CB Compliance-Berater
Beihefter zu Heft 1–2/2017

Compliance Across Europe

Cross Cultural Compliance, Vol. 1
Viadrina Compliance Center
European University Viadrina Frankfurt (Oder)
4th Viadrina Compliance Congress, 6th – 7th July 2016

Prof. Dr. Bartosz Makowicz (ed.)

Table of contents

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Preface

Dear Readers!

In their daily work, compliance officers encounter substantial challenges, whether convincing the executive board of the need to implement a compliance management system or ensuring that compliance does not become unpopular with other team members. Also, considering that a compliance officer usually has limited resources, and that neither legislation nor risk shows any sign of diminishing, one thing becomes clear: the job of a compliance officer is never easy!

The development of compliance is being accompanied by various conferences, contributions to specialist journals, dissertations and other research projects. However, nothing is more valuable than the broader exchange, namely, an international perspective and a comparison of the compliance know-how that colleagues have gained abroad. Whatever the legal regime: they must still recognize risks and address them appropriately thereby ensuring that a sustainable compliance culture is established within their organization.

This was one of the reasons why we decided to internationalize the annual Viadrina Compliance Congress, which was organized by the Viadrina Compliance Center and the Compliance Academy and whose strategic partners this year included the Viadrina Center "B/Orders In Motion". From the 6th to the 7th of July 2016, some 25 speakers from 15 European countries (including Belgium, Germany, France, UK, Ireland, Poland, Austria, Romania, Russia, Switzerland, Spain, Sweden and the Adriatic region) as well as organizations such as the OECD and GIZ met at the European University Viadrina in Frankfurt (Oder) for the 4th Viadrina Compliance Congress entitled "Compliance Across Europe". During the congress, they discussed the latest developments, shared their know-how and exchanged experiences in the field of cross-border compliance management.

This leads to another reason for the Viadrina Compliance Congress: for two years now, the Viadrina Compliance Center has been working on a research project that asks how global organizational structures (whether of multinational or global organizations) can implement compliance standards by taking socio-cultural differences in different countries into consideration. The concept of "Cross Cultural Compliance" (which was developed for this purpose), seeks to ascertain whether any of the known compliance measures are capable of functioning in different cultures. For example, some cultures tend to be more team-oriented and are therefore less receptive to unilateral rule enforcement. As with regions where other value systems exist, sufficient attention must be paid to such traits if a compliance management system is going to be equally effective in different regions.

Two days were clearly not enough to cover all the topics in detail. We have therefore concentrated on the essentials. The topics in this compendium were discussed by several panels, according to theme, and rounded off by two keynote speeches. The panelists represented business, science and public authorities from various European states. They brought their own unique perspectives to bear on the following topics: general challenges for compliance in Europe, cross-border compliance culture and governance, cross-border anti-corruption programs, cross-border compliance standardization and whistleblowing challenges.

We are very pleased that the conference has succeeded in stimulating a European dialogue on compliance. We are even happier, however, to present you the results of the conference in the form of individual contributions by the speakers collected in this compendium. We very much hope to have contributed not only to the European discussion on compliance but, equally, to have created a platform for European and international exchange that will help compliance officers to master the challenges of daily compliance in the long term.

The project continues. In January 2017, the Viadrina Compliance Center in co-operation with the Center for Public Policy and Good Governance at the Thammasat University in Bangkok hosted the conference "Compliance Across Asia"; meanwhile, the 5th Viadrina Compliance Congress will be held in Münster under the title "Compliance Across the Globe" in Germany. In this way, we wish to promote the internationalization of the exchange platform and broaden the valuable discussion between compliance officers and those who are interested in the development of compliance. By that the job of compliance officers might not get easier, but for sure more effective.

On behalf of the event organizers (Viadrina Compliance Center and Compliance Academy Münster), I would like to extend very warm thanks to the partners of the 4th Viadrina Compliance Congress (Viadrina Center B/Orders In Motion, Deutsches Institut für Compliance, Warsaw Stock Exchange, Deutsche Gesellschaft für Internationale Zusammenarbeit, Alliance for Integrity, Institut Compliance), sponsors (idox compliance, CMS Hasche Sigle, FGH Automobil GmbH) and media partners (Berufsverband der Compliance Officer, Bundesanzeiger Verlag, COMPLY, Compliance Berater, LexisNexis, Compliance Insider, ZRFC) as well as the City of Frankfurt (Oder) for its patronage and the great team for their hard work!

I wish you fruitful reading and look forward to welcoming you to the 5th Viadrina Compliance Congress "Compliance Across the Globe" in July 2017.

Prof. Dr. Bartosz Makowicz
Viadrina Compliance Center

Chapter 1: Challenges for Compliance in Europe

Prospects of success: making Compliance attractive

Dr. Rainer Markfort*

The 4th Viadrina Compliance Congress brings together experts from many different countries to discuss ideas on what the future of compliance will bring and what we can do to contribute to its development in our communities. Before looking ahead, we should start with an analysis of the status quo even though, at first glance, this may not seem very encouraging. By gaining a clear view of where we come from, we can better understand the deficiencies we encounter today (1.). Today, numerous business and social factors are driving the need for a more sophisticated approach to compliance. We must be patient as this evolution will take time (2.). However, only through our own initiative and commitment will we ensure the prospects of success for compliance in the future (3.)

I. Where does compliance stand today?

In Germany, compliance first emerged in 2005. Before then, no one had heard the word "compliance" except bankers and doctors. Daimler then became the subject of investigation by the US Department of Justice (DOJ) and the Stock Exchange Commission (SEC). One year later, the same happened to Siemens and since then a similar fate has befallen a series of large and small companies. Scandal after scandal followed and there were times when almost every day the newspapers were reporting about corruption, fraud, breach of antitrust regulations, manipulation of interest rates and other economic crimes taking place within many respected companies. Shockwaves rippled through the German Automobile Club ADAC (by far the largest NGO in Germany in terms of members) when manipulations of inquiries and fraud came to light. The same happened to FIFA, the only difference being that many had harbored suspicions regarding FIFA officials whereas the German Automobile Club was a somewhat 'holy' institution.

The amounts that corporations were paying in penalties consistently increased and society became used to reading about fines in the billions being imposed. At the same time, the reputation of these corporations were destroyed. Once upon a time, the name "Deutsche Bank" was synonymous with strength and glory. But what is left now?

A whole industry is constantly demonstrating what happens when compliance merely means applying the rules set by the regulator. The banking sector claims that it has practiced compliance for over 20 years. However, a closer look shows that this is only true in specific areas. Some of the biggest scandals in the past, which led to enormous penalties, have occurred in banks. So it appears there has been no value-based compliance for a long time and this may still be true today.

Today, many of Germany's large corporations have established compliance organisations, appointed compliance officers, implemented anti-corruption and anti-trust policies and trained their employees accordingly. Some of them did so after they experienced corruption and other criminal scandals and were forced to act owing to the pressure of investigative authorities and the public debate. Astute companies were quick to take these measures in order to avoid such situations.

After the initial phase of corporations tackling compliance, a big German corporation was repeatedly fined for breaching anti-trust rules. It responded by implementing a state-of-the-art Compliance Management System. This was one of the first tested by external auditors according to IDW PS 980, a newly developed standard. The accountants certified the Compliance Management System as being adequate, implemented, and effective. It may therefore be surprising to learn that this same corporation was again subjected to high fines owing to a new breach of anti-trust rules! How could this happen? Then it was announced that the board member responsible for legal matters and compliance had to quit his job for a personal breach of the compliance rules. This case clearly demonstrates that compliance requires more than policies and procedures. It does appear surprising that compliance scandals happen again and again. Did the compliance function fail to achieve its aims? Were there deficiencies in the company's policies or training? In view of these examples, we may have to admit that compliance is still in its infancy and, in this sense, needs time to develop.

II. Does compliance have a future?

Quite a few people are of the opinion that compliance is just hype and that it will fade away. The burden of compliance bureaucracy could endanger and challenge a company's competitiveness. Some argue that, in most countries of the world, business does not work without bribes and it is not the company's responsibility to make the world a better place to live.

A keynote speaker is not a prophet but he may dare a prognosis: Compliance has a future and will not vanish! The reason is that, today, compliance is no longer simply an issue between the authorities on the one hand and corporations on the other. Compliance is far more than this because public opinion has changed dramatically in the past years.

Twenty years ago, tax fraud was viewed as a trivial offence. Bribery and corruption, especially in foreign countries, was a legitimate means of obtaining business. In Germany and other countries bribes were even tax deductible. The biggest mistake in breaking anti-trust rules was to be seen to have been caught. Today, this is different: penalties and damages have increased as has the pressure resulting from investigations. Most of all, however, the corporation's reputation suffers to such an extent that it influences the value of products and the company as a whole. Here, we see that public opinion has a really dramatic impact which leads to change. Back in the 70s or 80s, the laws for the protection of the environment were tightened with the support of a strong social movement. At that time, a breach of environmental laws was viewed as a trivial offence, at least within the business community. Some entrepreneurs ignored the stricter rules and argued that following these rules would endanger their business and that they were responsible for creating jobs in society. Today, nobody would dare to suggest that environmental crime is a trifling affair.

One can therefore predict that compliance will undergo a comparable evolution and, for this reason, has a future. How long will it take? Probably one generation of managers. Recently, a study showed that managers' business attitudes are mainly influenced by their experiences during their first years in business. This finding may not be all that surprising. However, it does show that we must be patient: it may be difficult to convince today's director that corruption is evil. When this director was a young sales person early in his career, he might have used petty cash to obtain business. However, a young business person today, who has gained his first business experience against the backdrop of compliance scandals and internal investigations, will certainly have a different attitude when he becomes a manager or director.

III. How can we improve the prospects of compliance?

Compliance must become attractive! Compliance must add value to those who run the business and make profits for their company. Compliance should support and promote business and not hinder it. However, compliance is still rarely viewed in this way. Today, most managers understand that they may be held liable for the misconduct of their employees. However, they may still claim that in foreign markets they could lose business to competitors who are less rigorous with regard to compliance. Sales persons and people from procurement departments are unhappy about the amount of training and e-learning. They are annoyed and frustrated about having to check company policies on gifts and hospitality when they want to invite a business partner for lunch. They blame compliance for the bureaucratic hurdles they have to overcome before they can start business with a new partner. So what can we do?

Let's look at the example of third party checks, often referred to as "Business Partner Due Diligence". For business, the integrity check is not the most important thing when starting a new relationship. For people on the front line, it is more important to understand whether a new business partner will be able to deliver quality and whether he has good financial standing so that he might survive a longer business relationship or a challenging project. Now, if the Compliance Department were able to provide exactly this information at this very early stage (i.e. immediately after the first contact has been made), all stakeholders would be fine. The company's decision-makers would have relevant information available for their business decisions and the Compliance Department would be involved at a very early stage and might be in a position to check for potential risks. Business and compliance working hand-in-hand are much better at supporting compliance than policies and controls.

When management takes compliance seriously and entrepreneurial decisions are guided by values then compliance can be a useful tool for good leadership. People are much more creative, effective and, ultimately, productive when they work in an environment that reflects their own values and principles. A management that uses compliance as a leadership tool need not fear liability owing to their employees breaking the law.

* *Dr. Rainer Markfort* is a corporate partner in the Berlin office of Dentons. He focusses on advising corporations in critical situations. Dr. Markfort is also a member of the board of DICO – German Institute for Compliance and heads the working group on business partner compliance.

Finally, compliance will support competition. Brand, reputation, sustainability and corporate social responsibility are becoming increasingly important as they represent a substantial part of the added value of a product. In such an economic environment, compliance is a competitive advantage. In today's world, a product or company's value will, to a certain extent, be determined by good compliance. However, writing down a set of core values won't be enough. What we need (as in all other areas of business), is specific implementation, best practice, and support. At the same time, not every company has to reinvent the wheel. The wider stakeholders in the economy should come together to establish common rules for good business.
This was exactly the idea and goal when, in November 2012, German corporations, university professors, accounting and law firms took the initiative and founded the German Institute for Compliance, DICO. Today, DICO has more than 200 members, more than half of which are corporations from all sectors and industries. Over 200 individuals are personally engaged in six committees and 11 working groups. They discuss and develop guidelines, working papers and training materials on various topics such as business partner compliance, internal investigations, qualifications, compliance certificates and quality management. Other working groups cover healthcare compliance, data privacy, anti-trust and export control. They formulate opinions and develop proposals for legal initiatives. By this means, DICO protects the stakeholder interests to avoid bureaucratic and excessive laws and regulations. On the other hand, DICO members can rely on proposals and models that they have developed collaboratively. This is the best way to ensure compliance. We are taking the initiative, developing our own ideas and not waiting for the legislator to intervene. Let us take compliance into our own hands, work together to further its development and improve compliance's prospects of success in the future.

Some Challenges for Cross-Border Compliance across Europe

Pierre-Antoine Badoz*

Orange is a telecom operator and services provider formerly known as "France Telecom", the French incumbent. Since its creation, it has widely expanded geographically and now has a large international footprint. In Europe, it provides mass market telecom services in France, Belgium, Luxembourg, Moldova, Poland, Romania, Slovakia and Spain. In Africa and the Middle East, it offers services for mass market customers in 21 countries from Egypt to Ivory Coast, Jordan, Madagascar, Morocco and Senegal, to name but a few. Orange also provides telecom services for business customers in more than 200 countries and territories through its Orange Business Services subsidiary: cross-border issues are a daily challenge at Orange! Orange revenues totalled € 40 billion in 2015 with 156 thousand employees serving more than 252 million customers worldwide; 16 million of them are using "Orange Money", a mobile wallet service. Orange strategy focuses on the quality of networks and services and reasserts Orange's international ambitions in Europe and MEA countries as well as its commitment to continued expansion in mobile financial services and "connected objects".
Looking at Orange's strategy and assets through the "lens of compliance" makes one realise that each of them involves specific ethics or compliance risks and challenges. Orange strategy is supported by business development and M&A activities with potentially "non-fully compliant" targets in countries which are not necessarily Transparency International's leaders (according to its "Corruption Perception Index"). In addition, Orange's expansion in the internet of things and mobile financial services may lead to personal data protection and security issues or banking compliance challenges with the focus on anti-money laundering and counter-financing terrorism (AML/CFT). The Orange brand needs to be protected against reputational risks while stakeholders' trust in its ethical values must be continuously reinforced along with the awareness of every Orange employee in sharing, promoting and acting in accordance with these values. Other "must haves" are training employees whose activities may expose them to corruption risks, knowing every customer as required by both banking and telecom regulations and making proper due diligence vis-à-vis intermediaries and partners.
Last but not least, its international footprint exposes Orange to an ever increasing number of national and international laws and regulations involving corruption, sanctions, anti-trust, privacy, technical requirements, tax, environmental issues, etc. It also exposes Orange to differences in "cultural approaches to the rule of law".
Recently, various compliance issues concerning the telecom sectors have arisen, examples of which are listed below:

- Vimpelcom, the Russian operator is a subsidiary of Telenor, the Norwegian incumbent, which is listed on NASDAQ and registered in the Netherlands. In February 2016, it was fined $795 million for having paid a $114 million bribe to an Uzbekistani public agent in order to obtain its mobile license in Uzbekistan.
- A source reported that this action was "*a precursor for a much larger settlement coming down the line with TeliaSonera*" as Telia, the Swedish and Finnish incumbent, faces investigations by the US Department of Justice and Swedish prosecutors. It announced its withdrawal from all central Asian countries and suffered the dismissal of its CEO, CFO, legal director and several other top managers.
- Meanwhile, the American judiciary is working overtime with more than 80 ongoing FCPA investigations, five of which concern telecom operators or suppliers.
- In addition, the US is pragmatically investing part of the fines in recruiting FCPA prosecutors and FBI agents. In 2015, it also rewarded whistleblowers with more than $ 54 million. In the same year, Ms Yates, Deputy Attorney-General of the DoJ wrote a famous memo requesting American prosecutors to focus their efforts on the personal liability of managers.
- MTN, the South African telecom giant, was recently fined the equivalent of $ 5 billion and recently reached agreement with Nigerian authorities to pay close to $ 1.7 billion for "missing a deadline to disconnect unregistered customers".

These examples show that compliance is indeed a very hot topic in telecoms! At Orange, we therefore deployed a comprehensive compliance programme back in 2012, leveraging our previous anti-fraud and anti-corruption programmes. We used a "classical" 6-step approach to comply with the requirements of various guidelines (including the FCPA and the UKBA). Each of these steps (tone at the top, governance, risk analysis, policies & procedures, awareness & training, controls) raises very practical issues when deployed across our footprint. Let's take the example of step 1 "tone from the top": to start with, there is the very practical language issue as 6 different languages (Flemish, French, Polish, Slovak, Spanish and Romanian) are spoken within our European Business-to-Customer footprint. This number more than doubles within our European Business-to-Business footprint and more than doubles once again within our worldwide footprint where many employees speak neither French nor English. There is also the important issue of the person who carries the message: should it be the local CEO, the Division Executive Committee member or our Group CEO? The answer is not obvious, as the impact of the message is not necessarily commensurate with the speaker's position within the organisation as the following example shows.
At the end of 2015, our CEO and every ExCom member signed a short message renewing our Group's commitment of "zero tolerance towards corruption". This message was then sent to every manager in our Group, both in France and abroad (over 14,000 to be precise). When travelling and asking managers about this message, I discovered that not all of them outside France remembered having received it (contrary to the situation in France). After discussing this finding, one of our Chief Compliance Officers decided to duplicate the initiative within her local organisation. A similar commitment was then signed by the country CEO and local management committee and subsequently disseminated through the organisation with positive feedback and very high recognition ratio.
Governance is key for Compliance and sometimes full of tricky issues such as:

- Controlled entities and minority shareholders: owing to their position, minority shareholders must sometimes show strong conviction and marshall excellent arguments to increase local management's and other shareholders' awareness of compliance risks and convince them to deploy a robust and effective compliance programme.
- M&A and cultural misunderstanding: telcos, and especially incumbents, tend to have a strong corporate culture with centralised management which may conflict with one another or with the less structured new entrants.

Risks obviously depend on the country Orange operates in: the Customer Perception Index ranking of Orange European countries of operation ranks from 10 in Luxembourg to 103 in Moldova, not to mention some of our African or Middle-Eastern operations which hover around the bottom of Transparency International's ranking. Resources, due diligence, training, communication,

* *Pierre-Antoine Badoz*, Chief Compliance Officer – Orange.

every aspect of our compliance programme needs to be adequately adapted to the country in question – and to our local business. Adequate adaptation is essential: having insufficient controls in a difficult and complex environment is obviously problematic but having an overly strict and burdensome programme in a low risk environment would also be counterproductive. This will be the case if the procedure appears too complex or if operational staff does not understand why strict due diligence and training is necessary. This situation runs the risk that the procedure will not be followed adequately. Complaints may also be made about the time, resources and ultimately money being wasted on an apparently useless bureaucratic procedure, thereby undermining the support of management which is essential for compliance.
Policy and procedures: this is really where we need group policies but also local procedures to make sure that they are effectively enforced. I will illustrate my point with 2 examples. The first one concerns whistleblowing, which is an extremely sensitive issue in some countries (e.g. Belgium and France) owing to the fact that it is widely seen as denunciation. Accordingly, we rely not only on the alert mechanism but also on our networks of HR advisors, ethics advisors and compliance officers, respected employees or managers that people trust and are prepared to rely on for alerts.

The second issue concerns the procedures to enforce our gift and entertainment policy, which has to be adapted to the local culture. At Orange Poland, for instance, the management developed a clever solution to respect the cultural habit of significant business gifts during Christmas and New Year season whilst remaining compliant with our group's gift policy. The solution is that every top manager of Orange Poland has to give up the external gifts he or she receives in December and January. The resulting "pool of gifts" is then donated to an NGO through the Orange foundation in a widely publicised event. This effective solution is now publicised within the Group as it may also work as efficiently and positively in other operations. Finally, controls are essential to measure the effectiveness of compliance programmes and should be deployed adequately throughout the organisation. The only thing that may vary geographically is the level of resources needed to enforce them!
In conclusion, I would like to share two strong convictions: the first one is that compliance, more than any other business issue, is a domain where we should think globally and act locally. The second one is that being an ethical and compliant company is not only a winning formula in managing risks but is also becoming an increasingly important competitive advantage.

Chapter 2: Cross Border Compliance Culture and Governance

The Nordic Model of Governance

Helena Sjöholm*

The article highlights how the Nordic model of corporate governance reinforces ethics and compliance and the role and responsibility of the Nordic boards in these issues. It ends with a personal reflection on how the boards can reinforce good governance by their working procedures.
The article is written for a panel debate on cross border compliance culture and governance, with the aim of reflecting on socio cultural differences in the implementation of compliance and governance structures. The author has been asked to focus on the role of the boards for compliance and ethics from a Swedish perspective.

I. Good governance creates values

According to an analysis published by Boston Consulting Group at the beginning of June 2016, Nordic governance creates values. The analysis concludes that the success of Nordic companies is attributable to a unique governance structure[1].
This raises two questions:
- What characterises the Nordic model of corporate governance?
- What role and responsibilities does it gives to the Nordic board for securing good governance and compliance?

II. The role of the boards for compliance and ethics

The Nordic model of corporate governance gives the board a far-reaching responsibility to ensure that the organisation's working procedures are compliant and ethical. According to the Swedish Code on Corporate Governance (provision 3.1), the boards shall:
- define appropriate guidelines to govern the company's conduct in society, with the aim of ensuring its long-term value creation capability
- ensure that there is a satisfactory process for monitoring the company's compliance with laws and other regulations relevant to the company's operations, as well as the application of internal guidelines

The responsibility has also been stressed in the latest revision of the *Guidelines on Good Governance by The Swedish Academy of Board Directors* (2014). Many boards fulfil their responsibility by means of written guidelines, internal control reports and whistleblower systems. Many boards within the private and public sectors as well as Parliament have codes of conduct and there is an understanding that dealing with these questions properly will benefit the organisation and avoid costs in the form of trust, trademark or trial costs. Since 2010, all state-owned companies are to submit a GRI-report at the annual general meeting. Many companies have implemented procedures and allocated functions for monitoring compliance. Most board evaluations also ensure that the board members are satisfied with the internal control and ethical regulation and the extent to which processes are considered optimal. However, responsibility for compliance and ethics is not just limited to the board. The Nordic corporate governance model also gives the auditors, CEO and the shareholders a role to play in ensuring good governance, ethics and compliance. Therefore, it is worth taking a closer look at the Nordic model of corporate governance and how it supports compliance and ethics.

III. Roles and responsibilities in the Nordic governance model

Like other jurisdictions, the Nordic Companies Act stipulates that companies must have three decision-making bodies (the shareholder meeting, board of directors and CEO), and one controlling body (an auditor). However, their role and function differ in comparison with other international models of corporate governance[2].

1. The shareholders' meeting

The *shareholders' meeting* is the highest decision-making body. Theoretically, it can make all decisions in the company that are not, by law, a matter for another corporate body. Active and responsible ownership is fundamental to the Nordic model of governance. Although the law does not contain a legal obligation for shareholders to attend the shareholders' meeting and express their opinions, society takes the view that the owners should be involved by following the development of the organisation, expressing their opinion and expectations on the future development of the organisation and imposing ethical restrictions by decision at the shareholders' meeting. To further reinforce the owner's ability to ensure that the organisation is well-governed, the Nordic model stipulates that the board members are to be elected at the shareholders' meeting. A shareholders' meeting can also dismiss the board members without explanation at any time. In other words, if the shareholders consider that the board is not governing the organisation effectively and ethicall ,they can simply elect a new one. Since the shareholders' meeting is the highest decision-making body, they can also issue regulations on governance, ethics and compliance, which the board is obliged to follow (provided the obligations are legal).

2. The statutory auditor: controls and reviews the boards and CEO administration of the company

It is also the shareholders' meeting that elects the statutory auditor. The purpose of the *statutory auditor* is to control the organisation from an owner's perspective. In Sweden, the role of the statutory auditor is not just limited to examining the company's annual accounts and accounting practices. He/she is also to review the administration of the company by the board and the executive management. In state-owned companies, a special auditor is also elected with the task of informing the owners of whether business processes

* *Helena Sjöholm* is active in Sweden with services involving leading organisations, board evaluation and draft policies and guidelines that add values and create changes.

1 *"How Nordic Boards Create Exceptional Value"* published 8 June 2016 at https://www.bcgperspectives.com/content/articles/corporate-development-transformation-nordic-boards-create-exceptional-value/.

2 For more information on the Nordic model (2014) see *P. Lekvall* "The Nordic Corporate Governance Model" at http://www.sns.se/sites/default/files/the_nordic_corporate_governance_model_0.pdf (accessed on 31.07.2016).

are optimal and internal control is effective. The statutory auditor reports to the shareholders' meeting.
The direct link/interaction between the shareholders' meeting and the auditor allows shareholders to have an insight into the administration of the company and to act in situations where they consider the business is not being managed ethically, compliantly or optimally.

3. The board of directors: determines and ensures strategic focus and internal control

The board of directors is legally responsible for the management and organisation of the company and must therefore ensure that the company is run ethically and compliantly. The responsibilities of the board of directors are to:

- establish the overall aims and strategy of the company
- ensure there is a system for following-up and controlling the company's operations and risks as well as for monitoring the company's compliance with laws and other regulations
- appoint and, if necessary, dismiss the Chief Executive Officer
- ensure that the company's external communications are transparent, accurate, reliable and relevant.

According to the Nordic model of corporate governance, the board consists of non-executive members. It determines the organisation's decisions, policies, internal control by delegating powers to the Chief Executive Officer.

4. The Chief Executive Officer executes

The *Chief Executive Officer* is responsible for the day-to-day management of the company and answers to the Board of Directors. He/she conducts ongoing management in accordance with the latter's guidelines and instructions.

IV. Nordic governance focuses on ethics and compliance through the division of power

The Nordic model relies on several priniciples that reinforce the governing systems focusing on ethic and compliance:

- *The division of duties and responsibilities.* The laws and codes separate the role and responsibilities of the corporate bodies. They give boards great power to control the company and direct ethical discourse by stating that they should ensure internal control and make strategic decisions. In contrast, the CEO has a purely executive managerial function. The division of roles also serves to strengthen the integrity of the board vis-à-vis the executive.
- *Independent boards.* The board is non-executive (i.e. consists of members that are separate from executive management). The CEO's subordination to the board also reinforces the latter's independence. It gives the board room to maneuver if it believes the CEO is not running the business ethically and compliantly.
- *Hierarchical chain of command.* The corporate bodies are subordinate to each other. The general meeting elects members of the board and can make decisions about the organisation, which the board is obliged to follow. The board elects the CEO, makes decisions and give instructions to the CEO, which he/she is obliged to follow. The CEO, in turn, can make decisions and issue internal rules which the organisation has to follow. This hierarchical chain of command gives each body a role in ensuring a compliant organisation.
- *The board members have individual responsibility for the organisation.* The board is a collective decision-making body but its members bear individual fiduciary liability which is decided at the shareholders' meeting. This means that the board members must act in the best interest of the company because their appointment imposes a duty of care and a duty of loyalty.

Another characteristic of the Nordic model is that it is *owner-oriented*. The corporate governance model gives great power to the general meeting and emphasises the importance of active ownership. It provides great protection for minority shareholders: for example, each shareholder has the right to participate and vote in the shareholders' meeting, and the shareholders' meeting may not make any decision that gives undue advantage to one shareholder or individual to the disadvantage of the company or any other shareholder. In companies with several owners, these provisions prevent a dominant owner from making unethical decisions at the expense of a minority owner.
The model is based on *self-regulation*. The Companies Act is pragmatic and facilitates self-regulation and the Nordic corporate governance codes are regarded as a means of continuously improving governance.

1. A third corporate governance model

The Nordic corporate governance model can be seen as a third alternative to the unitary-board system (one-tier) and the dual-board system (two-tier). The unitary-board system (one-tier) consists of a general meeting and a board of executive directors. It is characterised by an integration of the governance and executive power. The executive directors appoint and elect statutory auditors and new board members. The dual-board system (two-tier) consists of a general meeting and two boards: the supervisory and management boards. In this model, the power of the company is, in practice, delegated to the management board since the decision-making power of the supervisory board *is limited to appointing and dismissing executive directors for material reasons."*[3]. At this point, the Nordic model differs from other governing models in three ways:

- The shareholders have the ultimate power
- The board has wide-ranging powers to run the company
- It makes a clear distinction between the non-executive board and the executive management function: the board of directors represents the will of the owners instead of corporate management.

2. Applying good governance

Every company has governance but not all have *good* governance. Good governance is ensured by working with the *right focus*: i.e. addressing the issues relevant to the organisations' compliance today and tomorrow. It does this by ensuring the business model benefits the shareholders and society, establishing *optimal working procedures* as well as *good relations and interaction* within the board, between the CEO, owners and society. These three issues are also the most challenging when it comes to implementing or changing the structure of corporate governance.
Good governance depends on each corporate body having the integrity to focus on their role and raise difficult questions. However, relations in governance structure are sometimes resemble *"follow the leader"* or *"the Emperor's new clothes"´*: in other words, no one questions or introduces new ways of looking at decisions, performance or behavior. In this situation, the corporate governance models with provisions for good governance just fade away and vanish.

3. How can boards further reinforce compliance and good governance?

Working with small, medium-sized organisations within the private sector and the public sector, I see that boards can reinforce ethics and compliance in the following ways:

- *Integrating dialog on ethics into the board and their own policy documents*. Boards are very good at adopting ethical rules for the employees but sometimes fail to discuss the ethical standards they should meet and how to implement them in practice. I also see that the *Rules of Procedure*, *Instructions to the Chief Executive Officer* and above all the *Reporting Instructions* can develop with an ethical perspective. For example, the aim of the Reporting Instructions are to focus on when and how the CEO should give financial information to the board. However, Reporting Instructions can be developed and provide more information or key-indicators on what, in the future, can affect financial results.
- *Integrating the stakeholder perspective into the board rooms*. Globalisation and digitisation bring new opportunities and risk. Today, it is not enough that just the CEO and organisation has a stakeholder perspective. In order to evaluate risk analysis and formulate future strategy, boards need an understanding of how the business model affects different stakeholders and how stakeholders can affect the business model. The stakeholder perspective is essential to formulating good strategy and a basis for good innovation.
- *Integrated reporting*. Many companies write sustainable reports, which is very positive, but it is often separate from the financial report. The reports could be more integrated with the aim of having a holistic view of the organisation's strategy, performance and governance. From this perspective, the framework for integrating reporting is very promising.
- *Margin for maneuver and optimal governance*. The basis for good governance is that each corporate body has an arena to act in. However, the roles are sometimes mixed up. The shareholders, desiring control, make detailed decisions. The CEO, desiring development, makes strategic decisions without the involvement of the board. The room for maneuver should be balanced by optimal working procedures and policies.
- *The engagement of the owners and statutory auditor.* The owners could be more involved in the controlling process and issue instructions on what to audit to a greater extent.

The aforementioned perspectives arise from the corporate culture and mindset of the owners, the board and the CEO, rather than the business mission.

3 See *P. Lekvall* p. 60 in *The Nordic Corporate Governance Model* (2014) at http://www.sns.se/sites/default/files/the_nordic_corporate_governance_model_0.pdf.

V. Conclusion

I would like to conclude with four statements:

- Statement 1: Good governance is an interaction between the corporate bodies. All bodies have a role to play in achieving good governance and compliance.
- Statement 2: The model of corporate governance determines the rules and structure for the interactions. Therefore, the corporate governance model is central to the analysis of governance.
- Statement 3: Its separation of power and hierarchical chain of command makes the Nordic model a good basis for governance and accountability.
- Statement 4: Integrity operates as a shield for good governance.

Compliance Culture & Governance

Philip Brennan*

The Editor asked me to summarise my presentation to the 4th Viadrina Compliance Congress on 6th July 2016, hosted by the Europa University, Frankfurt (Oder) and organised by the Viadrina Compliance Centre and the Compliance Academy. It was a privilege to be invited to speak in the company of such distinguished fellow speakers and attendees. The congress was an unquestionable success.

I. Culture of Compliance

Let me start by sharing some introductory views on creating an appropriate compliance culture. These are personal views, based on my experience. When I refer to compliance, I mean not just regulatory compliance, but also business ethics.

1. Tone from the top

Let me start with 'tone from the top'. There is no question in my mind that the predominant recipe for successfully implementing a strong compliance culture is having clear, frequently expressed and unequivocal support for compliance from the board and senior management team of the parent organisation. This must permeate to boards and senior management of subsidiaries, particularly in countries and cultures different to the parent. If employees do not detect this endorsement (and employees do detect these things) no Compliance function, no matter how good it is, will successfully inculcate a strong compliance culture. Words, however, are not enough. Directors and senior management must not alone speak positively about the importance of a strong regulatory compliance culture, they must also act, and be seen to act, as they speak (e.g. by refusing to sell products unsuitable to a customers' needs). They must 'walk the talk', so to speak. During the discussion after my presentation, a conference attendee made the point that middle as well as top management must also set the right tone. I could not agree more. To junior staff, their line of sign often does not go beyond middle management.

2. Recruitment

Personal values must be a key attribute of staff recruited at all levels in the organisation, from board members, to management, to front line staff. Behaving appropriately and doing the right thing must run in the genes of everyone in the organisation.

3. Spirit vs. letter of the law

The Corporate Code of Ethics, the Code of Behaviour and all the Policies should focus not just on the letter of the law or regulation, but also on the spirit. Culturally, some countries struggle with this. Regulation cannot cover everything. If a product or practice does not 'feel' right, the corporate ethos should discourage employees from engaging in it. More and more stakeholders expect organisations to act responsibly as well as legally.

4. It doesn't matter what competitors are doing

Boards and senior management should adopt a maxim that, once the actions of the competition offend their own compliance culture, they should not be replicated. There is often a strong temptation to set corporate standards by reference to what the competition is doing. This strategy is short-term and can result in a race to the bottom. Explaining that you were following the norm or the competition is not a defence when things go wrong.

5. Systems and processes

Regulation in financial services and indeed in many other industries is complex, extensive and ever-increasing. It is no longer possible to rely on human nature or human intervention to ensure that the organisation acts compliantly. A culture of compliance must be underpinned by systems and processes which automate, to the maximum possible extent, legal and regulatory responsibilities. So many of the compliance failures that arise are due not to deliberate action or inaction by people but to inadequate systems or, where human intervention is required, to human error.

6. Training and competency development

To embed a culture of compliance, organisations must strongly invest in training and competency development. This ranges from training on conduct and behaviour to technical training where employees need to know why and how to follow regulation.

7. The Chief Compliance Officer

I will speak more about this under the heading of governance. Suffice to say at this stage that the technical competence, ability to influence and independence of mind of the Chief Compliance Officer ("CCO") are critical factors in developing and maintaining a strong compliance culture. The CCO should be interviewed by a board member and the board, not management, should ratify the appointment. He or she should be the 'minder' of the board and senior management on regulatory compliance matters.

II. Governance

Let me turn now to the second subject matter we are considering – that of an appropriate governance structure to ensure that an organisation maintains a strong compliance culture. Again, based on experience, I am going to identify what I regard as the key elements of such a structure:

1. Ownership of the responsibility to comply

Establishing ownership and the role, scope and accountability of all parties relating to regulatory compliance is really important. It should be clear to everyone across the organisation that the ownership of compliance rests, not with the CCO or the Compliance function, but with the board which bears ultimate responsibility and which, in turn, delegates this to senior management.

So the board must hold management accountable for acting compliantly and the governance structure should position the Compliance function to act 'schizophrenically', as it were by, on the one hand, advising and assisting management on how to act compliantly and, on the other, independently monitoring the standards of compliance being operated by management and reporting to the board/audit committee on this.

2. COSO framework

My preferred governance structure for oversight of compliance, for those of you familiar with it, is the COSO framework, or at least an adaptation of it. This involves three lines of defence – management in the first line (being primarily responsible for compliance), the Compliance function in the second line (advising on and independently monitoring and reporting to the board on standards of compliance) and Internal Audit in the third line (overseeing and reporting independently to the board on the effectiveness of operation of the first and second lines).

3. Positioning, composition and independence of the Compliance function

The positioning, composition and independence of the Compliance function are, in my view, a really important part of the governance structure of any organisation. Let me share a few thoughts on this:

- The CCO should be a member of the executive management team. He/she needs to be in a position of influence among senior management and should have unfettered rights to monitor and review what he/she considers necessary. The CCO should have a power of veto on certain regulatory matters.
- The CCO should report functionally to the Chief Executive Officer and independently and directly to the chairperson of the board audit

* *Philip Brennan* is founder and Managing Director of Raiseaconcern.com, a body which works with employers in the prevention, detection, investigation and remediation of workplace wrongdoing.

committee. The board is ultimately responsible for compliance. Given that they have no role in the operation of the company, they must rely on management to assure them that the organisation and its employees are acting compliantly. However, they also need someone who understands the subject matter to validate management's assurance. This should be evidence based and independent. This is the role of the CCO and the Compliance function.
- Staff of the Compliance function should have a firm knowledge, not just of regulation but also of the operation of the business – one is just as important as the other.
- The Compliance function should be proactive and solution-minded rather than police men/women.
- The CCO should be accountable for the Compliance function in all jurisdictions. Local compliance officers should not report to local management but to the enterprise CCO.
- The CCO should manage the relationship with all regulators

4. Monitoring

Compliance should be regularly and independently monitored. Monitoring should be based on a risk assessment compiled independently by the Compliance function with input from management. Compliance officers should maximise the use of technology to identify areas of high risk.

5. Reward

A long time ago, I remember reading an article by Steven Kerr entitled "*On the folly of rewarding A while hoping for B*". It sums up for me the importance of building compliance into the reward structure. Reward should be based, not just on financial performance, but on a balanced scorecard involving numerous measures, an important one of which should be adherence to compliance standards. Compliance should be a qualifier: in other words, if a manager or employee fails to meet the appropriate standard, or worse still, is found to have breached regulatory compliance or ethical standards they should, in my view, be disqualified from receiving any discretionary remuneration that year.

6. Employee Disclosure

The final key tool in the compliance governance toolkit that I want to cover is the whole area of employee disclosure.

Ensuring an organisation remains compliant is not an easy job for anyone, at board, management, Compliance, Internal Audit or regulatory level. Monitoring compliance is labour-intensive. No matter how good risk assessments are, tail-risks can pop up from nowhere. Problems can be latent in systems. Wrongdoing deliberately perpetrated by individuals can be difficult to predict and detect.

Employees are the ones who are most likely to know where "the skeletons are buried" so to speak – where the latent problems reside, where things are likely to "blow up". Organisations, through their boards and senior management, should actively encourage employees to disclose concerns about wrongdoing and ensure that staff are regarded in a positive rather than a negative light for doing so. If a culture of employee disclosure is fostered, it can bring about a situation where every employee becomes a compliance officer, every employee engages in the monitoring of regulatory compliance and business ethics.

Creating the right culture here is of paramount importance. The identity of employees who make disclosures should, as far as possible, be kept confidential. Ensuring they are not penalised, even if their reasonable suspicion proves to be wrong, is equally as important (save of course where the disclosure is known to be false and is made for malicious or malevolent intent). Following up/addressing the issues raised and giving feedback to the disclosers are all part of the recipe for success.

Employees should be facilitated to disclose their concerns both inside and outside the organisation to a trusted recipient. The employer should focus on the concern disclosed, not on the discloser. Ideally, employers will want employees to raise their concerns with local business management. However, this is not always practical or possible. For this reason, there should be a trusted internal confidential recipient for employee disclosures. This should, in my view, be the CCO in the home country. Equally, there should be a trusted external confidential recipient employed by the firm to receive employee disclosures, to independently advise employees and to protect their identity.

If an organisation's culture encourages and looks positively on employee disclosure and if its governance structure facilitates it, it is an all embracing, focused and cost-effective manner of monitoring standards of regulatory compliance – a key part of the governance toolkit in protecting the reputation of the firm, irrespective of the business involved.

Cross-border Compliance, Corporate Governance and Culture in Russia

Anatoly Yakorev*

The Russian economy is deeply integrated with the EU. In 2014, the EU ranked as Russia's number one trading partner, accounting for almost 41 % of its trade. In 2016, Russia is the third largest trading partner of the EU and latter is still its number one trading partner. However, a lot has changed since the Russia's annexation of the Crimea, which heralded a new political and economic reality – with legal issues brushed aside.

After two years of sanctions and import substitution and economic sovereignty[1] announced by Russia not much has been achieved, except in the agriculture and a few other areas at the expense of a weakened Rouble and much lower quality of domestic produce. Russia's most pressing problems relating to sanctions concern access to capital markets and technology. A retaliatory food ban imposed by Russia in August 2014 failed to boost local production and gave rise to a shadow economy in which goods are smuggled in from neighboring countries disguised as their own produce. The Russian government decided on Wednesday (29 June, 2016) to prolong a ban on EU food imports from August until the end of 2017 in retaliation for EU sanctions over the Ukraine.[2] On 1 July 2016, the EU Council prolonged the economic sanctions targeting specific sectors of the Russian economy until 31 January 2017.[3]

I. Sanctions compliance

Despite the added workload of complying with constantly updated databases, creates a tangible need to have a robust compliance programme in place.[4] However, some companies prefer to end their dealings with Russia rather than spending money on improving their sanctions compliance out of fear of potential penalties. Apart from ongoing and extended sanctions, Russia has been hit with a recession whose nature is both cyclical and structural and which is exacerbated by low oil prices. Moreover, poor public governance combined with weak institutions makes it very hard for Russia to break this vicious circle. Having been cut off from any meaningful exchange with their peers within the EU and worldwide, public entities are beginning to lose efficiency and focus. As economic challenges spread globally and the threat of transnational corruption is recognised, regulators and prosecutors worldwide are improving their communication channels, making it very costly for global companies to make mistakes. For example, Apple was recently ordered to pay $ 14,5 billion by the European Commission.[5] Russia is not immune to this and multinationals operating in Russia are being punished.[6]

Another challenge is the increasing complexity of global regulation which increases the compliance costs of running businesses and provides little relief to companies which could still face stiff penalties. That is even more prevalent in high risk regions. It seems the only strategy is to seriously re-engineer companies' business strategy and ethical conduct in low integrity and high risk markets.

II. Compliance standards in banking

The Russian banking sector is being ravaged by the Central bank of Russia which is trying to flush out incumbent banks and preserve the stability of the

* *Anatoly Yakorev* is a Director for the Center for Business Ethics & Compliance (CBE&C), International University in Moscow.

1 https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-06-09-import-substitution-russia-connolly-hanson.pdf.

2 https://www.euractiv.com/topics/russian-food-ban/.

3 http://www.consilium.europa.eu/en/press/press-releases/2016/07/01-russia-sanctions/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%3A%20EU%20prolongs%20economic%20sanctions%20by%20six%20months.

4 http://www.tradesanctions.com/ofac-actions-against-russia-increase-certainty-for-compliance-programs/.

5 http://www.reuters.com/article/us-eu-apple-taxavoidance-idUSKCN114211.

6 https://www.statnews.com/pharmalot/2016/08/31/astrazeneca-bribes-china-russia/.

financial system. Surprisingly, Russian banks were among the first to implement Basel III[7] requirements mainly because access to the outside financial resources is vital for Russia. The Central Bank is now talking about implementing its own compliance standards.[8]

III. Compliance in state owned companies

Unlike banking, most large Russian state-owned companies have been reluctant to develop their compliance function. However, certain state owned companies (e.g. Bashneft) have eagerly allocated resources to ensure their compliance departments operate as effectively as possible. Bashneft's young and professional team recognise the need to have a robust anti-corruption compliance team in place and stand out with their commitment to making this function one of the best in the industry. Private companies usually throw resources at this function such as BP's joint venture "TNK-BP" which has developed its compliance function to be better than BP.[9] It is a good sign if any state owned companies manage to perfect their compliance department because their success story will invariably cascade down to other companies and partners in Russia.

Russia in 2016 is very different from what it was in 2014: There are many reasons for this: the slump in oil prices, loss of some external oil markets (that are among the major sources of revenue for Russia) as well as aggressive politics and propaganda have had a dramatic effect. China has not become Russia's big trading partner as expected because China takes sanctions seriously and does not wish to invest in the current political and economic period Russia is in. Politics has also had a profound effect on the economy in Russia because of belligerent policies and disregard for international law.

Violation of international law regulating the use of force and compliance may not go hand in hand in a country where institutions are weak and the law is selectively applied in accordance with a political agenda. Yet, as banking compliance shows, Russia is making impressive strides in anti-corruption laws having exemplary anti-corruption legislation that also includes provisions for establishing compliance in companies and organisations.

That said, ongoing anti-corruption efforts can roughly be split into three groups: the first led by the federal authorities, determined to weed out bad apples who have become a liability, demonstrated exceptional inefficiency or have been singled out due to the political agenda. The second group is represented by officially-assigned institutions such as the Ministry of Labor which was charged with the development of anti-corruption policies but lacks the teeth and authority to introduce any meaningful changes. It promotes documents that prescribe anti-corruption activities to underpin National Anti-corruption Plan. The third group is more into ousting political corruption through orchestrated leaks about corruption among senior public officials, fueled largely by the desire to remove them from positions of power. That's how people from Mr. Putin's inner circle were forced to bow out.

So the first group has been very successful by flagging some regional leaders and putting them behind bars and resolving in-house conflicts among competing law enforcement agencies. However, such actions are aimed at optimising bloated networks which also represent reputational risks since they have been in power for a long time. The third group is led by Alexey Navalny and his Anti-corruption Foundation's revelations.

IV. Anti-corruption legislation

Russia is a signatory to many conventions, including the Council of Europe Criminal Law Convention on Corruption, the UN Convention against Corruption, the UN Convention against Transnational Organized Crime, the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The key piece of legislation is the Federal Law on countering corruption 273-FZ. It contains almost all key international anti-corruption features: e.g. an intermediary or a third party, if they acted intentionally to elicit a bribe, shall be criminally liable under article 291.1 of the Criminal Code. Companies are not subject to criminal liability according to Russian criminal legislation (article 19 of the Criminal Code). The same applies to foreign companies that can only be punished under the Russian Administrative Offences Code. Since corporate bribery became an administrative offence under Art. 19.28 of the Code of Administrative Offences (akin to FCPA or UKBA), however, it has lacked a crucial component, namely the „adequate procedures" defense which a company may use to avoid liability. Even the minimum compliance measures that companies need to take (i.e. training, internal policies and procedures) pursuant to Art. 13.3 of the Federal Anti-corruption Law 273-FZ do not yet provide for the „adequate procedures" defense in courts. Nevertheless, lawyers have referred to it in certain cases.

V. "Soft law"

Any initiative launched by the business community in the form of the Collective Action and Integrity Pact could become a best practice, bringing more transparency into areas notoriously stricken by corrupt practices (e.g. bidding and tenders), or improving supply chain and interaction with third party agents. I led my first Collective Action in the energy sector called "Russian Energy Compliance Alliance" ("RECA") in 2010. I brought together the 15 foreign and Russian companies that existed at the time; the latter were reluctant to join but, following the support of the Federal Anti-monopoly Service, they realised that the federal agencies could also be interested in setting a level playing field for the market players. Later, as a member of the Coordination Council on implementing the Anti-corruption Charter of Russian Businesses at the Russian Chamber of Commerce,[10] I tried to introduce best international practice to the SMEs and their networks along with methodological recommendations from the Ministry of Labour as well as criteria for anti-corruption programmes to meet existing requirements of the Russian anti-corruption legislation. Of all civil society organisations that help businesses in this area, the Chamber of Commerce is the best suited and most competent to introduce compliance mechanisms to SME which normally lack the resources to implement this function. The Business Ombudsman's office was established in Russia in May 2013 to address the imperfections of the Russian court system and unfair treatment by prosecutors. I participated as the Council of Europe's independent expert in the project together with regional Business Ombudsmen called "Protection of the Rights of Entrepreneurs in the Russian Federation from Corrupt Practices – PRECOP RF."[11] Such initiatives help identify good business models that ensure protection from corrupt law enforcement agencies and biased court rulings.

VI. Compliance industry

On the back of changes in anti-corruption legislation, the domestic anti-corruption compliance market sprang up to establish a local compliance industry, which is normally frowned upon by Russian prosecutors. Yet any attempt to modify and localise the anti-corruption industry falls short of international expectations. As a result, internationally-accredited organisations like ICA find a lot of clientele because companies are ready to invest in compliance which is on a par with international standards rather than taking their chances with local providers. This is good news for cross-border compliance-related issues, especially if proper education is provided to compliance officers whose certification is recognised beyond the Russian borders. That would greatly simplify cross-border issues.

VII. Anti-trust compliance

The Federal Anti-monopoly Service is very active in Russia. Its main financial sanction is an administrative fine which ranges from 1 % – 15 % of the company's annual turnover. These fines are issued pursuant to the Code of Administrative Offences, which provides that administrative liability is fault-based. Accordingly, taking appropriate compliance measures could be perceived as substantive defense which would relieve a company from any administrative liability.

VIII. Cross-border governance

This is also gaining traction in places such as the Kaliningrad region, where small and medium enterprises strive to emulate the best corporate governance practice they have learned from their foreign partners. This region's Business Ombudsman – Georgy Dykhanov – kindly provided me with a few examples of successful cross-border governance lessons which, in turn, were taken further into mainland Russia to be shared with other Russian companies and suppliers.

IX. Corporate governance

Corporate governance may be stagnant in Russia at the moment (at least based on Deloitte's findings) but a new Corporate Governance Code (adopted by the Central Bank of Russia's Board of Directors 21 March, 2014) provides clear guidance for companies to implement the Code's principles and monitor its compliance. Public companies are required to comply with the Code or explain why they fail to do so. Companies must integrate these changes into their internal documents, organisational structure and corporate procedures. Based on the findings of Deloitte CIS Centre for Corporate Governance in 2015,[12] there are still relatively few independent directors: they are found in only 41 % of companies. Most directors (61 %) have connections to the state

7 http://www.bis.org/bcbs/publ/d357.pdf.
8 http://ibcongress.com/en/news/detail/bank-rossii-razrabotaet-standarty-komplaens.
9 http://www.techknowledge.me/files/theme/KC/Baltzer/BUCOA4Leaflet2015.pdf.
10 http://against-corruption.ru/en/.
11 https://www.coe.int/t/dghl/cooperation/economiccrime/corruption/projects/precop/precop_default_en.asp?toPrint=yes&.

authorities. Only 22% of companies perform the Board's self-assessment compared with 78% in the EU.

X. Cross-border culture

Following the exodus of large sections of the workforce many Russians have returned from abroad and taken up senior positions in Russian companies. However, this is not sufficient to offset the steady brain-drain as many mid-level managers continue to leave Russia. Russian capital has failed to repatriate from the West: only around 2,500 mid-sized companies were accounted for in the government's de-offshorisation programme. Falling education levels due to Russia adopting a liberal education model is also contributing to a poorly-equipped workforce. At the same time, there are examples of cross-border cultural successes in the Kaliningrad region bordering Poland and Lithuania that can be shared and replicated in mainland Russia.

XI. Main compliance challenges

After two years of sanctions, the number of consultancies that deal with fostering compliance and compliance services (including the Big Four, think tanks, NGOs and other organisations) has markedly declined. Many professionals and experts have left this field because there is little demand for their services and lots of foreign companies have also left. A potential solution is offered by automated and IT compliance solutions that help aggregate data once they localise their product and could fill this gap. For companies which still deal with Russia, the following sanctions and corruption issues remain top priority:

- Identifying gaps and overlap between sanctions and compliance due diligence
- Knowing Your Customer and Know Your Counterparty
- Getting owners' identities, PEPs, SDNs, conflicts of interest
- Awareness of ethnic criminal networks and transnational crime which operates with impunity because they are intertwined with federal enforcement agencies. However, Russia has finally recognised this as a threat and set up special police units to fight ethnic crime.

Corruption continues to be a huge and tangible risk especially regarding sanctions. As the "pie shrinks" it increasingly becomes a matter of the survival of the fittest. In addition, the global recession and other looming crises present global challenges along with the prosecution of non-compliant companies by the SEC and DOJ. Although foreign companies have stopped monitoring what is going on in Russia and are re-allocating their resources elsewhere, it would be prudent to continue watching this space because few do. Russia will emerge after sanctions with many problems and challenges (e.g. severe technological gaps, lack of investment and innovations, lower levels of professional workforce, degraded institutions and infrastructure), but will still have a lot of natural resources, a potentially large consumer market and an appetite for huge infrastructure projects. It all starts with cross-border compliance, governance and culture to maintain good levels of professional interaction and could later be replicated elsewhere in Russia because best practice must be emulated in order to save money and resources in our challenging times.

12 http://www2.deloitte.com/ru/en/pages/risk/articles/2016/corporate-governance-structures-of-public-russian-companies.html.

The Role of Middle Management in CMS

Dr. Oskar Filipowski*

I. Introduction

During the 4th Viadrina Compliance Congress 2016 held in Frankfurt an der Oder on 6th–7th July 2016, most of the speakers (covering the broad range of topics) stressed the importance of the so-called "tone at the top" in establishing a successful compliance management system ("CMS"). However, the meaning of the term was not elaborated further. In my opinion, this left an interpretative gap that should be addressed. Therefore, the aim of this short article is to share some insights on the issue.

II. What the "tone at the top" actually means

The concept of "tone at the top" originated from audit firms, where it referred to an organisation's general ethical climate, as established by its board of directors, audit committee, and senior management.[1] The term is broadly connected to both good governance principles and CMS. However, in my opinion, this approach to the "tone at the top" is only suitable for rather small organisations with a very flat structure. The "tone at the top" should also include middle managers for the reason I give below.

Even though today's business leans towards a horizontal organisational structure,[2] in most cases there is still a "management gap" between top management and regular employees that is filled with one or two layers of middle management (depending on the organisation). The general trend shows that leading global organisations build a complex matrix of responsibilities and reporting duties that allows them to manage the organisation effectively in various locations. However, a side effect of such a set-up is that the employees' perception of top management is that those people at the very top of the organisation are distant and inaccessible and do not understand employees. Therefore, employees place their trust in the middle management as they are accessible on a day-to-day basis. As a result, middle managers will be the natural first point of contact if any compliance doubts are raised or any non-compliance detected.

The other factor is that may discourage people from escalating compliance issues to the very top of the organisation is the fear of bypassing the official reporting line.[3] This may damage the relationship between employees and their direct manager who, after all, is responsible for supervising and evaluating their work. According to the ERC study,[4] 70% of employees would only talk to their direct manager about serious compliance issues or questions and 85% of respondents identified their direct superior as being the most important person for them in the organization.[5] Therefore, the other observation that can be drawn is that employees look up to their managers' behavior in order to determine what is allowed and what is not. As a result, everything that is done (or not done) by the middle management will, in most cases, be mirrored in their employees' behavior. The manager that e.g. forges his/her expenses shows that internal rules can be circumvented without fear of consequences. However, a manager who does not emphasise the role of compliance and does not discuss or inform his team of compliance policies and duties, is also sending a message that compliance is not something that has to be taken seriously.

III. Middle manager – man caught in the middle

As shown in previous section, employees are most likely to look up to their direct management in order to identify behavioral patterns that are expected or not tolerated. However, middle managers – in contrast to their top colleagues that guide the company at strategic level – have a duty to achieve their business goals and therefore will have fewer resources to promote compliance or (in the worst case scenario) those goals will promote unethical behavior. It was also discovered that middle managers often feel lost when challenged by compliance issues[6] brought by their employees, as they do not have the required expertise to solve them. Another dimension of this problem is that only few legal regulations (at least in Poland and most other European countries) penalise middle managers directly since overall responsibility for an organisation's (mis)performance is associated with top management.

Therefore, numerous organisations' compliance programmes look impressive from the outside with a high level of commitment and declarations made at the highest level but, in reality, are not effective because middle management

* *Dr. Oskar Filipowski* is a university teacher, legal counsel and coach and an author of numerous publications on competition law. He is responsible for compliance in KGHM Polska Miedź S.A. See the official event webpage at: http://compliance-academia.de/en/4vcc/(accessed on 04.09.2016).

1 See i.e.: *D. A. Wood*, "An Examination of How Entry-Level Staff Auditors Respond to Tone at the Top vis-à-vis Tone at the Bottom". Behavioral Research in Accounting. 27 (1). 2015.

2 As described by *F. Ostroff* "The Horizontal Organization. What the Organization of the Future Actually Looks Like and How It Delivers Value to Customers", Oxford University Press, 1999.

3 The approach to this issue may differ in different organisations, but generally larger and complicated organisations would rather have a more complex and formalised reporting structure.

4 Ethics Resource Centre, National Business Ethics Survey of the US Workforce, NBES 2013.

5 However no such study was made in Poland, my experience shows that the results of such study, would be comparable.

6 The KPMG Survey of Corporate Responsibility Reporting 2013, available at: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/corporate-responsibility/Documents/corporate-responsibility-reporting-survey-2013-exec-summary.pdf (accessed on 10.06.2016).

is "disconnected" from the process. Overcoming this problem requires the proper governance of the organisation. ISO 19600 provides effective guidance on how to divide compliance obligations between top management and middle management. The top management is responsible for building the proper framework, leading by example and establishing proper compliance policy[7]. They also have an overall responsibility to ensure proper resources for compliance are made available[8]. It must be recognised that "proper resources" is not just about sufficient funds, but also access to knowledge, people (e.g. compliance officers) and the time required to operationalise the compliance system at lower levels. In other words, middle managers must be ensured that they have a person to consult with if they are not able to tackle a compliance issue themselves, that they will have proper training to be able to recognise and resolve compliance issues and, finally, that they will be assessed (at least in some part) on the basis of their compliance performance. As the bank crisis in 2008 proved, a lack of good governance within the organisation also leads to non-compliance since employees (especially those at the management level) are tempted not to follow the rules if they believe they can benefit more from misconduct than doing things by the book[9]. It has to be added that some organisations with an appetite for high risk may willingly decide to adopt such a business model (which admittedly makes less sense nowadays considering that there are regulators all over the world hunting such organisations when they reach a certain size), although in most cases the governance model is not affected by CMS implementation as nobody wants to "hurt the business". In my opinion, governance is often a component that determines whether the compliance process works correctly or not. However, this issue is usually addressed at top level and will therefore not be elaborated further in this article. The last key issue on the list is the clear communication of the organisation's expectations towards middle managers. ISO 19600 (in section 5.3.5) again provides a very good idea of how to assign compliance responsibilities to middle managers. The steps briefly described above, give middle managers the resources and motivation to spread the compliance culture across the organisation. As a result, there is a good chance that compliance requirements will be fulfilled in general: middle managers are at the forefront of any successful compliance programme as they translate high level declarations into daily work. However it must also be remembered that a lack of commitment at middle management level can also be dangerous for any organisation because these are the people who have a proper knowledge of internal verification procedures and processes and therefore know how to cover up any misconduct they (or employees under their supervision) have committed.

IV. Closing remarks and summary

As elaborated in this article, the meaning of "tone at the top" covers not only top management but also middle managers that have direct access to employees within the organisation. Even though only few legal regulations impose legal responsibilities on middle managers (at least in Poland), their influence on the success of a compliance programme is enormous. For this reason, it is key to prepare them for their role of "the man in the middle" and to give them proper incentives that would encourage them to make compliance their priority. The organisation cannot succeed in this endeavour without proper governance. In this regard, ISO 19600 provides valuable guidance for most types of organisations.

7 For details see: ISO 19600:2015 point 5.3.3.
8 *Ibidem.*
9 The classic example is the situation where bank product managers where given very high bonuses, when they were able to get a certain turnover in a given year without any claw-back clauses or any other key performance indicators that would be connected with the quality and accuracy of the service provided.

Chapter 3: Cross Border Internal Investigations

How to act in cross border fraud

Geert Delrue*

The prevention and detection of corporate fraud might be a major problem in an international context. The investigation of an established fraud in an international environment may even be as problematic. A lot of legal provisions must be observed in every country where the private investigations are being carried out. For this reason, we must consider a lot of legal provisions when preventing and prosecuting crime in national legal systems. Different legal and practical questions and observations arise when investigating cross-border fraud. We can draw a distinction between the legal and empirical framework. In this contribution, we will concentrate on the empirical framework, whilst keeping in mind the legal framework.

At the start of a fraud investigation, important questions must be answered. What is the company's policy? Should there be an internal or criminal investigation? Other questions that arise later include: What sort of fraud are we dealing with: vertical or horizontal? Management or employee fraud? Internal vs. external fraud? Organised vs. simple fraud? Local or cross-border fraud? Moreover, what are the goals of the investigation: to identify the fraudulent procedure or the weak points in the chain of custody? Should we only try to find the goods or money that were embezzled or should we also try to trace other proceeds of the fraud?

First, the company's policy must be considered. Does it wish to keep most of the fraud detected internal, to avoid possible reputational damage? Or is a criminal investigation an option with the possible consequence of bad publicity? If an internal private investigation within the firm is chosen, then there will be fewer legal provisions to consider. On the other hand, when a criminal procedure is involved it must be ensured that certain legal provisions comply with the local criminal procedure of the country where the fraud was committed, where the investigation is being carried out or where the fraudster is living. For instance, any evidence collected contrary to the principles of the local criminal procedure cannot be used in a criminal court. However, not only local principles must be kept in mind but also those in the Universal Declaration of Human Rights.

Once it has been decided to pursue the criminal investigation, it is necessary to consider the legal regulations relating to prevention and prosecution. A possible next step is to determine whether it concerns vertical or horizontal fraud. Vertical fraud concerns the relationship between authorities and legal entities/individuals (e.g. corruption, tax fraud, social fraud). Horizontal fraud, on the other hand, concerns the relationship between individuals/legal entities and individuals/legal entities. Horizontal fraud can be divided in management fraud (e.g. cooking the books, insider trading) and employee fraud (theft of social goods or money and professional or commercial secrets).

Once this step has been taken, the next question is to decide whether we are dealing with simple or organised fraud. Simple fraud is generally limited to one object, has only one goal, is quickly perceptible, is slowly built up and has low professionalism. Organised fraud, however, is just the opposite: it is based on structures, targets more goals simultaneously, uses complex camouflage and cover up and is characterised by high professionalism.

Once the type of fraud has been established, the following step is to determine whether it concerns local (i.e. within the boundaries of a country) or transnational (i.e. cross border) fraud.

In case of a transnational private investigation, one must keep in mind that the fraudsters might be brought before justice in different countries. This implies that, during the transnational private investigation, one must comply with the provisions of criminal law and other legal areas (social law, civil law, tax law etc.) of the country in question. While carrying out a (trans)national fraud investigation we are acting in the empirical track but must consider that a criminal procedure can be introduced at any phase of the private investigation. As a result, the findings of the private investigation can only be used as evidence in criminal proceedings if they are collected in accordance with local legal procedures. This implies that evidence collected contrary to local legal procedures cannot be used as evidence in court. For example, a statement of a fraudster in which he/she confesses to have committed the fraud might not be admissible before court if no lawyer was present during the interrogation. Or if, during the investigation, you are at the home of the fraudster and you find stolen things that later turn out to be the property of the firm. In this case, it might not be legal to return these things to the firm without the explicit consent of the fraudster. The Belgian civil code provides that "One is the owner of a movable thing while it is in one's possession". In Belgium, a thief has to give his explicit consent to return the stolen goods to

* *Geert Delrue*, as a Belgian Law Enforcement Officer, is attached to the Economic Crime Department, section Anti Money Laundering.

the owner. If not, only a court decision can decide to return the stolen goods to the real owner.
The order of questions mentioned above is not fixed, i.e. they do not have to be posed in the same order as presented. It is even possible to formulate the first question as follows: "Are we dealing with local or transnational fraud?" and then ask, "Is it organised or not?" or "Is it management or employee fraud?" or "Is it horizontal of vertical fraud?" A completely different order of questioning is also possible depending on the case in question. One always has to keep in mind the firm's policy. Always start a private investigation considering that a criminal procedure might be involved, despite the possible negative consequence of reputational damage. Whenever a (trans)national fraud investigation arises, we must always take into account the applicable local legal provisions. This has the advantage that a criminal investigation can be started at any phase of the private investigation and the results can be used as evidence in the criminal procedure. When carrying out the (trans) national investigation it is important not only to find out how the fraud was committed but also what the fraudster did with the embezzled goods or money or where the other proceeds of his fraud have ended up. First of all, it is essential to ascertain the weak points in the chain of custody. How was the fraudster able to avoid the anti-fraud procedures? These findings are of vital importance in addressing the weaknesses particularly susceptible to fraud and thereby prevent future fraud.
Another objective of the investigation, which should not be forgotten, is finding out what happened to the stolen goods or money. Some fraudsters immediately purchase some luxury goods or go on luxury holidays. Concerning the purchase of (luxury) goods, it is possible to seize[1] the goods in question. Money in a bank account can be (temporarily) frozen or seized. Here we come to the final track of the fraud time-line: money laundering.
While investigating we need to understand why people launder money and how they do it. This can help us to carry out our investigation more efficiently.
People launder for various reasons:
- they want to accumulate wealth by avoiding seizure and confiscation;
- they want to avoid taxes by maximising their profits;
- they want to maximise and give a legal appearance to their illegal proceeds by reinvesting them in the legal economy, or
- they want to avoid a laundering conviction by denying a link with the underlying crime.

"Understanding how money laundering works" is essential for concluding fraud investigations. If you understand the process of money laundering you can also maximise the results of your investigation: discovering the proceeds of fraud and its destination. The three-phase model is still the simplest way of explaining how money laundering works.[2]
In each of these three phases there are specific typologies to recognise possible money laundering. These typologies are only tools to detect possible money laundering. In most cases, these typologies are normal legal transactions. However, when they are carried out in relation with some other typologies there is often money laundering involved. However, it is very difficult to detect money laundering schemes because they are usually made up of normal transactions.
To conclude, we can state that (transnational) fraud investigations involve a lot of questions, legal procedures and special knowledge in relation to fraud and money laundering. That is why thorough and specialised training in the conduct of legal and empirical investigations is of the utmost importance. After all, "You cannot detect what you don't know".

1 In some countries civil seizure is possible, in other countries a court order is necessary.
2 In some literature you can find a lot of other ML-models, but they tend to be more complicated.

Dealing with Compliance Cases at Siemens

Marcin Szczepański*

In many of his speeches, our President & CEO – Mr. Joe Kaeser – underlines the importance of Siemens being, or permanently striving to become, a compliant Company: "The lived ownership culture of our company makes the difference. People rightly associate Siemens with reliability, fairness and integrity". His statement can be supported not only by the trust expressed by Siemens' stakeholders but also several external awards and recognitions. One we are especially proud of is the Dow Jones Sustainability Index, where Siemens has been recognized for last couple of years as one of the most sustainable & compliant companies in our industry worldwide.
Of course, we cannot deny the fact that Siemens was not always a leader in this area. Moreover, we cannot forget what happened almost 10 years ago, in Autumn 2006, when the corruption affair at Siemens was revealed to the public. Many of us can still recall the shocking newspaper headlines, disclosing details of various malpractices committed in the name of our company by some of its employees and managers. This may seem like a bad dream today but it also serves as kind of a warning of what can happen when the company builds its success on insecure foundations. Our current achievements have only been possible thanks to the measures taken by Siemens' management and owners immediately after the incidents were revealed. In 2006, Siemens started the clean-up operation, later supported by independent experts from the international law firm Debevoise & Plimpton. During the next few months, a new company structure was implemented resulting in several new appointments to managerial positions across the company. Siemens also established a professional and comprehensive Compliance system based on international standards and equipped with all necessary procedures, tools and staffed with a team of qualified Compliance Officers across the entire company. In-Between, Siemens has adopted company-wide "Business Conduct Guidelines", which consist of a set of universal rules – akin to a constitution – with the Compliance Department acting as their guardian.
The effectiveness and independence of our Compliance organisation is primarily guaranteed by defined structures and responsibilities. Accordingly, the Chief Compliance Officer (currently Mr. Klaus Moosmayer) reports directly to the Siemens CEO, whereas at the levels of particular countries, independence and effectiveness of Compliance officers is assured by keeping their reporting lines with Compliance Headquarters. A Siemens Compliance Officer function combines the roles of an expert, facilitator and guardian, focusing on the areas of anti-corruption, anti-trust as well as data privacy and money laundering.
Siemens' Compliance system is based on the assumption, that managers are responsible for its implementation and maintenance in accordance with their areas of responsibility. It consists of 3 main pillars:
Prevent: from the time perspective this is currently the main focus area. It is based on periodical Compliance risk assessment, conducted each year across the company, with the focus on defining and weighting existing Compliance risks and adjusting policies and procedures accordingly (or even creating new ones if necessary), as well as developing supportive IT Tools to make our work more efficient and standardized. Another important part of our preventative activities is focused on communication and training to promote Compliance and ethics in business not only among our employees but also in relation to external counterparties, like: Compliance Trainings, Communication measures or Collective actions with external partners.
Detect: this part focuses on discovering potential weaknesses of our system inclusive wrongdoing or breaches of guidelines by our employees and partners. It is mainly based on the comprehensive "Compliance Control Framework", backed by tailor-made controls, implemented in accordance with the existing risks. Controls are strengthened by Compliance-related audits and reviews both conducted using local, dedicated organizations as well as external supporters. It is also worth mentioning that Siemens allows its employees, partners and all other stakeholders to report any misconduct they observe anonymously using a "Tell-Us" channel and the Ombudsman Office. Last but not least, this pillar also includes the topic of today's discussion, namely investigations of Compliance cases.
React: The main goal behind this pillar is to continuously improve the existing Compliance system by learning from the cases and adjusting accordingly existing processes and procedures as well as by remediating identified implementation weaknesses. Also, Compliance violations established by internal investigations lead to disciplinary measures.
The following explains the "Compliance Case Handling Process".
During the implementation of Siemens' Compliance system it was decided that Siemens should also establish a special investigative process and provide tools and qualified resources in order to be able to conduct clarification of allegations in a fair and objective manner, which resulted establishing in

* *Marcin Szczepański* graduated from Warsaw School of Economics (Master of Economy, Finance and Banking). Since 2006 he is a member of ACCA. *Marcin Szczepański* is Regional Compliance Officer at Siemens (Warsaw, Poland) since 2012.

Compliance Headquarters a dedicated team, mainly responsible for dealing with central cases but also for establishing rules and training other Compliance professionals throughout the company.
Information about potential misconduct is collected from several sources.
The anonymous channel "Tell-us": operated by an external provider, which is independent of Siemens, to assure confidentiality and prevent leakage of whistleblower data to Siemens. Accordingly, allegations can be reported anonymously and securely. In addition, Siemens engages an independent external law firm as an "Ombudsman Office", which allows personal contact to the whistleblower. Each report, from the ombudsman and/or "Tell-Us" is checked by the respective HQ Unit for plausibility and then handed over to the responsible Compliance Officer in a form which does not allow Siemens to trace the information contrary to the whistle-blower's wishes. All information received by the whistle-blowing system is first recorded and then examined by specialist lawyers to determine whether there are grounds for further action or investigation.
Other ways: Apart from using anonymous channels, Siemens employees and counterparties are encouraged to report observed violations directly to their supervisors or specialized departments including Human Resources, Legal or Compliance. The identity of Siemens employees who report compliance violations in person is protected by a special guideline that prohibits whistleblowers from being sanctioned or disadvantaged in any way if reports are made in good faith.
Each report, regardless of its source (including anonymous letters, text messages etc.), is registered and traced in a dedicated Global Case-Tracking IT tool. which enables to deal with particular cases in a structured way. Registration includes assignment to the relevant case category, providing details of the potential subjects/description of allegations/location/involved entities and individual etc. Compliance Case are evaluated in the next step, whether they should be treated as "central" and investigated by Compliance HQ or "local" and then clarified by the respective Compliance Officers. This distinction depends on the case category, seriousness of the allegation, potential damage as well as the position levels of the subjects.
Regardless of whether the case is deemed "central" or "local", the mandates represent the empowerment of the "case-handler" to conduct case clarification in mandated scope and in accordance with the respective procedure as well as with reference to possible violations of the law and/or Siemens' guidelines. Each mandate must be signed by the respective Compliance Head & General Counsel and then distributed among the respective stakeholders in order to inform them about the case handling procedure within their area of responsibility and oblige them to support this procedure as well as not to interfere with it.
Once the mandate has been signed, the typical research work starts under the presumption of subject's innocence and that his rights are safeguarded – typical research actions include:
- analysis of documents, like e.g.: contracts, invoices, protocols, other internal documentation, accounting entries, payment runs etc.
- analysis of documents found on subject's devices when necessary & legally justified,
- interviews with the whistleblowers (when not anonymous), witnesses and subjects.

After completion of the clarification procedure, a clarification report is being prepared, summarizing the case facts, findings as well as recommendations for the remediation actions incl. disciplinary consequences for the subjects. In cases, when there are not enough findings or the allegations cannot be confirmed, the case can be closed as "non-plausible compliance case" without any specific results.
Case remediation includes typically establishing of a Disciplinary Committee, which is organized at either Central or Local level, depending on the case category and consist usually of the representatives of Legal, HR and Compliance as well as supervisors of the subject/management of the respective Siemens entity. Its task is to evaluate the recommended disciplinary actions and decide about the sanctions taken in accordance with the applicable law and practice as well as with past sanctions in order to ensure fair and objective treatment.
One of the most challenging aspects of the case handling process is its internationalization. In a large multinational Company like Siemens, each case clarification requires cooperation with colleagues from many different countries – often located in different parts of Europe. The main challenge from my point of view is communication in a way which is understandable for everybody while at the same time addressing local specifics and risks. The situation becomes more complicated, when the case and subject are coming from a different country than the clarification team, what is typical for most of the central mandates. In such a case the clarification team looks for either supporters in the local Siemens organization (usually Compliance and/or Legal representatives) or in exceptional cases (e.g. due to the existing Conflict of interest risk or lack of capacities) to engage external support such as specialized legal or consulting firms, which can provide local expertise.

Conducting a cross border compliance investigation in a crisis

Nicolas W. Zwikker*

I. Introduction

Over the past few years, regulatory scrutiny and sanctions have attained dizzying proportions. The recent Telia Company[1] and the Deutsche Bank mortgage[2] issues are cases in point. Both in the financial and corporate world, matters are getting worse with significant clamp downs on integrity failings. It wouldn't surprise me if we are entering an age in which fines may force firms to shut down. The latest development is the Wells Fargo case, which has led to mass dismissals of employees and questions being raised by institutional investors in e.g. the Netherlands.[3] Cooperation between regulators on an international level[4], together with competition and prosecuting authorities have created new dynamics that CCOs need to specifically address in crisis situations. This article relates to situations and issues I have dealt with personally. The most important of these was the nationalisation of Fortis/ABN Amro in 2008 and subsequent developments when I was the firm's CCO, as well as later cases I dealt with as a crisis management consultant. My objective is to share experience and, in particular, situations that later proved to be valuable lessons. What do you specifically need to investigate and manage as a CCO in a crisis if the crisis results from an unforeseen incident (for instance a whistle-blower going to the press or criminal authorities) and raises serious issues of integrity and ethically sound practice? How do you go about it?

II. The Facts

It may sound obvious, but any sensible response to a crisis must start with an investigation and a clear understanding of the facts, placed in perspective.
This is easily said but there are many pitfalls. Here are just a few:
- Inadequate record-keeping can leave the CCO in the dark as to as to the plausibility of allegations or charges. It is imperative to be sure of at least some facts in order to assess what risks to the firm are involved and to decide next steps.
- Although available, it may not be able to retrieve data quickly and easily owing to a multitude of operational or IT issues.
- The people involved cannot be found. It strikes me that many incidents relate to past activities and dormant problems that later become active. In such cases, the inability to speak with the people who were involved in gathering not only the facts but also the circumstances can prove to be a significant handicap.
- The lack of time to analyse the available material.

In a crisis, the CCO has to deal with many obstacles standing in the way of assessing the risks involved by an impartial assessment and understanding of the facts[5]. One should always avoid jumping to conclusions, however strong the pressure may be to either dismiss allegations or to overreact. One must also bear in mind that events take their own course. Things seldom end the way they started.

* *Nicolas W. Zwikker* is a compliance expert and direcor of Zwikker compliance associates.
1 Telia Company, press release, 15.09.2016.
2 Deutsche Bank press release, 15.09.2016.
3 Pension fund giants APG and PGGM are reported to have insisted on the clawback of senior management remuneration.
4 See, for instance, the LIBOR benchmark manipulation case.
5 It is important to maintain high standards of fairness when conducting an investigation. I have encountered situations in which employees were interrogated rather than interviewed leading to frightful results.

III. Dealing with internal and external pressures, leadership

In a crisis, a great deal of operational responsibility falls on the shoulders of a few people (the CCO among them), but there are many stakeholders who wish to have their questions answered. The managing board, supervisory board, internal risk management, the communication department, internal audit, the relevant external regulators, the press and sometimes even politicians and shareholders will all, at some point, want to know the status and, more importantly, what is being done to prevent damage. Concerns and even fear can run high.

A CCO has a strong interest in taking the reins firmly in hand and organising the process of communication. Providing timely, full and consistent information to those involved is very important in maintaining internal calm and preventing uncoordinated activity.

Most larger financial institutions will have crisis teams that are well-prepared to deal with a regulatory crisis. This represents an effective means of organising communication and executing further measures.

However, I have generally found that a CCO who takes leadership can prove to be very valuable in keeping matters manageable and providing a level of comfort in a bad situation. Leadership will also help in providing a realistic view of the seriousness of the risks to the firm and the measures that will be required in the future to remedy failings.

Finally, leadership will also be required in dealing with the authorities.

In a crisis, there are many possible reactions to events ranging from internal denial to complacency. It is my firm belief that the CCO should keep an open mind and assess whether there has indeed been a lapse of standards, applying a broad risk management approach rather than simply following the formal letter of the law.

Although one's lawyers and their expertise are absolutely necessary, one should always avoid letting the legal approach take precedence over and above the recognition that standards may require improvement.[6] The long-term policy implications of a crisis are far more important than legal battles. I therefore feel that cooperation with the authorities is more effective in the long run than denial and opposition.

IV. Change

One can and should learn from a crisis. Identifying root causes are part of the total process of successfully managing a crisis. Moreover, there must also be a general recognition that things need to change and one must be prepared to use the momentum to achieve that recognition. Implementing change (which is not the same as executing a compliance programme) is the next big challenge, which again involves leadership and a fair amount of perseverance and courage. If failings are attributable to culture then this should be recognised and met head-on. If business models are to blame then they should be abandoned. If it is a question of poor management and inadequate control, that too should be changed.

V. Conclusion

A CCO managing an investigation during a crisis faces many internal and external difficulties. The stakes are high and increasing – as is the level of discomfort at managing board level owing to the risk of personal liability.

Nevertheless, provided that the firm recognises the issues there is also a momentum for change which should be used for maximum benefit. However, this takes time.

6 As *Churchill* once said: "Experts on tap, not on top!"

Chapter 4: Cross Border Anti-Corruption Programs

The National Crime Agency: Advice for SMEs on How to Protect Your Business from Bribery and Corruption

Ingrid Leonard*

The National Crime Agency's International Corruption Unit was set up in May 2015 and has given the UK an enhanced capability to combat international bribery and corruption. Supported by the Department for International Development, the International Corruption Unit (ICU) is made up of a team of more than 50 investigators with extensive experience in international corruption and financial investigation.

The ICU's main functions are to:

- investigate money laundering in the UK resulting from grand corruption overseas
- investigate international bribery offences involving UK-based companies or nationals or where there is a UK nexus
- trace and recover the proceeds of international corruption.

The unit also supports HM Treasury with the enforcement of financial sanctions, supports foreign law enforcement agencies with international anti-corruption investigations, engages with government and business to reduce the UK's exposure to the proceeds of corruption and works with business to support increased compliance with the UK Bribery Act 2010.

I. Outreach

The ICU has an Anti-Bribery Outreach Programme which aims to promote anti-bribery compliance to the private sector, encourage reporting of bribery allegations to the ICU and develop initiatives in support of the above. The ICU works with industry experts in anti-bribery compliance to promote the six principles of the Bribery Act and to deliver related capacity-building, particularly to Small and Medium Enterprise (SMEs). It does this by developing relationships with business networks and professional associations within a variety of sectors to reach its target audience, presenting at members' events around the UK and abroad to encourage companies to implement policies and mechanisms which safeguard their business against committing offences under the Bribery Act.

II. IFBT

The International Foreign Bribery Taskforce (IFBT) is a trans-border agreement set up to combat international bribery. Made up of specialised investigators from across the globe, the taskforce enhances the law enforcement response to bribery on an international scale by providing a platform for police experts from Australia, the United States, Canada and the United Kingdom to work collaboratively to strengthen investigations into international bribery offences and to support the aims of the Organisation for Economic Cooperation and Development (OECD) and United Nations (UN) anti-bribery conventions.

The IFBT holds an annual conference which allows law enforcement officers to share knowledge, skills and methodologies as well as to discuss case studies and coordinate international investigations, share up-to-date trends and typologies and discuss best practice in relation to existing bribery investigations. A collective law enforcement approach from a number of countries with robust anti-bribery legislation already in place will lead to an increase in the perpetrators and facilitators of bribery being brought to justice and reduce the number of individuals who believe that they can commit bribery with impunity.

The IFBT also meets regularly to discuss initiatives to encourage compliance with bribery legislation and to develop strategies to aid companies safeguard their business against bribery. It also contributes to awareness-raising, through the provision of multi-agency investigator panels at conferences and law enforcement stalls with officers on hand to give advice and guidance on compliance with bribery legislation.

III. Corporate Liability

Under section 7 of the Bribery Act, commercial organisations can be criminally liable for failure to prevent bribery if a person associated with their organisation bribes another person intending to obtain or retain business or a business advantage for that organisation.

* *Ingrid Leonard* is the Anti-Bribery Outreach lead on the International Corruption Unit, a unit she helped to set up. Further information and useful links can be found at the ICU pages on the NCA website: http:// www.nationalcrimeagency. gov.uk/ about-us/ whatwe-do/ economic-crime/ international-corruption-unit-icu.

If a person associated with a company engages in conduct which amounts to an offence under section 1 (active bribery) or section 6 (bribery of a foreign public official) of the Bribery Act, intending to obtain or retain business or an advantage in the conduct of business, that company could be liable to prosecution for failing to prevent bribery.

A commercial organisation will have a full defence to the section 7 offence if it can demonstrate that it had adequate procedures in place to prevent persons associated with it from bribing.

Whether or not a commercial organisation has adequate procedures in place will ultimately be a question for the courts to decide. However a vast amount of information, guidance and training materials on adequate procedures and preventing bribery is available for companies to consult. An excellent starting point is the Ministry of Justice Bribery Act 2010 Guidance[1] and their six principles, which form the basis for most commercially available anti-bribery solutions. The six principles are:

- Proportionate Procedures
- Top-level Commitment
- Risk Assessment
- Due Diligence
- Communication (including training)
- Monitoring and Review

While equal weight is placed upon each principle, Proportionate Procedures will be of particular significance to SMEs. This is because the guidance recognises that a commercial organisation's adequate procedures should be commensurate with the bribery risks it faces and the key characteristics of the business, such as its size and the scale and nature of its activities. This means that adequate procedures need not necessarily be sophisticated, expensive or onerous to implement.

IV. Facilitation payments, hospitality and promotional expenditure

Illicit small-scale payments paid to secure routine government action, sometimes referred to as facilitation or facilitating payments are bribes for the purposes of the Bribery Act. Hospitality and promotional expenditure is not prohibited by the Act, unless of course it is employed as a bribe.[2]

V. Understanding what is proportionate as an SME

British multinationals have reportedly been quick to respond to the introduction of the Bribery Act. Many SMEs who face bribery risks have been slower to respond, either because they are unaware that the Act applies to their operations or because they are unsure what an appropriate and proportionate response should be. A 2015 government report[3] revealed that a third of UK SMEs surveyed were not aware of the Bribery Act and its corporate liability provisions. Ultimately, the Bribery Act applies to all UK-based businesses both domestically and internationally and to foreign companies who carry on a business or part of a business in the UK. All companies who fall within these categories therefore need to take steps to consider what their exposure is and what measures are necessary to prevent wrongdoing. The starting point is to understand the risk profile of the organisation. A company which exports goods or services with a point of sale into markets where corruption is prevalent and which uses third parties to sell on its behalf will have a very different risk profile to a company that only sells within the UK. It may be proportionate for the latter to implement a low key prevention regime based on a written policy committing to do business without bribery and communicate that to employees. An exporting company would, on the other hand, need to implement a more sophisticated prevention regime if it is to combat the risk of bribery.

VI. What are the key features that an SME should consider in framing adequate procedures?

1. Ownership

Responsibility for the policy could be assigned to a single individual within a company's leadership team to ensure accountability, as part of a top-down strategy. Resources should be dedicated to implementing the policy and associated programme, with a clear reporting line to the policy owner. In SMEs, this might be part of a person's duties rather than their full-time job, depending on what resource is available and what is proportionate for that company considering its risk profile.

2. Employee Awareness

Bribery prevention procedures are redundant unless they are applied. Any policy should be communicated to employees so that they are aware of it and understand how to comply with it. Statements from senior management ('top-level commitment' – see Ministry of Justice guidance) can drive recognition and publicise the importance of the policy across the organisation. Dedicated training for employees covering the nature of bribery risks faced, the nature of the procedures to be employed to mitigate those risks and how employees should respond in a manner consistent with the policy, is essential. This is particularly important for employees in high risk roles, such as sales, those liaising with foreign governments or those operating in areas where there is a high risk of corruption. Mechanisms should also exist for employees to report any concerns, such as suspected breaches of the policy. This might be a point of contact within Human Resources or via an externally-managed reporting line.

3. Managing third party risk

Third parties, such as suppliers, distributors, agents, business partners, which a company relies on to perform services on its behalf, can present particular risks for that company, owing to the section 7 provision under the Bribery Act for liability for acts of bribery committed by 'associated persons'. The starting point in managing third party risk is to know who a third party is, what they will be doing on the company's behalf and whether that exposes the company to liability under the Bribery Act.

An effective strategy for an SME could include clear communication to third parties of a company's bribery policy and procedures and contractual provisions committing third parties to comply with applicable bribery laws, with a provision for termination of a contract in the event that these terms are breached.

4. Continuous Improvement

Regular review of procedures is important to enable understanding of how effectively those procedures are functioning with respect to the risk they are designed to mitigate and whether any improvements are needed. Risks change over time and new risks might emerge, warranting adaptation of the procedures in place.

VII. Contacting the ICU

The ICU would be particularly interested to hear from companies who have come across corrupt practices in their industry.

For advice on reporting possible bribery and corruption offences, or queries on the law enforcement approach to international corruption issues, please contact the ICU at: ContactICU@nca.x.gsi.gov.uk.

VIII. Whistleblowing

The National Crime Agency is a prescribed body for the purposes of bribery and corruption on the UK Department of Business, Innovation & Skills 'Blowing the Whistle to a Prescribed Person: List of Prescribed Persons & Bodies'[4] Individuals can therefore blow the whistle on bribery and corruption to the NCA rather than to their employer.

---

1 https://www.gov.uk/government/publications/bribery-act-2010-guidance.

2 Further information on what prosecutors would take into account when considering whether to prosecute in this area is available under http://www.cps.gov.uk/legal/a_to_c/bribery_act_2010/.

3 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440661/insight-into-awareness-and-impact-of-the-bribery-act-2010.pdf.

4 www.gov.uk/government/uploads/system/uploads/attachment_data/file/431221/bis-15-289-blowing-the-whistle-to-a-prescribed-person-list-of-prescribed-persons-and-bodies-2.pdf.

Preventing Cross-Border Bribery through Effective Compliance Measures

Christine Uriarte*

The following article summarises the presentation given by Christine Uriarte on 6 July 2016 at the 4th Viadrina Compliance Congress. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the OECD, the governments of its member countries, the European Union or those of parties to the Convention on Combating Bribery of Foreign Public Officials in international Business Transactions. This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

I. Introduction

Most multinational enterprises that are incorporated or listed in countries that are parties to the OECD Anti-Bribery Convention[1] have made significant progress establishing and implementing measures for preventing the offering, promising and giving of bribes to foreign public officials in order to obtain advantages in international business (foreign bribery). Nevertheless, bribery scandals continue to plague many international business deals, including major government procurements for infrastructure development. This article summarises the most important areas of progress in this field, as well as the remaining challenges, and offers suggestions on what can be done to overcome them. It also discusses business incentives for adopting effective compliance measures for preventing and detecting foreign bribery. It concludes with some ideas about what the future has in store for foreign bribery compliance.

II. Main areas of progress

The OECD Working Group on Bribery, which is composed of the 41 parties to the OECD Anti-Bribery Convention, conducts a systematic peer-review process to monitor implementation of the Convention. The parties, which account for more than 65% of world trade, share a common interest in ensuring a level playing field for international business. It is therefore not surprising that the review process generates reports with hard-hitting recommendations to improve the parties' legislative and institutional frameworks for combating the bribery of foreign public officials.[2]

So far, the review process involves four separate phases. Phase 1, which constitutes a desk review of parties' legislative provisions, commenced in 1999, when the Convention came into force. Phase 2, which assesses parties' institutional frameworks for implementing the Convention, commenced shortly thereafter. Phase 3, which began in 2010, is largely completed. A major component of Phase 3 is an assessment of parties' implementation of the 2009 OECD Council Recommendation on Further Combating Foreign Bribery. The Recommendation states that parties should encourage companies to adopt adequate internal controls, ethics and compliance programmes or measures for preventing and detecting foreign bribery.[3] An annex to the Recommendation provides guidance to companies on the adoption of such measures.[4] Phase 4 began in 2016, and focusses on horizontal trends among the parties, as well as specific continuing challenges faced by the individual parties.

The Phase 3 reviews show that companies, particularly multinationals, are making important progress adopting anti-bribery management systems for preventing and detecting the bribery of foreign public officials. A 2015 study of foreign investors conducting business in Vietnam supports this observation. It shows that companies from parties that had undergone Phase 3 monitoring by the time of the survey period were less likely to have bribed Vietnamese officials than companies from parties that had not yet undergone such monitoring.[5]

Progressive trends in corporate compliance that have been observed in companies from parties to the Convention that have undergone Phase 3 monitoring, include increased attention to the following:

- Managing the risks of foreign bribery specifically in companies' anti-corruption policies, codes of ethics and training, in addition to bribery more generally.
- Risks of bribing officials of state-owned and controlled enterprises.[6]
- Availability of whistleblower channels and protections.
- Risks of bribing through third-party business partners, including local agents, consultants, foreign subsidiaries, suppliers, distributors and contractors.
- Independence of board members, directors and the audit function, in particular from dominant shareholders.[7]

III. Continuing compliance challenges

Despite these significant advances during the OECD Working Group on Bribery's Phase 3 monitoring, further substantial progress is still needed. Recent surveys support this proposition, and one shows that compliance may have stood still over the last five years.[8] Small and medium-sized enterprises that are not listed on any party's stock exchange generally have low awareness of the risks of foreign bribery and are in the early stages of adopting compliance programmes. Substantial improvements are also needed in other areas, including coordination with compliance functions for related business misconduct, the use of incentives to drive sales, and internal audits. Although whistleblower channels and protections have seen major improvements, they are still underused. Also, there remains much more to be done by companies to manage their third-party risks.

Small and Medium-Sized Enterprises lagging behind

Small and medium-sized enterprises (SMEs) may be disadvantaged vis-a-vis large MNEs when it comes to compliance, mainly due to resources. It is difficult for SMEs to attend compliance events, where a significant amount of expertise on new trends in compliance is shared. Moreover, there is a plethora of guidance on compliance in the public arena, which is a very good thing, but it also makes it challenging for SMEs to distil and translate the information into implementable and cost effective compliance measures. This is the main reason why the OECD Good Practice Guidance on Internal Controls, Ethics and Compliance encourages business organisations and professional associations to play an essential role in helping SMEs in this regard, including by disseminating information, and providing training and advice.[9]

---

* *Christine Uriarte*, Senior Legal Analyst, Anti-Corruption Division, OECD.

1 The full name of the OECD Anti-Bribery Convention is the Convention on Combating the Bribery of Foreign Public Officials in International Business Transactions. Its 41 Parties are obligated to make it an offence to offer, promise and give bribes to foreign public officials to obtain advantages in international business. They are also required to make enterprises ("legal persons") responsible for such bribery. The Parties are the 35 OECD countries plus Argentina, Brazil, Bulgaria, Colombia, Russia and South Africa: http://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf.

2 The monitoring reports of implementation by the parties of the OECD Anti-Bribery Convention are automatically published here: http://www.oecd.org/daf/anti-bribery/countryreportsontheimplementationoftheoecdanti-briberyconvention.htm.

3 The full name of the 2009 OECD Council recommendation is the Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions: http://www.oecd.org/daf/anti-bribery/44176910.pdf.

4 Good Practice Guidance on Internal Controls, Ethics and Compliance: http://www.oecd.org/daf/anti-bribery/anti-briberyconvention/44884389.pdf.

5 Does the OECD Anti-Bribery Convention Affect Bribery? An Empirical Analysis Using the Unmatched Count Technique (*N. M. Jensen*, George Washington Schools of Business; *E. J. Malesky* Due University, 2015, Working Paper): http://www.natemjensen.com/wp-content/uploads/2014/09/20141205_OECD_Working-Paper_ejm.pdf. The study also shows that companies from Parties to the Convention with the strongest levels of enforcement bribed the least, and companies from non-parties bribed the most.

6 The increasing trend to focus on the risks of bribing employees of SOEs is a significant milestone, particularly in light of OECD analysis, which shows that between 1999 and mid-2014, SOE officials received 80.11% of total bribes in concluded cases of foreign bribery (See: OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials (2014): http://www.keepeek.com/Digital-Asset-Management/oecd/governance/oecd-foreign-bribery-report_9789264226616-en#.WAEZpvl9670#page4).

7 The G20/OECD Principles of Corporate Governance (2015), provide international benchmarks on ensuring the independence of the Board, etc., and other corporate governance issues: http://www.oecd-ilibrary.org/docserver/download/2615021e.pdf?expires=1476625553&id=id&accname=guest&checksum=8EB566AF165E8398EC9FB450534AAE19.

8 Corporate misconduct – individual consequences (Ernst & Young, 14th Global Fraud Survey, 2016): http://www.ey.com/Publication/vwLUAssets/EY-corporate-misconduct-individual-consequences/$FILE/EY-corporate-misconduct-individual-consequences.pdf; Steering the Course: Navigating bribery and corruption risk – A global study by Hogan Lovells (2016): http://www.hoganlovellsabc.com/_uploads/downloads/Steering-the-course-report.PDF; Beneath the surface: The business response to bribery and corruption 2016 (Eversheds): http://www.eversheds.com/global/en/what/services/fraud-and-financial-crime/bribery-corruption-report-zmag.page. The Eversheds report provides evidence of a lack of progress over the last five years.

Coordination with related compliance functions

In order to bribe foreign public officials, companies frequently engage in related illegal conduct. For instance, fraudulent accounting might be used to conceal the bribe payment as a legitimate expense in a company's books and records. The company might also launder the bribe payment, or request a tax deduction for the bribe by disguising it as an allowable expense such as a consultant's fee, or social and entertainment expense. If bribery is used to obtain a government procurement contract, it might also be part of a bid rigging scheme, or other unfair competitive behaviour. Ensuring closer coordination and information sharing between all the relevant compliance functions is therefore essential.

It is also important to integrate the anti-foreign bribery compliance function more broadly in major corporate decision-making right from the start. If, for example, a company's Chief Compliance Officer (CCO) does not have the authority to comment on the potential risks of entering a new market, or a merger and acquisition, until all the preparatory work has been done by the relevant business units, the CCO's advice may be seen as uninformed at best, and costly and obstructionist at worst. A recent survey showed that 53% of CCOs feel that their compliance work is perceived as an obstacle to smooth-running operations.[10]

Use of incentives

There continues to be overwhelming evidence that many companies' incentive structures run contrary to effective compliance. Put simply, if on the one hand people on the ground in sales are told not to bribe, and on the other hand they must meet projected sales goals to get their bonuses, they are going to have to weigh these competing messages. This puts them at risk of succumbing to bribe solicitations, especially in environments where corruption is pervasive. They may even try to self-justify their conduct, by convincing themselves that they are helping underpaid government officials achieve a more comfortable standard of living. One recent study shows that 57% of CCOs feel that sales pressure is a significant challenge to reducing bribery, and 59% of sales staff worries about being fired if unable to meet sales targets.[11] Companies must therefore place a strong focus on ensuring that their compensation packages do not tip the balance in favour of corruption. One way might be by incorporating compliance into their incentive systems, such as by only rewarding sales contracts that have been obtained through clean business practices.

Use of whistleblower channels

A 2016 OECD study indicates that only 61% of surveyed companies had established whistleblower procedrures.[12] OECD analysis further shows that only 2% of concluded cases of foreign bribery between 1999 and mid-2014 were disclosed to law enforcement by whistleblowers.[13] And among the 31% of concluded cases that were disclosed through self-reporting by companies to law enforcement, only 17% were detected internally through whistleblower reports.[14]

The low level of whistleblowing is often attributed to misplaced company loyalty and continuing fear of retaliation—not just fear of obvious overt forms of retaliation, such as loss of employment. Potential whistleblowers might worry that reporting bribery could damage relations with bosses, lead to less interesting work assignments, relocation, or reduced opportunities for promotion. They might also fear that their employers could discredit them by, for instance, trying to show that the they suffer from mental illness, engaged in whistleblowing on previous occasions, or by revealing embarrassing conduct in their personal lives. It might not be clear whether whistleblowing policies and laws provide protections from these kinds of actions.

Managing third-party risks

Effectively managing third-party risks is perhaps the most significant foreign bribery compliance issue. Companies seeking foreign business opportunities invariably need local business partners, including agents, consultants, suppliers, contractors, and for entering joint ventures. OECD analysis shows that 75% of concluded foreign bribery cases between 1999 and mid-2014 involved bribery through intermediaries, including sales and marketing agents, distributors, brokers, and members of the legal profession.[15] The risk of foreign bribery involving local partners increases in sectors and activities that require frequent contact with public officials, such as for the purpose of obtaining licenses and permissions. The risk is very high where local business partners have contact with government procurement authorities. OECD analysis also shows that 57% of concluded cases of foreign bribery between 1999 and mid-2014 involved bribes to obtain public procurement contracts.[16]

Although there has been real progress by companies on the need to conduct third party risk assessments and due diligence since the beginning of the OECD Working Group on Bribery's Phase 3 monitoring, a recent study shows that 20% of companies still do not pay adequate attention to this issue.[17]

Formidable monetary penalties have been imposed on several companies in recent years for bribery through intermediaries—some of the biggest penalties have been imposed in the United States for bribing foreign public officials through intermediaries, contrary to the Foreign Corrupt Practices Act (FCPA). Some of these cases involve bribing through foreign subsidiaries.[18]

The risk of bribing through intermediaries exists for controlled as well as non-controlled business partners. However, companies should at least have more tools at their disposal for managing the risks of bribing through business partners over which they have control. In particular, they should be able to ensure that such business partners implement adequate compliance measures.

Companies should also make sure that business partners over which they do not have control implement compliance measures that are adequate for addressing the bribery risks raised by the transaction in question, such as bidding on a government procurement project. Assessing the risk should involve all the pertinent factors, including the level of corruption in the foreign country and business sector involved, as well as the nature and size of the transaction. Where it is not possible to ensure that a potential business partner has in place adequate compliance measures to address the bribery risk, it is necessary to take appropriate steps, such as delaying the transaction until the issue can be rectified, or terminating the transaction when rectification is not possible.

In order to effectively manage third party risks, it is necessary to know the identity of the beneficial owners of potential business partners. Although the recent Panama Paper leaks succeeded in raising public awareness of this issue, policy-makers had been struggling with it for some time.[19] Impetus for change has been driven by Recommendations 24 and 25 of the FATF Recommendations, which specifically address transparency and beneficial ownership of legal persons and legal arrangements.[20] The Global Forum on Transparency and Exchange of Information for Tax Purposes is also a force for reform.[21] The G20 High Level Principles on Beneficial Ownership Transparency address the need to prevent the misuse of legal entities for illicit purposes, such as tax evasion and money laundering, as well as corruption. Although these standards are driving change at the national level, many jurisdictions still have a long way to go. In the meantime, it will be difficult for companies seeking business opportunities in such jurisdictions to be able to obtain and verify information about the beneficial ownership of their potential business partners. This will be a factor to take into account when conducting third party risk assessments in relevant jurisdictions.

Independence of the audit and compliance functions

The corporate governance structures of listed companies in particular have benefited greatly from new norms, including those at the international standard, following the global financial crisis. An independent audit function is essential for detecting and preventing corruption. In addition, CCOs will be much more effective if the corporate governance structure ensures their independence and direct access to key decision-makers. Recent analysis and surveys indicate that, generally speaking, foreign bribery prevention and

9 OECD, *op, cit.*

10 Steering the Course: Navigating bribery and corruption risk – A global study by Hogan Lovells (2016): http://www.hoganlovellsabc.com/_uploads/downloads/Steering-the-course-report.PDF.

11 Hogan Lovells (2016), *op, cit.*

12 Committing to Effective Whistleblower Protection (OECD, 2016): http://www.keepeek.com/Digital-Asset-Management/oecd/governance/committing-to-effective-whistleblower-protection_9789264252639-en#.WAZMNPI97IU. The survey was conducted in 2015 by the OECD Trust and Business Project.

13 OECD Foreign Bribery Report, *op, cit*, Figure 3, p. 15.

14 *Ibid*., Figure 4 on p. 17.

15 *Ibid.,* Figure 16 on p. 29.

16 *Ibid*., Figure 20 on p. 32.

17 Corporate misconduct – individual consequences (Ernst & Young, 14th Global Fraud Survey, 2016): http://www.ey.com/Publication/vwLUAssets/EY-corporate-misconduct-individual-consequences/$FILE/EY-corporate-misconduct-individual-consequences.pdf.

18 Information about United States settlements under the FCPA for bribing through foreign subsidiaries, including in cases against Avon, Bi-Rad Laboratories, and Hewlett Packard, can be found on the US Department of Justice website: https://www.justice.gov/justice-news.

19 G20 High Level Principles on Beneficial Ownership Transparency (2014): http://www.g20australia.org/official_resources/g20_high_level_principles_beneficial_ownership_transparency.html; and Recommendations 24 and 25 of the FATF Recommendations (2012): http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

20 FATF Recommendations (2012): http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

21 See the 2016 Terms of Reference to Monitor and Review Progress towards Transparency and the Exchange of Information on Request for Tax Purposes: https://www.oecd.org/tax/transparency/about-the-global-forum/publications/terms-of-reference.pdf.

detection could be improved through more attention to the independence of the internal audit and compliance functions.

OECD analysis shows that of the 31 % of concluded foreign bribery cases between 1999 to mid-2014 that were brought to the attention of law enforcement authorities through self-reporting, only 31 % were detected by the internal audit function.[22] Further study is needed to understand the reasons why the internal audit function is not detecting a higher percentage of concluded cases. But anecdotal evidence suggests that at least in some companies, the internal audit function could much more rigorously scrutinise payments entered in the books and records that might represent bribes, especially where the books and records contain expense categories that could easily be used to disguise such payments. Such evidence also indicates that in some companies, reports of suspicions of bribery by the audit function are frowned upon by senior management.

The independence of the CCO is another major area requiring further attention by many companies. One recent study shows that only 39 % of CCOs report directly to the CEO.[23] If the CCO must go through layers of management, such as the CFO or General Counsel, there is an increased likelihood that suspicions of company wrongdoing would be filtered, or not make it to the CEO or board level at all. Providing the CCO with sufficient independence sends a strong message that senior management is invested in the compliance function, and makes "tone at the top" a fact and not simply rhetoric.

IV. Convincing the private sector that compliance is necessary

Risk of enforcement

Enforcement of foreign bribery offences is on the rise. Between 1999 and 2014, 361 individuals and 126 companies were sanctioned in criminal proceedings in 17 Parties to the OECD Anti-Bribery Convention. More than one-quarter of the individuals were sentenced to prison. A number of fines set records, particularly those imposed pursuant to the United States Foreign Corrupt Practices Act (FCPA).

Although to date, companies mainly fear enforcement under the US FCPA, and the United Kingdom Bribery Act, 12 other Parties to the OECD Anti- Bribery Convention have also imposed sanctions for foreign bribery.[24] Since many of these sanctions have been imposed for bribing through intermediaries,[25] companies, particularly MNEs, are increasingly paying much more attention to the risk of bribing through local business partners (see discussion under "Managing third party risks"). The flip-side to increased due diligence on potential business parties, is that companies wishing to enter joint ventures, supply and distribution chains, or act as agents and consultants for MNEs, need to establish and maintain effective compliance measures to make themselves attractive business partners.

Smart business decision

Fear of foreign bribery enforcement actions is not the only reason for companies to implement effective compliance measures. Indeed, companies would be making a huge mistake if they focused on the risk of enforcement when conducting foreign bribery risk assessments. This is because of the myriad business incentives for making compliance a priority. Multilateral financial institutions, such as the World Bank, debar and cross-debar companies and individuals that violate the institutions' anti-corruption policies and procedures. Countries that belong to the OECD Export Credit Group have endorsed an OECD Council recommendation that obligates them to take measures for preventing and detecting bribery in relation to transactions benefitting from their support.[26] Pursuant to another OECD Council recommendation, adherents should require that firms bidding for government procurement contracts adopt anti-corruption compliance measures. [27]

There is also evidence that it is much harder for firms that engage in corruption to attract and keep talented employees. According to a recent study, 80 % of employees would not work in a company with a history of corruption.[28] Moreover, institutional investors, including mutual, pension, and sovereign-wealth funds, are becoming increasingly reluctant to invest in companies that have not demonstrated a commitment to principles of Corporate Social Responsibility. For instance, the Norwegian Wealth Fund – the largest sovereign wealth fund in the world – excludes companies that are suspected to have engaged in corruption.

V. Conclusion

Before the OECD Anti-Bribery Convention came into force in 1999, other than the United States,[29] most countries had not made it an offence to bribe foreign public officials in international business, and bribes were pretty much tax deductible around the globe.[30] Enterprises have come a long way since then. According to a recent study, 95 % of respondent senior executives recognised the critical importance of bribery and corruption issues.[31] However, this study and others show that there is still room for improvement. The next wave in compliance will likely be driven by increasing awareness that it is smart business to implement effective compliance measures for preventing and detecting foreign bribery. A 2016 study conducted by researchers from Harvard Business School shows that even though bribery might increase sales in certain business environments, the overall impact of bribery on a company's finances is almost zero.[32] This is likely due to the costs and uncertainty of dealing with dishonest customers, and the exposure to continuing risks of bribe solicitation. On top of being no further ahead in overall profits, firms that engage in the bribery of foreign public officials must live with the risk of enforcement and penalties, bad publicity, potential debarment from public procurement, and reduced availability of financing. They will also lose talented employees to competitors with cleaner reputations. It is beyond debate that establishing and implementing an effective compliance programme for preventing and detecting foreign bribery is one of the smartest decisions a company can make.

22 OECD Foreign Bribery Report, *op, cit*, Figure 4, p. 17.
23 Hogan Lovells (2016), *op, cit.*
24 These countries are: Belgium, Canada, France, Germany, Hungary, Italy, Japan, Korea, Luxembourg, Netherlands, Norway, Sweden and Switzerland.
25 OECD Foreign Bribery Report, *op, cit*, Figure 16, p. 29.
26 Recommendation of the Council on Bribery and Officially Supported Export Credits (OECD, 2006): http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=td/ecg(2006)24.
27 Recommendation on Public Procurement (OECD, 2015): http://www.oecd.org/gov/ethics/OECD-Recommendation-on-Public-Procurement.pdf.
28 Asia-Pacific Fraud Survey 2015: A live sciences perspective (Ernst & Young): http://www.ey.com/Publication/vwLUAssets/EY-asia-pacific-fraud-survey-2015-a-life-sciences-perspective/%24FILE/EY-asia-pacific-fraud-survey-2015-a-life-sciences-perspective.pdf.
29 The US FCPA came into force in 1977.
30 Pursuant to the Recommendation of the OECD Council on Tax Measures for Further Combating the Bribery of Foreign Public Officials (2009), Parties to the OECD Anti-Bribery Convention are required to make bribes to foreign public officials explicitly non-tax deductible: https://www.oecd.org/tax/crime/2009-recommendation.pdf.
31 Eversheds, *op, cit*.
32 An Analysis of Firms' Self-Reported Anticorruption Efforts (*P. Healy*, *G. Serafeim*, The Accounting Review, March 2016, Vol. 91, No.2, 489-511).

Self Regulation and Compliance: a perfect marriage

José F. Zamarriego*

I. Brief introduction of EFPIA

The European Federation of Pharmaceutical Industries and Associations (EFPIA) represents the pharmaceutical industry operating in Europe. Through its direct membership of 33 national associations and 42 leading pharmaceutical companies, EFPIA is the voice on the EU scene of 1,900 companies committed to researching, developing and bringing to patients new medicines which will improve health and the quality of life around the world. EFPIA principles applicable to member companies and associations establish the following requirements (amongst others): (i) subscribe to the aim of EFPIA; (ii) support EFPIA in attaining its objectives; (iii) defend the views expressed by EFPIA on core topics; (iv) implement high and transparent standards of conduct in dealings with external stakeholders and (v) abide by the EFPIA Statutes and Internal Rules (including EFPIA Codes).

* *José F. Zamarriego* has a Phd. on Economics & Business Studies by Universidad Complutense de Madrid, Master on Business Administration (MBA) by the University of Wales (Aberystwyth) and General Management Program in IESE Business School. He has been Director of Farmaindustria's Code of Practice Surveillance Unit since 2004, Chair of the Codes Committee, Compliance Committee and Steering Committee of EFPIA.

II. Legal & self-regulatory background

The pharmaceutical industry is one of the most regulated sectors. There are international and national legislative frameworks that regulate a variety of major activities and practices pharmaceutical companies pursue. For example, specific rules cover good manufacturing practices, research & development initiatives, clinical trials, the promotion of medicines, the interaction of pharmaceutical companies with its main stakeholders (highlighting: healthcare authorities, healthcare professionals, healthcare organisations, and patient organisations), etc. Moreover, as with other industrial and business sectors, general legislation also applies: e.g. regarding intellectual and industrial property rights, personal data protection, fair competition, etc. Notwithstanding previous legislation, we would like to draw attention to DIRECTIVE 2001/83/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 November 2001 (amending and superseding Directive 92/28) on the Community code relating to medicinal products for human use.

As we all know, a Directive is a legislative act of the European Union (EU), which requires Member States ("MS") to achieve a particular result without dictating the means of achieving that result. For that reason, laws in the MS may differ since Directives normally leave them with a certain amount of leeway as to the exact rules to be adopted.

The scope of the aforementioned Directive (Art. 2) covers, *"medicinal products for human use intended to be placed on the market in Member States and either prepared industrially or manufactured by a method involving an industrial process".*

Title VIII regulates Advertising and Information and Advertising (including Art. 86 to 100). In particular, two articles establish the following:

Article 97:

Member States shall ensure that there are adequate and effective methods to monitor the advertising of medicinal products. Such methods, which may be based on a system of prior vetting, shall in any event include legal provisions under which persons or organizations regarded under national law as having a legitimate interest in prohibiting any advertisement inconsistent with this Title, may take legal action against such advertisement, or bring such advertisement before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.

Under the legal provisions referred to in paragraph 1, Member States shall confer upon the courts or administrative authorities powers enabling them, in cases where they deem such measures to be necessary, taking into account all the interests involved, and in particular the public interest: – to order the cessation of, or to institute appropriate legal proceedings for an order for the cessation of, misleading advertising, or – if misleading advertising has not yet been published but publication is imminent, to order the prohibition of, or to institute appropriate legal proceedings for an order for the prohibition of, such publication, even without proof of actual loss or damage or of intention or negligence on the part of the advertiser.

Member States shall make provision for the measures referred to in the second subparagraph to be taken under an accelerated procedure, either with interim effect or with definitive effect. It shall be for each Member State to decide which of the two options set out in the first subparagraph to select.

Member States may confer upon the courts or administrative authorities powers enabling them, with a view to eliminating the continuing effects of misleading advertising the cessation of which has been ordered by a final decision: – to require publication of that decision in full or in part and in such form as they deem adequate, – to require in addition the publication of a corrective statement.

Paragraphs 1 to 4 shall not exclude the voluntary control of advertising of medicinal products by self-regulatory bodies and recourse to such bodies, if proceedings before such bodies are possible in addition to the judicial or administrative proceedings referred to in paragraph 1.

Article 99:

Member States shall take the appropriate measures to ensure that the provisions of this Title are applied and shall determine in particular what penalties shall be imposed should the provisions adopted in the execution of Title be infringed.

The pharmaceutical industry's primary obligation is to ensure that the medicines it produces benefit society. Medicines can have a critical impact on individual well-being and, for this reason, relationships with those who prescribe, dispense and use medicines must comply with the highest and most ethical, professional and responsible standards.

To this end, many years ago and according to the aforementioned EU Directive, EFPIA approved a self-regulation initiative consisting of several codes of practice that establish the minimum standards that pharmaceutical companies, national associations and members of EFPIA should follow. Nowadays, three EFPIA codes of practice exist:

- EFPIA CODE ON THE PROMOTION OF PRESCRIPTION-ONLY MEDICINES TO, AND INTERACTIONS WITH, HEALTHCARE PROFESSIONALS (*last version dated 2013*).
- EFPIA CODE OF PRACTICE ON RELATIONSHIPS BETWEEN THE PHARMACEUTICAL INDUSTRY AND PATIENT ORGANIZATIONS (*last version dated 2011*).
- EFPIA CODE ON DISCLOSURE OF TRANSFERS OF VALUE FROM PHARMACEUTICAL COMPANIES TO HEALTHCARE PROFESSIONALS AND HEALTHCARE ORGANISATIONS (*last version dated 2014*).

III. Building trust & confidence

The pharmaceutical industry displays a high level of commitment to welfare and patient care as well as society as a whole and makes great efforts at all levels to develop new medicines and improve those currently available. It is aware that it cannot permit itself to have a low level of credibility and confidence among the general population.

Recent studies and a comparison of eight different industry sectors reveal the pharmaceutical industry to be in seventh position in terms of trust. Other industry sectors achieve higher rankings in the following order: technology, food and beverages, consumer packaged goods, telecommunications, automotive, energy. Only the financial services sector is ranked below the pharmaceutical industry.

Leaving aside the peculiarities of this sector which could influence levels of trust (for example, having to deal and fight against population diseases, characteristics of existing national healthcare services across European countries, restrictions and limitations regarding the provision of information and the promotion related with medicines), pharmaceutical companies have recognised, since the approval of the first self-regulation initiatives, that they have to increase their efforts and commitment in an ongoing process of improvement with the aim of enhancing their levels of credibility and confidence among the general population (Society).

One way of achieving this goal could be to demonstrate the implementation of effective and serious self-regulation systems which guarantee that pharmaceutical companies pursue their activities in compliance with the most stringent ethical criteria of professionalism and responsibility.

In this sense (and taking into consideration the relevance and pioneer character of the initiative adopted by the pharmaceutical industry that has no precedent among other industry sectors), the next section will briefly outline the transparency initiative approved on 2013 and materialised in the "EFPIA Code on Disclosure of Transfers of Value from Pharmaceutical Companies to Healthcare Professionals and Healthcare Organizations" (hereinafter "Efpia Disclosure Code").

IV. Transparency initiative

In order to improve the understanding of the relationships between pharmaceutical companies and healthcare professionals and organisations, companies assumed the obligation to publicly disclose transfers of value to healthcare professionals and organisations. The first disclosures were made in June 2016 relating to transfers of value made during 2015 (subject to contrary provisions of national laws & regulations).

Each Member Association transposed the provisions of this Code into its national code by 31 December 2013. The Code sets out the minimum standards applicable to Member Associations, except where it is in conflict with applicable national law or regulation, in which cases deviations are allowed but only to the extent necessary to comply with such national law or regulation. Compliance with the Disclosure Code is an obligation of all EFPIA members.

Through this initiative, society will better understand how the relationship and collaboration between healthcare professionals and organisations benefits patients. It is a relationship that has delivered numerous innovative medicines and treatments and changed the way many diseases impact our lives. It will show that industry and professionals collaborate in a range of activities from clinical research to sharing best clinical practice and exchanging information on how new medicines fit into the patient pathway.

Transparency will also serve to demonstrate that such collaboration and relationship is conducted under strict rules, and even more importantly, respecting one basic principle, namely: "healthcare professional freedom and independence to decide which medicines should be prescribed".

As mentioned before, this initiative has been adopted by 33 European countries each of which has their particularities and singularities. For example, Denmark, France, the Netherlands, Portugal, Romania and Slovakia have specific transparency legislation in force, so deviations have been granted. When transposing this initiative at national level, most of the countries have to consider the applicable national legislation regarding competition and personal data protection and privacy.

Contributing to Sustainable Development Goal 16.5 and Strengthening Compliance with the Alliance for Integrity

Noor Naqschbandi*

Anti-corruption laws and regulatory standards have proliferated in recent years. Nowadays, consumers and non-governmental organisations are paying ever more attention to transparent supply chains. As a result, strengthening compliance and business integrity has moved up the corporate agenda. The private sector is increasingly aware of the fact that compliance is not only a necessity but also brings a competitive advantage.

Policymakers too are increasingly aware of the negative impact of corruption. This topic is being discussed at the international level: e.g, within the Group of Twenty (G20). Reducing corruption is an effective way of increasing foreign direct investment and decreasing the costs and risks of doing business. Furthermore, reducing corruption strengthens good governance and the rule of law. This is why the United Nations has identified corruption as a crucial, cross-cutting issue for the *Sustainable Development Goals* (SDGs). This global agenda for sustainable development outlines the major challenges for humanity and provides a comprehensive set of goals and concrete targets aimed at solving these challenges. Goal 16 ("Promote Peaceful and Inclusive Societies for Sustainable Development, Provide Access to Justice for All and Build Effective, Accountable and Inclusive Institutions at all Levels") and target 16.5 in particular (to "substantially reduce corruption and bribery in all their forms"), indicate the importance of strengthening good governance and integrity at all levels. Increasing integrity in the private sector promises not only a more secure business environment and fairer competition for companies but also benefits for the public sector. For example, fighting corruption improves public procurement processes and reduces inefficiencies in public spending. The general public also benefits from more inclusive and sustainable economic growth and reduced inequality.

Ever more countries are stepping up their law enforcement. However, punishment alone is not enough. Prevention is key to ensuring business integrity. This is precisely where the Alliance for Integrity steps in: it contributes to the attainment of SDG target 16.5 by strengthening corruption prevention and business integrity globally.

Within this context, the concept of "compliance culture" has assumed major importance. Experience shows that compliance goes far beyond adherence to the letter of the law. Rather, it should be integrated into the overall company culture and manifest itself in day-to-day business processes. Compliance programmes should exist not only on paper but also in practice. Therefore, an effective compliance management system should focus on the members of the respective organisation and function as a moral compass for the employees. Raising awareness of ethical behaviour should aim at internalising compliance as a value so that employees implement company regulations in their day-to-day practice. In order to build up a strong and resilient compliance culture, it is essential that the management sets the right tone. Accordingly, management should demonstrate its support and commitment to compliance by communicating its importance to staff continuously and adequately as well as by carrying out compliance trainings and activities on a regular basis to facilitate an understanding of this issue. Only once a compliance culture is in place and actively practiced at all levels of a company will it begin to gain traction and credibility.

Furthermore, compliance has also assumed greater significance in business operations at global level. A compliance management system for international companies will only be effective if it takes local peculiarities into account. Codes of conduct and other relevant guidelines and regulations should be translated into the local language. Moreover, they should be promoted by practical examples and continuous training, especially in areas where corruption is perceived as endemic. That said, any assumption of a widespread "culture of corruption" cannot go unchallenged. This excuse is often used by management and employees alike when operating in business environments where corruption is perceived to be deeply embedded. Employees will argue that the "rules of the game" are different and companies have no choice but to accept them. The label "culture of corruption" conveys the message that, in certain sectors or jurisdictions, it is impossible to operate in any other way. For example, employees working abroad may feel that moral values and codes of conduct in "far-off" corporate headquarters appear unrealistic or otherwise do not apply to them. To counter this, management and employees should consider the fight against corruption as universal and demonstrate the importance of a sustainable global compliance culture. All companies have a responsibility to shape the business environment by nurturing a compliance culture. However, even larger companies are uneasy about changing corporate practices on their own. Companies typically fear losing business, being side-lined because of their 'bureaucratic' approach or simply being overtaken by less diligent competitors. Therefore, the Alliance for Integrity believes that collective action by all relevant stakeholders is the best way to curb corruption and foster a compliance culture.

The World Bank Institute (WBI) defines collective action in its "*Fighting Corruption Through Collective Action, A Guide for Business"* as:

"[A] .. collaborative and sustained process of cooperation amongst stakeholders. It increases the impact and credibility of individual action, brings vulnerable individual players into an alliance of like-minded organisations and levels the playing field between competitors. Collective Action can complement or temporarily substitute for and strengthen weak local laws and anti-corruption practices".[1]

The **Alliance for Integrity** is a business-driven, multi-stakeholder initiative between multinational companies, civil society, political organisations, and international institutions. The aim of the global initiative is to promote integrity through collective action among companies, their business partners and other relevant actors in the economic system. Commissioned by the German Federal Ministry for Economic Cooperation and Development (BMZ) and implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, the Alliance for Integrity is currently active in Brazil, Ghana, India, Indonesia and the respective regions. The Alliance for Integrity seeks to make a lasting contribution to the longer-term vision of achieving a corruption-free business world. Within this broader remit, the global initiative implements four proven approaches to prevent and combat corruption.

Peer-to-peer learning and international dialogue: The best way to learn is from others who encounter similar problems. The Alliance for Integrity encourages its members to share their knowledge of challenges in different sectors and regions. Best practice examples provide suggestions and innovative ideas on how to effectively foster business integrity within a company and the economic system as a whole.

Public-private dialogue: The Alliance for Integrity aims to tackle the taboo on discussing corruption that is still prevalent in many societies. In order to enhance business integrity within companies and the economic system as a whole it is necessary to raise awareness among all relevant stakeholders. The Alliance for Integrity offers the opportunity to engage in the mutual exchange between businesses, political administrations and civil society representatives. The regular exchange between all relevant stakeholders from the public and private sectors helps to build confidence and trust among participants, encouraging them to pursue collective action.

Awareness raising and information-sharing across a wider professional audience: An important step in promoting integrity is the increased understanding and awareness of the negative effects of corruption among all of society's stakeholders. The Alliance for Integrity gathers knowledge and shares experience at conferences, workshops and other fora dealing with corruption prevention and compliance. Furthermore, the initiative distributes and discusses research results and promotes practical solutions for the implementation of compliance within organisations.

Compliance training and train-the-trainer: The Alliance for Integrity's workshops and training courses (such as the *De Empresas Para Empresa*s (DEPE) or "From Companies To Companies" programme), allow participants and their business partners to learn, train, and implement practical measures for increasing integrity in their organisation. For this purpose, the Alliance for Integrity has developed specific workshops and training courses.

The Alliance for Integrity approach

The Alliance for Integrity offers a practical, three-phase corruption prevention training programme that operates at global level.

In the first phase, representatives of large companies with considerable experience in the field of compliance receive instruction on the content and methods of the Alliance for Integrity's corruption prevention training. Employees of large companies specialised in compliance are usually familiar with both the theory and practice of implementing a compliance management system. By contrast, representatives of SMEs often have little or no prior knowledge of corruption prevention.

---

* *Noor Naqschbandi*, Director, Alliance for Integrity.
For further information, see http://www.allianceforintegrity.org.

1 World Bank Institute (2008) Fighting Corruption through Collective Action. A Guide for Business. Available online: http://info.worldbank.org/etools/docs/antic/Whole_guide_Oct.pdf (accessed on 29.07.2016).

Therefore, in the second phase, the representatives of large companies deliver compliance training on behalf of the Alliance for Integrity to representatives of SMEs. This approach (developed by the Alliance for Integrity) benefits both parties. Most SMEs do not have staff with expertise in the field of compliance. Very often, compliance tasks are handled by employees with a number of different responsibilities. This is why many SMEs suffer from an information deficit in relation to compliance. The Alliance for Integrity tackles this problem by encouraging peer-to-peer exchange and sharing of good practices between companies. As a result, SMEs that undergo training acquire practical instruments to combat the risk of corruption and thereby improve their competitiveness on the global market. Larger companies also benefit: on the one hand, it shows clients and business partners that that they are committed to business integrity and, on the other, conveys a credible and trustworthy compliance culture to their employees. Last but not least, larger companies can offer training to their business partners and suppliers who lack the necessary financial and human resources in this regard. This is not merely virtuous: some companies may be under a legal obligation to ensure their suppliers adhere to the minimum requirements of a compliance management system.One reason for this training programme's success is the 'train-the-trainer' approach: representatives of major companies enjoy more credibility as trainers than international experts because they have practical experience of compliance in companies. Unlike the usual 'top-down' approach, therefore, the Alliance for Integrity's training features an active exchange of experience and good practice.

Finally, in the third phase, participants of compliance training can access the 'Online Support Desk', where they receive operational support and background information on the topic. Many practical questions on how to implement a functioning compliance management system only arise after the training when the participants have settled back into their daily routine at the company. Therefore, the Alliance for Integrity's 'Online Support Desk' also includes a network of experts that answers specific questions within 72 hours. In this respect, it is important not only to give practical advice on how to implement compliance measures but also to ensure that training participants know they are not alone in the fight against corruption and that there is a network supporting this endeavour.

To date, the Alliance for Integrity has successfully trained over 500 representatives of companies and other organisations. The training programme has been implemented in ten countries all over the world (i.e. Argentina, Brazil, Chile, Colombia, Ghana, India, Indonesia, Mexico, Paraguay and Uruguay). The Alliance for Integrity encourages companies to become part of the network and to engage in collective action to increase integrity in companies and the economic system as a whole. Together, we can make a significant contribution to SDG 16.5 and foster a global culture of integrity and compliance.

Chapter 5: Cross Border Compliance Standardization

Cross Border Compliance – Standardisation Experience from Austria

Barbara Neiger*

Nowadays, it appears that *Compliance* has become a kind of buzz word in the contemporary business world. However, it only means: "to act in conformity with applicable regulations" and no one can say that there have been no regulations and that organisations did not act accordingly. However, in a business environment where regulations are increasing in number and complexity, it can be a real challenge for organisations to follow them. A new approach is required which goes beyond individual measures to ensure compliant behaviour in the conduct of business activities.

The theme of this congress is: "Compliance across Europe". In my contribution, I will present the approach of the Austrian business community in developing compliance standards as represented by a committee established at the Austrian member of the International Organisation for Standardisation.

The Austrian Committee ASI/PC 265 has been founded in June 2012. One reason for establishing the Committee at this time was the amendment of anti-corruption regulations in the Austrian Criminal Code at the beginning of 2012. Among the changes introduced, the concept of a public official was greatly expanded to include employees of companies in which the public sector has a greater holding than 50%. There are about 50 members of the Committee from all three sectors, with majority coming from various industries of the private sector. A small task force group was formed for the development of the first draft of the new standard. Its members met during the summer months and presented the first draft of the new standard to the plenum by the middle of September. Intensive discussions followed in several meetings. Finally, the text was approved by a majority at the end of 2012. The ONR 192050 Compliance Management System (CMS) was published on February 2013.

The ONR 192050 applies to all types of organisations in the private, public and civil sectors. It can be applied to the whole organisation or only part of it and be used for third party due diligence. The norm establishes requirements for an effective compliance management system in seven elements: top management, compliance officer, compliance risk management, instructions, training, effectiveness and communication.

All elements of the norm have to be developed and implemented in order that the compliance management system satisfies ONR 192050. This means that there can be no cherry picking of elements. However, the norm expressively states that the Compliance Management System ("CMS") has to be proportionate and adequate to the individual needs of the organisation. The extent of each element within an organisation depends on its individual situation (e.g. size, structure or type and location of business activity). The main trigger for adequacy and proportionality is a compliance risk assessment. So the argument that a CMS is only applicable to large and complex organisations and is an administrative burden for small and medium-sized companies does not really apply. In particular, this group of organisations are far more vulnerable to compliance failures than large organisations. Fines could easily endanger their existence. Furthermore, when small and medium-sized companies are suppliers to large corporates they are often confronted with numerous requests to demonstrate their approach to compliance. Being able to present a structured and systematic approach according to a best practice benchmark may facilitate their response to such requests.

Shortly after the publication of the ONR 192050, an international project committee for the development of the ISO 19600 started work in April 2013. The project for the development of a new ISO-Standard had already started in 2012 when Standards Australia (the Australian member of the International Organisation for Standardization), proposed the establishment of such a committee based on their standard for compliance management system AS 3806:2006. So, at the time the development of ISO 19600 started, Austrian and Australia (like pioneers) were the only two countries which had voluntary standards for CMS. They are voluntary in as much as these two standards were developed by users for users, unlike guidelines to the laws published by state authorities. Three delegates were nominated from the local Austrian Committee, of whom I was one. Intensive discussions at several international meetings followed for which the Austrian delegates were well equipped due to the intense and somewhat controversial discussions during the development of the Austrian norm ONR 192050. Talking to representatives of other countries revealed that they were having the same discussions on ISO 19600 in their own committees that we had when developing the ONR. The document "ISO 19600:2014 Compliance management systems – Guidelines" was published in December 2014. The ISO 19600 is currently being incorporated into the Austrian system of norms. The main obstacle is that no German version is available yet. It is currently "work in progress" and should be published before the end of 2016. However, in principle, incorporation into the local system of norms is not mandatory; organisations can always access and implement the official English version of an ISO standard. Besides these two voluntary norms, the German-based standard IDW 980 is used in Austria, mainly by listed companies.

The ONR 192050 establishes the requirements for an effective CMS. By satisfying the requirements, a CMS can be certified according to ONR 192050. The ISO 19600 is a "Guideline Norm", which means that it consists of recommendations and not requirements. Based on ISO understanding, guideline norms cannot be used for certification. Requirement norms use the words "shall or must" whereas guideline norms are characterised by "should and can". Furthermore, guideline norms are – by their very nature – usually quite lengthy while the wording of requirements norms is short and precise. In order to audit and certify management systems according to a guideline

* *Barbara Neiger*, neiger.C advisory, Austria.

norm, the wording has to be changed from "should" to "shall" and reduced in length. Moreover, any examples provided must be excluded.
As the ONR 192050 is a requirement norm, the certification scheme results directly from the text of the norm. Regarding ISO 19600, the aforementioned approach to the guideline standards was applied by Austrian Standards to establish the certification scheme for ISO 19600. Currently, there are two valid certificates issued by Austrian Standards on conformity assessment of CMS: one for ONR 192050 alone and one for both ONR & ISO 19600. I served as lead auditor in both certification audits and the surveillance audits one year after the certificate was issued. One holder of a certificate is a regional energy provider with a majority of public shareholders. The second holder of the certificate is a section of the administration of the City of Vienna. Both organisations have published their certificates on their web-pages and the certificates are registered in the official certification register of Austrian Standards.
In conclusion, I would like to share with you some experiences of these certification audits and the principal benefits of a certification. The main effects observed from the audit process are increasing awareness of the importance of compliant behaviour for the organisation and effective communication from the top. Due the considerable numbers of people involved in the audit through interviews or observations of their day-to-day tasks, the audit is well-known throughout the organisation. The certificate is used for external stakeholders to demonstrate commitment to business activities in compliance with applicable regulations. Referring to the example given at the beginning of my contribution: a small and medium-sized company is faced with numerous requests from its suppliers to demonstrate the approach to compliance. A certificate may not replace or substitute due diligence by the business partner but it may positively influence the extent of such investigation.
The external audit process provides a summary of information to management about the status quo of the organisation's CMS in comparison to an international best practice benchmark. Last but not least, the three-year certification cycle under the ISO scheme ensures a structured approach to continual improvement of the CMS.

Cross-Border Compliance Standardisation – A Swiss NGO Perspective

Daniel Lucien Bühr*

I. Introduction

Switzerland has always been an active member country in international standardisation bodies. This is because Switzerland, with its small domestic market, has a vital interest in accessing foreign markets and ensuring low technical barriers to do so. With the increasing importance of cross-border services, the interest in international standardisation has also expanded beyond technical product standards and, today, includes management system standards. Switzerland, through the Swiss Association for Standardisation SNV, has actively contributed to the establishment of "ISO 19600 – Compliance Management Systems" and is also actively involved in e.g. "ISO Technical Committee 262 – Risk Management". Today's globalised economy would not have developed without international standards. Many aspects of our life are based on international standards, from the DIN A-4 format to "ISO 9001 – Quality Management" and the international financial reporting standards (IFRS). It is evident that standards are necessary to reduce complexity and cost for companies and individuals and to abolish barriers that would otherwise restrict trade, development and prosperity. The same goes for management system standards for risk management and compliance management. "ISO 31000 – Risk Management" and ISO 19600 are two key standards for best practice risk and compliance management. They are the only international standards in their field (if one defines a standard as a generally accepted description of the state of the art which has been developed by an independent standardisation body in an open, transparent process and by consensus). Of course, there are many guidelines and frameworks available for risk and compliance management. However, none of the organisations issuing such guidelines are independent nor are their standards generally accepted by all members of society, nor are their processes entirely open to all interested persons. Therefore, the availability of international standards for risk and compliance management is an important step towards better management of compliance risks and a chance for global uniform best practices resulting in a significant reduction of complexity and cost.

II. Standards are, by nature, genuinely cross-border and cross-cultural

The way international standards are developed (for instance by the International Standardization Organization ISO), is genuinely cross-border and cross-cultural. ISO Standard 19600 was developed by experts representing 11 member countries from America, Europe, Asia and Australia. The almost 30 experts were delegated from their national standardisations organisations to participate in the ISO project committee. During a period of 2 ½ years more than 1,000 comments on the draft standard were discussed and accepted or rejected in the consensus process. Thus, by the very way international standards come to existence, they represent what international experts view as being the state of the art in a particular field. Clearly, international standards are not free from error. However, they are reviewed every couple of years and, during this review process, comments from all interested stakeholders are considered (again by consensus). Looking at the process of international standardisation, it quickly becomes clear that no state, government or company (however big and powerful) can outperform an international standard on its own. A single organisation can never be as independent, international, multicultural and inclusive as the ISO, for instance. Moreover, given the cost associated with the individual exercise of re-inventing the wheel, it becomes evident that organisations should make use of generally-accepted instruments whenever they are available (such as international standards). Failing to do so results in a waste of financial and human resources and sub-optimal management effectiveness.

III. To effectively promote compliance, access to know-how must be low cost and easy

International standards are particularly important – if not vital – for small and medium-sized organisations, including governments with limited resources. They cannot afford to create their own way of doing things and they may lack technical expertise. Imagine a regulator in a poor country who wishes to understand what the current state of the art in compliance management is for the supervision of its banks, insurance companies and asset managers. With a few hundred USD, government officials can buy the relevant standards and get access to information that would easily cost a few million USD and a lot of human resources to (sort of) establish on their own. Furthermore, when government officials decide to incorporate international standards into their regulatory framework they use the same terms and speak the same language as their counterparts in other countries. They can even ask them for advice and exchange experience over time.
What applies to small and medium-sized organisations and developing countries also applies to large organisations, rich countries and their agencies. They are not able to create a true standard either and, in terms of resources, it also makes no sense for them to re-invent the wheel. After all, imagine the cost that would be saved if all companies of a regulated sector were required to choose one single standard (e.g. ISO 31000) for their risk management system. From a domestic and especially global point of view, the reduction of complexity and cost for organisations, for regulators and for external auditors (who would then review and certify standardised processes), could easily amount to tens or even hundreds of billions of USD per year. Money that is currently wasted.

IV. Public organisations and standardisation

International standards for management systems are addressed to all organisations, private and public. Public organisations should assess and treat their risks and manage compliance with the same diligence as any private sector company or NGO. Since public organisations generally act under parliamentary supervision, they are careful to maintain their independence – particularly from certain industries and foreign governments. Against this background, it is evident that the public sector can only apply independent and generally-accepted standards. A German regulator will most likely not apply or require companies to apply guidelines issued by a US regulator, for instance. And a Swiss regulator or agency would not be able to apply guidelines developed by a business association when assessing a compliance defence argument raised by a company under investigation. Under such circumstances, regulators can only apply independent national or international standards.

* *Daniel Lucien Bühr*, Member and lecturer on compliance management systems with the Swiss Association for Standardization/SNV, Vice-Chair Ethics and Compliance Switzerland/ECS and Partner at law firm LALIVE, Zurich. The views expressed are personal views and do not necessarily represent the views of SNV and ECS.

By way of example, the Swiss Confederation applies ISO 31000 across the board in the Federal Administration for risk management. The Swiss Competition Commission refers to ISO 19600 (among other guidelines) as a benchmark to assess whether it should accept a company's compliance defence and reduce a competition sanction because the company acted diligently in designing, implementing, maintaining and continually improving its compliance management system.

V. Standards strengthen sound principles, good governance and foster accountability

Standards are, by nature, based on principles. ISO Standard 19600 is a 30-page document. This is a very short guideline for a topic that could easily fill thousands of pages if one goes into details. However, the principles matter more than the 1,000 details and 10,000 rules you can imagine. In practice, it is usually the case that organisations get the principles wrong rather than the details. ISO 19600 is centred on leadership, ethical values and culture. They are the key drivers of effective compliance management. If an organisation decides to allocate resources to compliance but top management does not lead by example and is not seen to comply in the organisation, then every dollar spent on compliance is a waste of money. It is not a coincidence that almost all material integrity and compliance crises have resulted from a lack of leadership, values and culture. Therefore, one needs to get this right before starting to spend time and money on day-to-day compliance management. This underlying concept is stated clearly throughout the entire ISO Standard. The same goes for the implementation of a good compliance governance framework. Unless the compliance function has direct access to the board, is independent from line management and is given appropriate authority and adequate resources, every single dollar and every hour spent on compliance management will be of little use or even useless, depending on how severe the governance failure is. Standards also foster accountability because they demand clear and documented functional tasks and responsibilities, which must be measured and audited for effectiveness and be subject to regular reporting to top management and the governing body. Any organisation without clear functions and functional accountability is prone to risk and failure.

VI. Summary

Many organisations complain about too much regulation and demand less regulation. However, what they should really be demanding is more global standardisation of regulation which, in itself, would reduce regulatory complexity and cost to the maximum. Systematic risk and compliance management are topics which, for a few years now, have been outlined in international standards, particularly in ISO Standards 31000 and 19600. Organisations are free to apply international standards or other guidance or no standards or guidance at all. Not following a generally-accepted international standard is an option but clearly a bad, expensive and risky one. Organisations following a multitude of guidelines or following an "invented-here" approach inevitably spend more time and money on developing a framework which, by its very nature, will not be able to match the quality of an international standard. However, it is not only a waste of resources to re-invent the wheel but also a receipt for sub-optimal effectiveness and increased risk, for a lack of transparency and expensive follow-on costs (for instance for educating the auditors and new employees on what exactly one is doing). Imagine the financial savings and improvement in effectiveness that could be gained if all regulated financial institutions in the world were to apply a small number of generally-accepted international standards: all professionals would speak the same technical language, they would respect the same principles and apply the same practices and it would be transparent and easy to understand for employees, auditors, investors and regulators. The gain in effectiveness and the savings achieved by the reduction in complexity and cost would certainly be massive, to say the least. The positive result would certainly be comparable to the well-known result of applying generally-accepted accounting standards as opposed to the situation that existed up to the 1950s, where every organisation essentially had its own individually-accepted accounting standard. Therefore, it is time to think and act big and move forward to a less complex, less expensive and more effective risk and compliance management based on international standards. All organisations should act *now*: companies, governments and NGOs, for their own and their employees' benefit and also for a better society.

Introducing Compliance to the Shop Floor – ISO 19600 and Germany

Michael Kayser*

When the International Organisation for Standards published the ISO 19600 Compliance Management Standard in late 2015, the reaction throughout Germany was scepticism to harsh critique in some compliance quarters. Critics questioned how the organisation responsible for technical standards could concern itself with a largely legal topic. "Amateurs vs. professionals" was the tag line on the one hand, "Nothing new here and therefore not required" on the other. Initially, the compliance profession's scepticism outweighed the curiosity that should have been warranted. This reaction may not be as surprising as it seems, given the development of compliance in Germany in the past. Understanding the history of compliance, and how Germany got to where it is today, may explain some of the controversy surrounding the reaction towards the standard.

I. Compliance in Germany

Germany has had its fair share of high-profile compliance cases, with a prominent case 2006 when Siemens got into trouble, closely followed by major breaches within Daimler, Deutsche Telekom, and Deutsche Bahn among others. These compliance cases where rigorously prosecuted with hefty fines being imposed. Consequently, calls for protective measures were made – particularly from and in relation to the supervisory boards and their potential liabilities. The call for compliance management systems grew stronger and (at least within large, publicly listed organisations), significant investment went into establishing related structures. Against this background, it is no surprise that the people charged with establishing and maintaining those structures came from a predominantly legal background, having previously been lawyers and solicitors or involved in internal audit or finance.

In the years that followed, compliance established itself as a predominantly legal concept affecting organisations, starting with the large, publicly listed companies. During this period, the focus started shifting from purely defensive characteristics to the implementation of preventative measures. At the same time, compliance requirements found their way into supply chain relationships, increasingly affecting the "*Mittelstand"* (i.e. organisations still considerable in size, but neither listed nor publicly owned). Over time, these developments contributed to a considerable level of compliance awareness and maturity in Germany.

II. Operational and Legal Aspects

Interestingly enough, it could be argued that promotion through supply chain relationships and the increasing focus on preventative measures saw organisational and operational aspects starting to move into the foreground, adding to the originally legal risk. Therefore, it seemed natural for standards organisations to step up to the challenge and get involved, particularly in relation to management system standardisation. Approaching compliance from an organisational and operational perspective can even be characterised as the point when it arrived in the day-to-day business world, offering the chance to make it mainstream – somewhat like to the concept of quality in the mid-80s.

III. The Approach

In developing ISO 19600 (and as with earlier management system standards), the aim was to provide guidelines and guidance for organisations that wished to firmly implement compliance in their respective organisations. In developing this concept, nothing radically new was invented. Rather, the work involved taking various concepts, guidelines and principles that existed locally to a certain level of detail, such as the national standards of Austria and Australia, general worldwide principles (as formulated by the UN Global Compact) and various other initiatives (e.g. the ones published by the OECD). In its development, it incorporated experience already gained over the past few years, including that of compliance-mature environments. Consequently, the result reflects rather than contradicts existing practices, adding an operational dimension and (most importantly) a universal international understanding of the concept of a compliance management system. From a German perspective, it translated a legal view into an operational, management system- based approach.

* *Michael Kayser* is a seasoned professional with over a decade experience in high-stakes, mission critical technology based services. A veteran of the e-learning and assessment industry, he leads market leading compliance services provider Idox Compliance now.

IV. Adoption, Use and Benefits

As is generally the case with every standard, the benefits of ISO 19600 will vary across sectors, types of organisation and regions. Heavily regulated sectors such as the financial industry that have had experience with compliance measures, processes and procedures for many years (sometimes without the desired effects) will probably not be the first to use ISO 19600. Equally, large and publicly-listed corporations that are already operating compliance management systems and have been doing so for years (as is the case in Germany), will not be the first to implement the standard in their respective organisations. Those organisations starting to establish such management systems will be interested in using ISO 19600 as the guiding basis for their efforts (particularly in Germany). For those companies, ISO 19600 is an obvious choice to demonstrate their compliance management arrangements to clients and customers in an increasingly global economy with international business relationships.

For organisations that consider themselves "compliance mature", using the standard as a benchmark and requirement in relation to their business partners provides an opportunity for improving compliance management across the supply chain and increasing efficiencies in managing compliance across these relationships. In this context, for those requiring evidence of a certain quality of compliance management, ISO 19600 provides an international, universal point of reference for the compliance management system an existing or future business partner has in place. It can be a powerful tool for compliance officers in mature organisations in Germany and elsewhere. It has the potential to assist in the adoption and implementation of compliance in one's own organisation and provides an objective requirement for business partners and suppliers in support of one's compliance efforts. This aspect, in particular, has led to a more measured view and evaluation of ISO 19600 in Germany. In addition, the argument that compliance is essentially a legal matter is beginning to be put in perspective. With ISO 19600, translating a concept or principle (here, compliance) into operational measures and processes, implementing it across an organisation "on the ground", supports a preventative approach. It translates the (usually) abstract concept of compliance into tangible, concrete operational processes, procedures and measures. Using a shared terminology and approach with other management system standards, it facilitates understanding and implementation within the organisation. In the process, it recognises existing structures and processes, utilising and expanding them where necessary.

V. Where Are We Now?

After the controversy that ensued with the publication of the standard, media coverage was considerable and debate and discussion within the profession was lively and passionate. As the debate continued, two aspects became increasingly evident: the standard would come and, more importantly, it could be considered as actually complementing existing compliance efforts. As for the standard itself, adoption across Germany has begun with a number of organisations aligning their compliance management systems with ISO 19600. Even the first certifications have been completed and the providers of such certifications are growing in number. Adoption in neighbouring regions is also picking up, as is international adoption – particularly in Asia. It is therefore to be expected that adoption will also grow via international supply chain relationships.

VI. Outlook

The compliance community and beyond is increasingly considering the approach that the compliance standard offers, similar to the developments we have seen with ISO 9001. In that sense, ISO 19600 can bridge the abstract threats and operational risks that an organisation can evaluate and mitigate using appropriate operational measures. It provides compliance managers with a tool – and often language – that the operating business can understand, is often already familiar with and can relate to. It is, however, increasingly recognised that it can contribute positively when implementing cross-border, cross-organisational compliance programmes. In addition, the association of accounts with their proprietary audit standard means that ISO 19600 is increasingly viewed as a precursor and route to a successful audit certificate. What happened in Germany is introducing the topic into the wider business community and bringing compliance out of its ivory tower. Considering history, ISO 19600 may not have the game changing impact in Germany that it had in other regions (incidentally, ISO 9001 did not have that effect either), but it is on its way to becoming a formidable tool in the compliance manager's toolkit.

ISO 19600 – An Open and Flexible Standard in a Regulated Context that also offers Benefits at International Level

Prof. Dr. Peter Fissenewert*

ISO 19600 can be used to internationalise standards of compliance management for use by countries throughout the world. As a cross-border code applicable to all branches, the norm can be used to achieve internationally uniform framework conditions for establishing and implementing compliance management systems in the most diverse types of organisation. The norm considers not only a company's international activities and organisation but also its size (i.e. medium-sized companies), insofar as many clauses include the express reference that the norm's scope of application depends on the organisation's structure and complexity. Compliance is like a suit, tailored to a company's size and individual characteristics.[1]

In addition, the norm provides recommendations on how to observe principles of good governance (i.e. proportionality, transparency and sustainability). In this respect, ISO 19600 also takes account of value systems in that it consists not only of obligations which organisations are compelled to fulfil but also those they wish to fulfil and which comprise of society's social and ethical values. Today, it is generally recognised that compliance solutions must be determined by the needs of the organisations in question. This often has the consequence that compliance management systems differ markedly from country to country. The variety of solutions increases when other countries are considered. At this point, the first crucial question arises: how can standards, which are characterised as fixed, ensure flexibility? ISO stands for "International Standard Organization". It is an international association of organisations responsible for norms and develops international norms in all areas with the exception of electricity and electrical appliances (for which the International Electrotechnical Commission (IEC) is responsible) and telecommunications (for which the International Telecommunications Union (ITU) is responsible). Standards or norms are rules that are recognised by society as a whole or in certain areas.

At international level, compliance is found in different national settings. The consideration of cultural peculiarities differs not only from case to case but also state to state. There are even regional cultural peculiarities within a country. Against this background, the question arises as to what extent an internationally active company is prepared to subject itself to a minimum cultural standard which is to be applied independently of any less strict cultural requirements that may exist. In law, something similar already exists. Such "supra-legal standards" can be found in the fields of environmental protection, product liability and labour conditions. A corresponding minimum standard is required by rating agencies for ethical investment. Accordingly, lists of criteria ask what percentage of the workforce are affected by a certain rule.[2] These criteria have to be established centrally and be observed by all companies regardless of national legislation.

However, it must also be observed in this respect that a central compliance department might be overstretched if it had to deal with each and every cultural peculiarity in every country. This would be impossible due to linguistic and cultural barriers. For this reason, the central criterion of the great cultural guideline should be expanded with decentralised cultural components. The minimum standard should be set centrally but the consideration of national peculiarities must take place locally. Thereby, it is particularly important to consider national cultures. Accordingly, other cultures may make it necessary to pursue e.g. anti-corruption strategies in South European countries more intensively than in Scandinavia. The example of anti-corruption strategies (i.e. following the law and prosecuting infringements) is closely connected to respecting different cultures. Accordingly, respecting foreign culture can lead to liability since German management can also be personally liable under German law for infringing compliance requirements abroad.

---

* *Prof. Dr. Peter Fissenewert* is a partner at law firm Buse Heberer Fromm. He is specialized on consulting companies and entrepreneurs, associations and institutions in all corporate law matters.

1 See also *Makowicz*, in: *Makowicz*, Praxishandbuch Compliance Management, Grundsätze der Compliance, 1–10, p. 4, 2016.

2 See *Behringer* in Compliance kompakt, 2010, p. 398; cf. e.g. the FTSE4Gob Inclusion Criteria, available under: http://www.ftse.com/products/downloads/FTSE4Good_Index_Series.pdf?32.

This is not only seen in criminal liability (under German law) for bribes made to public officials and private persons from a foreign country, which has existed for a long time. Moreover, there is a significant risk of the company (from a foreign perspective, this is the parent company in Germany) making compensation claims against its management board in Germany owing to compliance infringements abroad. This was made clear by the seminal "Neubürger Judgement" issued by the *Landgericht München I* (hereinafter "Munich I District Court"). Siemens AG sued their former financial chairman for compensation of 15 million euros because he had infringed his compliance duties. The Munich I District Court allowed the action.[3]

The charge against Neubürger, the former financial chairman, alleged that he had breached his compliance duties as member of the board in relation to cases of corruption abroad. The Munich I District Court justified its judgement as follows: "The accused failed to take any or at least adequate measures to clarify and investigate the breaches, to prevent their occurrence and to punish the workers responsible, despite having them repeatedly brought to his attention." The District Court continued: "Above all the repeated occurrence of breaches or at least serious suspicions in connection with cases of corruption abroad show that the current system is not adequate. However, in this case, it is the responsibility of each member of the board and thereby the accused, as part of his supervisory duty, to ensure that within the board a functioning compliance system is agreed." Consequently, the District Court stated: "Accordingly, international bribes represent a statutory breach that cannot be justified by claiming that, without them, it would not have been possible to succeed economically on corrupt foreign markets." Concerning the applicable standard of care and compliance duties of a member of the board, the Court stated: "Considering the dangers involved, the board would only satisfy such a duty if it established a compliance organisation that was designed to prevent loss and control risks."

Regarding the management's compliance duties in Germany, it is insignificant in which country bribes are paid. In this case, even minor negligence can lead to liability. This is clearly stated in the District Court's decision. Moreover, high compensation amounts may threaten the very existence of the board member concerned.[4]

The judgement of the Munich I District Court is not only forward-thinking regarding the standard of the board's liability in German stock corporation law; it also affects the management of a GmbH. Observing the flexible standards of ISO 19600 is of crucial importance for the success of compliance management at international level. Ideally, compliance will then be regarded as the standard for all employees at all corporate levels and internationally.

3 LG München I, 10.12.2013 – 5 HK O 1387/10.

4 *Stucken/Senff*, Compliance-Management in China: Praxishandbuch für Manager, 2015, p. 164.

Chapter 6: Whistleblowing Challenges

Romanian Whistleblowing Regulations: From Exemplary to Incomplete

Dr. Raluca-Isabela Oprişiu*

Compliant conduct is said not to be separated from ethics and morals. In Romanian society (formerly often perceived as immature and corrupt), situations of abuse, waste or fraud used to be the norm. However, ethical rules are changing and compliance has also become highly topical in Romania. Public and private companies are looking for the right way of conducting their activities on the basis of legally and ethically irreproachable principles, often realising that the local customs are not easy to cope with. Although Romania took the lead in establishing protection for whistleblowers in the public sector in 2004, reporting itself is still traditionally connected with the communist past and the terrorised society in which "everyone informed on everyone else"[1]. The wind has changed slowly and the rules which first looked good only on paper are starting to be effective in practice, too. The following report offers a general overview of the most relevant aspects of whistleblowing in Romania and the relevant case law of the High Court of Cassation and Justice.

I. Compliance and Ethics in the Public Sector

Romanian Law no. 571/2004 ("Law 571")[2] was one of the pioneering laws in Eastern Europe to deal with the protection of whistleblowers in the public sector. Public authorities were compelled to harmonise their internal by-laws with legal provisions within 30 days from the entry into force of such law. However, this did not always turn out to be successful. One example is a decision where policemen were found guilty in the first instance of breaching internal rules which prevented them from communicating with the press[3]. In the private sector, no equivalent protection was provided by the generally applicable labour law; this was seen as a gap which has since been filled by labour law courts, using the principles of non-discrimination, proportionality etc[4].

II. The Whistleblower (Ro. *avertizor de integritate*)

On the basis of art. 3 lit. b of Law 571, only employees of public authorities and civil servants can claim the status of a "*avertizor*" (i.e. "whistleblower") and thus be able to report a violation of law or other irregularities covered by the legal provisions. Independent contractors are not protected by the above-mentioned regulations. A special situation exists in respect of so-called "competition whistleblowers (Ro. *avertizori de concurenta*)." Such whistleblowers have been encouraged by the Romanian Competition Council since 03.03.2016 to notify any breaches of competition law on a secure and anonymous platform[5]. Any whistleblowing in either the private or the public sector is covered by art. 35 of Competition Law no. 21/1996[6]. The Competition Council may apply certain mitigation procedures in such cases.

III. Protection of Whistleblowers

A whistleblower submitting a report is generally protected against dismissal and any kind of detriment suffered consequently to his disclosure action[7]. Art. 7 par. 1 lit. b of Law 571 gives this person the right to ask for the presence of a trade union representative or the press if invited to a disciplinary commission after having reported internal wrong-doings. In most cases, a whistleblower will contest any disciplinary measures and thus have their proportionality confirmed by a Court. The employer bears the burden of proof regarding causality between the disciplinary sanction and the whistleblowing. Concerning proof of the allegations made by the whistleblower, the latter must demonstrate his good faith according to the aforementioned principles of art. 4 of Law 571. If the Court subsequently discovers that the sanctions were disproportionate, it will annul the internal decision and reinstate the whistleblower if he has been dismissed.

IV. The Motivation of a Whistleblower

According to the definition of "whistleblowing" in art. 3 lit. a of Law 571, such reporting must be made in good faith. The principles of responsibility (art. 4 lit. c) and of good faith (art. 4 lit. h), expressly referred to, state that a whistleblower may benefit from legal protection even if the information turns out to

* *Dr. Raluca-Isabela Oprişiu*, LL.M. Eur. Integration, Avocat (Attorney-at-Law RO), STALFORT Legal. Tax. Audit.

1 On the historical sensitivity of this topic, see: Radu Ogarca in: "Whistle Blowing in Romania", 2009, http://feaa.ucv.ro/RTE/013S-14.pdf (accessed on 27.08.2016).

2 Law no. 571/2004 regarding the protection of the staff of the public authorities, public institutions and other units that notifies breaches of law, published in the Official Gazette no. 1214/17.12.2004.

3 Decision no. 2567/2011 in the file no 9662/1/2010 pronounced on 05.05.2011 by the Administrative and Fiscal Contentious Section of the High Court of Cassation and Justice (http:// www.scj.ro/1093/ Detalii-jurisprudenta?customQuery%5B0 %5D.Key=id&customQuery%5B0 %5D.Value=94159, accessed on 27.08.2016).

4 According to Raluca Dimitriu "There is an oasis of detailed regulations in an ocean of uncertainty" – see p. 245 in: "Romania: First Steps to Whistleblowers' Protection", published in Whistleblowing – A Comparative Study (*G. Thüsing/G. Forst*, eds.), Springer International Publishing 2016.

5 https://secure.secway.info/ro/start.php (accessed on 27.08.2016).

6 Competition Law no. 21/1996, republished in the Official Gazette no. 153/29.02.2016.

7 See decision no. 5857/2011 in the file 7159/2/2009 pronounced on 06.12.2011 by the Administrative and Fiscal Contentious Section of the High Court of Cassation and Justice (http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=91626, accessed on 27.08.2016).

8 Decision no. 5545/2011 in the file no. 9562/57/2010, pronounced on 22.11.2011 by the Administrative and Fiscal Contentious Section of the High Court of Cassation and Justice http:// www.scj.ro/1093/ Detalii-jurisprudenta?custom-Query%5B0 %5D.Key=id&customQuery%5B0 %5D.Value=80655 (accessed on 27.08.2016).

be incorrect, provided he was convinced of the truth of the facts described and the reported violation of law. Art. 7 par. 1 of the Law presumes the good faith of a whistleblower.

Unfortunately, there is only limited case law to substantiate such principles. A not entirely comprehensible decision no. 5545/2011 of the High Court of Cassation and Justice[8] held that a policeman was denied promotion because of a TV appearance in which he described the grading system of his police department and the personal abuse of his senior officers. Given the fact that only two of his three allegations were proved to be correct, both the judge of the first instance and the judges of the High Court decided that the punishment was appropriate.

Moreover, a highly debated decision of the European Court of Human Rights in the case of Bucur and Toma against Romania[9] tackled issues connected to whistleblowing, privacy, freedom of expression and revealing classified information on a government wiretapping intelligence programme of the Secret Intelligence Service (Ro. *SRI*). In this case, the European Court decided that Mr. Bucur had acted in good faith when taking the steps for disclosing illegal SRI conduct and was convinced that this outweighed the interest of maintaining public confidence in the SRI (para. 115). In connection with the topic of motivation, there was a public discussion in Romania on whether to provide for financial incentives or rewards to whistleblowers using the models in other countries. No decision has yet been taken but this is expected to be introduced for competition issues linked to considerable pecuniary sanctions.

V. Anonymity of Whistleblowers

Anonymous reports are controversial in Romanian law and are closely connected to the concept of good faith. O*n the one hand*, art. 7 of Governmental Ordinance no. 27/2002[10] provides that anonymous petitions are not to be taken into consideration. Especially in relation to petitions of irregularities involving employment issues, art. 18 lit. c of Law no. 108/1999[11] imposes a duty on labour inspectors to protect the identity of the whistleblowing employee by withholding the information that their checks are based on a report received for the authority's attention. *On the other hand*, it is exactly this aspect of anonymity which makes whistleblowing systems so attractive in the private sector. Private companies search for the right compliance tool (either web-based or by involving external ombudsmen who encourage employees to notify wrongdoings, etc.). Hence, the right to remain anonymous should be reinforced.

VI. The Reported Wrongdoings

Art. 5 of Law 571 protects whistleblowers where they report violations of the law in terms of corruption[12], conflicts of interest, abuse of authority, public tenders, misuse of public resources as well as mismanagement and other irregularities. A clear example can be found in a textbook case of the High Court of Cassation and Justice regarding the sanction applied to an employee of the Central Military Emergency Clinical Hospital, who had complained about the wrongful managerial activity of his hierarchical superior (among other things)[13].

VII. Recipient of the Report

According to art. 6 of Law 571, the report has to be presented to the hierarchical chief but can directly be disclosed to the press or parliamentary commissions, trade unions, NGOs etc. The whistleblower himself can choose to whom to disclose the information taking into account the particularities of each case and his intentions. One case from 2009 showed that, in practice, some Romanian judges from the first instance were not familiar with such alternatives because they permitted a policeman, who had directly informed the press, to be punished for by-passing the internal reporting system and informing the press directly.[14]

VIII. Summary

Romania introduced legislation providing special protection for whistleblowers in the public sector as early as 2004. Such detailed legislation provides a high level of protection compared to other European countries. However, it has not led to a consistent jurisprudence that encourages a high number of whistleblowers to come forward.

In the private sector, discussions started much later but the topic has attracted great attention. Romanian companies that wish to be taken seriously on the private market by competitors and clients are already taking the first steps in implementing active compliance systems and (in some cases) whistleblowing mechanisms. The Competition Council (the Romanian anti-trust authority), has taken the lead in this respect and established a special platform for competition issues. Such actions, together with a considerable number of arrests of senior officials on bribery charges, have contributed to changing the citizens' attitudes towards ethics, the institutions and their trust in the morals and civic values so deeply affected by history.

9 For a summary of the most important facts and arguments see http://www.right-2info.org/cases/r2i-bucur-and-toma-v.-romania (accessed on 27.08.2016).

10 Governmental Ordinance no. 27/2002 regarding the regulations of the activity to solve petitions, published in the Official Gazette no. 84/01.02.2002.

11 Law no. 108/1999 for the establishment and the organisation of the Labour Inspection, republished in the Official Gazette no. 290/03.05.2012.

12 It was the corruption offences which determined the adaptation of the whistleblowers' protection. Given the success of the Romanian anti-corruption body (DNA – *Directia Nationala de Anticoruptie*) in recent years, the general perception of the population has changed regarding reporting corruption cases. According to the last report, published on 27.01.2016 by the European Commission, around 85-90% of the cases leading to convictions originate from citizens' complaints (p. 10, fn. 40, http://ec.europa.eu/cvm/docs/com_2016_41_en.pdf, accessed on 27.08.2016).

13 Decision no. 4743/2008 (ref. no. 8972/2/2007) pronounced on 16.12.2008 by the Administrative and Fiscal Contentious Section of the High Court of Cassation and Justice (http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=46479, accessed on 27.08.2016). The complaining physician brought also consistent proof on the medical career and the inacceptable behavior of his commander.

14 See decision no. 2567/2011 quoted above under fn. 3.

"Whistleblower protection" – legal threats and challenges in Poland

Marcin Gomoła*

Poland is one EU country which does not have a dedicated national regulation covering the issue of whistleblower protection. Until 2014, there was no regulation regarding compliance in the Polish economy – apart from the banking and finance sector, which was regulated by EU rules and local regulations. As of 31 March, 2016 the first national compliance conference took place at the Warsaw Stock Exchange. As a result of this and many conferences afterwards, the Warsaw Stock Exchange and Polish Financial Services Authority adopted the Corporate Governance Code which established a system of compliance in October 2015. The whistleblower protection topic is a continuation of these regulations. The protection of whistleblowers is not regulated in the Polish legal system, except one provision in banking law. The regulation of a whistleblower status (particularly its legal protection) is not easy to achieve in Poland, mainly due to Polish historical experience and the social perception of a „denunciator" (as whistleblowers may appear to be). Polish cultural heritage means that even today it is not easy to say whether a „whistleblower" is regarded as a hero or a traitor. These doubts are highlighted in a Polish survey organised by Batory's Foundation in 2013. The results were as follows:

- 77% of respondents believed that an employer would negatively react against an employee who reported irregularities,
- 4% of respondents believed that the employer would use the information obtained to prevent similar irregularities,
- 1% of respondents believed the employer should reward the whistleblower,
- 80% of Poles believed that an employee who reported irregularities to the relevant departments in the interests of the employer or the public interest should be entitled to legal protection,
- 63% of respondents believed that a whistleblower would not obtain effective legal protection.

Whistleblowers inform their organisations about: conflicts of interest, fraud, acts of corruption, offences and similar irregularities taking place in the organisation where they work. Often, the consequence of such reporting (or denunciation) is to ostracism in the form of mobbing, harassment and humiliation by colleagues as well as social problems. Therefore, special treatment and care should be given to the person who, despite these negative consequences, has finally decided to report irregularities. This is especially important considering that, in many cases, the whistleblower's information is the only evidence of fraud that exists.

Although the information about irregularities provided by whistleblowers may be accepted and highly valued, there are simply no regulations protecting whistleblowers either directly or indirectly in Poland. The pressure on

* *Marcin Gomoła*, Compliance Officer, T-Mobile Polska S.A.

whistleblowers together with an unfavorable legal environment which, in its extreme form, can even take the form of civil and criminal charges or multi-million Euro compensation claims is not helping whistleblowers. Whistleblowers are confronted with legal pitfalls, starting with regulations on protection of privacy, reputation and personal data, to regulations requiring care for the good name of the employer, which may be affected by the whistleblower's reporting on irregularities. Whistleblowers who reveal irregularities must therefore take into account the charges of slander and causing unjustified suspicion. We have found that every single legal Act in Poland, relevant for the protection of whistleblowers (e.g. the Labor Code, Civil Code, Penalty Code, Data Protection Act) includes provisions that can be easily used to the detriment of whistleblowers. At the same time, protective provisions are lacking. The only way of protecting whistleblowers is to regulate this topic within the internal procedures of a company.

For example, the whistleblower's civil legal liability for infringing the personal rights of a person against whom action should be taken may be applied based on Sec. 24 of the Polish Civil Code. This regulation states that those whose personal rights are threatened by actions of others, may request action, unless it is not unlawful. An infringement may also demand that the person responsible takes the action necessary to remove its effects, in particular, making a statement in the appropriate content and form. The conditions laid down in the Code may also demand financial compensation or payment of an appropriate amount of money for a specific publication. Victims may seek compensation on general principles if a breach of a personal right gives rise to material injury.

Whistleblowers are also open to the threat of criminal liability in accordance with Sec. 212 of the Polish Criminal Code. One of the legal grounds is found in Sec. 212 § 1 of the Criminal Code which imputes to another person, group of persons, institution, legal person or entity without legal personality of such behavior or characteristics that could humiliate him in public or expose him to loss of trust necessary for a particular position, profession or activity.

Another criminal regulation, which might be used against whistleblower, is the duty of confidentiality regarding confidential information protected by law according to Sec. 265-266 of the Criminal Code (esp. Sec. 265. § 1). Whoever discloses or, contrary to the provisions of this Act, uses information classified as "secret" or "top secret", is punishable by imprisonment from 3 months to 5 years. Also Sec. 266 of Polish Criminal Code states that, whosoever, in violation of the law or obligation he has undertaken, discloses or uses information with which he is familiar due to his function, work, public activity, social, economic or scientific activity, shall be subject to a fine, restriction or imprisonment of 2 years.

In criminal proceedings, the institution of the "anonymous witness", applies in exceptional cases (e.g. whenever life, health or property of significant value is threatened, see Sec. 184 et seq. of the Polish Code of Criminal Procedure). This can be seen as a form of "whistleblower protection" but is limited to the number of criminal offences. However, the solution provided by such regulation can be applied to provide general protection to whistleblowers. Moreover, the identity of whistleblowers in criminal proceedings can be withheld on the basis of Sec. 184 Polish Code of Criminal Procedure, which states that, if there is a justified fear of danger to life, health, liberty or property of significant value of the witness or the person closest to him, the court, and in preparatory proceedings the prosecutor may decide to hide the identity of the witness, including personal data. The procedure in this regard proceeds without the parties to proceedings and the subject is kept secret as classified information(i.e. "secret" or "top secret").

It is worth mentioning that confidentiality regulations adopted in a company's internal procedures protecting whistleblowers may cause problems under the Act on the Protection of Personal Data. In the light of this regulation, employers interested in such a mechanism may bear the risk of breaching data protection. Based on these rules, it may turn out that the employer will be obliged to disclose the personal data of whistleblowers to the person implicated in the irregularities. This is because Sec. 25 of the Law on the Protection of Personal Data, provides that the employer is obliged to inform the person to whom the data relates, *inter alia*, about the source of the data, the purpose and scope of data collection, the recipients or categories. Confidentiality is essential to the effectiveness of internal alert procedures.

Currently, the only „weapon" that whistleblowers still have is anonymity. However, this also significantly weakens the force of his argument in most cases and dissuades those who wish to make use of information by means of the whistleblower process. They cannot rely on the information anonymously but must use legal methods to investigate the whistleblower's credibility as this may be the only basis on which to formulate charges. If a whistleblower uses a tip-off portal he may stay anonymous but this makes it hard to use such information in formal proceedings (i.e. court hearing of evidence).

Therefore, a procedure that will protect the whistleblower from offences and improper treatment is vital in each and every company. Whistleblower protection regulations should not be based on simple "black-and-white" solutions but rather constitute guidance, and "navigation rules" instead of simple answers. Such an approach results from the fact that whistleblowing tends to be seen as a corporate "shadow zone". When preparing such a procedure it must be recognised that whistleblowers are motivated differently namely, to avoid conflicts of interest, unnecessary risks and to protect the company's interests.

There are also other challenges and "grey areas" that must be addressed in such a regulation. The first "grey area" is that the whistleblower may act in "bad faith" and accuse somebody of wrongdoing for a personal reason. Indeed, the whistleblower in this case may even be part of the fraudulent activity but, for whatever reason, has decided to reveal the irregularities and acquire the status of whistleblower. It must be clearly regulated and communicated, that this status is not available to persons who act in bad faith, is not given in advance and is not permanent. The protections granted by the status of whistleblower must also be clearly regulated and communicated. What whistleblower status means for (i) the whistleblower himself, and (ii) organisation must be clearly defined. Whistleblowers should be given a guarantee that they will be protected from i.e. dismissal and, in some justified cases, a guarantee of legal and personal security as well. For the company it means that such a person is privileged and cannot easily be removed from the company.

The second grey area arises when the whistleblower appears as a part of a fraudulent activity but then finally decides to blow the whistle on it. There is no simple answer to the question "What should we do now?" and, furthermore, there is no simple way of regulating such a situation. The only way is to professionally assess and decide whether the pieces of information provided by the whistleblower are sufficiently valuable to justify whistleblower status for this person regardless of his motivation to be whistleblower. There are plenty of reasons why such a person decides to become a whistleblower and what kind of information she/he brings. Accordingly, regulation must give a significant portion of discretion to the Compliance Officer when "dealing" with such a person. It must be stressed that, from the company's perspective, it is not really important what motivates the whistleblower. What matters is rather the accuracy of information provided by whistleblower, which may lead to uncovering the fraud.

A separate problem that arises in some jurisdictions (mainly common law countries), is whether to remunerate the whistleblower for information provided or not. The topic needs to be examined in detail as there are different types of whistleblowers. Those who are employees should be treated differently to those who are (i.e. customers or contractors, or third parties). For example, an employee is obliged to be loyal to his employer and is remunerated accordingly but a customer and contractor may not be necessarily loyal beyond the scope of the relevant contract. Therefore, additional incentives for the whistleblowers in the latter category should be considered (including those of a contractual nature).

Internal regulation on whistleblower protection should recognise that the person entitled to confer "whistleblower status" is the Compliance Officer who is also responsible for protecting the whistleblower form dismissal. He must closely cooperate with HR and the board member responsible for compliance. Such regulation should also determine (i) the definition of whistleblower, (ii) the scope of protection (corresponding to the legal environment), (iii) the time-limits for such protection, and (iv) the position and relevant authorisation for the Compliance Officer enabling him to confer such a status on a person and to keep him at the company for as long as he is a whistleblower. This should also be used as a basis for the further nationwide regulation of whistleblower protection.

Post scriptum

Everyone has almost certainly heard of Julian Assange or Edward Snowden or native whistleblowers and the accompanying scandals. Apart from the momentary flash of attention in the press (usually immediately after the scandalous disclosure of information), they are actually seen as lonely people – heroic, and modeled after Roman gladiators blessing Caesar before a fight to delight the audience. Such a picture – and such a fate – is not a good example and certainly does not convince ordinary people to "blow the whistle" in their own backyard. The image of a "Desperado" is not enough motivation to take on the difficult role of the whistleblower – even if the cause is a worthy one. Whether whistleblowers will be deemed heroes or traitors depends on what legal protections they are given internally; this determines their position both culturally and socially. At present, the legal regulation in Poland makes a whistleblower appear like „Don Quixote", fighting alone in the name of „higher cause". We can change this, starting from our internal TMPL regulation. What we can easily do is to communicate and create a „whistleblower culture" across the organisation and ensure the anonymity and proper treatment of persons who have made the difficult decision to share information about irregularities with us. We should recognise the protection of a whistleblower as a vital tool to avoid risks in the company and protect its reputation.

COMPLIANCE
ACADEMY

Bleiben Sie am Ball?

Haben Sie schon eine gut funktionierende Compliance-Struktur und können damit durch treffsichere Entscheidungen punkten?

Die Compliance Academy bietet Ihnen maßgeschneidertes Expertenwissen rund um Compliance an.