ranking executive officers. All too often, the CCO reports to the Chief Legal Officer, who in turn reports to the Company Secretary or the CFO. The sense of urgency on compliance and integrity risks may well become lost within the daily hassle of further legal risks waiting for better times, while the risk develops into a risk that may affect the license to operate. Finally, some organizations have bestowed the Human Resources (HR) department with the responsibility for integrity management. This must be regarded a highly undesirable situation. HR focuses on assisting the organization's management with employment-related matters. Their first aim is to assist management and some of the core tasks of integrity management should be in more neutral hands. For instance, receiving whistleblower information through Human Resources is a *contradictio in terminis*.

Understanding and assessing the potential impact of compliance and integrity risks within modern organizations and the intricate consequences of full-fledged incidents is a task that should not be accepted lightly and regarded as something to do on the side. The CRO on the Executive Board could easily become the Chief Risk and Compliance Officer (CRCO), giving compliance and integrity management (ethics) the proper place within the chain of command. However, compliance requires more than just a seat at the executive table. In those instances where compliance and integrity risks may adversely affect the organization and yet are set

aside by the other members of the Executive Board – in a two-tier board – the CRCO must be able to step up the discussion on the risk level to the Supervisory Board, thereby ensuring that these risks are taken fully into consideration by all levels of governance within the organization. The decision to ask the Supervisory Board to make a final assessment of the compliance risk and the impact it may have upon the organization is not a step that should be taken lightly. It should be the joint decision of the Executive Board; otherwise it may poison internal management relations. Requesting the Supervisory Board to overrule the Executive Board will have serious consequences, but may be the ultimate way of trying to protect risks from exploding into a full-fledged compliance incident.

3.3.4 The Chief Compliance Officer

The description regarding the positioning of the CCO *supra* shows that the duties and authorizations can be regarded as a consequence of the CCO's position as the independent conscience of the organization. Consequently, the CCO:

- assists the Executive Board proactively in realizing the objectives of compliance. The CEO and CFO oversee the operations, and the CCO verifies compliance risks on decisions after having assessed these risks on a regular basis with the senior management and operational management;
- reports periodically (and when necessary independently) to the Supervisory Board (two-tier) and/or Audit Committee;
- is responsible for the organization's corporate compliance, integrity and fraud policies;
- supervises (where applicable) the country-specific compliance of the organization's subsidiaries;
- advises and supervises the divisional/local/business unit compliance officers of the subsidiaries; and
- executes the laws and regulations on insider trading with regard to the members of the Executive Board, the Supervisory Board and/or Audit Committee and all other relevant staff.

Resulting from this are the following tasks and responsibilities of the CCO:

- to develop, implement and monitor compliance activities and tools at corporate level for the organization;
- to review key compliance risks as reported by subsidiaries/divisions/business units, with the purpose of identifying material compliance risks organization-wide;
- to regularly adapt the compliance program in light of legal developments, developments in the businesses in which the organization is active, and developments and changes within the organization;
- to make recommendations to the Executive Board on ways and means to make business processes better geared to cater for compliance by the organization's divisional/local/business unit and staff with applicable regulations and codes of conduct.
- to perform and arrange *ad hoc* compliance reviews;

- to report *at regular intervals* to the Executive Board, the Supervisory Board (two-tier) and the Audit Committee on the implementation of the compliance program, progress made, issues, incidents and remedies, reports serious incidents *ad hoc* as may be appropriate.
- to coordinate the activities of the divisional/local/business unit compliance officers;
- to monitor that all relevant staff within the organization receive fit-for-purpose awareness and compliance training;
- to organize integrity workshops and other sessions to enhance the organization's compliance culture;
- to coordinate, draft and update the organization's codes/policies, and monitor the effective roll-out of and compliance with such codes/policies;
- to support internal and external auditors in preparing and conducting audits of the effectiveness of the program;
- to support directors and management in maintaining the 'right tone at the top';
- to act as the 'compliance face' for the organization both within and outside and at all levels of seniority;
- to be responsible within the organizations (including all subsidiaries/divisions/business units/local) for all matters related to the development and implementation of the compliance program;
- to act as a sounding board for all within the organization on compliance and integrity-related matters.

3.3.5 The 'joint committee'

Compliance risks are inextricably interwoven with operations, and compliance is not the only department (partially) coping with a particular risk. Also, the tasks to be performed by compliance are sometimes quite similar to tasks performed by other departments of the organization. Consequently, from the point of view of efficiency, but also to prevent overlapping or even contradictory activities, it is advisable to establish some sort of 'joint committee', in which different departments synchronize activities. Departments such as Quality, Human Resources, Audit, Risk Management and Legal can divide or synchronize tasks. Looking at compliance risks from a broader perspective, it is far more efficient for all parties to agree on how best to mitigate the risk in a combined effort, than having every department doing its own part of the risk, thereby creating blind spots and/or inefficiencies. The CCO should chair such a joint committee.

The duties and tasks of such a joint committee are:

- to assist the CCO with the annual review of the compliance program on how to (i) monitor the effectiveness of the program; (ii) identify any compliance risk areas and weaknesses; and (iii) establish compliance objectives for the year;
- to coordinate activities between the different departments (compliance, internal audit, legal, human resources and quality management) necessary for the execution and administration of the compliance program;

- to provide solicited or unsolicited advice to the CCO;
- to advise on the development, implementation, maintenance, and administration of the compliance program;
- to advise on how to increase the awareness of all employees regarding the compliance program;
- to discuss and advise on investigations of reported violations of the compliance program or any other issues discovered through the annual compliance review or any other audit process;
- to advise on investigations into or studies of matters within the joint committee's scope of responsibilities;
- to advise the CCO as to the status of the compliance program and ongoing developments relating to compliance matters;
- to assess the adequacy of internal and external compliance auditing and controls.

3.3.5.1 The divisional/business unit/local compliance officer

In larger organizations consisting of various subsidiaries, divisions, business units or local entities, it is necessary, for the effective implementation of compliance, to create compliance departments with a divisional/business unit or subsidiary compliance officer. It should be borne in mind, however, that to prevent a compliance department becoming too large with respect to the compliance tasks that need to be performed, an organization may choose to have compliance officers at divisional or business unit level with no further compliance staff members within the division or business unit. For some organizations, it may be more effective to create a Compliance Shared Service Center at corporate level to support the divisional, business unit or local compliance officer with the performance of his tasks.

At subsidiary, division, business unit and/or local level, the compliance officer assists the general management in executing their responsibility for compliance. Compliance is the responsibility of the business and therefore management should be assisted on compliance matters. The ultimate responsibility for compliance nevertheless rests with the first line of defense.

The duties and responsibilities of the subsidiary, division and/or business unit compliance officer are:

- to perform and arrange *ad hoc* compliance reviews within the subsidiary, division and/or business unit;
- to make recommendations to the CCO on ways and means to make business processes better geared to cater for compliance by the staff of the organization's subsidiaries, divisions and/or business units with applicable regulations and codes of conduct;
- to report to the CCO on compliance-related matters and support the management of the subsidiary, division and/or business unit in maintaining the 'right tone at the top';
- to review the key compliance risks within the subsidiary, division and/or business unit with a view to identifying and reporting material compliance risks to the CCO;

- to monitor that all relevant staff in the business unit receive fit-for-purpose awareness and compliance training;
- to report *at regular intervals* to the management of the subsidiary, division and/or business unit and the CCO on the implementation of the compliance program, progress made, issues, incidents and remedies;
- to report serious incidents in the subsidiary, division and/or business unit on an *ad hoc* basis as may be appropriate to the management of the subsidiary, division and/or business unit and the CCO;
- to support internal and external auditors in preparing and conducting audits of the effectiveness of the compliance program in the subsidiary, division and/or business unit;
- to set up and maintain a compliance network in the subsidiary, division and/or business unit;
- to be responsible for the implementation of the compliance program in the subsidiary, division and/or business unit;
- to act as a sounding board for management and staff in the subsidiary, division and/or business unit on compliance and integrity-related matters.

Finally, the legal position of the CCO and the compliance officers in the subsidiaries, divisions and/or business units must not be harmed in any manner as a result of the execution of his compliance duties under the external and/or internal regulations. Their employment contracts should not be ended by management without a formal approval of the Supervisory Board or Audit Committee and a national court or other national labor authority. This is necessary to maintain the necessary independence of the compliance professionals.

3.3.6 Reporting

As discussed *supra*, the CCO should report to the Executive Board and be entitled to directly address the Chairman of the Supervisory Board (two-tier level) and/or the Chairman of the Audit Committee.

The CCO periodically submits reports to the Executive Board and the Audit Committee on the implementation of the compliance program, the progress made regarding the compliance process(es), training and the compliance environment, (ongoing) compliance issues, recent incidents and deployed remediation.

The CCO is the functional head of the compliance department. The structure and size (headcount) of the compliance department depends on the complexity and the size of the organization. Often, the CCO is situated at the headquarters of the organization and the different layers of the organization will have their own compliance department. For instance, every country in which the organization operates may have its own compliance department. Business units may also have their own compliance department. Thus, alongside the CCO, an organization may have divisional compliance officers and/or local compliance officers. These compliance officers are situated within the operations of the organization and have dual reporting lines. They have a functional reporting line to the CCO, as well as a reporting line to their general manager of the division/business unit, with a copy to the CCRO.

On a quarterly basis, the general management of the business units should also report on compliance to the Executive Board through a Letter of Representation (LoR).

3.4 VARIOUS EXAMPLES OF COMPLIANCE PROGRAM REQUIREMENTS

There are many examples of requirements set by local and international authorities regarding compliance programs. Within the financial system in particular, the requirements have become more and more explicit. For example, the Bank for International Settlements describes the responsibilities of the compliance function and how the compliance program should be implemented, including the review of policies and procedures. Already in 2005, the Bureau of Industry and Security (BIS) of the US Department of Commerce described the requirements of an effective compliance function and a compliance program. In Principle 1, BIS explicitly stated that 'the bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board should assess the extent to which the bank is managing its compliance risk effectively.' The responsibility of the first line of defense is stated clearly in Principle 2, which states that the bank's senior management is responsible for the effective management of compliance risks. In Principle 5, BIS explicitly states that the compliance function should be independent. In comment 21, BIS explains that the concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. In fact, cooperation is required.[12]

The requirements for an effective compliance program will be discussed *infra* from the point of view of several authorities and institutions whose requirements are of guiding influence to many organizations that have set up their compliance function over the past decade.

3.4.1 ISO 19600 guidance and uniformity for the organization of compliance

Due to the increasing attention that is being devoted to compliance with laws and regulations and internal ethical and other standards and the notion that organizations must demonstrate that they promote compliance throughout the supply chain in our global economy, the International Organization for Standardization (ISO) has developed a guidance for all organizations on how to set up compliance.[13]

The compliance requirements in the financial sector have been expanded constantly, and since the credit crisis, further internationalization has taken place in the financial world with regard to compliance requirements. This is understandable at a time when global interdependence has steadily increased. The supervisory authorities make increasing demands in terms of compliance throughout the entire production process. As a result, compliance requirements are slowly but surely also being imposed on suppliers and customers in the industrial production process, services, etc. Compliance is no longer relevant only to financial institutions, which now have to include customers and affiliated banks in their compliance framework in addition

12. Basel Committee on Banking Supervision.
13. Compliance Management System Guidance 19600, 2014. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber = 62342.

to their internal compliance. There is also a steady increase in attention devoted to compliance by supervisors of non-financial undertakings. The increase in fines and prosecutions of organizations in the Netherlands and abroad means they sense the need to be in control of compliance with laws, regulations and internal standards.

ISO 19600 provides structure for compliance within organizations. It is all about establishing the organization and assigning tasks in order to have visibility on compliant conduct by the organization and its employees. It is not so much about the personalities, but about what the organization has to do and what needs to be taken into account to be demonstrably compliant. The aim of ISO 19600 is to make compliance part of day-to-day business operations.

An additional advantage of ISO 19600 is that it is not a standard but a guideline. The Dutch representation was committed to this to prevent the guideline being applied to SMEs resulting in excessive costs. The organization must act in the spirit of the guideline and ensure that it is properly embedded in the organization. The ISO 19600 guideline enables organizations to see whether the organizations in their supply chain are fulfilling the compliance requirements. Certification is not really necessary. Compliance focuses on adherence to laws and regulations as well as internal standards. Compliance requires a certain conduct.

ISO 19600 is applicable to all types and sizes of organizations. It deals with a variety of compliance matters such as leadership, planning, support (resources, competence, awareness, training, behavior, culture, communication, documentation), operations (controls to manage obligations and desired behavior), performance evaluation (monitoring compliance performance, evaluation, compliance reporting, audit & management review), and improvement (management of non-compliance including escalation procedures). ISO 19600 is risk-based and fits within the existing ISO risk management framework.

Of particular note is the special focus of ISO 19600 on the role of leadership and its commitment to create a compliance culture within the organization. According to paragraph 5.3 of ISO 19600, leadership and commitment entail:

- upholding core values of the organization;
- ensuring establishment of procedures and provision of resources;
- ensuring integration of Client Management System in business processes;
- communicating importance of effective compliance management; and
- ensuring alignment between operational targets and compliance obligations.

In paragraph 7.3.2 attention is devoted to the necessity of a compliant culture. First, ISO 19600 emphasizes the role of top management in creating a compliant culture:

- creating an environment where reporting of non-compliance is encouraged and the reporting employee is safe from retaliation;
- identifying and acting promptly to correct and address non-compliance; and
- ensuring that operational targets do not compromise compliant behavior.

According to the guidance, a compliance culture requires:

- a clear set of published values;
- management to be actively seen abiding by values;
- leadership by example;
- visible recognition of achievements in compliance;

the case of third-party due diligence an employee has to fill out a computerized form with information on the third party and possibly its ultimate beneficial owner from far and near, the employee will be tempted to circumvent the system and engage directly in a deal with the third party.

The manufacturers of the (financial) systems should develop systems that are easy to use and safeguard compliance at the same time.

What if the ultimate beneficial owner turns out to be a sanctioned party? Generating information from different sources that are but a click away is possible and user-friendly. Also, the look and feel should be user-friendly; no unnecessary information, just letting the employee go through the motions, while also generating information for others such as compliance officers. Finally, the proverbial 'stop' button is necessary in vulnerable processes to prevent wrong deals being done.

The issue of user-friendliness brings us to increasing the possibility of compliance with the softer shared values and norms through the use of an intranet, which would bring great benefits for the monitoring of soft controls. Even in organizations with several hundred employees it is worthwhile setting up a compliance intranet site that contains all the necessary information such as the training the employee still has to undergo, the compliance procedures applicable to his position, frequently asked questions, etc. Also, tooling can be linked to the intranet site offering direct access to a whistleblower tool or a tool to claim expenses such as travel costs and entertainment. All these tools offer monitoring possibilities. However, when creating such an intranet site, it is important to bear in mind that the employee's attention has to be drawn to the intranet site. This can be achieved by linking tools to the intranet and – why not – a little fun factor.

The importance of compliance has increased dramatically since the beginning of this century, and so, therefore, has the significance of monitoring of both soft and hard controls. Many of the soft controls are rapidly 'hardening', but the human factor remains the most important – and also difficult – element to control.

10. Stakeholder and Reputation Management

F.R.P.M. van der Grint[1]

10.1 INTRODUCTION

The worldwide flow of scandals related to fraud, bribery, mismanagement, personal gain, boardroom fights, etc., have put compliance in the spotlight in almost all self-respecting organizations. In some cases this has been demanded by regulators (e.g. banking after Libor), whereas in others it is a demonstration of good behavior and/or change towards shareholders and (legal) authorities. As a result, the increase in the importance of compliance leads to an increase in expectations. This triggers a new challenge for organizations. Their stakeholders all have different ideas about what compliance is, what they can expect and what it can do (not what it cannot do …).

Traditionally, the compliance function looks at laws, rules and regulations enacted by lawmakers and regulators, and at rules and bylaws set out by companies in integrity management guidelines and regulations. It is quite a judicial function, where the rules of the game are available in writing, there for everyone to read and to interpret and discuss. But societal developments have added new rules which are not so clear and certainly not written down. Companies and organizations have increasingly become actors in the court of public opinion. And public opinion does not judge according to formalistic rules; it judges according to which corporate behavior society finds acceptable or unacceptable at any given time. And what is acceptable today may not be acceptable tomorrow.

In the same vein, it is important to understand that we live not only in a democracy with its known rules, but at the same time in a 'mediacracy'. The power of (social) media in the process of forming society's ideas of what it expects from organizations and corporations has become much greater over the past decade or so. Organizations therefore also have to play by the rules of this mediacracy. And those rules change all the time and are not in any way formalized. It makes the job of assessing compliance and managing risks exponentially more difficult. It also makes the job of the compliance

1. With thanks to Ingo Heijnen for his contribution to this chapter.

manager much more complex: it requires an ability to judge behavior not only on the basis of the formal rules, but also on what is socially acceptable.

One can argue that it is not the job of a compliance function to assess an organization's compliance with society's definition of acceptable behavior. Reputation managers are expected to do this and to advise senior management on how to adjust behavior in order to maintain and strengthen the organization's reputation as an actor in society – and with that its license to operate. And while this is indeed the traditional segregation of functions, today's reality requires a different approach. It is in the best interest of organizations to broaden the (perceived and formalized) responsibility for managing risks for the said license to operate. Compliance managers are naturally well placed to play a role in this development. Their formalized involvement in (re)defining corporate behavior gives them a natural position in assessing how an organization is coping with the informal rules of being a good, and therefore acceptable, citizen. Under this premise, it makes sense for anyone in a compliance function to understand how an organization makes an impact on its surroundings, on the ecosystem in which it operates. Understanding who your stakeholders are, how they relate to you as an organization and to each other, what their evoked set of norms and values is, how they are being influenced and how they can be influenced – having knowledge as well as an operational understanding of these aspects – makes the compliance manager infinitely more effective in his role.

In this chapter, we will therefore cover the following aspects of managing reputation and risk, with a focus on what is known as stakeholder and issue management:

1. How reputations are formed and why it pays off to build and defend them.
2. Reputation management in a mediocracy.
3. The role of leadership behavior.
4. The importance of trust and credibility.
5. Stakeholders: analysis.
6. Managing your stakeholders to manage risks.

10.2 HOW REPUTATIONS ARE FORMED AND WHY IT PAYS OFF TO BUILD AND DEFEND THEM

Back in 2002, the IKEA retail chain and the Van der Valk hotel chain faced a very similar problem in the Netherlands. They were confronted with collapsing rooftops at one of their sites. These situations occurred more or less at the same time. IKEA's rooftop at its Utrecht site gave way because of a surplus of rainwater – suggesting faulty construction. Van der Valk's parking deck roof in Tiel collapsed spontaneously – the result of a 'stupid mistake' when the deck was constructed. Public reaction to the occurrences, however similar they seem technically, were strikingly different. IKEA was off the hook very quickly – it was not their fault that such heavy rains fell that summer. Van der Valk's management, however, came under heavy scrutiny. Whereas the IKEA store was allowed to reopen only one week after the accident, Van der Valk's motel had to remain closed for two months, with strict government inspections at all of the company's sites.

A study of both cases demonstrates different reactions among similar stakeholder groups. The media criticized the Van der Valk management, but not IKEA's. The

media also reported on the danger to customers at the Van der Valk site; it was not even mentioned in the IKEA reports. Local government reacted strongly against Van der Valk, but were invisible in the case of IKEA. The responsible ministry started a 'thorough investigation' of all Van der Valk outlets, but nothing of the kind for IKEA.

What caused this difference in stakeholder reactions? The overriding dominant factor is reputation. IKEA's reputation as a socially responsible, employee- and customer-friendly company meant that media and politics were restrained. But Van der Valk's reputation as a more closed business played against them.

While reputation is a widely and often used term in boards and, especially at times of crisis, is seen as the most important company asset to manage, today it is still not the best understood management aspect. People use reputation as a generic word, but what it really is and how it should be managed is often poorly developed within entities. The most frequently used description of reputation is that of Fombrun.[2] Together with a team of communications scientists he developed six reputation drivers, each of which can be managed and therefore influenced.

Fombrun's reputation drivers are:

- emotional appeal (from stakeholders to a company);
- vision & leadership (of the company management and board);
- financial performance (often the main measure of success);
- workplace environment (as experienced by employees and perceived by external audiences);
- social responsibility (in relation to the 'license to operate');
- products & services (why do we have this company in the first place).

Although the words that describe the drivers may differ (other words used are innovation, governance and citizenship), the advantage of using a set of drivers to determine reputation is that drivers can measured. By doing so, reputation becomes more than just a gut feeling, a temporary suggestion based on unfavorable press cuttings, or reactions in the CEO's peer group.

The importance of managing one's reputation is now beyond discussion. Fombrun & Low[3] wrote in their 'The Real Value of Reputation': 'Global forces are causing shifts in public perceptions of companies that in turn drive changes in regulatory, political and financial structures around the world. Companies that enjoy strong and favorable reputations have a competitive advantage in these global markets. Iconic brands and exemplary reputations help companies "translate" their offering to new customers, because the values they embody provide a shorthand interpretation of what they have to offer.'

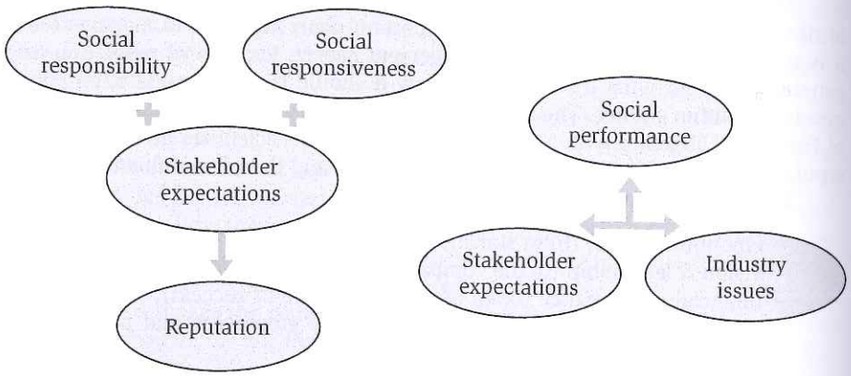
While Fombrun's drivers are mostly used by communications professionals, we believe the drivers in the model of Brammer & Pavelin[4] are equally interesting. They have found that reputation is determined by:

- social performance;
- financial performance;

2. Van Riel & Fombrun 2007.
3. Fombrun & Low 2011.
4. Brammer & Pavelin 2006, pp. 435–455.

- market risk;
- long-term ownership;
- business activities.

Although one could argue that this is just another mix of words for the same principles, the interesting part of Brammer & Pavelin's view is that they herald the need for a 'fit' between a company's social performance and the expectations among stakeholders.



Figures 1 and 2: Models according to Fobrum and Brammer & Pavelin

If corporate social performance could be split between social responsibility (driven by the company and sector) and social responsiveness (driven by society), both should be linked and related to the stakeholder expectations. If not, social responsibility can be an expensive but inefficient, if not counterproductive, exercise. As such, reputation management is the management of the 'fit' between the company's social performance, the issues related to the industry in which it is operating and the expectations of stakeholders surrounding the company.

So why is it important to build and defend a reputation? One could argue, and many people have, that damage to reputation is only temporary and that in any event it will not harm or affect the core of the organization. There are enough companies and organizations out there with a bad or damaged reputation but with a thriving business. Think of large oil companies, think of pharmaceuticals, to name just two. There is, however, enough scientific evidence that suggests that companies with a good reputation perform better on the stock exchange, will attract better talent and will have better business deals. But, most of all, a sound reputation provides a buffer for when things do go wrong. The court of public opinion will be more lenient on those who have earned their trust previously and have been able to create a positive, reliable, trustworthy perception.

What does this mean for a compliance manager?

Clearly, compliance experts have to deal with laws, rules, company values and culture and in some sectors also an 'oath'. But, in relation to reputation management, the compliance function should also be aware of the relationship between the

company's social performance, industry issues and stakeholder expectations and how these influence the risk of a company losing its license to operate.

10.3 REPUTATION MANAGEMENT IN A MEDIACRACY

In matters of compliance and integrity, the legal and financial contexts are not the only aspects to take into account. The social context in which an organization operates is equally important. This context today is largely based on the fact that we live in a mediacracy. And this has an effect on how stakeholders interact with organizations, since stakeholders base their judgment of a reputation in part on information they receive from these parties, including media. A compliance manager needs to anticipate this reality, which is hard and becoming harder every day.

One definition of the concept of 'mediacracy', or media-democracy, is an expression of the idea that (democratic) countries are mainly ruled by those who have the power to influence public opinion through the media. Often this concept is also applicable to the media themselves, who are a steering power in a country. The concept is a mix of Greek and Latin, meaning 'ruling through media'.

A mediacracy has four characteristics:

- *A focus on people and what they are doing wrong*. The best stories are about people, not about companies. What goes wrong is news; was goes well is not.
- *Fierce competition between media*. Media are in a constant rat race. And they have to cope with 'public journalists' who broadcast constantly on social media.
- *Extreme populism*. What is seen in politics throughout the world is also seen in the media. Populism leads the editorial agenda. On this, we should stress that because of Brexit and the US elections there is a renewed debate on the value of truth. Whether this will reduce populism in media remains to be seen.
- *Image is everything*. People share photos and video. Those with the best image win the media battle.

Whoever is involved in the science of reputation management and managing the license to operate for an organization will have to understand how media need to be managed. Not only traditional, journalistic media, but also social media. There is a school that says that directing the dynamics in these media nowadays is impossible. The speed at which news and stories are disseminated is seen as just too high – an organization cannot keep up. We tend to disagree. The management of stories, how they are delivered and by whom has never been so important.

There are certain truths and rules to be taken into account. Here are the top five truths when dealing with the mediacracy:

1. *Speed is of the essence* – when dealing with issues, incidents and/or crises, communicate – fast. There is no time for long deliberations. Because while you are still thinking, there are people out there who will not wait to express their opinions or reveal new facts, thereby upping the pressure. An organization can gain speed by preparing for the worst case.

2. *Think in scenarios* – and by doing so, be prepared for what else could come your way. It will make your response time much shorter and your impact a lot greater.
3. *Communicate with facts* – and make sure the media possess the correct facts. Fight 'untruths' or 'alternative truths'.
4. *Create visible leadership* – be seen and be heard at times when it matters, show you take the lead and create new perspectives for stakeholders involved. To avoid misunderstanding, demonstrating leadership does not necessarily mean your leaders should always be the visible communicators themselves.
5. *Calibrate your moral compass* – and make sure that what you find morally acceptable is echoed by your stakeholders. Show responsibility and show that you care about your surroundings and the world at large.

Finally there is one other important truth to consider: in crises, reputational damage always occurs first, often long before financial and/or legal damage. Today there are still legal battles about companies that no longer even exist (e.g. World Online), while the reputational damage was there immediately and at least contributed to the downfall of these companies. Similarly, Volkswagen's reputation was already heavily damaged by the Dieselgate scandal, long before the financial settlements were reached.

10.4 THE ROLE OF LEADERSHIP BEHAVIOR

Leaders and executives play a crucial role when an organization is being judged on its social performance, intentions and credibility. More than ever before, we live in an era when an organization is measured by the behavior of its leaders. There is an enormous focus on 'people' when the media and politicians set out to judge. This is true of all types of corporations, whether they are for profit or not for profit.

A general sense of distrust towards corporate executives and politicians has emerged from the scandals that kicked off the 2008 crisis, and even before that, when Enron in the United States collapsed. Time and again, some bad examples among executives and politicians have shown behavior that was seen as egocentric, greedy, snobbish, elitist and other similar traits. This (perceived) behavior by executives, influences more than before the overall perception and reputation of an organization. When a board member shows conduct that does not comply with what stakeholders expect, the whole company will come under fire.

Today, therefore, when an organization is in crisis, a high-ranking scapegoat is rarely far away and will be sacrificed to defend the corporate reputation. At Rabobank, there were two board members who did not survive the Libor scandal. Tony Hayward had to resign as CEO of BP after the Deepwater Horizon disaster and in 2016 Saatchi & Saatchi CEO Kevin Roberts was sacked after denying gender bias in the advertising world. Those board members were not necessarily the ones who created the problems. But they were held accountable for the culture they allowed to develop within their organizations. In the case of Hayward, it did not help that at some time during the crisis when the oil had destroyed a lot of natural resources around Florida's coastline and fishermen could not go out and earn their wages, he complained that he 'wanted his life back'. These examples show that leaders are

judged on a wide range of behavior, not only related to financial aspects or technical dramas, but increasingly also based on aspects that 'society deems unacceptable'. Sometimes, as in Kevin Roberts' case, it is the CEO's own behavior or utterances that lead to his downfall, whereas in other cases a leader is simply held accountable for failures in his organization that just should not have occurred, irrespective of the fact that the leadership itself was not directly responsible.

In this age of mediacracy, socially unacceptable behavior will not only be scrutinized but will lead to public defamation of individuals. In those cases, as so often, a picture says more than a thousand words. We have seen once respected leaders literally being depicted as criminals, including with black bars over their eyes in newspaper pictures, following revelations of behavior that was certainly unacceptable but not necessarily criminal. Actors on social media are ruthless in this respect – individuals' sound reputations can be destroyed in a matter of hours on Facebook and Twitter.

This insight should lead, and indeed does lead, to a culture of more scrutiny within organizations. Behavior that was once accepted or ignored will no longer be tolerated. It is just too costly from a trust and therefore reputation point of view. Leading by example has taken on a new dimension and is absolutely essential when it comes to displaying the right behavior. But since leaders too are only human, it requires an open, honest and bold corporate staff to help them display this and not go astray. It is typically the reputation and compliance managers who can play this role, supported by the corporate legal function.

10.5 THE IMPORTANCE OF TRUST AND CREDIBILITY

There is also another way of looking at the interaction between reputation and stakeholders. Especially at times of incidents and crises, companies start to communicate about 'restoring trust'. Whether this a smart way of communicating is a separate discussion, but let us look at 'trust' a little more closely.

$$\text{Trust} = \text{intention} \times \text{result}$$

Our definition of trust is straightforward: trust is built upon the intention of a company in relation to the results the company is achieving. And results here can be seen as results within the range of drivers as described by either Fombrun or Brammer & Pavelin.

The aggregate of a company's intentions forms the basis of its existence. It is the DNA of the organization. Sometimes it is called 'mission'; a more modern term is 'purpose'. Companies that have an ill developed intention and/or a poorly communicated intention have a more difficult task in establishing trust. They have to rely on the much used goals-strategy-results approach, which will only establish a temporary and – what we call – 'minor trust'. This is the type of trust that can easily disappear with an incident or several quarters of disappointing financial results.

To gain major trust, companies must not only have a clear and communicated intention, they also have to have a well described perspective for all their stakeholders. Intention and perspective are by their nature long-term, and therefore much more suitable for establishing sustainable trust – the kind of trust that helps a company to protect its reputation, even in difficult times.

Credibility

So trust is an operative word for reputation managers, and of course also for compliance managers. The same goes for the word credibility. Both functions in an organization, reputation management and compliance management, thrive by establishing and safeguarding the credibility of their employers. In communication campaigns, credibility is the springboard towards an authoritative position, which is a position that provides the highest reputational resilience.

Figure 3: Credibility is the springboard towards authority

Many leaders of organizations strive for positions of authority. We have often seen company position papers or communication briefings that either try to achieve it or pretend they are already there and want to build upon it. What is often forgotten is the fact that a position of authority is impossible without an established position of credibility. While everybody understands that the statement 'I am credible' does not have any power and even comes across as pretty silly, there are still enough managers to be found who believe 'I am an authority' is less silly. Just look at the websites where the corporate description contains the words 'we are an authority in …'

There is no authority without credibility and there is no credibility without awareness. Yet awareness can be bought. High advertising budgets spent in print and online media can bring products and companies the awareness they strive for. For the most part they are also easy to measure. Credibility, however, cannot be bought, for the simple reason that you can only earn it.

$$\text{Credibility} = \text{trust} \times \text{recognition}$$

We have described *supra* how sustainable trust relies on an organization's intentions. Since credibility relies on trust, it is clear that there is also a tangible relationship between credibility and intentions.

Trust and recognition are both to be provided by third parties – try to sell 'I trust myself' or 'I give myself recognition'. Yet trust can be steered by means of intentions,

and intentions can be clearly communicated, demonstrated and proved. Furthermore, trust can be steered by means of results, and results can also be communicated, demonstrated and proved.

Given the importance of recognition in gaining credibility, one has to look at stakeholders to gain recognition. Third parties – spread across all relevant stakeholder groups – can provide recognition, but must have a reason to do so. That makes credibility dependent on the interaction with stakeholders. And stakeholders mostly rely on information provided by third parties if they judge companies.[5] In the next section the most important aspects of stakeholder management are reviewed.

10.6 STAKEHOLDERS: ANALYSIS

'Make your friends before you need them.'

Stakeholders are not necessarily your friends. But they can certainly be friends, if managed well. First and foremost, stakeholders are those groups of individuals who have a vested interest in an organization. So stakeholders are those people who will have exposure to the organization in some shape or form and who will have a view on the acceptability of that organization. In that capacity, stakeholders can determine whether or not an organization has a sustainable future. Because, with enough negative pressure from stakeholders, organizations can be in very dire straits and ultimately they may collapse. The Medici Bank experienced this already back in 1494, when the excessive lifestyle of the owners caused stakeholders to lose their trust in the bank.

Communicating with stakeholders is often seen as the playground for communications departments. This is an enormous misunderstanding of what stakeholder management is, what it entails and whose responsibility it is. Ultimately, stakeholder management is the responsibility of the board(s). But only in few instances do boards discuss their full stakeholder field, let alone have awareness of who the key players are in each of the relevant groups.

As we have said before, compliance managers need to be aware of stakeholder expectations. They should see them as one of the drivers for compliance and integrity in their understanding of a company. This means a compliance manager cannot have the luxury of looking into only one stakeholder group (e.g. solely regulatory stakeholders). In today's society a variety of audiences form opinions on issues related to compliance and integrity.

Infra we describe some fundamental aspects of stakeholder management, all of which can be helpful in determining key players surrounding your own company.

Inventory

The inventory of relevant stakeholders can best be drawn up per group:

- shareholders (founders, family owners, stock owners);
- financial community (investors, analysts, banks, insurers);
- customers (end users of products and/or services);

5. Mahon & Wartick 2003, pp. 19–35.

- trade parties (e.g. wholesale, retail);
- suppliers (producers, OEMs);
- boards (management, supervisory board);
- employees (in various layers);
- works council(s);
- unions;
- pension funds;
- government (national, regional, local);
- politicians;
- EU and EC;
- regulators;
- supervisors;
- consumer organizations;
- NGOs;
- universities;
- sector organizations;
- competition (peers);
- media;
- opinion leaders;
- the public.

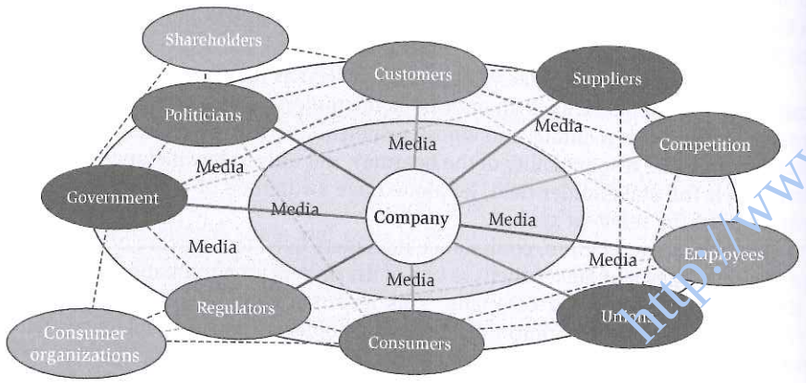


Figure 4: Stakeholders' model

In order to make stakeholder management effective, specific names of persons for each stakeholder group need to be mentioned. This is a critical and ongoing effort – every company must be aware of the key influencers. But being aware is not enough, nor is it enough to simply keep a list of people. A relationship needs to be established. This relationship is key for the organization to ensure support and even endorsement from third parties in cases when it really matters. Corporations under scrutiny will always be looking for third parties, for their stakeholders, to provide them with support, verbally or actively, to help them out. If and when such third-party endorsement is required – and in today's environment this may be the

case every single day of the week – the third parties of choice need to know the company, its intentions, results and perspective. Only then can stakeholders put an organization's or executive's behavior into perspective and provide a new angle for bystanders watching and judging.

As it is impossible to establish a meaningful relationship in one day, ongoing investment in stakeholder relations is an important requirement. Especially in times of crisis, third-party support is vital. Therefore we very much believe that 'making friends before you need them' is a truth that should not be underestimated.

Mapping

Knowing who your stakeholders are is one thing. Knowing what their position is in relation to important subjects for the organization is quite another. While stakeholder inventory is an ongoing exercise, stakeholder mapping is even more an activity that requires continuous contacts and monitoring. Several mapping tools are available and which one is best depends on the situation and issues at hand. Here we present a number of these tools, as a reference.

Circle of Influence

This tool is used to determine which stakeholders around your organization are in favor or against certain positions/viewpoints/products (themes and/or issues). It shows the level of support and opposition at various tier levels.

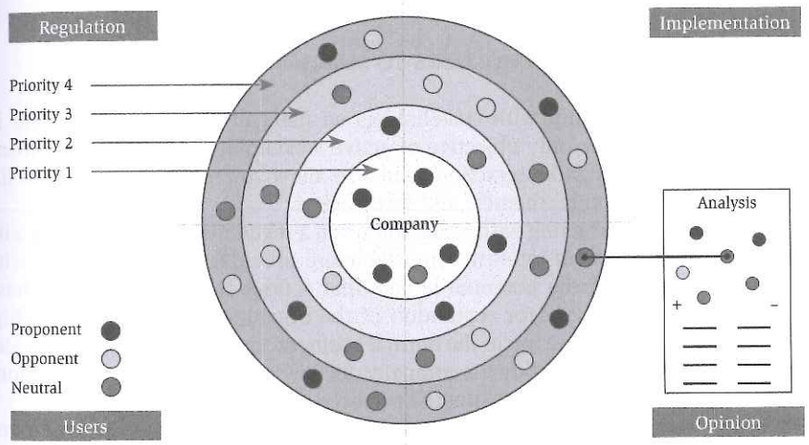


Figure 5: Circle of Influence

Stakeholder Position

Another much used tool is the Stakeholder Position quadrant, in which supporters and opposition are mapped against two (related) topics. It shows immediately where you have enough third-party endorsement and where you still have some work to do. With regular updates, it can also track changes of positions.

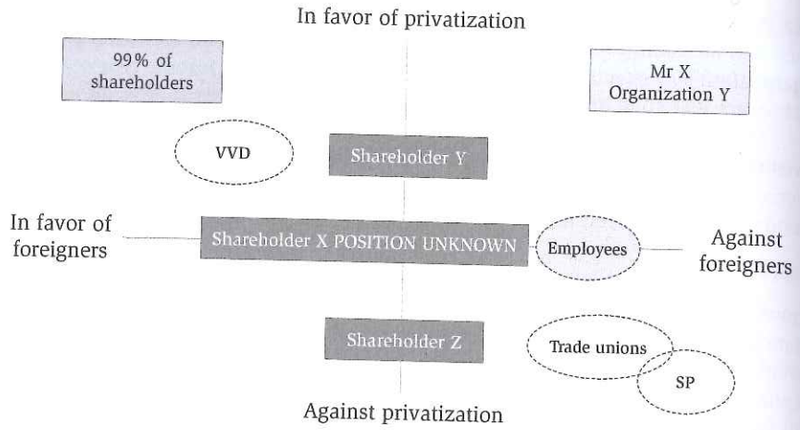


Figure 6: Stakeholder Position quadrant

Stakeholder Network Analysis

A more sophisticated but also more expensive tool is the Stakeholder Network Analysis. It shows which influencers are influencing others. By making the right combinations, approaching stakeholders can be much more effective.

10.7 MANAGING STAKEHOLDERS TO MANAGE RISK

Establishing a relationship with stakeholders so that you can call upon them in times of need is not the only objective of active stakeholder management. Having ongoing conversations and interactions will also allow you to gain insights into the stakeholder's own agenda, themes, and focus areas.

For instance, interacting with trade unions on a regular basis provides you with insights into their areas of interest – and therefore provides the organization with intelligence concerning the potential impact that actions by the unions may have on the credibility, trust and/or reputation of the organization and its leadership. Engaging with customers on top of the normal business course of action also provides important intelligence that allows a company, for instance, to manage expectations or provide an early warning for potential publicly voiced dissatisfaction.

Active stakeholder management is the action of *listening* to stakeholders, *engaging* with them in conversations and *influencing* their perception and acceptance of the organization. By doing so, an organization can generate intelligence, prevent damage and therefore manage risks. Stakeholder management may not be the first task of the compliance manager, as other functions will be better suited to it. But the compliance manager needs to understand if and how a company is actively managing these parties – because this provides a level of prediction for the company's ability to prevent damage and to contain issues.

BIBLIOGRAPHY

Brammer & Pavelin 2006
S. Brammer & S. Pavelin, 'Corporate reputation and social performance: the importance of fit', *Journal of Management Studies*, 43(3), 2006, pp. 435–455.

Fombrun & Low 2011
C.J. Fombrun & J. Low, 'The Real Value of Reputation', *Communication World*, 28(6), 2011, pp. 18–22.

Mahon & Wartick 2003
J.F. Mahon & S.L. Wartick, *'Dealing with stakeholders: how reputation, credibility and framing influence the game'*, *Corporate Reputation Review*, vol.6, 2003, pp. 19–35.

Van Riel & Fombrun 2007
C.B.M. van Riel & C. J. Fombrun, *Essentials of corporate communication- Implementing practices for effective reputation management*, London: Routledge 2007.

16. Extraterritorial Jurisdiction[1]

Prof. S.C. Bleker-van Eyk

16.1 INTRODUCTION

In this chapter the concept of extraterritorial jurisdiction will be discussed, due to the enormous importance of this issue to both national and international companies, their executive officers and their employees. The dangers of extraterritoriality of foreign legislation are highly underrated, however, and the consequences can be enormous. Companies are only slowly beginning to realize that there really is an issue. The word 'extraterritoriality' is now used more frequently in day-to-day practice, but many company lawyers do not genuinely understand what it means for them and for their company and – even worse – compliance officers are held responsible for not having tackled such issues. It already seems enough of a challenge to ensure compliance with laws and regulations in one's home jurisdiction and those relating to one's subsidiaries and activities abroad, but the task becomes three-dimensional when the extraterritorial laws of foreign countries also impact activities in all other locations.

This extraterritorial reach, brought into being by foreign countries, is an increasingly important phenomenon that affects not only natural persons that are suspected of having committed criminal offenses, but also corporate enterprises. Such enterprises are often unwillingly or unknowingly involved in illegal activities; sometimes companies are entirely unaware that they have crossed a line that should not have been crossed. It is therefore high time to consider the subject of 'extraterritoriality' in greater depth, because companies are increasingly encountering the long, extraterritorial arm of, for example, the United States of America.

1. Parts of this chapter were previously published in Bleker-van Eyk 2013, pp. 53–61 and Bleker-van Eyk 2012.

16.2 EXTRATERRITORIAL JURISDICTION AS A DRIVING FORCE OF COMPLIANCE

In recent years we have seen increasing attention being paid to compliance in non-financial companies, owing to growing awareness of the extraterritorial application of anti-corruption legislation. Since 1997 the OECD Anti-Bribery Convention has enabled the US to enforce its legislation more effectively in other countries, as the States Parties to it – not only the OECD Member States – meet the requirement of dual criminality once they have ratified it. Real awareness in boardrooms of the extraterritorial application of foreign legislation only seems to have developed after the passing of the United Kingdom Bribery Act (UKBA), however.[2] No doubt Great Britain is not so far away that European directors can sleep at night. Most of them slept fine with the Foreign Corrupt Practices Act (FCPA), which presented – and still presents – a far greater danger. Competition cases have also created a good deal of turmoil in recent years, though they are rarely regarded as compliance matters, usually still being dealt with by legal departments. The question is whether this is correct. Competition cases fall under national and international legislation and can entail substantial risks. As stated earlier in this book, the purpose of compliance is to promote the observance of national and international laws and regulations, as well as internal rules and standards, to protect the integrity of the organization and its directors and staff. The aim is to control the risks of non-compliance with laws, regulations and standards and to prevent the damage that could result. However, the compliance function often does not realize that it may also have to take into account foreign legislation, even when the company has no subsidiary in that foreign country. During the past twenty-odd years compliance has slowly become aware of the extraterritorial ramifications of anti-bribery, export control or sanctions legislation. As soon as the executives within a company start feeling the hot breath of foreign enforcement agencies, the compliance departments grow rapidly. The extraterritorial application of American export rules is still the driving force behind the creation of many compliance roles in the industrial world.[3] This does not apply by definition to all laws and regulations, but particularly to those related to achieving the company's key objectives. It is fair to say that compliance derives its *raison d'être* from a company's license to operate. Compliance risks are risks that can pull the proverbial rug from under the company, or at least cause major material and reputational damage.

The extraterritorial effect of legislation is being experienced worldwide by an increasing number of companies because American anti-terrorism legislation regularly exceeds the territorial boundaries of the United States. Various companies (mostly financial institutions and large industrial conglomerates) headquartered outside the United States have felt the painful effects of this phenomenon in recent years. This began with the FCPA, particularly after the ratification of the OECD Anti-Corruption

2. Bleker-van Eyk 2012.
3. Cf. the United States: Directorate of Defense and Trade Controls (DDTC) http://www.pmddtc.state.gov/compliance/index.html; Bureau of Industry and Security (BIS) http://www.bis.doc.gov/complianceandenforcement/emcp.htm; Office of Foreign Assets Control (OFAC) http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

Convention (ACC) and later on the UKBA. This will be discussed in chapter 17 on Anti-Bribery & Corruption *infra*. Like the US legislator, the British legislator – and in its wake the British judiciary – is also moving beyond its territorial boundaries. However, the most dangerous exponents of 'extraterritorialism' are the so-called 'export controls' and 'sanctions' provisions in the US. This will be discussed later in more detail in the chapter 18 on Export Controls & Sanctions *infra*.

16.3 THE DEFINITION OF EXTRATERRITORIALITY

Extraterritorial jurisdiction is the extension of jurisdiction over offenses that have been committed outside the territory of a country. States are sovereign and independent. In principle a state determines the scope of its legal system, and as such, the use of extraterritorial jurisdiction is an extremely controversial subject. It is contrary to the territorial sovereignty of the state when another foreign state claims extraterritorial jurisdiction over its subjects.

The starting point is and remains that every state should decide on its own laws and regulations, and on how compliance with these rules is to be enforced. Nowadays the world has become a global village where cross-border economic activities create new challenges for states in their attempt to control the activities of their own (corporate) citizens. States also want to control the activities of foreign persons within their territorial borders and, finally, to protect their own interests and those of their citizens. Sometimes the level of control requires a state to take actions beyond its territorial limits. All these cross-border activities create overlapping jurisdictional claims.

There are countless international treaties that obligate states to establish jurisdiction in a certain way in respect of offenses committed not on their own territory but elsewhere in the world. The extraterritorial jurisdiction can be divided into various core principles:[4]

- The *active personality principle*, which means that jurisdiction can be claimed for acts committed by the country's own citizens.
- The *passive personality principle*, in which jurisdiction is claimed in respect of offenses committed against a country's own citizens.[5]
- The *universality principle*, which claims jurisdiction on the basis of the seriousness of the existing offenses.
- *Derivative or subsidiary jurisdiction*, in which a country also acquires jurisdiction over the offense by means of a transfer of criminal proceedings. The basis for this lies in the various treaties in which one party requests the other party to take over the criminal proceedings. That state then actually takes over the original jurisdiction of the requesting state.[6]

4. Klip & Massa 2010, p. 506.
5. Sjöcrona & Orie 2002, p. 72.
6. In the Netherlands the legal basis is incorporated in Art. 522hh paragraph 2 of the Code of Criminal Procedure and in the European Convention on the Transfer of Proceedings in Criminal Matters of the Council of Europe.

- The *principle of protection*, protecting specific interests of the state justifying extraterritorial intervention, for example in the case of counterfeiting.
- The *subjective territoriality principle*, in which the extraterritorial jurisdiction is claimed because, for example, an act committed abroad has an effect within the state claiming jurisdiction. Conversely, it is also possible that the offense was started in the state claiming jurisdiction, but its effect is generated primarily outside the boundaries of that state.[7]

16.4 PRINCIPLES OF EXTRATERRITORIALITY

16.4.1 The active personality principle

Jurisdiction can be claimed for offenses that have been committed by the claimant country's own nationals. The nationality of the offender is the basis on which extraterritorial jurisdiction is claimed. Countries may refuse to extradite their own nationals; for instance, the Netherlands does not extradite its own nationals without a bilateral or multilateral extradition agreement. An example of extradition in the Netherlands is the approval by the Dutch Supreme Court of the extradition of a Dutch CEO to the US on a charge relating to the violation of the FCPA.[8] Despite this, due to political pressure, the CEO has not been extradited to the US.

16.4.2 The passive personality principle

Here jurisdiction is claimed on the basis of the nationality of the victims of a crime. This principle is rarely applied, although it may arise, for example, in the aftermath of wars.

16.4.3 The principle of universality

Under this principle countries can claim jurisdiction based on the severity of the crime. Extraterritoriality is part of the international agreements among countries. Best known are international crimes such as war crimes, crimes against humanity, genocide, piracy, aircraft hijacking and international drug trafficking. Today these are considered international crimes and jurisdiction may be claimed on the basis of the principle of universality.

In the case of piracy there has long been a difference of opinion as to whether universal jurisdiction applies. The crime of piracy can take place on ships and in aircraft. Maritime law has described the question of extraterritoriality in such a way that the state which liberates the ship can claim jurisdiction.[9] Over time a large number of states have accepted the *universality principle* for piracy. That means that within certain limits (figuratively speaking) states consider that they have jurisdiction over

7. Council of Europe, Convention on the Prevention of Terrorism, Art. 14(2); UN Convention Against Transnational Organized Crime, Art. 15(2).
8. Dutch Supreme Court, Case 01631/024, July 8, 2003.
9. Art. 19 of the Convention on the High Seas 1958.

offenses committed by foreigners having regard to the nature of the offense and the circumstances under which it was committed. Legislations do not all claim universal jurisdiction to the same extent. In the case of piracy, hijackings and international drugs trade, war crimes, crimes against humanity and genocide, a claim for jurisdiction can reasonably be made on the basis of the universality principle.[10]

On the basis of the universality principle, all countries have the right (or perhaps even the *duty*) to penalize certain serious crimes, regardless of where the crime took place or the nationality of the perpetrator or the victim. In international law the *Lotus* case is the basis for the principle of universality. The Permanent Court of International Justice of the League of Nations[11] reasoned at the time that any country is entitled to adopt legislation that allows the country to prosecute crimes committed abroad. In his dissenting opinion in the *Lotus* case[12] Judge Moore suggested that piracy allows for universal jurisdiction. Nowadays it is accepted that a jurisdictional claim may be based on the principle of universality in cases of piracy, hijacking and international drug trafficking, war crimes, crimes against humanity and genocide.

Article 5 of the Statute of the International Criminal Court states that the jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole. The Court has jurisdiction in accordance with this Statute with respect to the following crimes:

- the crime of genocide;
- crimes against humanity;
- war crimes;
- the crime of aggression.

This leaves us with the question of whether terrorism can be regarded as an act to which the principle of universality applies. Terrorists are not ordinary criminals; they act out of political and often also religious motives. They use terror to achieve their objectives. Their status may change from that of a terrorist to that of a recognized representative of a state.[13] International law has a different regime with regard to the legal position of revolutionaries. Terrorists form a separate category with which the world is still struggling, both literally and figuratively. But countless regional and international treaties have been concluded to establish jurisdiction over terrorists. Many national legislators have also established jurisdiction over terrorists in their national legislation.

Extraterritoriality is part of the international agreements which states have entered into for many years. Well-known examples are international crimes such as war crimes, crimes against humanity, including genocide,[14] piracy, aircraft hijacking

10. Brownlie 1990, pp. 304–305.
11. This was the predecessor of the International Court of Justice of the United Nations.
12. PCIJ, Series A, no. 10, 1927, p. 70. www.invispress.com/law/international/lotus.html.
13. Yasser Arafat, the leader of Al Fatah is a good example. He was regarded as one of the first terrorist leaders in the 1970s. Finally, he became one of the peace negotiators together with Israel and Egypt in the White House in Washington DC as official leader of the Palestinian People.
14. The list of crimes are to be found in Art. 5 of the Statute of the International Criminal Court.

and the international drugs trade, in which the universality principle is nowadays accepted. Here we encounter the second core principle referred to above: the *universality principle*.

On the basis of the universality principle, all states have the right (and perhaps also the duty) to penalize certain serious crimes, regardless of the location in which the crime took place or the nationality of the offender or the victim.[15] In terms of international law the question of extraterritoriality of jurisdiction arose in the *Lotus* case. It concerned a question relating to piracy. The Permanent Court of International Justice of the League of Nations ruled at the time that every state was entitled to adopt legislation allowing the state to prosecute offenses committed abroad. In his dissenting opinion in the *Lotus* case Judge Moore stated that piracy created the possibility of universal jurisdiction. This means that any state in which the pirate is located at a particular time may prosecute the piracy.

The principles relating to *derivative or subsidiary jurisdiction*, i.e. the protection of specific interests of the state, and the *subjective territoriality principle* will not be discussed in greater detail here, because they are of less significance in the context of the extraterritorial effect of foreign legislation on Dutch business – as articulated in the central question of this chapter.

16.5 THE LINK BETWEEN JURISDICTION AND THE STATE

The sovereign state sets the groundwork for the extraterritorial enforcement of jurisdiction. Legislators increasingly focus on the relationship between the 'fact', the 'offender' and the 'victim' of the offense or on the extraterritorial scope of the jurisdiction. A crime committed by a (corporate) citizen of country X in country Y may be considered so important to country X that it will want to claim extraterritorial jurisdiction. In 2004 the Dutch law 'Wet Terroristische Misdrijven' (Terrorist Crimes Act) came into force. This law is an amendment to the (Dutch) Criminal Code. Article 4 concerns the extraterritorial effect of Dutch jurisdiction, stating that Dutch criminal law is applicable to terrorist acts committed outside the Netherlands if the terrorist is a Dutch citizen or if he is currently staying in the Netherlands and, as a consequence, such persons can be prosecuted in a Dutch court.[16] Many may feel that the search for a link between the territory, the offender and the victim is too 'far-stretched'. Consider this example: the Prosecutor in Rotterdam wants to prosecute a Nigerian human rights and environmental activist for complicity in plotting a terrorist attack in the Niger Delta. Terrorism researcher Quirine Eijkman expresses her concern that there may be an ulterior political motive, because she can see no direct link with Dutch interests.[17] However, a clear link with the Netherlands exists, because five years earlier the man was granted asylum and still resides in the Netherlands. The territorial link is even more abstract when it concerns the use of modern means of communication. In the US the FCPA opens the possibility of claiming jurisdiction in cases where a crime is committed by

15. Van den Wyngaert 2009, p. 157.
16. Art. 4 paragraphs 13 and 14 of the Criminal Code.
17. NRC (Dutch Newspaper) 09-03-2011.

means of an email sent abroad as long as it can be proven that the email passed through a server within US territory.

However, extraterritoriality may also arise in a more abstract form if a country wishes to protect its interests abroad. The use of the US dollar most frequently requires passage through the US-based clearing system as banks make transfers between them. The use of US clearing through New York or elsewhere in the USA must not facilitate the financing of terrorism. As world trade mostly takes place in US dollars, the territorial jurisdictional claim of the US concerning any wrongdoing within global trading activities involving the US dollar is greatly expanded. Also, certain products and know-how may trigger the application of extraterritorial jurisdiction, as will be discussed later in chapter 18 on Export Controls and Sanctions.

At a very practical level, even in transactions that only involve non-US legal entities, companies with international staff might be subject to US law due to the mere fact that one of the employees negotiating the contract is a US passport or Green Card holder. Further down the line, employees with American citizenship or a Green Card may be compelled to inform the US authorities of their knowledge of possible infringements of US laws and regulations on issues such as anti-trust, anti-bribery and corruption, export controls or sanctions.

16.6 EXTRADITION RISK

Extradition is mostly based on bilateral or multilateral treaties. Where corruption is concerned the ACC plays a dominant role. Article 10 'Extradition', makes clear that any 'Bribery of a foreign public official shall be deemed to be included as an extraditable offence under the laws of the Parties and the extradition treaties between them' and that 'if a Party which makes extradition conditional on the existence of an extradition treaty receives a request for extradition from another Party with which it has no extradition treaty, it may consider this Convention to be the legal basis for extradition in respect of the offence of bribery of a foreign public official', adding that jurisdiction should be 'interpreted broadly so that an extensive physical connection to the bribery act is not required'. Such a broad risk of extradition for the violation of laws of which employees may not have been made aware must present a major surprise when applied.

Ultimately it is up to the state to decide to what extent it will cooperate on its own territory with the exercise of extraterritorial authority by another state. Most forms have been established through bilateral and multilateral treaties, usually concerning extradition. In the Netherlands, for example, we have the case against a Dutch CEO with regard to a request from the United States to extradite the director of a Dutch multinational for an offense under the FCPA. It is not intended in this article to examine the subject of extradition and the double criminality requirement in detail. However, due to the specific importance of the FCPA for business in the Netherlands, it is sensible to devote attention to this specific point.

On February 1, 2001 the Dutch Criminal Code was amended with regard to the provisions of the ACC. The 'small print' in the Convention turns out in practice to have major consequences for Dutch business. These concern particularly relationships with the United States and their consequences on the basis of the FCPA. The FCPA dates from 1977 and has a limitation period of 12 years. As a result of

the ratification of the ACC[18] and the changes in the Dutch Criminal Code, *double criminality* has existed since February 1, 2001. The double criminality requirement is fulfilled in the extradition law between the Netherlands and the United States. In other words, the offense for which extradition is sought must be punishable in both states. This has applied since February 1, 2001. Extradition[19] is set out in Article 10 of the ACC.

Notably, this meant that up to 2013 Dutch businesses could still be prosecuted for corrupt acts committed with foreign public servants in the Netherlands or elsewhere and that the US could claim jurisdiction through a connection with the US. Surrender is possible, including with retrospective criminalization, because the prohibition of retroactive effect has expressly not been included in Dutch extradition law. This is understandable in itself, for example from the perspective of prosecuting war crimes in World War II. After all, the treaties that make war crimes punishable (the four Geneva Conventions) only came into being after the Second World War. Finally, if we look at the link between the corrupt act and the jurisdiction of the US, the OECD ACC states that 'the territorial basis for jurisdiction should be interpreted broadly so that an extensive physical connection to the bribery act is not required'.[20]

With regard to fines there is a long list, but recently, especially after the Yates Memorandum, attention is also given to the individual perpetrators.[21]

The following (incomplete) list gives an impression of the fines imposed in recent years as a result of a violation of the FCPA above USD 250 million:

- Siemens: USD 800 million (2008) (total of USD 1.6 billion in several related fines in this case);
- KBR/Halliburton: USD 579 million (2009);
- BAE: USD 400 million (2010);
- Snamprogetti/ENI: USD 338 million (2010);
- Technip SA: USD 338 million (2010);
- Daimler AG: USD 185 million (2010);
- Alcoa: USD 384 million (2014);
- Teva Pharmaceutical: USD 519 million (2016);
- Braskem S.A.: USD 957 million (2016);
- JPMorgan: USD 264 million (2016);
- VimpelCom: USD 795 million (2016).

Fines related to sanctions can exceed billions of US dollars.

In May 2013 the French energy giant Total SA, a huge multinational with significant legal resources, agreed to a USD 245 million settlement for breaches under US criminal law related to the payment of bribes to secure oil and gas contracts in Iran. Total's Chief Financial Officer seemed to stress the challenge to global companies of

18. Art. 9 (Mutual Legal Assistance) states: 'Where a Party makes mutual legal assistance conditional upon the existence of dual criminality, dual criminality shall be deemed to exist if the offence for which the assistance is sought is within the scope of this Convention.'
19. In principle, the Netherlands does not extradite its own nationals. The Dutch do not refer to the term 'extradition' but 'transfer' the suspect to be tried abroad.
20. Note 25 to the Convention. The notes are officially part of the Convention.
21. https://www.justice.gov/dag/file/769036/download.

monitoring such extra-jurisdictional risks when in the context of the fine he stated that the company had 'not committed any offence under applicable French law'.[22]

16.7 DRASTIC INCREASE IN EXTRATERRITORIAL RISK

Following the US example, the UK has significantly strengthened its territorial claim through the enforcement of the UKBA. The scope of the UKBA is wider than that of the FCPA. The UKBA prohibits not only the bribery of foreign public officials but *any* kind of bribery, including low-level 'facilitation payments' and intra-business bribery. To top it all off, the UKBA makes the absence of an effective anti-bribery compliance program a criminal offense. Breach of the law can lead to a prison sentence of up to ten years and an unlimited fine, and penalties can be imposed on both individuals and companies. It is not surprising that UK boards of directors are concerned – but to what extent are boards of non-UK firms aware of the risks they are running?

What is the effect of the UKBA on foreign companies? The UK courts clearly have jurisdiction over foreign companies if the crime took place within the territory of the UK, but they are also able to claim jurisdiction over foreign companies for crimes committed outside the UK in a number of situations. It is possible for a foreign company to be prosecuted for a failure to have adequate systems and controls in place to prevent bribery as long as the foreign company carries on a business, or part of a business, in any part of the UK. This can mean that having a subsidiary in the UK can trigger a UK prosecution for a non-UK company involved in corruption, even if the UK subsidiary was not involved in the act of bribery itself. In chapter 17 on Anti-Bribery and Corruption, the UKBA will be discussed in more detail.

16.8 DUAL-USE GOODS: THE SINK-HOLE IN THE COMPLIANCE STRUCTURE

In order to prevent the export of what might be termed strategic goods to countries at war, to unstable regions, to countries where human rights are violated, or to embargoed countries, the Member States of the EU and a number of other countries – the US among them – have signed a treaty, the so-called Wassenaar Arrangement, which places restrictions and license requirements on the trade in strategic goods, including clearly military and less obvious dual-use goods (for example chemicals used in the production of a detergent which can also be used for the production of chemical weapons – or metal tubes that can be used for civil engineering projects but also for gun turrets). The export control legislation of both the EU and Member States does not control the export of commercial (or civil) goods, however. Whether or not an item is an unrestricted commercial or civil product will depend on whether it is present on official Military or Dual Use Lists. The definition is further impacted by the nature of the purchasing party, such as military or government-owned customers, or so-called 'suspect' customers that might be considered dangerous

22. 'Total agrees penalty to settle US bribes charge over Iran deal' Financial Times May 29, 2013.

in countries that feature on various and differentiated United Nations, US, EU or related country embargo lists.

16.9 A TIME FOR COMPLIANCE TO LOOK OVER ITS SHOULDER

It would seem that a significant proportion of the international business community is blissfully unaware of the extraterritorial effect of American export control legislation. And not just US legislation, but also European and national export laws! There is no easy rule of thumb to guide companies on the risks they run in terms of the anti-corruption, anti-terror or export control legislation that carries extraterritorial risk; indeed the list of legislation that needs to be reviewed is ever-expanding. However, ignorance is no defense in the face of the law, and companies need to evaluate the extent to which their operations expose them to such risks. Screening for extraterritorial risk typically requires close collaboration between legal, compliance and front office departments to identify exposed business practices and export goods. Asking the question of whether your organization has potential concerns in this area is a price worth paying to avoid a surprising prosecution or extradition request from a third country in relation to a business activity commonly considered to be outside the scope of its jurisdictional reach. Compliance needs to be aware of the extraterritorial trap and an even more difficult task: compliance needs to sharply raise awareness among the executives of the organization while training its legal colleagues. In 2016 a company was fined due to the fact that the legal officer had never heard of extraterritorial jurisdiction and told compliance that it was sheer rubbish. Times are changing and compliance officers may well be held criminally responsible for non-compliance; the same fate awaits the executive officer. In January 2017 the executive officer in charge of Regulatory Compliance at Volkswagen in the US was arrested by the FBI.[23] This action is fully in accordance with the so-called Yates Memorandum, in which the Deputy Attorney General of the US, Sally Q. Yates, announced that alongside fines and other penalties, the responsible employees of companies should also be held criminally accountable for wrongdoings of the company. According to Mrs. Yates:

> 'the Department [of Justice of the US] fully leverages its resources to identify culpable individuals at all levels in corporate cases. To address these challenges, the Department convened a working group of senior attorneys from Department components and the United States Attorney community with significant experience in this area. The working group examined how the Department approaches corporate investigations, and identified areas in which it can amend its policies and practices in order to most effectively pursue the individuals responsible for corporate wrongs.'[24]

23. http://money.cnn.com/2017/01/09/news/companies/volkswagen-emissions-scandal-arrest.
24. Deputy Attorney Department of Justice, Yates Memorandum, https://www.justice.gov/dag/file/769036/download, p. 2.

BIBLIOGRAPHY

Bleker 2012
Dr. S.C. Bleker-van Eyk, 'Extraterritorialiteit: het meest onderschatte thema', in: C.A. Wielenga et al. (ed.), *Jaarboek Compliance* 2012, Capelle aan den IJssel: Nederlands Compliance Instituut 2012, pp. 51–67.

Bleker 2013
Dr. S.C. Bleker-van Eyk, 'The Extraterritorial Web', *Business Compliance*, 05/2013, pp. 53–61.

Brownlie 1990
I. Brownlie, *Principles of Public International Law*, New York: Oxford University Press 1990.

Klip & Massa 2010
A.H. Klip & A.S. Massa, *Communicerende grondslagen van extaterritoriale rechtsmacht*, Maastricht: Maastricht University 2010.

Sjöcrona & Orie 2002
J.M. Sjöcrona & A.M.M. Orie, *Internationaal strafrecht vanuit Nederlands perspectief*, Deventer: Kluwer 2002.

Van den Wyngaert 2009
C. van den Wyngaert, *Strafrecht & Strafprocesrecht in Hoofdlijnen*, Apeldoorn: Malku 2009.

Other references

Chazan 2013
G. Chazan, 'Total agrees penalty to settle US bribes charge over Iran deal', *Financial Times* May 29, 2013.

Smith & Perez 2017
A. Smith & E. Perez, 'Volkswagen executive arrested in emissions scandal', *CNN* 9 January 2017.

U.S. Department of Justice 2015
U.S. Department of Justice, Individual Accountability for Corporate Wrongdoing, September 9, 2015.

17. Anti-Bribery & Corruption

Prof. S.C. Bleker-van Eyk[1]

17.1 INTRODUCTION

At the heart of corruption lies what is natural to all men: reciprocity. Ever since the time of the cavemen, mankind has survived on 'returning a favor'. It lies at the core of survival within the tribe. It was the means of exchange before currency took over that task. The caveman who was good at hunting exchanged meat for bread. When a member of the tribe was unfit to hunt, he would still get the meat in order to get his strength back, which was a way of ensuring the survival of the tribe, for he would hunt when fit again and give meat to the ones who were then unfit to hunt but graciously gave him meat during his illness.

Reciprocity can easily slide towards corruption. The hunter promises extra meat to his fellow tribe member without exposing him to the danger of the hunt in return for allegiance when the time comes to select a leader. Because of the slippery slope into the gray zone, corruption has been persistent within all civilizations and throughout the centuries. The use of currency assists in setting a fair price for services rendered. However, currency is an asset that enables man to obtain all kind of goods and can enhance his welfare and hence his wellbeing and man is often inclined to pursue more welfare and as a result be more open to corruption. Evolution has shown that corruption cannot be erased from society. In fact, corruption is the cancer that constantly lurks within society and it is very difficult or almost impossible to eradicate it. Corruption is a threat to society. Corruption can kill, not only through the criminal act of killing, keeping dictators in power, but also through discarding safety measures when building, etc.

In our modern civilization, currency opens the possibility for better estimating the value of services and goods. Also, the media can easily reveal corruption. The cancer can only be treated through extraction. As a result, the effort is globally focused

1. The author would like to express her gratitude to Margriet De Smaele, who screened this publication against the latest laws and regulations. Margriet De Smaele taught me almost everything I know about US Export Controls.

on prohibiting corruption and only allowing 'facilitation payments' under stringent conditions. A worldwide quest to eradicate corruption is now well on its way, using enforcement with large penalties and incarceration as a deterrent.

17.2 BRIBERY, CORRUPTION AND DEFINITIONS

The first question to be dealt with when discussing corruption concerns the definitions of corruption and bribery. Bribery is 'the crime of giving money or other valuable things or rights to another as an inducement to him to act in a certain way, or to reward him for having so done. It is penalized by statute in various contexts, such as bribing judges, voters, members of local authorities or public officers'.[2] Corruption is 'the perversion of anything from its original pure state, used particularly of accepting money or other benefit in consideration of showing favor to or benefiting the donor'.[3] With regard to the efforts made by the OECD to combat corruption, the most effective definition is that given by Senturia: 'corruption is the *misuse* of *public* power for *private* profit.'[4] Corruption is on the 'receiving' side, whereas bribery is linked to the act of offering, giving or promising. However, much more is at stake. The actual acceptance is forbidden, but also the solicitation and the promise of a bribe. Also, the term 'bribe' is not as restricted as it may seem. Article 1(1) of the OECD Anti-Corruption Convention (ACC) defines corruption as follows: 'it is a criminal offence ... for any person intentionally to offer, promise or give any undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official, for that official or for a third party, in order that the official act or refrain from acting in relation to the performance of official duties, in order to obtain or retain business or other improper advantage in the conduct of international business.'[5] The ACC has been ratified by 41 states, six of which are not OECD Member States.[6]

Corruption has become a widespread disease affecting international business transactions. Bribery is one of the most common and troubling problems faced by international managers. They often deeply resent giving bribes and yet in some countries bribery appears to be a condition under which business transactions take place. It has become 'usual practice' in many countries and is a secondary source of illegal income for many a foreign public officer. Worse, in some less-developed countries, bribery or 'grease money' is the official's primary source of income. As President Clinton stated, corruption is 'inconsistent with democratic values, such as good governance and the rule of law. It is also contrary to the basic principles of fair competition and harmful to efforts to promote economic development'.[7]

2. Walker et al. 1980.
3. Walker et al. 1980.
4. Senturia 1993. *See also* Svensson, 2005, p. 20.
5. http://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf.
6. Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Czech Republic, Denmark, Estonia, Finland, France, Denmark, Germany, Greece, Hungary, Iceland, Ireland, Italy, Israel, Japan, Korea, Latvia, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.
7. W.J. Clinton, Statement by the President, November 10, 1998.

Even where law exists, managers face dilemmas as they try to do business abroad. Competitive pressures, the perception that 'everybody's doing it' and the idea that a practice may not be wrong because it is firmly rooted in local cultural values complicate moral decision-making. Where the latter is concerned, it is necessary to stress that there are limits to the respect for localized values.[8] Also, we have to keep in mind that the local custom can be in contradiction with the local values. The fact that in some parts of Eastern Europe or Africa corruption has become a fact of life does not imply that corruption is an Eastern European or African cultural value.

17.3 THE ACC

The FCPA will be discussed in the following section. However, it is important to refer to the FCPA at the beginning of the current section, because it became the impetus of US striving towards a more global approach to combating bribery and corruption. In 1977 the US was by far the most important Member State within the OECD and it still is. The US used its influence within the OECD to encourage its trading partners to prohibit bribery in international business transactions and to enact legislation similar to the US FCPA. Within the framework of the OECD, the concept of combating bribery began to take root. The Committee on International Investment and Multinational Enterprises (CIME) began to discuss the issue of bribery in international business transactions. This discussion was not new to CIME, because in the 1976 OECD Guidelines on Multinational Enterprises, a reference to the corruption of foreign officials and political parties was already discussed. The OECD Guidelines on Multinational Enterprises state that organizations should not render any bribe to a public officer or give (unless legally permissible) any contribution to political candidates, and should abstain from improper involvement in local political activities. It is obvious that organizations should not bribe any public servant or holder of public office. The Lockheed affair is a well-known example of bribery of national authorities of host states by Lockheed, in order to convince the holders of important public offices to recommend Lockheed aircraft to the national governments.

The illegitimate sphere surrounding the subject of bribery is obvious. Less apparent, but just as conspicuous, are the contributions paid to local political parties. It is evident that if organizations contribute considerable funds to local political parties, the parties may well become dependent on the organization's contributions and the party may be willing to render special services to the organization in order to obtain more funds.

It should be noted that these discussions stemmed from the fear of political involvement of large multinational organizations in the national political affairs of foreign states, which increased at the end of the 1960s and peaked in the 1970s. From the 1980s and 1990s the discussion focused on the prevention of corruption and the time was right to take important measures within the Western world, especially within the OECD. In 1994, the OECD Council adopted a general Recommendation on this issue and as a result the Working Group on Bribery in International Business Transactions was established. The main purpose of this Working Group is to develop a program of systematic follow-up to the 1994 Recommendation. In 1997 the 1994

8. Green 1994, p. 292.

Recommendation was reviewed.[9] This Recommendation reflects the broad approach the OECD has taken on the issue of combating corruption in international business transactions. As a result, an important step in the joining of forces against corruption was taken through the adoption of the ACC. That was in 1997, exactly twenty years after the FCPA.

The ACC focuses on the corruption of foreign officials. Article 4(1) a) gives the definition: 'foreign public official' as 'any person holding a legislative, administrative or judicial office of a foreign country, whether appointed or elected; any person exercising a public function for a foreign country, including for a public agency or public enterprise; and any official or agent of a public international organization'. An official does not have to be elected or be officially appointed. The crux lies in a person who legitimately represents the (national, municipal or other) governmental organizations. For instance, an architect representing the municipal authorities while negotiating building requirements with developers, construction or infrastructure companies is to be regarded as a public official. This brings us to quite an interesting reflection: what if the architect pretends to hold the required powers, but in fact is cunningly placing himself in the midst of the building process? Can a contractor be held responsible in case of bribery even though the architect has no official status? Legally this becomes an interesting question, because courts tend to grant him public stature, due to the fact that the municipality has not taken sufficient action against the architect by failing to state his lack of official capacity. The contractor can be prosecuted, but in this case there is also a civil claim on the part of the contractor against the municipality. The previous example shows that before doing business, due diligence is necessary. Below, in chapter 18 on Export Controls and Sanctions, attention will be devoted to the importance of third-party due diligence, which is equally important with regard to anti-bribery and corruption!

With regard to the prosecution of corruption, Article 4(3) of the ACC states: 'When more than one Party has jurisdiction over an alleged offence described in this Convention, the Parties involved shall, at the request of one of them, consult with a view to determining the most appropriate jurisdiction for prosecution.' That is understandable because every state in the world has some kind of anti-corruption legislation and the crime of corruption will almost always be punishable in the state of the public official as well as the state of the organization or individual carrying out the act of bribery. Hence, the question of extradition may arise. Article 10(1) of the ACC states: 'The bribery of a foreign public official shall be deemed to be included as an extraditable offence under the laws of the Parties and the extradition treaties between them.' Article 10(2) follows by declaring that 'If a Party which makes extradition conditional on the existence of an extradition treaty receives a request for extradition from another Party with which it has no extradition treaty, it may consider this Convention to be the legal basis for extradition in respect of the offence of bribery of a foreign public official.'

9. The text of the 1997 Recommendation of the Council on Combating Bribery in International Business Transactions has been inserted in section 10a.

17.4 THE FCPA

In the aftermath of the Watergate affair, the military coup in Chile[10] at the request of ITT, the Lockheed bribery scandal involving payments by US companies to public officials including in the Netherlands and Japan, there were political repercussions within those countries and the reputation of American companies was sullied throughout the world. In response, in 1977 under President Jimmy Carter, Congress passed the Foreign Corruptive Practices Act. Through this Act, the United States declared its policy that American companies should act ethically when bidding for foreign contracts and should act in accordance with the US policy of encouraging the development of democratic institutions and honest, transparent business practices.

The importance of the issue of corrupting foreign public officials has increased considerably since governmental influence and hence the impact of public officials on economic transactions has grown. The risk of corrupting a foreign official has become an issue of daily relevance on the grounds of:

- the globalization of the world economy resulting in transnational business; and
- the commercialization of public services, changing the role of public officials from mere bureaucrats to entrepreneurs.

Since the passage of the FCPA, US businesses have operated at a disadvantage relative to foreign competitors who have continued to pay bribes without fear of penalty. In his statement of November 10, 1998 accompanying the signature of the International Anti-Bribery and Fair Competition Act (S. 2375), President Clinton stated that ever since the 1977 FCPA:

> 'US businesses have faced criminal penalties if they engaged in business-related bribery of foreign public officials. Foreign competitors, however, did not have similar restrictions and could engage in this corrupt activity without fear of penalty. Moreover, some of our major trading partners have subsidized such activities by permitting tax deductions for bribes paid to foreign public officials. As a result, US companies have had to compete on an uneven playing field, resulting in losses of international contracts estimated at USD 30 billion per year.'
>
> After the approval of the FCPA, amending chapter 2*b* Securities Exchanges of Title 15 Commerce and Trade of the United States Code, the US began to lobby with a view to convincing its major trading competitors to pass similar national laws, leading to the ACC as mentioned in the previous paragraph.
>
> 15 US Code § 78dd-1 states as follows 'to make use of the mails or any means or instrumentality of interstate commerce corruptly in furtherance of an offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to –

10. United States House of Representatives, United States and Chile During the Allende Years, 1970–1973, Hearings before the Subcommittee on Foreign Affairs of the House of Representatives, US Government Printing Office, Washington 1975, pp. 405 *et seq.*

(1) any foreign official for purposes of –

(A)

(i) influencing any act or decision of such foreign official in his official capacity,

(ii) inducing such foreign official to do or omit to do any act in violation of the lawful duty of such official, or

(iii) securing any improper advantage; or

(B) inducing such foreign official to use his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality,

in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person;

(2) any foreign political party or official thereof or any candidate for foreign political office for purposes of –

(A)

(i) influencing any act or decision of such party, official, or candidate in its or his official capacity,

(ii) inducing such party, official, or candidate to do or omit to do an act in violation of the lawful duty of such party, official, or candidate, or

(iii) securing any improper advantage; or

(B) inducing such party, official, or candidate to use its or his influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality,

in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person; or

(3) any person, while knowing that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly, to any foreign official, to any foreign political party or official thereof, or to any candidate for foreign political office, for purposes of –

(A)

(i) influencing any act or decision of such foreign official, political party, party official, or candidate in his or its official capacity,

(ii) inducing such foreign official, political party, party official, or candidate to do or omit to do any act in violation of the lawful duty of such foreign official, political party, party official, or candidate, or

(iii) securing any improper advantage; or

(B) inducing such foreign official, political party, party official, or candidate to use his or its influence with a foreign government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality,

in order to assist such issuer in obtaining or retaining business for or with, or directing business to, any person.'

Finally, the FCPA provides an exception related to offers or payments to foreign officials (facilitation payments) provided in exchange for routine government action. The FCPA states that its anti-bribery prohibition 'shall not apply to any facilitating or expediting payment to a foreign official, political party, or party official the purpose of which is to expedite or secure the performance of a routine governmental action'. According to the FCPA a 'routine governmental action' is:

'an action which is ordinarily and commonly performed by a foreign official in – (i) obtaining permits, licenses, or other official documents to qualify a person to do business in a foreign country; (ii) processing governmental papers, such as visas and work orders; (iii) providing police protection, mail pick-up and delivery, or scheduling inspections associated with contract performance or inspections related to transit of goods across country; (iv) providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products or commodities from deterioration; or (v) actions of a similar nature'.

17.5 FCPA PROSECUTION AND COMPLIANCE

The FCPA enforcement lies with both the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC): the SEC has authority for civil enforcement of the FCPA over issuers and their officers, directors, employees, agents, and stockholders acting on the issuer's behalf. The SEC has a specialized FCPA unit with attorneys in Washington, D.C., and in regional offices.

In order for an action to constitute a violation of the FCPA, a payment must be made 'corruptly'. The perpetrator must have the intent to wrongfully influence the recipient. As a result, a violation may be possible even if no bribe was actually paid. Even if the identity of the recipient is unknown, or even if the company does not ultimately receive a benefit as a result of the payment, a violation takes place through the simple intent to commit an act of bribery. Also, the act must have been done 'willfully', which means that the person must act with a 'bad purpose' or knowledge that the conduct is unlawful, although this requirement is not so rigid that the person should know exactly which act he has violated. Note, however, that proof of willfulness is relevant only to violations by individuals; willfulness is not required to establish corporate criminal or civil liability!

According to Chapter Eight of the US Federal Sentencing Guidelines (USFSG),[11] 'the fine range for any other organization should be based on the seriousness of the offense and the culpability of the organization. The seriousness of the offense generally will be reflected by the greatest of the pecuniary gain, the pecuniary loss, or the amount in a guideline offense level fine table. Culpability generally will be determined by six factors that the sentencing court must consider. The four factors that increase the ultimate punishment of an organization are:

(i) the involvement in or tolerance of criminal activity;
(ii) the prior history of the organization;
(iii) the violation of an order; and
(iv) the obstruction of justice.

The two factors that mitigate the ultimate punishment of an organization are:

(i) the existence of an effective compliance and ethics program; and

11. United States Sentencing Commission, 2014 Federal Sentencing Guidelines Manual, the 2014 Guidelines Manual (effective November 1, 2014), Chapter Eight, Introductory Commentary, Principle III.

(ii) self-reporting, cooperation, or acceptance of responsibility.'

A Voluntary Self-Disclosure (VSD) can mitigate the harshness of possible penalties. In general, it is said that a VSD will reduce the penalty by 50%. However, it should be noted that this cannot be proved in practice. In most cases the negotiations end with the penalty reflecting the seriousness of the infraction and it is influenced by the maturity of the organization's compliance, the cooperation throughout the negotiations, the disciplinary actions taken against the violators within the organizations, criminal prosecution of individuals and, last but not least, the financial resources of the organization. This subject will also be touched on in the next chapter on export controls and sanctions.

As already discussed above in the introductory chapter on extraterritorial jurisdiction, since the Yates -Memorandum[12] it has become obvious that the penalties applied when sentencing are strongly influenced by the sanctions applied to the individual violators as well as the strong wish not only to inflict financial penalties, but also to prosecute individuals on all levels, including the executive level.

It is of importance that an organization also focuses on preventing measures. However, it should be kept in mind that where preventive measures combating bribery within an organization are concerned, the system can never be watertight. It is impossible to fully prevent such a crime. For instance, if an employee is very eager to obtain a promotion, he may be tempted to promise, offer or give a bribe with a view to obtaining a commission and hence impressing his superiors. A system must be developed to achieve the highest possible level of protection against corruptible practices. Through such a system, instances of bribery can be prevented or the system can be used in court as proof that the enterprise exercised due diligence in seeking to prevent and detect criminal conduct by its employees and other agents.

In Chapter Eight, §8B2.1 of the USFSG deals with the requirements of an effective compliance and ethics program, also described in the 2012 *Resource Guide* to the US Foreign Corrupt Practices Act.[13] According to the *Resource Guide* 'DOJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low risk area because greater attention and resources had been devoted to a higher risk area.'

Due to the importance of Article §8B2.1 of the USFSG on an 'effective compliance and ethics program' was also inserted in full *supra* in chapter 3.

In conclusion, the USFSG is looking for an effective program to prevent and detect violations of law. In the event of a violation, the organization should be able to redress it swiftly and effectively. This program must be reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct. Effectiveness should be seen in connection with the principle of due diligence.

A good compliance system can prevent instances of bribery. However, if bribery does occur, it can be detected by and mitigated through compliance structures. In

12. https://www.justice.gov/dag/file/769036/download.
13. Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act, 2012.

the worst-case scenario, the act of bribery may be prosecuted. In the latter case, the existence of an effective compliance system can serve as mitigating circumstances to the defense leading to a reduction of sentence. With regard to affirmative defenses, the FCPA only offers two distinct defenses:

- if the organizations can provide proof that the act is a lawful payment under local written laws; or
- if the organization can prove that the money spent was reasonable, *bona fide*, and directly related to the performance of a contract, or marketing, promotion, or product demonstration.

Finally, in the 'Principles of Federal Prosecution of Business Organizations'[14] the *US Attorney's Manual* reflects upon the

> 'Duties of Federal Prosecutors and Duties of Corporate Leaders. Corporate directors and officers owe a fiduciary duty to a corporation's shareholders (the corporation's true owners) and they owe duties of honest dealing to the investing public and consumers in connection with the corporation's regulatory filings and public statements. A prosecutor's duty to enforce the law requires the investigation and prosecution of criminal wrongdoing if it is discovered. In carrying out this mission with the diligence and resolve necessary to vindicate the important public interests discussed above, prosecutors should be mindful of the common cause we share with responsible corporate leaders who seek to promote trust and confidence. Indicting corporations for wrongdoing enables the government to be a force for positive change of corporate culture, and a force to prevent, discover, and punish serious crimes.'

New in November 2015 is Chapter 9-28.010 stating that 'the prosecution of corporate crime is a high priority for the Department of Justice. By investigating allegations of wrongdoing and bringing charges where appropriate for criminal misconduct, the Department promotes critical public interests. These interests include, among other things: (1) protecting the integrity of our economic and capital markets by enforcing the rule of law; (2) protecting consumers, investors, and business entities against competitors who gain unfair advantage by violating the law; (3) preventing violations of environmental laws; and (4) discouraging business practices that would permit or promote unlawful conduct at the expense of the public interest.' According to the *US Attorney's Manual*

> 'one of the most effective ways to combat corporate misconduct is by holding accountable all individuals who engage in wrongdoing. Such accountability deters future illegal activity, incentivizes changes in corporate behavior, ensures that the proper parties are held responsible for their actions, and promotes the public's confidence in our justice system. Prosecutors should focus on wrongdoing by individuals from the very beginning of any investigation of corporate misconduct. By focusing on building cases against individual wrongdoers, we accomplish multiple goals. First, we increase our ability to identify the full extent

14. United States Department of Justice, Offices of the United States Attorneys, *US Attorney's Manual*, Title 9, Chapter 9-28.000 'Principles of Federal Prosecution of Business Organizations', revised November 2015.

> of corporate misconduct. Because a corporation only acts through individuals, investigating the conduct of individuals is the most efficient and effective way to determine the facts and the extent of any corporate misconduct. Secondly, a focus on individuals increases the likelihood that those with knowledge of the corporate misconduct will be identified and provide information about the individuals involved, at any level of an organization. Thirdly, we maximize the likelihood that the final resolution will include charges against culpable individuals and not just the corporation.'

In Chapter 9-28.210 the focus is once again on the individual wrongdoers. It states that the

> 'prosecution of a corporation is not a substitute for the prosecution of criminally culpable individuals within or without the corporation. Because a corporation can act only through individuals, imposition of individual criminal liability may provide the strongest deterrent against future corporate wrongdoing. Provable individual culpability should be pursued, particularly if it relates to high-level corporate officers, even in the face of an offer of a corporate guilty plea or some other disposition of the charges against the corporation, including a deferred prosecution or non-prosecution agreement, or a civil resolution. In other words, regardless of the ultimate corporate disposition, a separate evaluation must be made with respect to potentially liable individuals. Prosecutors should not allow delays in the corporate investigation to undermine the Department's ability to pursue potentially culpable individuals.'

The latter will happen when a foreign company is negotiating a plea bargain with the DOJ, while in the meantime trying to dismiss personnel that committed the violations and hence losing their ability to force employees to cooperate with the company during the investigation.

The addition and revision of the US Attorney's Manual in 2015 are the precursors of the 2016 Yates Memorandum emphasizing the importance of prosecuting individuals.

17.6 THE UKBA

The UKBA is a pivotal point in the effort to combat bribery and corruption. Not only because the United Kingdom has decided to follow the example of the US in claiming extraterritorial jurisdiction, but because it goes far beyond the corruption of foreign officials. The UKBA forbids any kind of corruption, be it the corruption of officials (foreign or national) or intra-business bribery. The scope of the UKBA is much wider than that of the FCPA and in addition to the bribery of a public official it also contains the following offenses:

- Section 1: offering, giving or promising to give a 'financial or other advantage' to another individual in exchange for 'improperly' performing a 'relevant function or activity' (active);
- Section 2: being bribed: requesting, accepting or agreeing to accept such an advantage, in exchange for improperly performing such a function or activity (passive);

- Section 6: promising, offering or giving a financial or other advantage to a foreign public official, either directly or through a third party, where such an advantage is not legitimately due;
- Section 7: the broad and innovatory offense of the failure of commercial organizations to prevent bribery on their behalf;
- Section 14: criminalizing those senior officers of the organization with whose 'consent or connivance' the bribery was committed (although where the bribery takes place overseas, they must have a 'close connection with the UK').

Also, so-called 'facilitation payments' are fully banned. The FCPA leaves room for small facilitation payments. By contrast, the UKBA allows no such payments, however small they may be.

Section 7 is quite remarkable, because unlike the US legislation it does not offer a reduction of penalties in the case of an effective compliance and ethics program; the mere absence of an effective compliance program is a criminal offense.

The penalties are harsh and bribery can lead to a sentence of up to ten years and an unlimited fine, both for the individual and the company.

The UK court claims jurisdiction when bribery has taken place within the territory of the United Kingdom, but also if the offense was committed outside the UK. The offense can be prosecuted within the UK in the case of a foreign company having:

- a subsidiary or a representative in the UK;
- a British citizen as an employee who is involved in an act of bribery or a British citizen in a management position who knows or should have known about the fact;
- a listing on the London Stock Exchange;
- an organization with agents/representatives in the UK;
- (important) activities in the field of sales & marketing in the UK.

The effect of the UKBA on foreign organizations is not yet fully clear. The Serious Fraud Office (SFO) has only recently started prosecutions and the British courts still have to start creating case-law further explaining the international realm of the UKBA. The requirements for a good defense under the UKBA still have to be set in practice. The minimum requirements for an effective compliance program under the UKBA will at least encompass elements such as:[15]

- risk assessment;
- top level commitment;
- due diligence;
- clear, practical & accessible policies & procedures;
- effective implementation;
- monitoring and review.

15. Jonathan Cotton, partner at Slaughter & May, during a corruption seminar at De Brauw Blackstone Westbroek, Amsterdam, January 25, 2011.

In the 'Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing', the SFO states six Principles regarding procedures that organizations should have in place:[16]

> '1. A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities. They are also clear, practical, accessible, effectively implemented and enforced.
>
> 2. The top-level management of a commercial organisation (be it a board of directors, the owners or any other equivalent body or person) are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable.
>
> 3. The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented.
>
> 4. The commercial organisation applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery risks.
>
> 5. The commercial organisation seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training that is proportionate to the risks it faces.
>
> 6. The commercial organisation monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.'

Regarding Principle 1, the SFO gives an indication of possible procedures that organizations should have in place in order to prevent bribery:

> '– The involvement of the organisation's top-level management (see Principle 2).
> – Risk assessment procedures (see Principle 3).
> – Due diligence of existing or prospective associated persons (see Principle 4).
> – The provision of gifts, hospitality and promotional expenditure; charitable and political donations; or demands for facilitation payments.
> – Direct and indirect employment, including recruitment, terms and conditions, disciplinary action and remuneration.
> – Governance of business relationships with all other associated persons including pre and post contractual agreements.
> – Financial and commercial controls such as adequate bookkeeping, auditing and approval of expenditure.
> – Transparency of transactions and disclosure of information.

16. Ministry of Justice, The Bribery Act 2010, Guidance about procedures which relevant commercial organizations can put into place to prevent persons associated with them from bribing, March 2011.

> – Decision-making, such as delegation of authority procedures, separation of functions and the avoidance of conflicts of interest.
> – Enforcement, detailing discipline processes and sanctions for breaches of the organisation's anti-bribery rules.
> – The reporting of bribery including "speak up" or "whistle blowing" procedures.
> – The detail of the process by which the organisation plans to implement its bribery prevention procedures, for example, how its policy will be applied to individual projects and to different parts of the organisation.
> – The communication of the organisation's policies and procedures, and training in their application (see Principle 5).
> – The monitoring, review and evaluation of bribery prevention procedures (see Principle 6).'

Is it an offence?	FCPA	UK Bribery Act
Bribery of FPOs	Yes	Yes
Domestic bribery	No	Yes
Private sector bribery	No	Yes
Facilitation payments	No	Yes
Strict liability	No	Yes
Failure to keep accurate records	Yes	No
Liability for acts of third parties	Yes	Yes

Figure 1: showing the offenses under the FCPA and the UKBA

17.7 CONCLUSION

In conclusion we can safely state that the UKBA has taken combating bribery and corruption to a new level. Only time will tell what the impact of the UK's extraterritorial jurisdiction will be. Time has already taught us that the extraterritorial claim made by the US has been very successful and the financial penalties for foreign companies have been enormous. Many companies have paid hundreds of millions of US dollars in fines.