*Edited by*
Maria Krambia-Kapardis

# Financial Compliance
## Issues, Concerns and Future Directions

palgrave
macmillan

# Financial Compliance

Maria Krambia-Kapardis
Editor

# Financial Compliance

## Issues, Concerns and Future Directions

palgrave
macmillan

*Editor*
Maria Krambia-Kapardis
Faculty of Management
and Economics
Cyprus University of Technology
Limassol, Cyprus

ISBN 978-3-030-14510-1 ISBN 978-3-030-14511-8 (eBook)
https://doi.org/10.1007/978-3-030-14511-8

Library of Congress Control Number: 2019932965



This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*To my husband Andreas,*
*Our children Elena and Konstandinos-Raphael,*
*And my parents*
*For all their love and support*

# Acknowledgements

In June 2018, an International Conference on Compliance was held at Cyprus University of Technology, in the coastal town of Limassol. The speakers came from the USA, Australia, UK, France, and Cyprus. The aim of the conference was to raise awareness and build capacity for those working as compliance officers in the financial sector. The venue proved to be too small, and the issues discussed raised the need for a comprehensive book to be published to assist practitioners, researchers, and students who wished to practice as financial compliance officers. Thus, I take this opportunity to thank the sponsors of the conference, namely: PwC Cyprus; OPAP Cyprus; Map S. Platis; Y Georgiades and Associates LLC; Zygos; Omnimedia; and Legal News.

In assembling, editing and fine-tuning this volume, I feel immense gratitude toward a number of people for their contribution, support, and presence.

Firstly, I would like to thank all the chapter contributors/authors for their enthusiasm, patience, and support. Secondly, I would like to thank the editorial team at Palgrave Macmillan and in particular Ruth Noble and Tula Weis for their trust and continuing support throughout the journey. Without their support and hard work, this would not have been possible.

Thirdly, I would like to thank my family—my husband, Andreas, and our children, Elena and Konstandinos-Raphael, who encouraged me with their words of wisdom and empathy to pursue the idea of editing the book but, also, to stop, look, and enjoy life with compassion and

gratitude, while doing it. Finally, I am indebted to my parents Takis and Eleni who, despite the hardships of war and migration, worked hard to ensure that both my brother and myself had a good education and equipped us with resilience in life.

# Contents

# Notes on Contributors

**Stuart Bazley** is Visiting Professor in Financial Regulation and Compliance Law at BPP University Law School, London, where he is co-leader of an LL.M. programme in financial regulation and compliance law and programme leader for an LL.M. in commercial law.

**Anthony Bottoms** is Emeritus Wolfson Professor of Criminology in the University of Cambridge and Honorary Professor of Criminology in the University of Sheffield.

**Salomi Dimitriou** is a Lecturer in Accounting at the University of Central Lancashire and a Special Scientist at Cyprus University of Technology.

**James A. Fanto** is the Gerald Baylin Professor of Law at Brooklyn Law School and Co-Director of the school's Center for the Study of Business Law & Regulation.

**Mark Foulsham** is a CEO and Founder of Keyenable Ltd.

**Maria Krambia-Kapardis** is an Associate Professor of Accounting, Cyprus University of Technology, a Fellow Member of the Chartered Accountants of Australia and New Zealand and a Certified Fraud Examiner.

**Maria Lancri** is a French lawyer practicing as a Counsel with GGV Avocats à la Cour—Rechtsanwälte since 2015.

**Ioanna Stylianou** is a Lecturer in Statistics and Econometrics at the University of Central Lancashire Cyprus (UCLan) and Research Fellow at the University of Cyprus. She is the Course Leader for the Economics and Business Administration division at the University of Central Lancashire Cyprus.

**Justice Tankebe** is a University Lecturer in Criminology and a Fellow at St. Edmund's College, University of Cambridge.

**Eva Tsahuridu** is an Associate Professor and Industry Fellow at the School of Accounting, RMIT University, Melbourne, Australia.

# List of Figures

# List of Tables

# Introduction

Much has been written in recent years about human behavior and the tendency to avoid or bypass regulations and good behavior. At the same time, governments all around the globe have enacted legislation to prevent and punish those who do not comply. In legal entities like corporations where there are diverse culture and behavior, it has been difficult for regulators to ensure legislation is enforced and complied with. Thus, they have opted to pass the onus onto compliance departments, new entities appointed or set up, whose role is to ensure legislation is complied with. Such a task has many challenges and, at the same time, opportunities for those involved.

The current book aims to set the scene for the financial compliance in an effort to minimize the personal risks faced by those in compliance departments by raising awareness on the issues impacting on their work, discussing the concerns and suggesting policy implications that will turn the challenges into opportunity to improve their work. Unlike other books on compliance, the current book focuses in the first two chapters on what is described as compliance 'as viewed from below'; that is to say, a ground-level look at how compliance occurs. The chapters that follow are mostly concerned with how those who have a responsibility to enforce laws and regulations can achieve their ends with optimum efficiency and effectiveness—an approach that can reasonably be described as compliance 'as viewed from above'. As Professor Sir Anthony Bottoms explains in Chapter 1, these two types of analysis are in principle interconnected because an enhanced understanding of 'compliance from

below' (how and why compliance occurs) should enable enforcement agents to develop more sophisticated and effective compliance strategies.

Generally, all professions and, more specifically, professionals, for their work to be appreciated and relied upon it, ought to be legitimate. In setting the theoretical framework for the profession, legitimacy theory is considered as a milestone for the work carried out by compliance officers. In Chapter 1, Professor Bottoms sets the conceptual groundwork for later contributions in the book by exploring and categorizing the reasons why people comply with laws and regulations. He first explains the mechanism-based approach utilizing lessons from criminology and sociology and then moves on to discuss a typology of compliance mechanism based on instrumental, normative, situational compliance, and compliance based on habit or routine. Next, Sir Anthony discusses the Nielsen–Parker holistic compliance model and its three explanatory variables. In considering each set of variables separately, he compares them with his 'Typology of Compliance Mechanisms.'

Building on the conceptual groundwork of Chapter 1, Dr. Tankebe in Chapter 2 explores the role of legitimacy as a mechanism for compliance. As he argues convincingly, legitimacy is best viewed as a continuous dialogue; building and sustaining legitimacy requires the lawful, fair, and effective use of authority in everyday decisions. Tankebe reviews the literature and explains that research evidence makes it clear that legitimacy matters when it comes to encouraging compliance with laws and regulations.

Professor Fanto, in Chapter 3 of the book, explores the background and reasons for the uncertain professional status of the 'young' compliance occupation and identifies several negative effects or consequences of the compliance officer's uncertain professional status. The chapter also covers the oxymoron control over compliance officers by legal authorities and practitioners where it is sometimes passive or complacent.

In Chapter 4, Mrs. Lancri discusses the fact that compliance is a mindset and both hard and soft laws have a major role to play in ensuring the work of the compliance officer is carried out efficiently. The case of France is also discussed, and reference is made to the Sapin II legislation.

Protection of personal data is a topic that has raised a lot of discussion in the second decade of the twenty-first century and brought out of the shadow a concern for many citizens. Mr. Foulsham, in Chapter 5, discusses the General Data Protection Regulation and highlights the

realities of adopting the regulation and as he navigates his way through the essence of the regulation also considers how high-profile failures may have a dramatic impact on business success.

Professor Bazley in Chapter 6 considers aspects of the UK financial services law and regulation that require governance of risk and the maintenance of an internal compliance function. First, the chapter examines a number of key components of the law and financial services regulatory regime that require financial institutions to establish internal governance arrangements and systems of control devoted to the identification, control, and management of risk in financial services. He then provides an insight into the evolving nature of 'compliance,' the characteristics and responsibilities of a firm's compliance function, its positioning within a firm's overall control environment, and the extent to which a compliance officer and those working in a compliance function (including those working as a money laundering reporting officer) are accountable for their professional activities. Finally, Professor Bazley discusses the issue of personal liability, when things go wrong.

An issue many compliance officers are concerned with is their *legal obligation and protection* if they blow the whistle. Associate Professor Tsahuridu, in Chapter 7, discusses the issue of whistle-blowing and its effective management, exploring the role that effective management of whistle-blowing can play in ensuring organizations to comply with their legal and ethical obligations well as the incidence and reasons of inaction and silence by observers when misconduct exists.

In Chapter 8, I build on the work of Kristy Grant-Hart and discuss the skills required by the compliance officer in an effort to be effective in carrying out his/her duties. I acknowledge that the compliance officer is not an island and the success of his/her work depends on the Board's political will to provide the necessary resources to the compliance department to enable it to thrive and flourish.

As illustrated in some chapters, the compliance occupation is 'young' and the expectations imposed by the regulators and other stakeholders may at times be unreasonable. The authors of Chapter 9, Krambia-Kapardis, Dimitriou, and Stylianou, first contextualize the compliance program and the impact of non-compliance and then, utilizing Porter's theoretical model of the expectation gap, report findings from an empirical survey of compliance officers in Cyprus. The issues raised by these authors have implications for the future of the 'young' occupation and the development of the compliance profession.

This edited book with contributions from Europe, USA, and Australia is unique for it brings together both practitioners and academics to discuss and elucidate the issues, concerns, and future directions of the financial compliance profession.

Maria Krambia-Kapardis

CHAPTER 1

# Understanding Compliance with Laws and Regulations: A Mechanism-Based Approach

*Anthony Bottoms*

## 1 Introduction

The purpose of this chapter is to lay some conceptual groundwork for later contributions in the book, by exploring and categorizing the reasons why people comply with laws and regulations. The focus of the discussion will, therefore, be upon what the sociologist Frank Parkin (1982: 79) once memorably described as compliance 'as viewed from below': that is to say, a ground-level look at how compliance occurs. By contrast, later chapters are—entirely properly—mostly concerned with how those who have a responsibility to enforce laws and regulations can achieve their ends with optimum efficiency and effectiveness—an approach that can reasonably be described as compliance 'as viewed from above'. Despite their differences, however, these two types of analysis are in principle interconnected, because an enhanced understanding of 'compliance

A. Bottoms (✉)
University of Cambridge, Cambridge, UK
e-mail: aeb11@cam.ac.uk

A. Bottoms
University of Sheffield, Sheffield, UK



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_1

from below' (how and why compliance occurs) should enable enforcement agents to develop more sophisticated and effective compliance strategies.

In presenting this analysis in the context of a book whose main substantive focus is regulation in the field of business, I am very conscious that my own research career has concentrated on (in the clichéd phrase) 'crime in the streets' rather than 'crime in the suites'. It follows that my examples are principally derived from my main field of study. However, some business examples are included, and some attention will also be paid to a leading strand of theorization about regulatory compliance, the 'Nielsen–Parker holistic compliance model' (Nielsen and Parker 2012; see also Parker and Nielsen 2011, 2017).

## 2 A Mechanism-Based Approach

The conceptual approach adopted in this chapter is based on the view that, when explaining social phenomena, we need to pay special attention to *social mechanisms*. In contemporary social science, an early advocate of this view was the social philosopher Jon Elster. He argued that 'we will never have any general theory of collective action', because the variety of potentially interacting motivations is 'simply too large' to be encompassed in such a theory (Elster 1989b, p. 205). That did not mean, however, that social scientific analysis is impossible. Rather, Elster concluded that social analysts should instead focus on 'small and medium-sized mechanisms that apply across a wide range of social situations' (p. 205), or, alternatively stated, 'plausible, frequently observed ways in which things happen' (p. viii). In focusing on mechanisms, he argued, we are also focusing on explanation: 'To explain an event is to give an account of why it happened. Usually ….this takes the form of citing an earlier event as the cause of the event we want to explain…..[But this] is not enough: the causal mechanism must also be provided, or at least suggested' (Elster 1989a, pp. 3–4).

Advocacy of the importance of social mechanisms in the explanation of social phenomena has subsequently been taken forward by a number of writers, and it has now burgeoned into a sub-field known as 'analytical sociology', with its own internal debates about key topics such as theories of action and causality (see, e.g., the collections of essays in Hedström and Bearman 2009a; Demeulenaere 2011a). For present purposes, it is not necessary to delve into these complexities,

but it is important to outline some basic points about mechanisms as explanations. In doing so, I shall rely in particular on some writings by the Swedish sociologist Peter Hedström (2005; see also Hedström and Bearman 2009b), who is widely seen as having been particularly 'responsible for the [systematic] theorization of [the analytical sociology] approach' (Demeulenaere 2011b, p. 24).

At the beginning of his monograph on analytical sociology, Hedström (2005, p. 1) emphasizes the desirability of developing 'precise, abstract, realistic and action-based explanations for various social phenomena'. This goal is of obvious relevance to this chapter, which tries to answer the explanatory question 'why do people obey laws and regulations?' In pursuit of his stated objective, Hedström (2005, Chapter 1) advocates a number of key features of sociological explanations, some of which I shall paraphrase here.

Firstly, then, explanations must be truly *explanatory* and not simply descriptive—that is, they must address the question *why* things happen. It is a commonplace of social science education that 'a correlation is not a cause', yet it is not always recognized that even advanced statistics are often simply correlational. Analytical sociology emphasizes that descriptions and correlations, although certainly valuable, are not enough; instead, in any given social situation it is crucial to ask the 'why' questions. Analytical sociology further argues that the best way of answering such questions is 'by detailing mechanisms through which social facts are brought about', also that these '*mechanisms invariably refer to individuals' actions and the relations that link actors to one another*' (Hedström and Bearman 2009b, p. 4, emphasis added).[1] In the present context, the 'why' questions of interest are of course centred upon why, in a given social context, the level of compliance with a law or regulation is as it is (whether this be high or low, expected or unexpected).

Secondly, given the focus in analytical sociology on the actions of individuals (see the italicized phrase above), it is important also to emphasize that 'sociology, as a discipline, is not concerned with explaining the actions of single individuals. [Hence] the focus on [individuals'] actions, is merely an intermediate step in an explanatory strategy that seeks to understand change at a social level' (Hedström 2005, p. 5). Put another way, the overall strategy is to 'explain why, acting as they do, [individuals] bring about [specified] social outcomes' Accordingly, in our context, faced with a given level of compliance with a law, we need to explain how the actions of individuals are, in aggregate, producing that level of compliance.[2]

Thirdly, since analytical sociology is not ultimately concerned with the actions of single individuals, it must to an extent rely on generalisations, and its analyses must therefore contain a degree of abstraction. However, analytical sociologists insist that in developing explanatory theories, researchers 'must refer to the actual mechanisms at work' and resist the temptation to build models of mechanisms 'that could have been at work in a fictional world invented by the theorist' (Hedström 2005, p. 3).[3] This realism is an important characteristic of analytical sociology. It is certainly also a helpful characteristic when one is seeking (as this chapter does) to analyse 'compliance as viewed from below' in a way that might be useful to people—such as compliance officers or police officers—who are facing real-life challenges in delivering effective and just compliance.

Finally, it is noteworthy that Hedström's (2005) book is called *Dissecting the Social*—a title which he chose in order to emphasize that analytical sociology aims to 'gain understanding by dissecting the social phenomena to be explained' (p. 2). More specifically, in Hedström's theorization, the term 'to dissect' means: 'to decompose a complex totality into its constituent elements and activities, and then to bring into focus what is believed to be its most essential elements' (p. 2). Taking this point together with the earlier ones, when analysing a given social situation a researcher should not only consider in detail the mechanisms in play among the people involved, she/he should also address the social relations in operation in that specific social situation (including the interactions of actors with differing mechanisms), in order to build an overall explanation of the social outcome.

In the present context, the implication of this approach is that we need to construct a typology of the principal mechanisms that, in the real world, sometimes cause legal compliance—or in other words, what Elster (1989b, p. viii) called the 'plausible, frequently observed ways in which things happen'. In any specific situation where compliance is an issue, we will further need to consider how these mechanisms operate, given the social relations in play in that specific context.

One further issue must be addressed before we move on. The late Martin Hollis (2002), in his wonderfully clear textbook on the philosophy of social science, paid special attention to the existence of, and the potential tensions between, two major traditions in social scientific theorization, which he called, respectively, 'explanation' and 'understanding'. The 'understanding' tradition is, unlike the explanatory tradition,

primarily interpretative, and in its pure form, it proposes 'that the social world must be understood from within, rather than explained from without…Instead of seeking the causes of behaviour, we are to seek the meaning of action' (Hollis 2002, pp. 16–17). Hedström (2005), whose focus is firmly on explanation, shows only limited interest in the interpretative tradition,[4] but in my view, the best social science takes full account of both traditions and seeks to develop them in creative synthesis (Bottoms 2008). From this perspective, it is encouraging that within the field of regulatory compliance, there is a consensus that research in both these traditions has made important contributions to the field (Parker and Nielsen 2011, pp. 3–8).[5] While the present chapter focuses especially on mechanisms as a crucial tool with which to develop explanations of compliance, it endeavours to take full account of interpretative research that might help us to understand what 'compliance' means in specific situations—and to recognize that it might mean different things in different situations.

To illustrate the potential of a mechanism-based approach to explanation that also pays attention to interpretative issues, I shall first discuss an example of compliance processes in action, derived from a research project in which I was involved. After that, I shall turn to a full discussion of the main mechanisms of compliance.

## *Explaining Lower-Than-Expected Compliance: A Study in English Prisons*

In the late 1990s, the minister responsible for English and Welsh criminal justice policy in the then UK government[6] decided to introduce a new policy for prisons in this jurisdiction known as the 'Incentives and Earned Privileges' policy (or 'IEP'). The intention of the new policy, shortly stated, was to improve prisoners' behaviour by linking prison 'privileges' (i.e. certain non-standard benefits available to prisoners) more closely to prisoners' good behaviour than had previously been the case. In other words, privileges would not be granted easily, but would have to be *earned*, and, as the name of the policy implies, the hope was that the 'carrot' of valued privileges (such as extra family visits) would act as *incentives* to improved behaviour.

The theoretical model underpinning this policy is, of course, one of rational choice. Such a policy strategy, to be effective, requires that

the incentives really are incentives—that is, that the benefits available through the policy are truly valued by the people to whom the policy is applied. In the present case, this condition was met: the privileges within the IEP scheme were indeed seen as valuable by the great majority of prisoners. The government and its advisers therefore confidently expected that prisoners' behaviour would improve when the IEP scheme was implemented.

The government then commissioned a research project, led by my Cambridge colleague Alison Liebling, to evaluate the effects of IEP during the first year of its operation. Unexpectedly, the principal finding of the research study was that, taking together the five prisons studied, there was no overall change in prisoners' behaviour during that first year (Liebling et al. 1999; Bottoms 2003).[7] Perhaps understandably, this result was met with some resistance by our research sponsors, who regarded it as seriously counter-intuitive.[8]

We were, however, able to demonstrate that the result was fully explicable. During the research project, we had been able to develop (from questionnaire responses at the beginning and the end of the year) a series of scales measuring prisoners' perceptions of their particular prison; the main such variables were 'relations with staff', 'perception of staff fairness', 'perception of regime fairness' and 'possibility to make progress'.[9] Aggregating the results from the five prisons, the scores for *each* of these four measures were found to have declined significantly during the first year of operation of IEP; moreover, for three of the variables (staff fairness, regime fairness and progress) there was evidence of decline *in all five prisons*. Other data showed that most prisoners regarded the principles of the IEP scheme as fair, but they thought that the way in which the policy was being implemented was unfair. A main reason for this perception was that (for reasons too complex to explain here) the new policy gave basic-grade staff more power, and this extra power, prisoners thought, was often being applied arbitrarily.

The concept of 'fairness' has loomed large in the preceding paragraph, and fairness is of course a normative principle, closely linked to that of 'justice'.[10] Also, there is a great deal of evidence that people will, generally speaking, behave more co-operatively with authorities when they perceive their treatment by authorities to be fair rather than unfair (see Chapter 2 by Justice Tankebe in this volume). So the explanation of the initially puzzling results of the IEP research was that they embodied a clash of compliance mechanisms. The creators of the IEP policy,

adopting an instrumental, rational choice theory of compliance, had assumed that valued privileges would lead to improved behaviour, and it would seem that this could have occurred, because the recipients of the policy (the prisoners) were not hostile to the principles of IEP, and they regarded the privileges on offer within the scheme as valuable incentives.[11] However, this result was not achieved, because the way in which the policy had been implemented was seen to be contrary in significant ways to normative principles of fairness. This led to a greater reluctance to comply with the incentives-based scheme; in essence, many prisoners took the view that, given the way the policy was being implemented, they were not going to 'jump through the hoops' that the scheme required. Thus, two kinds of compliance mechanism, incentives and normativity, were in conflict.

### *Purposes of the Analysis of Compliance*

The IEP study is, of course, a very specific example, but it can readily be seen to have wider implications, not least because we have already identified two broad types of compliance mechanisms (instrumental and normative). From this starting point, it is necessary to take the analysis further in two main ways. Firstly, we need to identify other principal mechanisms of compliance, beyond the instrumental and the normative, as well as the sub-types of each principal mechanism. Secondly, we will need to identify, at least in outline, possible ways in which these mechanisms might interact (as the instrumental and normative mechanisms did in the prisons example).

I have tackled these issues in previous work (Bottoms 2001, 2002), but I now believe that some modifications are necessary to the analyses presented in those earlier papers.[12] I have not, however, altered my view that the best conceptual framework for understanding 'compliance from below' is to work with four principal mechanisms. These are now described as (i) instrumental/prudential compliance; (ii) normative compliance; (iii) situational compliance; and (iv) compliance based on habit or routine. These main mechanisms, with their sub-types, are set out in Fig. 1, which it is hoped will act as a useful road map for the discussion in the remainder of this chapter.

Since the principal purpose of the chapter is, in Hedström's (2005, p. 2) helpful terminology, to 'dissect' the phenomenon of legal compliance, the main focus of the discussion of the various mechanisms will be

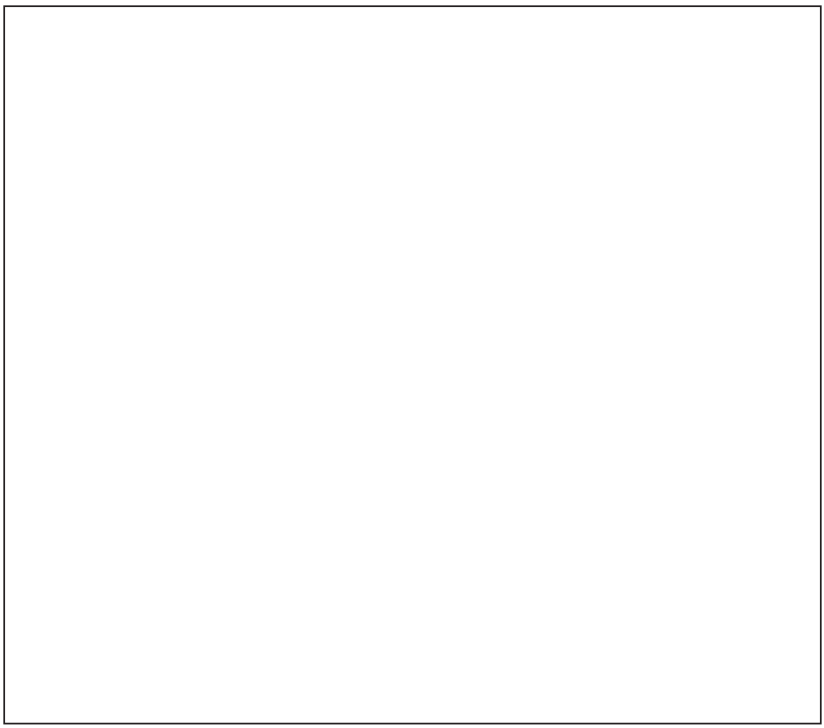

**Fig. 1** A mechanism-based typology of legal compliance (*Source* Author)

upon their *characteristics as causal mechanisms.* Issues of effectiveness will occasionally be mentioned, but within the framework of a single chapter, it is not possible to provide a thorough discussion of the effectiveness literature in addition to a 'dissective' analysis.

A final introductory comment concerns the meaning of the term 'compliance'—a matter which, as Decoene and Beyens (2013, pp. 216–221) have pointed out, has been the subject of debate among researchers in both medicine and social psychology. As regards the main topic of this chapter—compliance with laws and regulations—the approach taken is straightforward, defining such compliance in a behaviour-based manner as 'acting in a way that is consistent with (or at least, not inconsistent with) the requirements of a given law, regulation or official programme (such

as the IEP)'.[13] In some parts of the discussion, however, the examples that best illustrate the conceptual issues being discussed concern broader forms of compliance, such as compliance with social norms that are not part of any regulation or programme. Where this is the case, I have not hesitated to include the example.

## 3 A Mechanism-Based Typology of Legal Compliance

### *Instrumental (or Prudential) Compliance*

The first main mechanism to be considered is that of instrumental, or prudential, compliance. This is, normally, compliance based on self-interest: a person decides that it is in his or her own best interests, and therefore it is prudent, to comply with the regulation.[14] The principal sub-types of this mechanism are, obviously, compliance as a response to incentives and compliance as a response to disincentives, and I shall deal with these before turning to the third and rather different sub-type, that of 'creative compliance'.

*Incentives and Disincentives as Mechanisms of Compliance*

Incentives and disincentives as modes of compliance can be considered together, although, of course, in the field of legal regulation disincentives are more commonly deployed, and this has generated a large research literature on the subject of deterrence (for a recent summary, see Nagin 2013). Four issues concerning the characteristics of incentives and disincentives merit special attention.

Firstly, incentives and disincentives must always be considered from the perspective of the persons whom it is hoped to influence. It is all too easy for members of an enforcement agency to believe that they know what will influence those at whom the strategy is aimed, yet to get that prediction wrong. A well-documented case of this kind arose in youth crime policy in England and Wales in the early 1980s, when the then Conservative government announced with much publicity that it was introducing a more rigorous, or 'tougher', regime into detention centres for male young offenders, in order to act as a deterrent. (This was colloquially referred to as the 'short, sharp shock regime', and it was influenced by the concept of the military 'glasshouse'.) At the Conservative Party conference, a senior minister said that these centres 'will be no holiday camps … we will introduce on a regular basis drill, parades and

inspections' (Thornton et al. 1984, p. 1). However, evaluative research by prison psychologists showed that the new centres had similar reconviction rates to existing centres. Crucially, also, what would deter had been misperceived; for example, in one centre it was found that 'the "new" activities (drill, extra physical education, etc.) reduced the amount of time spent on work …. [but since] work tended to be less popular than these new activities, [this] … *involved the displacement of a relatively unpopular activity with a relatively popular one*' (Thornton et al. 1984, p. 203, emphasis added). This experience shows how important it is for those who introduce incentives or disincentives to ensure that they understand the situation from the point of view of potential regulatees.

Secondly, it is an inherent feature of enforcement strategies based on instrumental or prudential principles that, to be effective, the law or regulation must be constantly enforced. Unlike some other modes of compliance (see further below), an instrumental policy does not, in itself, aim to induce *internalized compliance*; instead, those subject to the policy are expected always to calculate the costs and benefits of compliance in particular situations. Accordingly, if a legal or regulatory agency significantly decreases a relevant element of its enforcement activity, and the recipients of the policy notice this, then one can in principle expect lower compliance rates after the diminution in enforcement activity. Empirically, this kind of decay after initial deterrent effects has been frequently (although not invariably) noted after police 'crackdowns' in small locations (Sherman 1990). It is therefore not surprising that a recent overview of research findings on random breath testing (RBT) for drink-driving in Australia concluded that RBT best practice must include, on a jurisdiction-wide basis, *credible and consistent enforcement practices that receive appropriate publicity*.[15] The review adds that the application of these best practice principles is 'critical' for 'RBT to be an effective drink-drive deterrent' (Ferris et al. 2015, p. 80).

Thirdly, a number of matters need to be considered about how regulatees might respond to an instrumental strategy. An obvious point—but one that is easy to overlook—is that incentives and disincentives are only relevant to people who might contemplate engaging in the specified activity. Hence, increasing a lottery prize will not increase ticket sales among people who disapprove of lotteries on principle; similarly, an enhanced probability of detection for drug supply, or stiffer sentences for that activity, will make no difference to the behaviour of people who deliberately eschew all aspects of illegal drugs. Another reliable research

result is that more immediate disincentives are more likely to have an effect on compliance than a disincentive that will come into operation only at some time in the future, and this is a principal reason for the now very well-established finding that a higher probability of detection is significantly more likely to have a deterrent effect than is the probability of receiving a more severe sanction if one is apprehended (Nagin 2013). Finally, it must be noted that there can be different reasons for a compliant response even among those who comply with a law or regulation for instrumental reasons. A good illustration of this is found in Valerie Braithwaite's (2009, 2013) research into compliance with (or defiance of) tax laws, in which she described the two main 'motivational postures' of compliers as 'commitment' and 'capitulation'. A similar distinction—described as a difference between 'substantive' and 'formal' compliance—has been drawn by Robinson and McNeill (2008) in the field of community penalties. An example of this difference, they suggest, would be that of two offenders on an unpaid work order, one of whom genuinely engages with the spirit of the penalty (he works hard at the assigned task, seeing this as reparation to the community for his offence), while the other unenthusiastically does the minimum necessary to count as fulfilling the terms of the order.

Fourthly and finally, it is a pervasive feature of the research on instrumental compliance that the degree of such compliance may be affected by the normative context in which the incentive or disincentive is offered. A result of this kind has already been seen in the IEP study, but a further example will illustrate a slightly different point, more directly related to incentives.

Klepper and Nagin (1989) administered a scenario-based survey on tax evasion to adult part-time masters-level students of management in the USA, nearly all of whom had experience of working as middle-level managers in either the private or public sectors. The results showed that many respondents were willing to consider under-reporting income to the tax authority when the sanctions would be financial penalties imposed confidentially by the authority. (As predicted by rational choice theory, such 'gambles' were much influenced by the degree of probability of detection.) However, the judgements of respondents changed significantly when the scenario included the possibility of criminal prosecution, with its attendant publicity: in this situation, 'any non-zero chance of criminal prosecution [was] an absolute deterrent' (p. 239). This result presumably arose because of respondents' perceptions of the

likely social consequences to them of a criminal conviction, including social stigma and shame. These wider normative consequences therefore constituted a powerful disincentive to cheating on one's tax liability.

*'Creative Compliance'*

We now turn to the third sub-type of instrumental compliance, 'creative compliance'[16] (see Fig. 1). This sub-type is perhaps of special interest in the context of this volume, because creative compliance has been identified as occurring especially in relation to regulation in the field of business, notably in financial services. Indeed, it has been described by Doreen McBarnet (2013, p. 71) as 'the *dominant* culture of compliance in business, and …among those "high net worth" individuals with the resources and power to manage law to suit their own purposes' (emphasis added). McBarnet's telling analysis of the character of creative compliance deserves extensive quotation:

> Rather than simply accepting and meeting the substantive obligations imposed by law, those opting for creative compliance focus on ways of arguably complying with the technical drafting of the law, while simultaneously frustrating its purpose.[17] Practices may well be adjusted, but they will be adjusted technically rather than substantively, so that the same practice continues substantively…repackaged into another legal form. (pp. 71–72)

She describes this kind of activity as 'legal engineering' and adds:

> Legal engineers know that they are not following the intentions or spirit of the law. Bankers and banking lawyers talk in interview about their legal practices as 'bullish' or 'sailing close to the wind' ….. In the mindset that underlies and fosters legal engineering, all the responsibility for control is placed on the regulators. If they can't make regulations 'legal engineering-proof', or spot the failings in the schemes, it is fair game to exploit that situation. Ideas such as responsibility, the public good, morality, ethics or integrity do not enter into the equation. (p. 86)

In short, then, creative compliance can be described as a response that is technically compliant, but with the intention of being as non-compliant as the relevant law allows. As such, it clearly merits identification as a separate sub-type under the heading of instrumental compliance. We should also note the severe challenge to regulators that is posed by this kind of activity. Those engaging in creative compliance frequently have available

significant financial resources, with which they can employ the best lawyers, whose job is then to devise schemes, sometimes of formidable technical complexity, in order to defeat the avowed purpose of the law. If the regulators nevertheless manage to achieve an imposition of liability, there will be another attempt next year to devise a 'better' scheme and so on.[18]

Arguably, the practice of creative compliance can in some circumstances have wider social consequences. Doreen McBarnet (2013, pp. 72–74) has suggested that, contrary to received wisdom, the global banking crisis of 2008 was not caused only by 'innovative financial products that were too readily believed to disperse risk' ('financial engineering'). A second cause (or mechanism) creating the crisis was, she claims, 'legal engineering'—as described above—which saw lawyers 'creatively removing the "obstacles" of prudential regulation, accounting requirements [etc.]…intended to control or disclose risk….Circumventing capital adequacy regulation was a crucial driver behind much structured finance'. This is, of course, an empirical claim about the events of 2008 which can be assessed only by those with the relevant knowledge (which does not include this author). The claim is, however, important in the present context because it is illustrative of an analytical sociology approach to explanation—that is, it aims to refine the explanation of the banking crisis by drawing attention to the actions of individuals (lawyers seeking 'creative compliance'), which, it is claimed, was one of the mechanisms leading to the crisis.

### *Normative Compliance*

The word 'norm' has several meanings in English, so what is its connotation in the present context? A helpful basic source is a (slightly truncated) dictionary definition, according to which a norm is '*a principle or standard …. that reflects people's expectations of behaviour … and serves to regulate action and judgment*' (Longman 1984). A key phrase in this definition is that of the '*expectations* of behaviour' among a given social group, and we need to note that 'expectations' is a value-laden term.[19]

Norms as expectations of behaviour have a dual character: they *enable* and they *constrain* (Giddens 1984). If we are familiar with the norms of a given group or context, this allows us to navigate daily life more easily in accordance with the local customs and expectations: thus, norms can smooth, enable and encourage social action. (Conversely, of course, unfamiliarity with the norms of a different culture can create problems,

as—e.g.—first-time Western visitors to Japan quickly discover.) But in addition, because norms *regulate* action and judgement, they act as a constraint, nudging people towards behaving in the way that the norm expects. Individuals will not necessarily follow these expectations, but even if they act in clear defiance of the norm, they will know what the social expectations are, and we can be certain that very often people will be influenced to act congruently with the conduct that the norm prescribes.

The cultural and moral norms of a society will often (but not necessarily) underpin its laws and regulations, a point sometimes described as the 'mirror thesis' ('the law mirrors the norms').[20] Where this is the case, we can expect to find that normative factors are of great importance in shaping legal compliance, especially since many norms will have been fully internalized by members of the society. I shall return to these more personal normative judgements shortly, but first I shall consider *legitimacy*—a sub-type of normative compliance that is always of great importance when one is considering compliance with formal laws and regulations.

*Legitimacy and Compliance*

Legitimacy, in its social-scientific sense, has been defined by a leading authority as 'power which is *acknowledged as rightful* by relevant agents, who include power holders and their staff, those subject to the power and third parties whose support or recognition may help confirm it' (Beetham 2013a, p. 19, emphasis in original).[21] Such acknowledgement is, however, not necessarily either total or unchanging. This means that relations between power holders and those subject to power can be likened to a continuous dialogue (Bottoms and Tankebe 2012), in which:

> What we [as subjects] acknowledge as legitimate, here and now, is what, here and now, makes sense as a legitimation of power as authority; and discussions about whether it does make sense will be engaged, first-order discussions using our moral, social, interpretive and other concepts. (Williams 2005, p. 11)

We have already seen this process in action in the IEP study. A new policy for prisons was introduced by a properly elected government minister. Prisoners did not contest the fact that he had the right to introduce the policy, nor did they object to the principle that 'privileges must be earned'. But they made it very clear that they considered many of the

ways in which the policy was being introduced in their particular prison were *unfair,* so that—'here and now', as Williams puts it—staff were behaving in a less legitimate way than they had done before the policy was introduced. This example also illustrates the point that judgements of legitimacy are not made only in relation to major issues of principle (such as 'Is the law against the possession of cannabis justified?'); they can concern much more mundane matters concerning the detailed enforcement of laws and regulations by small groups of staff or even in some circumstances by an individual officer.

In the IEP study, the delegitimating factor was a widespread sense of unfairness, and there is strong support in empirical studies that the fairness or unfairness of state agents is a key dimension of legitimacy—both in the sense of *procedural fairness* and that of *distributive fairness* (see Bottoms and Tankebe 2017, also Tankebe's chapter in this volume). Other delegitimating factors that have been identified are *unlawful actions* by the power holder and evidence that power holders are *ineffective* in performing their primary tasks (Bottoms and Tankebe 2017).

Judgements of legitimacy are clearly normative judgements,[22] and this emphasizes the point that, as Paul Tucker (2018, p. 157) put it in a recent text on independent, non-elected, government bodies, 'values are part of the fabric of a political community'. Tucker goes on to make an interesting point about the relationship between instrumental and value-based principles in independent agencies within governmental structures. We do not, he suggests, typically respond to obviously poor performance by agencies by suggesting that the incentives structures were incorrect; indeed, if we think about agencies solely in terms of instrumental principles, we will quickly go wrong.[23] To maximize legitimacy, we therefore need to achieve what he calls 'incentives - values compatibility'; that is, we need to align the incentives structures within the agency to the achievement of its true purposes, delivered in a legitimate way.

*Acceptance of, or Belief in, Social Norms*

This sub-type of compliance requires little elaboration. If a person sincerely holds a particular normative belief, it is reasonable to predict that she/he is more likely to act in accordance with that belief than someone who does not hold that belief. (To take some questions from Braithwaite's [2013, pp. 113–114] survey, someone who affirms

that 'Paying tax is the right thing to do' will obviously be less likely to under-report income than someone who says 'I don't care if I am not doing the right thing by the tax office'.) Of course, we do not always act in accordance with sincerely held beliefs (we can be tempted to do otherwise), but this does not detract from the importance, in many circumstances, of normative beliefs as a mechanism of compliance.

Since people derive many of their normative beliefs from their childhood experiences, drawing a distinction between compliance based on normative beliefs and habitual compliance based on early socialization can, in practice, be difficult (Decoene and Beyens 2013, p. 210). However, in principle these two mechanisms are separable, so it is important to include both in a dissective typology of mechanisms. An empirical example of the separateness of the two mechanisms would arise where a teenager who has been brought up to believe that theft is wrong, and has habitually behaved accordingly, is suddenly invited by school friends to join a shoplifting expedition. If, after considering the matter, he refuses, then his habitual legal compliance has, in this situation, become compliance based on his normative beliefs. In the business context, a similar situation might arise where a new employee is invited by longer-serving colleagues to 'bend' some rules relating to transactions that he is handling.

*Normative Attachment and Compliance*

Although normative beliefs can and do on occasion act as causal mechanisms of legal compliance, research in social psychology shows that most of the time people do not 'function on this explicit moral reasoning level, or habitually make conscious norm-based decisions' (Decoene and Beyens 2013, p. 210). There is, by contrast, extensive evidence that people may be influenced by the moral context of the situations, or the social groups, in which they find themselves, or which they choose to join—as has been shown by, for example, classic experimental studies such as those of Solomon Asch and Stanley Milgram. (For a summary and assessment of these studies, see Smith and Haslam [2012, Chapters 5 and 7].) In this area of analysis, therefore, Decoene and Beyens (2013, p. 222) are right to say that criminology 'could benefit from a renewed friendship with social psychology'.[24]

In my 2002 paper on compliance, I discussed issues of this kind more criminologically, and specifically with reference to Travis Hirschi's (1969) concept of 'attachment'. Within Hirschi's broader theory of social

control, the concept of attachment is linked to the notion of individuals' 'bonds to society'—which are clearly normative. In that earlier paper, I gave examples of such attachments both in the field of desistance from crime (normative links to romantic partners) and as regards the normative climate within schools, which has been shown to influence juvenile delinquency rates over and above the individual propensities to crime of those attending the school. I further pointed out that attachments to non-legally compliant individuals or groups, such as criminal peers, can have the reverse effect (Bottoms 2002, pp. 34–36).

All this remains valid and pertinent to both explanation and policy in the field of legal compliance. A related topic that was not discussed in my 2002 paper, but which is clearly relevant to compliance in the field of business regulation, is that of corporate reputational issues. There is significant evidence that businesses can be influenced to comply with regulations if there is a normative climate in relation to that particular industry such that non-compliance will be reputationally damaging to the firm (see, e.g., Kagan et al. 2003 on the compliance of pulp and paper manufacturing mills with pollution regulations).[25] Such a normative climate then acts as an incentive, analogous to the incentive provided by public disclosure in the Klepper and Nagin (1989) study—see above.

A contrasting example might be that of an employee who, in terms of her personal morality, was originally a 'committed complier' (in Valerie Braithwaite's terms), but whose prolonged cultural exposure to the culture of a firm operating an aggressive version of 'creative compliance' alters her motivational posture. The policy implication, of course, is that if regulators can work with industry representatives and the general public to create a culture normatively favourable to compliance, this is likely to be beneficial to the overall compliance rate.

It is necessary, finally, to return briefly to the relationship between this sub-type of compliance and that of normative beliefs. As has been seen, there is an analytical difference between these two sub-types, yet they remain related in complex ways. For example, when a leading researcher on legitimacy asks questions such as how morally wrong it would be to break various specific laws (on a five-point scale from 'very wrong' to 'not wrong at all'), he can very reasonably describe the resultant data as a measure of 'personal morality', in contrast to measures of legitimacy (see Tyler 1990, p. 44). In the language used in this chapter, however, this measure of 'personal morality' almost certainly contains

both an element of 'normative belief' and an element of 'compliance arising from normative attachment'. Yet even within such a measure, one might be able to make some further, and relevant, differentiation. Thus, for example, Wikström et al. (2012), in their UK study of juvenile delinquency, constructed a 'generalized [personal] morality scale' (pp. 132f.) which, as a key part of their 'crime propensity index', was a good predictor of criminality.[26] However, the researchers also found that, even after controlling for individual crime propensity, 'young people's rate of crime …. was highest … in [social] settings with a weak law-relevant social context', such as the city centre (p. 363). In other words, *both* the personal morality of the individual *and* the moral context of particular social settings were, in this study, relevant to the explanation of whether a young person chose to commit crime or to comply with the law.

*Compliance Through Normative Cues*

A recent strand of research in social psychology has shown, intriguingly, that people can be influenced to comply not only by the normative climate of a particular social setting, but also by normative cues that are signalled in one-off encounters. Major theoretical texts that underpin this approach are Cialdini's (2014) *Influence* and Thaler and Sunstein's (2009) *Nudge*, but here, I will simply illustrate the possibilities of the approach with two striking examples of norm compliance.

Keizer (2010, Chapter 3, Study 5) carried out an experiment in which a confederate of the researcher wheeled a bicycle along a street and then 'accidentally' dropped some oranges while she/he was trying to put them into a bag (all the time continuing to hold the bicycle). Would passers-by help the confederate to pick up the oranges? The answer: in the 'baseline' condition, as described above, 40% of passers-by helped the cyclist, but in a second condition, when a further confederate could be seen sweeping up litter nearby, the helping rate for the cyclist doubled (83%: $P < 0.001$). As the author concludes, this result (together with others from related experiments) supports 'the expectation that subtle cues of respect for a norm'—in this case, that it is good to keep streets tidy—can influence compliance with a similar or related social norm—in this case, that it is good to help strangers in difficulty. Indeed, 'one person armed with a broom was able to boost helping others in need by … 100 per cent' (p. 51).

The second example shows that normative cues towards compliance can be triggered even by words in a letter. Researchers in the UK Cabinet Office became interested in the science of normative cues and carried out an experiment in collaboration with the tax authorities. In the UK, personal income tax that is not deducted at source is payable on two set dates each year. There are penalties for late payments, but these still occur, and delays in payments cost the government very large sums of money. In a randomised controlled trial, the tax authorities sent out five differently worded reminder letters to those who had not paid their tax by the due date. Details are shown in Table 1, which also shows that the wording that was most effective in triggering payment combined references to (i) what 'most people do' (with the implication: 'you don't want to be different, do you?'); (ii) 'your local area' (so: 'we're not talking about people who live in other places'); and (iii) 'a debt like yours' (subtext: 'you're a bit exceptional in having a debt, and you'll want to clear it, won't you?').

This kind of letter improved early payment by 5.4 percentage points over the control condition, which is, as Halpern (2015, p. 114), rightly claims, 'not bad for a single extra line of text in a letter that was going out anyway'. Clearly, this kind of result has implications for compliance officers, who may wish to consider in what ways normative cues could be effectively used in their particular regulatory environment.

**Table 1** Tax payment rates by late-paying individuals, one month after receiving differently-worded reminder letters

| | *% paid* | *Increase over control* |
|---|---|---|
| Standard letter (control group) | 33.6 | – |
| "UK norm" letter | 35.1 | 1.5 |
| "Local norm" letter | 35.9 | 2.3 |
| "Debt norm" letter | 37.2 | 3.6 |
| "Local + debt norm" letter | 39.0 | 5.4 |

*Source* Adapted from Halpern (2015, p. 115)
Wording of letters was as follows
(i) "UK norm" = "nine out of ten taxpayers pay on time"
(ii) "Local norm" = "most people in your local area pay their tax on time"
(iii) "Debt norm" = "most people with a debt like yours have already paid"
(iv) "Local + debt norm" = "most people with a debt like yours in your local area have already paid"

### *Situational Compliance*

In my earlier writing on types of compliance (Bottoms 2001, 2002), this third type of compliance was described as 'constraint-based compliance', and in the more developed 2002 paper, it was divided into two sub-types, respectively titled 'physical restrictions' and 'social-structural constraints'.

Richard Jones (2007, p. 174) rightly criticized this categorization on two grounds. Firstly, he pointed out that the category 'physical restrictions' effectively excluded analogous forms of restraint that are virtual rather than physical, such as blockages placed in software programs. Jones suggests, following Lessig (1999), that a better term than 'physical' would be 'architectural', a word which Lessig uses in a broad sense 'to refer to such wide-ranging phenomena as … built architecture, … the laws of physics insofar as they affect human movement and communication, … computer and network hardware, … and the "virtual" architecture of software' (Jones 2006, p. 177). Secondly and more importantly, in relation to 'architecture' Jones (2007, p. 174) argues that rather than emphasizing only 'constraints' as a way of achieving compliance, 'it seems more theoretically desirable to speak of the ways in which architectural compliance-seeking approaches always simultaneously both constrain and enable'. While the simultaneity of constraints and enablements *in relation to compliance* can be questioned,[27] Jones is certainly correct in emphasizing that 'architectural' features can sometimes enhance compliance by the way in which they enable certain forms of action. It is equally the case that the other sub-type in this category identified in my earlier papers ('social-structural constraints') is better theorized as including social-structural enablements as well as constraints.

As shown in Fig. 1, we can therefore appropriately identify four subtypes within this mechanism of compliance, namely (i) 'architectural constraint-based'; (ii) 'architectural enablement'; (iii) 'social-structural constraint-based'; and (iv) 'social-structural enablement'.

A useful generic name embracing all these sub-types is *situational compliance*. This term has the merit of emphasizing that this type of compliance is truly distinct from both instrumental and normative compliance: that is to say, the compliance—whether architectural or social-structural—is caused by specific features of the situation and not by instrumental or normative mechanisms. As all criminologists will instantly recognize, the term 'situational' is borrowed, with gratitude,

from the genre of 'situational crime prevention', which has been influential in crime prevention policy since the 1970s (see Clarke 2018).

*Architectural Constraint-Based Compliance*

Architectural constraint-based compliance itself has three subdivisions, depending on whether the constraint is applied to the potential target, the potential rule-breaker or the possible means used to break the rule.

Applying constraints to the potential target, thus making the target harder to access, is an extremely common way of attempting to promote legal compliance. At a basic level, it happens every evening in millions of homes and businesses as people lock doors and close windows. More advanced physical constraints are used in some shops (bars on jewellers' windows) and in banks (very thick doors to vaults), and these may be supplemented by technological devices such as controlling entry to certain spaces with numerical codes. As noted above, within the cyber world, virtual constraints may also be utilized to prevent access to, for example, sites containing images of sexual abuse.

Applying constraints to potential rule-breakers is also a very familiar practice, seen most obviously in the use of imprisonment as a penalty. When someone is in prison, by definition he/she cannot commit crimes in the community, and this has led to the development of a scholarly literature on 'incapacitation', which has attempted to estimate the crime-reductive effects of various versions of an increased (and usually selective) use of imprisonment.[28] It is important to recognize, however, that imprisonment is not the only way of applying architectural constraints to potential law-breakers in an attempt to improve compliance. For example, in many countries the range of available non-custodial penalties now includes the possibility of ordering the defendant to stay at home at specified times, electronically monitored by wearing a 'tag'. Less formally, teachers in schools often deliberately place potentially troublesome pupils at some distance from one another within the classroom, so that they are not tempted to start fighting, and at professional soccer matches in England, the police routinely adopt a similar tactic in relation to the fans of the two teams, channelling them to the stadium by separate routes, under police supervision.

These examples all relate to personal offenders, but of course constraints can also be applied to corporate offenders, forbidding them for a time from engaging in certain activities, or, in extremis, removing their licence to trade, or closing down the company altogether. In

this connection, it is worth remembering that the final two sanctions in the first iteration of Ayres and Braithwaite's (1992, p. 35) well-known 'responsive regulation enforcement pyramid' are those of 'licence suspension' and 'licence revocation'.

'Architectural' compliance can be enhanced not only by placing restrictions on potential targets and on potential offenders, but also by restricting access to the *means* of committing an illegal or disapproved-of act. This is why, for example, virtually every state has strict controls on the sales of poisons, and also why most states have extended the same logic to the availability of firearms. However, rather than enter here into the contentious US-dominated literature on gun control, I will illustrate the relevance of this form of situational control through a well-documented example in which greater compliance with the social norm against committing suicide was an *unintended* consequence of an altered situation. This occurred in Great Britain in the 1970s, when extensive supplies of natural gas were discovered under the North Sea (off the east coast of England) and the government decided for economic reasons to 'mine' this supply, and simultaneously to discontinue production of the previously used gas ('coal gas', derived from the burning of coal stocks). Many families in Great Britain use gas cookers in their kitchens, and significant numbers of suicides had previously taken place using the toxic coal gas readily available in so many domestic ovens. But North Sea gas is non-toxic, so after the change, this method of suicide was no longer available. The national suicide rate dropped, and careful scholarly analysis has shown that the only plausible reason for the reduction was the alteration in the nature of the gas supply (Clarke and Mayhew 1988). This research has therefore shown that even a deeply personal decision such as trying to end one's own life can be significantly affected by a situational change in the available means to achieve one's purpose.

*Architectural Enablement*

Good examples of compliance through architectural enablement may be found in the sphere of road traffic. In their book *Nudge*, Thaler and Sunstein (2009, pp. 41–42) provide an illustration from their home city of Chicago concerning a stretch of lakeside road which has 'stunning views' but also 'a series of S curves'. Approaching the S curves, there is a mandated speed reduction (to 25 mph), but in the past, many drivers failed to obey this requirement, and the accident rate was high. In an

attempt to improve the situation, the city authorities painted a series of stripes on to the road as a visual signal to drivers:

> When the stripes first appear, they are evenly spaced, but as drivers reach the most dangerous portion of the curve, the stripes get closer together, giving the sensation that driving speed is increasing…..One's natural instinct is to slow down. When we drive on this familiar stretch of road, we find that those lines are speaking to us, gently urging us to touch the brake before the apex of the curve. (p. 42)

Thus, 'nudging' can work in a situational manner, as well as by offering cues to normative principles that are held by an observer (see previous section).[29] But architectural enablement can also go beyond nudging, and a good illustration here is the fact that traffic accidents are significantly lower (per thousand vehicles) on designated motorways than on other types of road.[30] The reasons for this are straightforwardly situational and include the banning of pedestrians and very slow vehicles on motorways, and the fact one can only enter or leave such roads at a limited number of designated points.

In other contexts, such as pollution control from industrial waste, it will no doubt be possible for those with appropriate technical knowledge to identify analogous examples of strategies of architectural enablement, both of a 'nudging' and of a wider situational character.

*Social-Structural Constraint-Based Compliance*

This sub-type is, as we shall see, not a mechanism of compliance that can be ethically commended as something that law enforcement personnel should seek to cultivate. It arises, as I explained in my first essay on compliance, in situations where people are 'cowed into submission by the coercion [of] a power-based relationship' (Bottoms 2001, p. 93). In order for such compliance to be truly situational, the person complying will not be motivated by instrumental concerns, nor will he or she find any normative reasons to comply. The best term to characterize the nature of this kind of compliance is therefore—as David Lockwood (1992, p. 43) has suggested—that of 'fatalism'. As he puts it, in conditions of entrenched social inequality a sufficient condition of obedience 'is simply that the structure of power, wealth and status is believed to be inevitable', and so it is fatalistically accepted by those without power.

Colleagues and I encountered such fatalistic compliance when conducting research in a so-called Vulnerable Prisoner Unit in a high-security prison (Sparks et al. 1996, Chapter 6). This unit (consisting of two prison wings) was reserved for those prisoners—such as sex offenders and those with debts to other prisoners—who would face hostility, and perhaps injury, from other prisoners if they were located in the mainstream prison system. Given this situation, they had little option than to accept the regime that the staff offered. Unfortunately, some staff realized this and behaved in an unprofessional manner: as one staff member candidly explained, 'the power can go to your head easy' (p. 214). But given the prisoners' powerless condition, even staff malpractice was usually accepted by prisoners without formal complaint.

It is instructive to compare this mode of compliance with that of 'creative compliance'. Creative compliance is possible only when those expected to comply have considerable economic and social resources; social-structural constraint-based compliance occurs only when those expected to comply feel powerless. In different ways, both modes of compliance show that, in real-life social situations, social power can significantly affect the dynamics of compliance.

*Social-Structural Enablement*

A good example of social-structural enablement is to be found in policies relating to the public availability of criminal records. Concern has been expressed, particularly by American criminologists, that in recent years, given informational and internet developments, 'criminal records have become cheaper to access *and* more widely accessible' with the result that 'millions have moved from the category of "potentially discreditable" to the category of "formally discredited"' (Uggen and Blahnik 2016, p. 229, emphasis in original). This development has consequences in a number of spheres, but particularly in relation to employment, making it significantly more difficult for those with criminal records to obtain jobs, especially satisfying jobs. This has led to some increased attention to the potentialities of policies (already adopted in some countries) of 'sealing' criminal records in order to enhance the possibility of desistance from crime. Such policies can take a variety of forms,[31] but on almost any analysis, they seem likely to have either a positive or neutral impact on offending levels (Kurlychek et al. 2016), so they seem well worth pursuing as a policy to enhance compliance through social-structural enablement.

### *Compliance Based on Habit or Routine*[32]

The fourth principal mechanism of compliance is concerned predominantly—and to a greater extent than any of the other three mechanisms—with unthinking compliance. Within this mechanism will be found compliance based on both routine and habit, which themselves need to be distinguished.

Turning first to *routine*, consider the type of law that, in many countries, requires the parents of children between certain ages to send them to a school (whether public or private) that is registered with the state. Compliance with such laws is typically high. But compliance requires that active steps be taken, on every weekday in school term, to send children to school. In the average household, there is no debate about whether the law should be complied with; instead, on mornings in school terms there is a semi-organized bustle involving breakfast, packing a school bag with sandwiches and homework and so on. In other words, unthinking routine prevails. This is not a unique example—the law requiring the wearing of seat belts in cars similarly results in routine belt-attachment as people get into their vehicles, the driver checks that everyone has belts fastened, and so on.

Both of these examples concern laws that require specific and positive actions to be taken if one is to comply with them, and 'legal compliance by routine' occurs particularly (although not exclusively[33]) in relation to that kind of law. However, many laws simply require one to refrain from doing a particular act (say, burglary or street robbery), and in these circumstances, compliance *by habit* comes more into the picture. Obviously, most adult members of the general population would never even consider committing a burglary or a street robbery—we can say that they have a *settled mental disposition* (or habitual way of thinking and acting) that rules out this kind of behaviour. An interesting attempt to describe mental dispositions was made by the philosopher Richard Wollheim (1984, p. 34):

> Mental dispositions …. are persistent phenomena, which manifest themselves intermittently. They do not occur, nor are they events. They are mutable. Dispositions have histories, which are made up of events, and these histories are varied … Dispositions vary in their beginnings, for some are innate, some arise in the mind, and some are acquired. They persist in different ways, for some remain constant and some change, and they may mature or decline or fluctuate.

This characterization is, in my view, helpful because it draws attention to two contrasting points. Firstly, habits or mental dispositions are described as relatively 'persistent phenomena'. This is important because if such phenomena exist—and the criminological evidence on 'crime propensity' (Wikström et al. 2012) suggests that they do—then they refute strong versions of psychological situationalism, which argue that people's behaviour is so situationally influenced that concepts such as 'character trait' have to be abandoned. (On this debate in a philosophical context, see Sreenivasan 2013.) Secondly, however, habits or mental dispositions are not immutable, and they can and do change as people encounter fresh sets of circumstances. This point is also confirmed in the criminological literature, where research on desistance from crime has shown that offenders—even persistent offenders—can and frequently do, over time, reduce their crime propensity and acquire a fresh set of routines and habits of thought (for a summary, see Shapland and Bottoms 2017). These observations of course refer to individuals, but similar features are seemingly also found in corporations, since the concept of a 'corporate culture' within a given firm or organization is frequently used, and of course such cultures can change over time.

## 4 Interactions Between Different Mechanisms of Compliance

The analysis in this chapter has proposed four principal mechanisms of compliance: instrumental, normative, situational and habitual. Following the recommendations of analytical sociologists, uncovering these mechanisms, and their sub-types, has involved a process of 'dissection', in which the aim has been 'to decompose a complex totality into its constituent elements and activities, and then to bring into focus what is believed to be its most essential elements' (Hedström 2005, p. 2).

However, in any real-life analysis of compliance—whether undertaken as a social scientist or a law enforcement officer—initial 'dissection' is only a preliminary step. One also needs first, to consider whether—and, if so, how—different mechanisms of compliance might be interacting with one another, and second, how the mechanisms are operating within the social structures and relationships in that particular situation.

The latter point is considered briefly in the next section, but first we will discuss potential interaction effects between the three most 'active' mechanisms of compliance, namely the instrumental, the normative and the situational.

### *The Instrumental and the Normative*

Interactions between the instrumental and the normative have been fairly frequently noted in the research literature, and we have already seen examples of such interactions in the IEP prisons study and in the Klepper-Nagin questionnaire study on taxpaying.

Interactions between the instrumental and the normative can in principle work both ways (i.e. normative → instrumental or instrumental → normative). In the Klepper-Nagin research, the addition of a significant normative dimension (exposure to public disapproval as a 'tax cheater') acted as a major incentive to compliance. The data in that paper were derived from a 'scenario-based' questionnaire, but its core finding has been confirmed in real-life research, perhaps most notably in the path-breaking series of experimental studies on misdemeanour-level domestic violence in the USA, reported by Lawrence Sherman (1992).[34] From these various sources, a reasonable conclusion from the empirical evidence is that there is an integral connection between normative and instrumental compliance, such that *incentives and disincentives work best for persons or corporate entities that have strong ties to a social group (e.g. a family, a local community or fellow members of a business community), in a context where reputation matters to the social standing of the individual or corporate entity in that group, and members of the social group have clear normative expectations that are related to the behaviour at which the law or regulation is aimed.*

The previous paragraph describes situations in which normative factors act to *enhance* instrumental compliance. However, as the IEP study shows, other kinds of normative factor (in that research, perceptions of unfairness by staff, i.e. lack of legitimacy) can act to *inhibit* instrumental compliance.

In the reverse direction of causality, can instrumentally conceived enactments enhance normative compliance? In principle, they can, although the empirical evidence here is more tentative. Perhaps the main examples of this kind of effect have occurred when a law created

for its hoped-for instrumental effect subsequently generates a normative change. An interesting illustration of this kind of process has been observed as regards drink-driving in Great Britain. A new law on this topic was passed in 1967, for the first time authorizing breath tests on drivers, and (save in exceptional circumstances) mandating compulsory disqualification if one was found guilty of driving when over the legal limit. At the time of its enactment, this law was very much seen as an attempt to secure compliance by instrumental (deterrent) means, since public normative attitudes on drink-driving were, at the time, certainly not consistent with the 'mirror thesis' (see Note 20 above). A degree of normative contestation continued for a decade or two,[35] but perceptions gradually changed, and now—half a century after the law was passed—there is a very widespread public consensus that this is a normatively just law.

### *Interaction Effects from Situational Measures*

Situational prevention measures can and do, in some circumstances, have secondary effects both of an instrumental and of a normative kind. By contrast to instrumental–normative interactions, however, in this instance the causation does not seem to operate in both directions.

That situational prevention can create longer-term instrumental effects should come as no surprise to anyone. Thus, for example, an agency that is managing a gold bullion store will obviously wish to protect it with some serious hardware, to prevent thieves from accessing the bullion (=reduction of opportunity, a key feature of situational crime prevention). The serious hardware will, however, inevitably have the secondary effect of acting as a significant disincentive to all but the most determined and professional thieves. Secondary instrumental effects of this kind can even occur as an *unintended* consequence of a situational measure. Thus, in the 1970s in Great Britain, a law was passed requiring motorcyclists to wear a crash helmet, in order (through a situational measure) to reduce the severity of injuries in accidents. In the year after this new law came into force, in Greater London the rate of thefts and unauthorized takings of motorcycles decreased by a quarter, although the equivalent rate in respect of other motor vehicles rose significantly. Why did the reduction occur? Home Office researchers explained the change by noting that many unlawful takings of motorcycles are

'opportunist' (i.e. committed without planning), so 'it is reasonable to think that some potential users (aware of what was a well-published requirement [to wear a helmet]) have been deterred from illegally taking two-wheelers because of their increased visibility if not wearing a crash helmet' (Mayhew et al. 1976, p. 18). A situational change focused on safety had therefore promoted instrumental compliance with the theft laws, based on an increased probability of detection.

Situational prevention can also result in an enhancement of normative compliance. The leading example of this kind of effect is that described by Welsh and Farrington (2008) in their Campbell Collaboration review of research on the effects of improved street lighting on crime. The authors conclude that the five most recent such evaluations (all of which were UK studies) 'showed that improved lighting led to decreases in crime' (p. 19). However, a puzzling feature of the results was that, in these areas, night-time crimes did not decrease to a greater extent than daytime crimes: in other words, crime decreased as much when the lights were off as when they were on. This was surprising because improved street lighting had been promoted as a form of *situational* crime prevention, reducing opportunities for crime by lighting dark places, as well as making offenders more visible (and so easier to detect). Welsh and Farrington suggested that the most plausible explanation for the unexpected 'daytime' finding was that improved street lighting resulted in 'increasing community pride and informal social control'. To support this suggestion, the authors cited evidence from one area where the improvement in lighting was very obvious and where data showed that 'tenants thought that their quality of life had been improved' (p. 19). In other words, improved lighting had given rise to a normative effect of improved well-being among residents, which in turn seemed to have led to improved informal social control even in daylight hours, and hence less crime.[36]

## 5 The Nielsen–Parker Holistic Compliance Model

In the field of business (or regulatory) compliance, most writers focus on what I have described as 'compliance from above' rather than 'compliance from below'. It is therefore of special interest, for the purposes of this chapter, that a leading pair of authors on regulatory compliance (Christine Parker and Vibeke Lehmann Nielsen) have written in both of these 'voices'. Their leading paper on 'compliance from below'

(Nielsen and Parker 2012) sets out an explanatory model, which is now described as the 'Nielsen–Parker Holistic Compliance Model' (see Parker and Nielsen 2017, p. 220). This is reproduced here as Fig. 2,[37] and—as may be seen—it combines three distinct sets of explanatory variables. The core set concerns the regulatee's interests and motives (box on left-hand side of the diagram); to these are then added (i) three 'psychological or organizational factors inside the regulatee' (Nielsen and Parker 2012, p. 450), which I shall describe as 'internal influences' (boxes above the horizontal line), and (ii) the 'external influences' shown in the box below the horizontal line.

It will be useful to consider each of these sets of variables separately and to compare each with aspects of the analysis in this chapter—which I shall refer to in shorthand as the 'Typology of Compliance Mechanisms' or TCM. As will be seen, a significant point arises from each of these comparisons.

### *Business Motives*

The regulatee's interests and motives are central to Nielsen and Parker's (2012) explanatory model. In their 2012 paper, they hypothesize that firms will have three principal 'business motives for compliance', namely

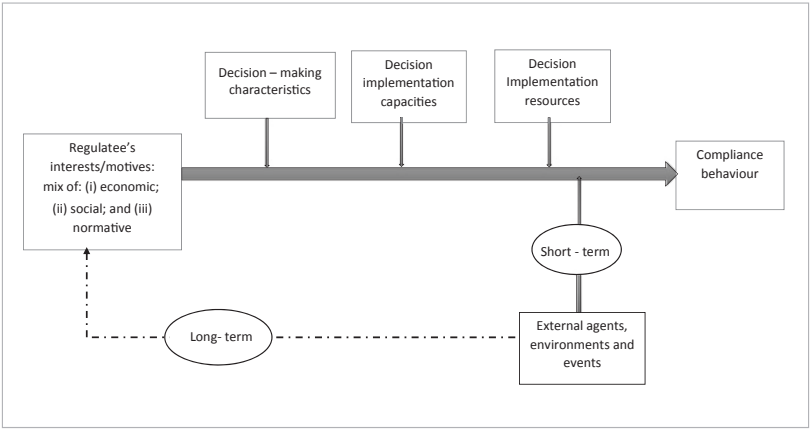


**Fig. 2** The Nielsen–Parker holistic compliance model (*Source* Nielsen and Parker [2012, p. 448], as modified in Parker and Nielsen [2017, p. 220])

economic or material motives, social motives and normative motives. Economic motives are said to relate 'broadly to the motives of the stereotypical amoral calculator' (p. 431); they therefore, in the language of the TCM, constitute a mechanism for compliance based on incentives and disincentives. Social motives are said to relate to 'earning the approval and respect of significant others with whom an actor interacts', a group which could include 'other businesses … employees, customers, local communities, the wider public, family and friends' (p. 432, emphasis deleted). Again, this corresponds closely to a sub-type in the TCM, namely that of compliance through normative attachment. Nielsen and Parker note that, in the field of business compliance, some theorists have proposed merging the categories of economic and social motives, given that 'social stigma might lead to … economic and other losses', but they resist this suggestion because, they argue, acts of non-compliance arising from economic and from social motives sometimes require different policy responses by regulators (p. 432). As has been seen, the TCM analysis, while recognizing that 'social motives' can sometimes have instrumental effects, also supports keeping these categories separate, because differing mechanisms are in play. Nielsen and Parker's third category of motives, 'normative motives', refers to 'compliance as a result of internalized moral judgements by people about the substance and procedures of the law' (p. 432). This category clearly maps on to the TCM sub-type of 'normative beliefs', although close examination of Nielsen and Parker's text suggests that they also intend 'normative compliance' to include what in the TCM is the further sub-type of legitimacy.

In an empirical study of Australian firms (see Note 20 above for details), Nielsen and Parker showed through a principal components analysis that firms' motives for compliance (or otherwise) could indeed be appropriately classified into the economic, the social and the normative.[38] The same empirical study also showed, however, that the great majority of firms 'rate[d] all the motives fairly highly' (p. 443): that is, they held a plurality of motives, although the researchers found that there were 'small gradations of difference as to how they do so' (p. 445).[39]

Comparing Nielsen and Parker's compliance model with that of the TCM, there is clearly considerable congruence between the three principal motives that these authors have identified and the main sub-types within the instrumental and normative mechanisms of the TCM. Perhaps

surprisingly, however, there is nothing in the Holistic Compliance Model about situational compliance, but on reflection, this difference probably reflects the differing theoretical purposes of the two typologies. The TCM is explicitly focused on identifying the main mechanisms of compliance 'as seen from below', whatever the source of the mechanism. By contrast, the Holistic Compliance Model is more concerned with the relationship, within business regulation, between regulators and regulatees, with a strong policy focus on improving compliance, and perhaps situational compliance mechanisms are rarely discussed within such relationships.[40] There is, of course, room for both approaches, and it is hoped that the analysis in this chapter will complement that of Nielsen and Parker. Moreover, on one point there is a firm concurrence between the two analyses: both agree that much compliance is multifaceted and that the interconnections between different (and often plural) reasons for compliance need to be carefully considered in any serious look at compliance or non-compliance in a particular social situation.

### *Internal Influences*

The 'internal influences' identified by Nielsen and Parker (Fig. 2, above horizontal line) refer to matters such as the characteristics of decision-making within the firm (are decisions emotionally or rationally driven?; is compliance seen as important or as an 'afterthought?'); the capacity of the firm to act strategically in implementing decisions; and the resources available to the firm, since differences in resource levels are known 'in large part to explain differences in compliance behavior' between firms (Nielsen and Parker 2012, p. 449). In relation to compliance with the mainstream criminal law, the analogue of these 'internal' matters would of course be psychological differences between individuals.

It is at this point that a note of caution must be raised. For certain purposes, including those important to regulatory compliance officers (and therefore to Nielsen and Parker), these 'internal' variables can be very important—as would also be attested, for example, by probation officers working to promote desistance from crime with individual offenders. But that is less the case in other contexts, and these other contexts include the work of analytical sociologists and overall analyses of particular social policies. As regards analytical sociology, we need

to recall that, as Hedström (2005, p. 5) put it, 'the focus on [individuals'] actions is merely an intermediate step in an explanatory strategy that seeks to understand change at a social level'—which means that such analyses, although hopefully realistic, must necessarily contain an element of generalization, rather than individuation (see the introduction to this chapter). As regards social policy, it is useful to look back to the IEP example and to recognize that no detailed individual-psychological research was needed to identify the main mechanisms in play in that situation, nor to understand why the policy did not have the desired effect. Accordingly, an important difference between Nielsen and Parker's Holistic Compliance Model and the analysis of this chapter is that 'internal' influences relating to regulatees are more important for the former than the latter.

### *External Influences*

This final element in the Nielsen–Parker model is extremely wide-ranging in scope. As can be seen in Fig. 2 (box below horizontal line), it covers 'external agents, environments and events'—which means that it embraces matters as diverse as the actions of the regulator; decisions of professional bodies such as those for accountants or lawyers; social pressures in relation to a particular industry (see, e.g., Note 25 above in relation to pulp and paper mills); and specific events such as fresh legislation. In the TCM, this wide range of potential influences would be handled more specifically—for example, relations with the regulator would be considered under both 'legitimacy' and 'instrumental compliance', and social pressures would be seen as potentially influencing compliance by normative attachment.

Despite this analytical difference, both approaches to understanding compliance emphasize the potentially very great importance of these 'external' influences. As previously indicated, in the TCM the analytic strategy is first to identify the mechanisms in place, in a 'dissective' analysis; then to consider possible interactions between mechanisms; and finally to relate this mechanism-based analysis to the social structures and relations in play in the particular context. The authors of the Holistic Compliance Model similarly see compliance as a very complex matter, and they note that this has implications for compliance officers. Citing various authors such as Baldwin and Black (2008) on 'really responsive regulation', they conclude that such officers need to develop:

> understanding and insight into the multifarious actors and mechanisms that interact with one another to influence and create compliance. It is foolhardy to assume that just because one or two factors have been addressed….compliance will automatically increase. …. [I]t is up to regulators to have the skill and ultimately the courage … to craft solutions and alliances that are responsive to the complex social, economic and political contexts in which they work. (Parker and Nielsen 2017, pp. 230–231)

## 6 Conclusion

The quotation from Parker and Nielsen (above) rightly emphasizes the multifaceted and interactive complexity of compliance processes. The analysis in this chapter has tried to provide a set of tools with which one can begin to unravel this complexity.

It has been argued, following the recommendations of analytical sociologists, that a mechanism-based approach offers the best framework for the explanation of legal and regulatory compliance, while at the same time granting the 'interpretative' tradition of social science greater weight than most analytical sociologists would allow. Particular attention has been paid to the 'dissective' dimension of mechanism-based analyses, as recommended by Peter Hedström; and in a 'dissective' analysis, four principal mechanisms of legal compliance have been identified, namely instrumental (or prudential) compliance, normative compliance, situational compliance and compliance based on habit or routine. The first three of these mechanisms are also shown to have some distinct subtypes within the general mechanism, and the specific features of these sub-types require careful attention (see Fig. 1 for an overview). To complete the analysis, interactions between the mechanisms, and their functioning in real-life situations, have been considered.

As has been indicated, this chapter builds on some earlier work of this author on legal compliance (Bottoms 2001, 2002), some aspects of which have seen constructively criticized by other scholars (see Note 12 above). This chapter tries to provide an improved analysis, while also to an extent widening the substantive scope of the discussion in an attempt to address some features of compliance in the field of business regulation. How far it succeeds in these dual aims is, of course, for readers to judge.[41]

## Notes

1. See further Hedström (2005, Chapter 2), where he defends the view that mechanism-based explanations are more satisfactory as causal explanations than are two alternative possibilities, namely 'covering law explanations' and 'statistical explanations'.
2. This approach is commonly, and fairly, described as a version of 'methodological individualism'(MI). However, as various writers—including Hedström (2005, p. 5, n. 4)—have pointed out, acceptance of this proposition does not entail acceptance of more extreme MI statements, such as Elster's (1989b, p. 248) 'there are no societies, only individuals who interact with one another'. For a helpful discussion of MI and analytical sociology, see Demeulenaere (2011b, pp. 3–9).
3. On this point, Hedström (2005, p. 3) follows the 'analytic realist' approach of Talcott Parsons (1937, p. 730), in which 'the concepts of science are not fictional…[yet they]correspond not to concrete phenomena, but to elements in them which are analytically separable from other elements'.
4. He agrees with Max Weber that the 'individual is the sole carrier of meaningful conduct' (p. 153), but is much more interested in quantitative than in qualitative research, and—for example—deeply sceptical of Pierre Bourdieu's concept of *habitus*, which he regards as 'mystifying' (p. 4).
5. For a good example of interpretative research in the field of business compliance, see the work of Lauren Edelman in the area of employment discrimination in the USA, summarized in Edelman and Talesh (2011). Edelman showed that organizations initially responded to new laws on discrimination by 'developing written rules, procedures and policies in an attempt to achieve legal legitimacy, while simultaneously limiting law's impact on managerial power and unfettered discretion over employment decisions' (p. 107). This could be fairly described not as committed compliance, but rather as 'creating structures *designed to symbolize attention to law*' (p. 110, emphasis added). Edelman then outlines a sequential process whereby 'organizational actors tend to construct laws in ways that are consistent with traditional managerial logics and goals. As these constructions of law become institutionalized over time, they subtly and gradually affect how courts …. understand the meaning of law and what constitutes rational compliance with law, [since] judges take … cues from norms and practices that become institutionalized within organizations …. [In sum], …. organizational constructions of law gain not only organizational, but also legal legitimacy' (p. 110). Thus, what is meant by 'legal compliance' gradually and subtly shifts over time.

6. Within the UK, there are three separate legal jurisdictions, and therefore, three separate prisons systems—England and Wales; Scotland; and Northern Ireland. The IEP policy was applied only to England and Wales.
7. This was assessed by a simple measure of change from the beginning to the end of the year in which the IEP policy was implemented. Methodologically, the research would have been stronger if it had included control group prisons as well as IEP prisons; however, the research team's suggestion to this effect was vetoed by the minister on the grounds that he wanted the policy to be implemented in all prisons.
8. One of the five prisons showed an improvement in behaviour, but there were compelling reasons to conclude that this improvement was attributable to factors other than IEP: see Bottoms (2003, p. 157).
9. These quantitative measures were based on extensive prior qualitative research by Alison Liebling in other prisons. They are therefore an example of a methodological approach that she has subsequently come to describe as 'quantified ethnography'.
10. For example, 'justice as fairness' is a central feature of John Rawls' (1972) seminal text on justice.
11. As the research team made clear in its report, the implication of this point is that with different implementation strategies, prisoner behaviour would probably improve. Since the time of the research, there have been a number of changes to the implementation of the IEP scheme, but no formal further research evaluation has been undertaken.
12. While some of these modifications have arisen from my own further reading and reflection, I wish also to acknowledge with gratitude the helpful critiques of these earlier papers by Richard Jones (2006, 2007); by Gwen Robinson and Fergus McNeill (2008); and by Stef Decoene and Kristel Beyens (2013).
13. Decoene and Beyens (2013, pp. 219–220) particularly advocate the potential importance for criminology of Herbert Kelman's social-psychological work on compliance, identification and internalization, which he summarized in an important semi-autobiographical paper (Kelman 2006). Decoene and Beyens quote at length Kelman's original definitions of these three concepts (p. 219), without making it clear that these were developed in the experimental context of his early work, i.e. 'a one-time and one-way persuasive communication [in the laboratory], intended to influence a specific attitude or behavior of individual members of the audience' (Kelman 2006, p. 7). Subsequently, Decoene and Beyens refer to Kelman's later work on social influence in the broader context of social systems, but they do not specifically quote his rather different definition of compliance in this context, i.e. 'adherence to the rules

or norms of a system (including its laws and customs) – i.e. the behavioral requirements it sets for its members' (Kelman 2006, p. 11)—a definition that is similar to that adopted in this chapter. Kelman (pp. 17–18) also makes clear that in this broader social context the concept of legitimate authority significantly complicates the model presupposed by the original experiments, in which 'people [were] presumed to react [simply] on the basis of their personal preferences'.

14. Although instrumental compliance is usually undertaken to further the interests of the regulatee, this is not necessarily the case, since as Unger (1976, p. 25) has pointed out, an instrumental choice can be made because of an 'altruistic concern for welfare of others, as long as the ultimate basis of this choice is one's own will'.
15. In more detail, the stated best practice principles (always jurisdiction-wide) are: (i) random but strategically deployed RBT stops; (ii) full enforcement of the programme; (iii) publicity; (iv) 'no one gets off'; and (v) targeted strategies for recidivist drink-drivers.
16. This is McBarnet's (2013) term; Braithwaite (2013) calls the same phenomenon 'game-playing'. While there is certainly an element of game-playing in this kind of activity, I have preferred 'creative compliance' because of the seriousness of the intent, and of the consequences, that can be involved.
17. The term 'arguably' is used deliberately in this sentence. As McBarnet (2013, p. 72) goes on to explain: 'The argument may fail …. But the existence of an arguable case usually provides immunity from any suggestion of non-compliance. It is simply a failed case rather than a fraud. Creative compliance thus creates "fraud insurance", enabling business, as simple non-compliance does not, to simultaneously avoid both the criminal label and legal control'.
18. In this connection, a further issue raised by some is concern about potential conflicts of interest arising from the so-called revolving door, i.e. the movement of individuals between public office and the private sector: see Transparency International UK (2012).
19. A more technical and formal definition of a social norm, which helpfully elaborates the element of expectation within such norms, has been provided by Bicchieri (2017, p. 35): 'A social norm is a rule of behaviour such that individuals prefer to conform to it on condition that they believe that (a) most people in their reference network conform to it (empirical expectation) and (b) most people in their reference network believe they ought to conform to it (normative expectation)'.
20. The caveat 'but not necessarily' is important. As Brian Tamanaha (2001, p. xi) has pointed out, the mirror thesis very often does not apply in colonial societies; for example, in Micronesia—where he worked—the law had

been 'transplanted in its entirety from the United States', with the result that the norms of the legal system were very different from the culture and values of the indigenous society. In the field of business regulation, there can also on occasions be a significant difference between the norms enshrined in regulations and the norms of at least some regulatees. For example, Nielsen and Parker (2012) carried out a survey of nearly 1000 businesses who were subject to the Australian federal law on competition and consumer protection (the Trade Practices Act 1974, or 'TPA'). The authors classified a minority of respondent businesses (80 out of 943) as 'dissenters' because, although these firms recognized as important 'a variety of social and normative motives that would [in general terms] tend to support compliance as important', nevertheless they reported 'a principled disagreement with the very goals of the TPA' (p. 444).

21. In this source, Beetham distinguishes between the social scientist's understanding of legitimacy and that of the political philosopher, for whom legitimacy is 'power which is *rightful* according to rationally defensible standards or principles' (emphasis in original). For a more extensive discussion of this distinction, see Bottoms and Tankebe (2017).
22. This might be questioned when a judgement of illegitimacy is made on the grounds of lack of effectiveness—for is not effectiveness simply an instrumental concept? For a persuasive rejection of this view, see Beetham (2013b, pp. 136f.).
23. On this point, see also Elster (1989b), who treats 'rational, selfish, outcome-oriented behaviour' (p. 37) as a starting point in his analysis of social order. However, he eventually concludes ('with some reluctance': p. 250), firstly, that social norms independently motivate individuals' order-related behaviour, and secondly, that such norms cannot be regarded as merely rationalizations of self-interest (Chapter 3).
24. However, this will require careful attention to definitional issues (see the comments in Note 13 above). It is also very important to remember that the present chapter is an exercise in analytical sociology and that, ultimately, 'sociology, as a discipline, is not concerned with explaining the actions of single individuals' (Hedström 2005, p. 5). See further discussion in the concluding section of this chapter.
25. In this industry, the authors described the near-ubiquity of 'social pressures' on mill managers from local communities and environmental activists, such that 'many … managers spoke to us of having to meet the terms not only of their regulatory license but of their "social license"' (p. 69). A qualitative analysis within the research project also suggested that 'variations in social pressures have a significant effect on firms' relative environmental performance' (p. 69).
26. In this study, the construct 'crime propensity' is comprised of two variables: 'generalized morality' and 'ability to exercise self-control'. However,

the overall crime propensity score is, over time, more closely related to 'morality' than to 'ability to exercise self-control'—see Wikström et al. (2012, graph on p. 139).

27. It is of course correct that any 'architectural' feature simultaneously constrains and enables. However, use of some types of feature (such as a prison cell) will generate significantly more constraint than enablement, while other features will have the reverse effect.
28. For a short summary of differing methods of attempting to estimate incapacitation effects empirically, see Bottoms and von Hirsch (2010, pp. 113–120). Given that any form of incarceration will probably produce at least a small reduction in crime, a key issue is the cost effectiveness of various sentencing strategies with an incapacitative element, and students of incapacitation quickly learn that cost effectiveness is very difficult to achieve, given the expensiveness of imprisonment.
29. Indeed, apparently similar physical interventions can trigger different mechanisms of compliance. For example, painting stripes on the road in Chicago produced situational compliance because of the illusion created by the decreasing distance between stripes; by contrast, painting footprints leading to litter bins on sidewalks in Copenhagen led to less litter being left on the sidewalk, but this was because of the normative cue ('good citizens put litter in bins') that the footprints had created (see Halpern 2015, p. 94, reporting results obtained by Pelle Hanson in Copenhagen).
30. In Great Britain, motorways carry 21% of vehicular traffic, but only 6% of road fatalities occur on them, despite high average speeds: Department for Transport (2018, p. 16).
31. For example, one type of policy prevents the public disclosure of convictions received as a juvenile, provided that there are no adult convictions. Another kind of policy 'seals' a criminal record after a certain period without convictions, thus allowing an ex-offender to lawfully reply 'no' to a question on an employment recruitment form asking whether the applicant has at any time been convicted of a criminal offence.
32. This section draws on aspects of the discussion in Bottoms (2001, pp. 93–94).
33. An important form of compliance that is frequently used *by offenders themselves*, when they are trying to move away from crime, involves structuring their daily routines so as to avoid locations where temptations to re-offend might arise. (Temptations might occur, e.g., through chance meetings with friends who are still offending, or by going to a bar where fights often break out). This might be regarded as a cross between compliance by the creation of routines and a version of architectural compliance. For a full discussion, see Bottoms (2013).

34. Sherman reports on results from several experimental studies in which police officers responded to less serious domestic violence incidents *either* by arresting the suspect *or* by some less severe action, the choice of officer response being randomly mandated in advance. One key set of results was summarized by the author as follows: 'Evidence that the effects of arrest vary by suspect comes from …. [three] cities, …. [where the] data suggest that unemployed suspects become more violent if arrested, but that employed suspects do not. This consistent pattern supports a hypothesis that the effects of criminal punishment depends upon the suspect's "stakes in conformity", or how much he has to lose from the social consequences of arrest' (Sherman 1992, p. 17): i.e. those who had greater 'stakes in conformity' were more likely to comply in future because of the social shame of arrest.
35. For a detailed examination of the enactment and early history of the Road Safety Act 1967, see Light (1994).
36. Welsh and Farrington (2008, p. 19) recognize that one might hypothesize a reverse causal effect, i.e. the normative change 'comes first, causing improved street lighting on the one hand and reduced crime on the other'. The available data did not permit scrutiny of this hypothesis in all areas. However, in the two areas where time-related data were available, the authors were clear that this alternative hypothesis could be rejected.
37. The text included in some of the boxes in the model differs somewhat in the two sources cited at the foot of Fig. 2. Where there is such a difference, the figure always uses the text of the 2017 source, except that the text in two boxes (those that, in the 2017 source, contain only the words 'Characteristics' and 'Capacities') has been amplified by reference to the 2012 source.
38. However, in this empirical analysis four, not three, factors were identified, because 'normative motives' were found to split into two distinct factors. One of these related to 'a general attitude that one should obey the law because it is the law'; the other related to specific attitudes towards the particular legislation that regulators were, in that empirical study, enforcing (Nielsen and Parker 2012, p. 441).
39. As an exception to this general picture, a minority of firms (about 8%) expressed normative disagreement 'with the very substance of the law' (p. 445) that was being enforced by the regulators—see further at Note 20 above.
40. One can imagine reasons why this might be so; although from the perspective of regulatees, situational measures are likely sometimes to be potentially sensible ways of improving compliance.
41. I am grateful to my Cambridge colleague Justice Tankebe for his helpful comments on an earlier draft of this chapter.

## References

Ayres, I., and Braithwaite, J. (1992). *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press.

Baldwin, R., and Black, J. (2008). Really Responsive Regulation. *Modern Law Review, 71*(1), 59–94.

Beetham, D. (2013a). Revisiting Legitimacy, Twenty Years On. In J. Tankebe and A. Liebling (Eds.), *Legitimacy and Criminal Justice: An International Exploration* (pp. 19–36). Oxford: Oxford University Press.

Beetham, D. (2013b). *The Legitimation of Power*, second edition. Basingstoke, Hampshire: Palgrave Macmillan.

Bicchieri, C. (2017). *Norms in the Wild: How to Diagnose, Measure and Change Social Norms*. Oxford: Oxford University Press.

Bottoms, A. E. (2001). Compliance and Community Penalties. In A. E. Bottoms, L. R. Gelsthorpe, and S. Rex (Eds.), *Community Penalties: Change and Challenges* (pp. 87–116). Cullompton, Devon: Willan.

Bottoms, A. E. (2002). Morality, Crime, Compliance and Public Policy. In A. E. Bottoms and M. Tonry (Eds.), *Ideology, Crime and Criminal Justice: A Symposium in Honour of Sir Leon Radzinowicz* (pp. 20–51). Cullompton, Devon: Willan.

Bottoms, A. E. (2013). Theoretical Reflections on the Evaluation of a Public Policy Initiative. In L. Zedner and A. J. Ashworth (Eds.), *The Criminological Foundations of Penal Policy: Essays in Honour of Roger Hood* (pp. 107–194). Oxford: Oxford University Press.

Bottoms, A. E. (2008). The Relationship Between Theory and Empirical Observations in Criminology. In R. D. King and E. Wincup (Eds.), *Doing Research in Crime and Justice*, second edition (pp. 75–116). Oxford: Oxford University Press.

Bottoms, A. E. (2013). Learning from Odysseus: Self-Applied Situational Crime Prevention as an Aid to Compliance. In P. Ugwudike and P. Raynor (Eds.), *What Works in Offender Compliance: International Perspectives and Evidence-Based Practice* (pp. 67–89). Basingstoke, Hampshire: Palgrave Macmillan.

Bottoms, A. E., and von Hirsch, A. (2010). The Crime Preventive Impact of Penal Sanctions. In P. Cane and H. M. Kritzer (Eds.), *The Oxford Handbook of Empirical Legal Research* (pp. 96–124). New York: Oxford University Press.

Bottoms, A. E., and Tankebe, J. (2012). Beyond Procedural Justice: A Dialogic Approach to Legitimacy in Criminal Justice. *Journal of Criminal Law and Criminology, 102*(1), 119–170.

Bottoms, A. E., and Tankebe, J. (2017). Police Legitimacy and the Authority of the State. In A. du Bois-Pedain, M. Ulväng, and P. Asp (Eds.), *Criminal Law and the Authority of the State* (pp. 47–88). Oxford: Hart.

Braithwaite, V. (2009). *Defiance in Taxation and Governance: Resisting and Dismissing Authority in a Democracy*. Cheltenham: Edward Elgar.

Braithwaite, V. (2013). Resistant and Dismissive Defiance Towards Tax Authorities. In A. Crawford and A. Hucklesby (Eds.), *Legitimacy and Compliance in Criminal Justice* (pp. 91–115). London: Routledge.

Cialdini, R. B. (2014). *Influence: Science and Practice*, fifth edition. Harlow, Essex: Pearson Education.

Clarke, R. V. G. (2018). The Theory and Practice of Situational Crime Prevention. In *The Oxford Research Encyclopedia of Criminology and Criminal Justice* (online publication). Oxford: Oxford University Press.

Clarke, R. V. G., and Mayhew, P. (1988). The British Gas Suicide Story and Its Criminological Implications. *Crime and Justice, 10*, 79–116.

Decoene, S., and Beyens, K. (2013). Compliance Dynamics: A Multidisciplinary Review and Exploration of Compliance Dynamics in the Belgian Context. In P. Ugwudike and P. Raynor (Eds.), *What Works in Offender Compliance: International Perspectives and Evidence-Based Practice* (pp. 208–226). Basingstoke, Hampshire: Palgrave Macmillan.

Demeulenaere, P. (Ed.). (2011a). *Analytical Sociology and Social Mechanisms*. Cambridge: Cambridge University Press.

Demeulenaere, P. (2011b). Introduction. In P. Demeulenaere (Ed.), *Analytical Sociology and Social Mechanisms* (pp. 1–30). Cambridge: Cambridge University Press.

Department for Transport. (2018). *Reported Road Casualties in Great Britain: 2017 Annual Report*. London: Department for Transport.

Edelman, L. B., and Talesh, S. A. (2011). To Comply or Not to Comply—That Isn't the Question: How Organizations Construct the Meaning of Compliance. In C. Parker and V. L. Nielsen (Eds.), *Explaining Compliance: Business Responses to Regulation* (pp. 103–122). Cheltenham: Edward Elgar.

Elster, J. (1989a). *Nuts and Bolts for the Social Sciences*. Cambridge: Cambridge University Press.

Elster, J. (1989b). *The Cement of Society*. Cambridge: Cambridge University Press.

Ferris, J., Devaney, M., Sparkes-Carroll, M., and Davis, G. (2015). *A National Examination of Random Breath Testing and Alcohol-Related Traffic Crash Rates, 2000–2012*. Canberra: Foundation for Alcohol Research and Education.

Giddens, A. (1984). *The Constitution of Society*. Cambridge: Polity Press.

Halpern, D. (2015). *Inside the Nudge Unit: How Small Changes Can Make a Big Difference*. London: W.H. Allen.

Hedström, P. (2005). *Dissecting the Social: On the Principles of Analytic Sociology*. Cambridge: Cambridge University Press.

Hedström, P., and Bearman, P. (Eds.). (2009a). *The Oxford Handbook of Analytical Sociology*. Oxford: Oxford University Press.

Hedström, P., and Bearman, P. (2009b). What Is Analytical Sociology All About? An Introductory Essay. In P. Hedström and P. Bearman (Eds.), *The Oxford Handbook of Analytical Sociology* (pp. 3–24). Oxford: Oxford University Press.

Hirschi, T. (1969). *Causes of Delinquency*. Berkeley: University of California Press.

Hollis, M. (2002). *The Philosophy of Social Science: An Introduction*, revised edition. Cambridge: Cambridge University Press.

Jones, R. (2006). 'Architecture', Criminal Justice and Control. In S. Armstrong and L. McAra (Eds.), *Perspectives on Punishment: The Contours of Control* (pp. 175–196). Oxford: Oxford University Press.

Jones, R. (2007). The Architecture of Policing: Towards a New Theoretical Model of the Role of Constraint-Based Compliance in Policing. In A. Henry and D. J. Smith (Eds.), *Transformations of Policing* (pp. 169–190). Aldershot, Hampshire: Ashgate.

Kagan, R., Gunningham, N., and Thornton, D. (2003). Explaining Corporate Environmental Performance: How Does Regulation Matter? *Law and Society Review, 37*(1), 51–90.

Keizer, K. (2010). *The Spreading of Disorder*. Proefschrift, University of Groningen. Available online.

Kelman, H. (2006). Interests, Relationships, Identities: Three Central Issues for Individuals in Negotiating Their Social Environment. *Annual Review of Psychology, 57*, 1–26.

Klepper, S., and Nagin, D. (1989). Tax Compliance and the Risks of Detection and Criminal Prosecution. *Law and Society Review, 23*(2), 209–240.

Kurlychek, M. C., Bushway, S. D., and Denver, M. (2016). Understanding and Identifying Desistance: An Example Exploring the Utility of Sealing Criminal Records. In J. Shapland, S. Farrall, and A. E. Bottoms (Eds.), *Global Perspectives on Desistance: Reviewing What We Know and Looking to the Future* (pp. 244–264). London: Routledge.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Liebling, A., Muir, G., Rose, G., and Bottoms, A. E. (1999). *Incentives and Earned Privileges for Prisoners: An Evaluation*. Home Office Research Findings No. 87. London: Home Office.

Light, R. (1994). *Criminalizing the Drink-Driver*. Aldershot, Hampshire: Dartmouth.

Lockwood, D. (1992). *Solidarity and Schism*. Oxford: Clarendon Press.

Longman Group. (1984). *Longman Dictionary of the English Language*. Harlow, Essex: Longman.

Mayhew, P., Clarke, R. V. G., Sturman, A., and Hough, J. M. (1976). *Crime as Opportunity*. Home Office Research Study 34. London: Her Majesty's Stationery Office.

McBarnet, D. (2013). Questioning the Legitimacy of Compliance: A Case Study of the Banking Crisis. In A. Crawford and A. Hucklesby (Eds.), *Legitimacy and Compliance in Criminal Justice* (pp. 71–90). London: Routledge.

Nagin, D. S. (2013). Deterrence in the Twenty-First Century. *Crime and Justice, 42*, 199–263.

Nielsen, V. L., and Parker, C. (2012). Mixed Motives: Economic, Social and Normative Motivations in Business Compliance. *Law and Policy, 34*(4), 428–462.

Parker, C., and Nielsen, V. L. (2011). Introduction. In C. Parker and V. L. Nielsen (Eds.), *Explaining Compliance: Business Responses to Regulation* (pp. 1–33). Cheltenham: Edward Elgar.

Parker, C., and Nielsen, V. L. (2017). Compliance: 14 Questions. In P. Drahos (Ed.), *Regulatory Theory: Foundations and Applications* (pp. 217–232). Canberra: Australian National University Press.

Parkin, F. (1982). *Max Weber*. Chichester: Ellis Horwood and London: Tavistock.

Parsons, T. (1937). *The Structure of Social Action*. New York: Free Press.

Rawls, J. (1972). *A Theory of Justice*. Oxford: Oxford University Press.

Robinson, G., and McNeill, F. (2008). Exploring the Dynamics of Compliance with Community Penalties. *Theoretical Criminology, 12*(4), 431–449.

Shapland, J., and Bottoms, A. E. (2017). Desistance from Crime and Implications for Offender Rehabilitation. In A. Liebling, S. Maruna, and L. McAra (Eds.), *The Oxford Handbook of Criminology*, sixth edition (pp. 744–766). Oxford: Oxford University Press.

Sherman, L. W. (1990). Police Crackdowns: Initial and Residual Deterrence. *Crime and Justice, 12*, 1–48.

Sherman, L. W. (1992). *Policing Domestic Violence*. New York: Free Press.

Smith, J. R., and Haslam, S. A. (Eds.). (2012). *Social Psychology: Revisiting the Classic Studies*. London: Sage.

Sparks, R., Bottoms, A. E., and Hay, W. (1996). *Prisons and the Problem of Order*. Oxford: Clarendon Press.

Sreenivasan, G. (2013). The Situationist Critique of Virtue Ethics. In D. C. Russell (Ed.), *The Cambridge Companion to Virtue Ethics* (pp. 290–314). Cambridge: Cambridge University Press.

Tamanaha, B. Z. (2001). *A General Jurisprudence of Law and Society*. Oxford: Oxford University Press.

Tankebe, J. (in this volume). Legitimacy and Regulatory Compliance. In M. Krambia-Kapardis (Ed.), *Financial Compliance: Issues, Concerns and Future Directions*. Basingstoke: Palgrave Macmillan.

Thaler, R. H., and Sunstein, C. R. (2009). *Nudge: Improving Decisions About Health, Wealth and Happiness*, revised edition. New York: Penguin Books.

Thornton, D., Curran, L., Grayson, D., and Holloway, V. (1984). *Tougher Regimes in Detention Centres*. London: Her Majesty's Stationery Office.

Transparency International UK. (2012). *Fixing the Revolving Door Between Government and Business*. Policy Paper No. 2. London: Transparency International UK.

Tucker, P. (2018). *Unelected Power*. Princeton: Princeton University Press.

Tyler, T. R. (1990). *Why People Obey the Law*. New Haven: Yale University Press.

Uggen, C., and Blahnik, L. (2016). The Increasing Stickiness of Public Labels. In J. Shapland, S. Farrall, and A. E. Bottoms (Eds.), *Global Perspectives on Desistance: Reviewing What We Know and Looking to the Future* (pp. 222–243). London: Routledge.

Unger, R. M. (1976). *Law in Modern Society*. New York: Free Press.

Welsh, B. P., and Farrington, D. P. (2008). *Effects of Improved Street Lighting on Crime*. Campbell Systematic Review 13: 2008. Oslo: The Campbell Collaboration.

Wikström, P.-O. H., Oberwittler, D., Treiber, K., and Hardie, B. (2012). *Breaking Rules: The Social and Situational Dimension of Young People's Urban Crime*. Oxford: Oxford University Press.

Williams, B. (2005). *In the Beginning Was the Deed: Realism and Moralism in Political Argument*. Princeton: Princeton University Press.

Wollheim, R. (1984). *The Thread of Life*. Cambridge: Cambridge University Press (Reprinted 1999, New Haven: Yale University Press).

**Anthony Bottoms** is Emeritus Wolfson Professor of Criminology in the University of Cambridge and Honorary Professor of Criminology in the University of Sheffield. He was also Director of the Institute of Criminology at Cambridge University from 1984 to 1998. His main recent interests in criminology have focused on compliance; desistance from crime; the legitimacy of criminal justice institutions; and penal theory. He is a recipient of the Sellin-Glueck Award from the American Society of Criminology, for international contributions to criminology; and of the European Criminology Award from the European Society of Criminology, for lifetime contributions to European criminology. He was elected as a Fellow of the British Academy in 1997 and was knighted in 2001.

CHAPTER 2

# Legitimacy and Regulatory Compliance

*Justice Tankebe*

## 1 Introduction

In *The Problem of Order*, Dennis Wrong argued that a challenge that had always confronted all societies was the challenge of aligning individual private interests with those of the collective (Wrong 1994). Herein lies the problem of compliance, and it follows that, first, all social groups—whether they are financial institutions, police departments, or, even organised criminal entities—always demand that their members obey a body of more or less defined regulations. Second, and this is implicit in the first, compliance can never be taken for granted; there are always forces of different intensity that encourage individuals to act in ways that deviate from what is required of them. Third, acts of non-compliance are not created equal; they are highly variable in the seriousness of their impact on individuals, organisations, and wider society. For example, in November 2012, Mr. Kweku Adoboli was convicted for what the presiding judge, Mr. Justice Keith, described as 'fictitious hedging trades' that caused the loss of $2.25bn to UBS[1] (*R. v Kweku Adoboli*, 2012). The 2008 global financial crisis, for which Mr. Adoboli was a mere footnote, resulted in unemployment, and housing and political crises, which persist until today.[2] There are also countless cases of corporations found

J. Tankebe (✉)
Institute of Criminology, University of Cambridge, Cambridge, UK
e-mail: jt340@cam.ac.uk



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_2

complicit in facilitating tax evasion and money laundering, even by (suspected) terrorist and organised criminal networks.

Consequently, questions about compliance have attracted intense attention in recent years. Various national and international regulations against money laundering, corruption, and tax evasion have either been enacted or strengthened (Allfred et al. 2017; Ferran 2012). Understanding why people break rules has therefore never been more urgent. But it is a task that has long concerned criminologists who have sought to understand and explain why people break rules in different settings (e.g. Hirschi 1969; Wikström et al. 2012). Bottoms (2002, see also Chapter 1 in this volume) identifies four principal mechanisms of compliance: *habit* by which compliance happens because people see obedience as the only viable cause of action (Wikström et al. 2012); sometimes compliance arises from (boundedly) rational decision-making processes in which people consider the potential costs and rewards of lawbreaking (*instrumental or prudential compliance*). It also sometimes happens that *structural constraints*—such as difficulty in accessing vulnerable targets or the means of criminal conduct—prevent people from acting out their criminal propensities. Finally, Bottoms identifies *normative* mechanisms according to which compliance arises from perceptions that laws or systems of authority are morally valid. As Hirschi put it, "crime occurs because there is *variation* in the extent to which people believe they should obey the rules of society and, furthermore, that the less a person believes he should obey the rules, the more likely he is to violate them" (Hirschi 1969, p. 26). A sub-type of normative compliance is legitimacy, which is the focus of this chapter.

Legitimacy is the soul of all social systems, from relatively simple entities to nation states and multinational corporations. Without legitimacy, these systems are moribund. Sherman (1978) wrote in *Scandal and Reform* that scandal was a "mighty weapon" that could both topple governments and instigate change. The same can be said about legitimacy: as a mighty weapon, legitimacy is double-edged. With it power-holders can procure a certain quality of compliance and cooperation from power-audiences. However, claims about illegitimacy are almost always the grounds for resistance, sabotage, defiance, and non-compliance. As Boulding (1967) noted, when institutions lack legitimacy, they fall with such rapidity that there is hardly time for investigation (see also, Sparks 1994). The purpose of this chapter is threefold: first, it offers an overview of legitimacy theory. Its key concern here is to lay out the meaning of legitimacy and some of its most essential features. Second, it discusses

Bottoms and Tankebe's (2017) fourfold dimensions of legitimacy: namely lawfulness, procedural justice, distributive justice, and effective use of authority. Third, it reviews some of the empirical literature on the potential role of legitimacy in nurturing and sustaining compliance within organisations. As the review will make clear, legitimacy matters for encouraging compliance with laws and regulations.

## 2 What Is Legitimacy?

Legitimacy theory is founded on a view of human actors as "norm-users, whose interactions with each other depend on mutually recognisable patterns that can be articulated in terms of right versus wrong conduct, or of what one ought to do in a certain setting" (MacCormick 2007, p. 20). Given this, an attempt to explain people's reactions to regulations starts with considerations of the normative status of those regulations (Beetham 1991). By normative status, we mean the legitimacy of regulations and those whose duty it is to ensure compliance. Legitimacy itself is the subject of varied definitions. According to Boulding (1967, p. 299), legitimacy refers to the "acceptance of an institution or an organisation as right, proper, justified and acceptable". For Beetham (2013, p. 19), legitimate is "power that is *acknowledged as rightful* by relevant agents, who include power-holders and their staff, those subject to the power and third parties whose support or recognition may help confirm it". Both definitions have the advantage of drawing attention to a central feature of legitimacy: the notion of "right" or "rightful" speaks to the "inherently social" nature of legitimacy (Reus-Smit 2007, p. 159).

How best can we think about or understand legitimacy? Drawing on work by Max Weber (1978), Bottoms and Tankebe (2012) outlined a theory of legitimacy as dialogue. As they put it:

> legitimacy needs to be perceived as always dialogic and relational in character. That is to say, those in power (or seeking power) in a given context make a claim to be the legitimate ruler(s); then members of the audience respond to this claim; the power-holder might adjust the nature of the claim in light of the audience's response; and this process repeats itself. It follows that legitimacy should not be viewed as a single transaction; it is more like a perpetual discussion, in which the content of power-holders' later claims will be affected by the nature of the audience response. (2012, p. 129)

A number of issues flow from this view of legitimacy as a continuous dialogue. *Primus*, such a view invites an enquiry into the nature of dialogues. Brownlee (2011) has outlined five "conditions for dialogue". First, a dialogue requires "reciprocity between the parties … For a dialogue to occur, each party must be an active participant in the interaction in that each must intentionally play the dual roles of communicator and receiver" (pp. 57–58). Legitimacy as perceived by power-audience has little to do with what power-holders claim about themselves; it flows from power-audiences. As we shall see below, the condition of reciprocity relates to a key component of procedural justice which requires that those in positions of authority—for example, supervisors—explain and listen to the views of employees. Second, dialogues are "more sustained and extensive interactions" (p. 58), hence, never to be understood as episodic transactions. As she put it, dialogues are not "simple call and response or an exchange of threats, or wordless meeting of minds". Third, the parties in a dialogue recognise each other's contributions and are willing to adjust their positions vis-à-vis those contributions. Even where they are not entirely civil (Bottoms and Tankebe 2013) dialogues carry a symbolic message of a desire to reach common understanding (Brownlee 2011). Four—and this flows from the first condition—dialogue connotes fairness and equality such that "each has an equal right not only to speak when she wishes (provided that she respects the equal rights of the other), but also to be heard and to be understood" (p. 58). Finally, genuine dialogue is uncoerced, not staged, manipulated, or conducted under duress. Unless there is voluntary engagement, what the parties to a power relationship communicates loses credibility.

*Secundus*, talk of legitimacy-as-dialogue implies the primacy of context. Dialogues occur in certain cultural, political, and economic contexts, which contexts shape directly or indirectly the nature, direction and outcome of the dialogues. From this point of view, an indispensable starting point for any study of legitimacy is knowledge of the historical and societal realities in which power-holders seek to establish and maintain legitimacy, and how these realities define the expectations and responses from audiences. We cannot fully understand narratives and counter-narratives about legitimacy in a vacuum, and it is for this reason that Beetham (1991) writes about "legitimacy-in-context". Bottoms and Tankebe (2017, p. 88) put it this way: "legitimacy dialogues are always

contingent on specific features of the place and time in which they occur and are influenced by the history and culture of that place and time; and this means that the specifics of legitimation and legitimacy can be very variable".

*Tertius*, a dialogue implies the active involvement of two or more actors. This immediately contrasts it with a monologue, which the *Oxford English Dictionary* defines as "a dramatic composition for a single performer; a dramatic entertainment performed throughout by one person". Those who are subject to legitimate power cannot be portrayed as automatons or mere spectators passively observing the actions of power-holders, nodding to their performances. As Reus-Smit (2007, p. 159) put it, "auto-legitimation is an oxymoron – an actor can jump up and down, declaring loudly that his or her actions are legitimate, but if nobody accepts this, then they are not correctly described as such, even if he or she is making a legitimacy claim". It follows that we cannot speak of the facticity of legitimate power in the sense that the fact that a person is vested with power necessarily imbues that power with legitimacy (cf. Mbembe 2001, p. 3). Therefore, in the study of legitimacy-as-dialogue, we are simultaneously concerned with the active roles of *power-holders* and *power-audiences*. Thus, Bottoms and Tankebe (2012, 2013) differentiate between power-holder and audience dimensions of legitimacy—the former describes the belief on the part of power-holders (e.g. managers and supervisors) that their role and authority is morally acceptable to them. Audience legitimacy, on the other hand, concerns judgements by those subject to authority that the system of authority or those exercising power have the right to that power.

*Quartus*, when our focus is on organisational legitimacy, we need always to differentiate between *internal* and *external* legitimacy (Sparks 1994). Internal legitimacy concerns legitimacy dialogues between management and employees. Externally, there are multiple audiences making sometimes conflicting legitimation demands … governments, legislators, and regulators, and wider heterogenous public (Beetham 2013). The relationship between organisations and their institutional and individual actors is variable. However, as institutional theorists have shown, there are "both formal and informal pressures exerted on organizations by other organizations upon which they are dependent and by cultural expectations in the society within which organizations function" (DiMaggio and Powell 1983, p. 150). As Suchman (1995) points out,

the heterogeneity of institutional environments makes it difficult to build and sustain legitimacy; as such difficulty persists, organisations become vulnerable to the negative consequences of unexpected events, what Taleb (2007) calls "black swan events". This means that whether in dealings with diverse audiences internal or external to an organisation, a key test for power-holders concerns how to navigate and respond to legitimacy pressures in their institutional environments.

## 3 Mechanism for Legitimising Organisations

According to Bottoms (see Chapter 1), "when explaining social phenomena, we need to pay special attention to *social mechanisms*"; that is to say, to account for why those social phenomena happen. A question that naturally, therefore, arises from our discussion so far concerns the mechanisms that organisations can use to build and sustain legitimacy. The term *legitimation* is usually used to refer to this process of seeking to cultivate, sustain, and reproduce a claim to the rightful exercise of authority. Legitimacy—that is, "an attribution conferred on a power-holder by his or her audience(s), acknowledging that he/she [has] the right to rule" (Bottoms and Tankebe 2013, p. 64)—may be thought of as the "outcome" of the process, even though this outcome is fluid (Dunn 2013). Our concerns in this section are therefore with legitimation mechanisms. In their theory of legitimacy, Bottoms and Tankebe (2012, 2017) proposed four such mechanisms for establishing and maintaining audience legitimacy: lawfulness; procedural justice; distributive justice; and effectiveness.

### *Lawfulness*

In modern societies, the starting point for a study of legitimacy is law. Beetham (1991) considers it "the first and most basic level of legitimacy". It concerns not only the legal source of power, but also the extent to which those in authority such as compliance officers act in accordance with established rules. Thus, in a study of law's legitimating role, we are concerned with matters related to the "rule of law", which rests on principles of due process and equality (Allan 2001). The law must also be applied prospectively, which allows those who are subject to a given order to know in advance the kinds of sanctions that are to be applied should non-compliance occur (Tamanaha 2004). Following Aristotle's *negative approach*,[3] Bottoms and Tankebe

(2012, pp. 137–138) argue that we can better understand the role of law in legitimation by looking at those instances where power-holders have been found to break rules. Thus, when compliance officers engage in misconduct and bankers violate financial regulations, they undermine a key pillar of their legitimacy. Mathiesen (1965) showed, from his study in a Norwegian prison, that perceived illegality can attract "censure" from power-audiences as they seek to point out to power-holders the inherent contradictions between claims and behaviour.

Thus, when we think about the practices of institutions and seek to question the rightfulness of such practices, a key judgement point is the law. Have they acted in accordance with the spirit and letter of the law? It is also the case that institutions often seek to defend themselves against criticisms by saying that they have not broken any laws. However, law per se offers insufficient grounds for legitimation. Simply because an organisation can demonstrate that it has acted strictly according to a given regulation, may not be enough to prevent it from being viewed as illegitimate. The reason is this: laws do not always reflect prevailing social norms (Tamanaha 2001; Arsovska and Verduyn 2007). Even if laws reflected social norms at a particular time, changes in law can sometimes lag behind changes in social laws, depriving law of its moral foundations. Conversely, some social norms can be stubbornly resistant to change such that changes in law may outpace change in social norms. It is in this sense that Taleb (2018, p. 55) observes that "laws come and go; ethics stay". It is also sometimes the case that law is imposed on parties in a power relationship without any recourse to culture and values of that society or group. As Gouldner (1954, pp. 184–185) found in his study of a mining plant in the United States, employees did not believe that "management has the right to institute any kind of rule, *merely because they have the legal right to do*" *(emphasis in original)*.

The inadequacy of law for establishing legitimacy underscores the importance of the other dimensions of the Bottoms and Tankebe model. This leads us to the second of their legitimation mechanisms: ***procedural justice***.

### *Procedural Justice*

Procedural justice may be defined as the perceived fairness of the processes used in day-to-day decisions and exercise authority

(Sunshine and Tyler 2003). According to Tom Tyler, procedural justice has two dimensions: *quality of decision-making* and *quality of treatment* (Tyler 2003). Quality of decision-making has various specific sub-elements: voice/participation, impartiality, trustworthy motives, and correctability. The "voice" dimension captures the extent to which those in positions of authority allow people, whether employees or clients, to express their points of view when making decisions. It means decision-makers offer people an opportunity to ask questions, are seen to listen actively, and taking account of people's views in the decisions or actions. One of the ways decision-makers seek to invite people's views is by requesting feedback or suggestions for improvement.

Impartiality denotes the absence of bias or discrimination in decision-making. It requires that decision-makers are "unmoved by certain sorts of consideration – such as special relationships and personal preferences… to treat people alike irrespective of personal relationships and personal likes and dislikes" (Cupit 2000, cited in Rothstein 2011, p. 230). It is often mistaken for neutrality; however, as Rosanvallon (2011) points out, unlike neutrality which means "detachment or even refusal to intervene", impartiality requires active engagement. To act impartially is to apply rules consistently, explaining how rules are being applied and why, explaining how decisions have been reached, and referring to rules and evidence rather than personal views (see Mazerolle et al. 2013).

The notion of "trustworthy motives" refers to "inferences about the intentions behind actions, intentions that flow from a person's unobservable motivations and character" (Tyler and Huo 2002, p. 61). The reference to character is important here because it gives people some indication as the commitment of power-holders to social norms that the parties in a power-relationship share. Do the demeanour, actions, and inactions of power-holders exemplify these shared norms? Unless people are convinced that the motives of those in authority are sincere and that they have the interests of people at heart, the possibility of establishing a normative relationship is remote (see Ullmann-Margalit 2017, Chapter 11). The procedural justice literature suggests that power-holders can convey their good motives by being consciously approachable and not intimidating, being sincere and caring (e.g. the tone, questions about the person) by excluding personal feelings and beliefs from decision-making, by listening to and discussing people's views, and by explaining reasons and purpose for decisions (see Mazerolle et al. 2013; Tyler and Huo 2002).

*Quality of treatment* concerns the need to treat people with appropriate dignity and recognition *as a persons*, including (where relevant) recognition of their particular needs and characteristics. Bottoms and Tankebe (2012, p. 145) describe this component as the "more personal" of the elements, focused on "whether the decision-maker treats the subject in a true sense as a human being, with needs for dignity, privacy, respect for his or her moments of weakness, and so on". Signals of respect and disrespect are culturally variable, such that what conveys respectful treatment among members of a particular religious or ethnic background might be viewed as disrespectful among those of a different group. However, the evidence from procedural justice literature suggests that basic courtesy, showing that people and their rights are important, taking issues raised seriously and taking time to discuss them, and providing the right information at the right time are some of the ways to convey respect (see Mazerolle et al. 2013). According to Honneth (1996, pp. 131–132), "because the normative self-image of each and every human being … is dependent on the possibility of being continually backed up by others, the experience of being disrespected carries with it the danger of an injury that can bring the identity of the person as a whole to the point of collapse". Consequently, a great deal of resentment and defiance can arise from actual or perceived disrespect; consequently, compliance officers seeking to establish legitimacy make their task easier by creating a work environment that prioritises respectful and dignified relations.

### *Distributive Justice*

Distributive justice and procedural justice are often embraced in the broader notion of organisational justice (Colquitt et al. 2001). According to Aristotle, distributive justice is: "Exhibited in the distribution of honours, property, or anything else which is divided among the members of the community. For in such matters men (sic) may receive shares that are either equal or unequal to the shares of others" (cited in Johnston 2011, p. 68).

Johnston (2011) has noted that the terms translated as "equal" and "unequal" are *isos* and *anisos*, and are more accurately translated as "fair" and "unfair". Consequently, distributive justice concerns the fairness in the distribution or allocation of resources across different persons or groups (Tyler and Fagan 2008; Colquitt et al. 2001). These may take

the form of symbolic or concrete resources (Lerner and Clayton 2011). Symbolic resources include questions of respect, offering a voice and listening. For employees, concrete resources may include salaries and tangible resources for work. However, resources are not only "positive"; there are also "negative" resources such as sanctions or punishment. Here again, questions arise as to the distribution of these negative resources across different persons and groups. Are certain individuals or groups more likely to be the subject of investigations, dismissals, suspensions, or other forms of punishment? When those in positions of power are perceived to use their authority in ways that are discriminatory, they inevitably attract censure and resentment. Hence, we see, for example, the birth of *Black Lives Matter* in the USA as a protest against minorities being disproportionately the target of police violence.

### *Effectiveness*

Effectiveness concerns the ability of institutions to fulfil their mandate. All social systems have specified goals that they seek to achieve. For criminal justice agencies, it is the goal of reducing harms in society and increasing public safety. For financial service regulators such as the UK's *Financial Service Authority*, the Financial Services and Market Act 2000 defines its objectives as building "market confidence", "public awareness", "the protection of consumers", and "the reduction of financial crime". For regulatee corporations, the principal goal is to "produce goals and services that consumers needed and wanted and to make an acceptable profit in the process" (Carroll 1991, p. 41). These goals and the intensity with which they are pursued may differ across time and space, but it remains the case that the effective use of authority towards achieving those goals will be a normative expectation for relevant audiences for these organisations. Thus, Coicaud (2002) argues that every claim to legitimate power requires actual or attempted satisfaction of societal needs, in whatever way these needs might be defined. The implication for compliance officers is that they must be seen to be effective in helping corporations achieve regulatory commitments if they are to retain legitimacy. Compliance officials risk their legitimacy if employees are unsure about their effectiveness in helping these employees navigate ethical dilemmas and in responding clearly to complaints about unethical behaviours.

In conclusion, building legitimacy requires compliance officers to act lawfully, to ensure processes for everyday decision-making are experienced as just, to allocate resources justly across different competing groups and individuals, and to ensure effective use of authority to achieve

organisational mandates. It is not sufficient for compliance officials to have policies that express commitments and intentions to pursue these legitimation mechanisms. Effective legitimation requires the closing of the gap between rhetoric and practice. Employees will form their views about the legitimacy of compliance officials based on direct or vicarious experiences rather than policy pronouncements. According to Tyler (2011, p. 256):

> Every encounter that the public have with the police…should be treated as a socialising experience that builds or undermines legitimacy. Each contact is a "teachable moment" in which people learn about the law or legal authorities.

## 4 Legitimacy and Employee Behaviour

As we noted above, legitimacy is a problem for all social systems. It is a problem for corporations and their regulators. But the question that these varieties of power-holders are bound to ask is whether there is any evidence to show that legitimacy matters for securing compliance. We have already suggested that "the presence or absence of legitimacy carries large consequences for all parties in a system of power relations" (Sparks 1994, p. 15). The evidence we review here confirm Sparks further claim that "only legitimate social arrangements generate commitments towards compliance on moral rather than just expedient grounds" (p. 15; see also Beetham 1991). Before considering that evidence, an important caveat is in order. It is that legitimacy matters not only for its instrumental value; the structures of leg itimacy are such as to place upon power-holders (e.g. regulators, corporations, and supervisors) a normative obligation to exercise power in accordance with certain principles which are valid in and of themselves (see Tankebe 2009; Watson, forthcoming).

We start with Gouldner's (1954) classic study of mining factory between 1948 and 1951. Although obviously an old study, the findings emerging from the study has clear resonance for regulators seeking to influence the behaviour of regulates today. Gouldner posed the question: "*what is it about bureaucracy* which elicits hostility, fostering tensions within the organization itself or between the organization and the public with which it deals?" (p. 181, emphasis original). Gouldner found that the legitimacy of rules mattered greatly for their compliance either by employees, management, or both. There were rules, such as those against smoking in company premises that were scarcely enforced; indeed, they were jointly violated by employees and managements. When his researchers asked why employees ignored no-smoking signs, one answered as follows:

> Yes, these are not really Company rules. The fire insurance writers put them in. The office seems to think that *smoking doesn't hurt anything,* so they don't bother us about it. That is, of course, until the fire inspector (from the insurance company) comes around. Then as soon as he gets into the front office, they call down here and the *word is spread around for no smoking.* (pp. 182–183)

It was not just the fact of the external origin of the rule that triggered non-compliance. Gouldner observed that what the initiators of the rule had failed to do was to justify it in shared values within the plant. Similar challenges arose in cases where rules or procedures were initiated by either management or employees. Here, Gouldner found that the non-initiating party considered the rule illegitimate and tended to violate it. In other words, in our terms, the initiation and implementation of these rules failed the legitimacy dialogue test, opting rather for arbitrariness. However, this was not the case with safety rules in the plant; here, both parties jointly initiated the rule and felt they could legitimise it in terms of their respective values. The result was high compliance, including formal and informal reward and punishment structures to ensure obedience.

Clearly, Gouldner's findings continue to speak to regulatory compliance today. As the financial crisis and cases of tax avoidance such as that by Google demonstrate, there are important questions not only about compliance or non-compliance per se, but also the quality of compliance that can be expected from regulatees. While the challenges are clearly multifaceted, a message from Gouldner's evidence is that if regulators are to avoid non-compliance or "creative compliance" (see Chapter 1 by Bottoms), they need to take seriously the task of legitimising the making and enforcement of regulations. This, as we have discussed above, involves a continuous dialogue between regulators and their regulatees. The same is also true for management as they seek to encourage compliance with internal and external regulations.

More recently, various quantitative studies from diverse organisational settings show that legitimacy matters for compliance. Gobena and Van Dijke (2016) analysed survey data from 231 small and large business owners in the Ethiopian to establish the factors that encourage what they called "voluntary tax compliance". Two key findings emerged from their data; first, "procedural justice was associated with voluntary

tax compliance only when legitimate power of the tax authority was low and when coercive power of the authority was high" (p. 31). Second, coercion was only important in securing "forced tax compliance". These findings indicate that treating regulatees fairly makes a difference to the quality of compliance that regulators can expect from them (see also, Kogler et al. 2013; cf. Ariel 2012).

Other studies have examined legitimacy and workplace rules. Feldman and Tyler (2012) conducted a web survey of 599 Israeli employees about the work experiences to establish whether such experiences explained any differences in compliance with workplace rules. Compliance was measured with items such as "How often do you comply with organizational instructions and regulations?" and "how often do you use company rules to guide what you do on the job?" (p. 55). The results showed that where employees perceived that performance evaluation procedures were legal and that they were offered an opportunity makes an input during performance review, the likelihood of compliance with rules increased. As the authors concluded, "evaluations of the procedural justice of performance appraisal hearings more strongly influenced judgments of overall workplace fairness, perceptions of management legitimacy, and employee rule-adherence behavior when employees believed fairer workplace procedures were required by law" (Feldman and Tyler 2012, p. 46).

In the context of law enforcement, evidence from various studies supports the importance of legitimacy within organisations. For example, Tyler and his colleagues collected survey data from 209 law enforcement officials and 210 military officers about organisational legitimacy and rule-adherence (Tyler et al. 2007). The results showed that experiences of fair procedures and a perception that rules align with one's values predicted the likelihood that people will follow job requirements, follow organisational rules, and defer to policies. Similarly, Bradford and his colleagues surveyed 1043 police officers from Durham Constabulary and reported that perceptions of organisational justice were associated with greater self-reported compliance (Bradford et al. 2014; see also Bradford and Quinton 2014; Tankebe and Meško 2015). The implication is that building legitimacy with organisations can encourage "self-regulation" which, in turn, may reduce misconduct and unethical behaviours by regulatees.

## 5 Conclusion

Let us conclude our discussion with a few observations. First, we have seen that legitimacy requires compliance officers to act in accordance with regulations and laws, to demonstrate effectiveness in achieving their core mandates, to employ procedures that are fair to employees, and to avoid discrimination in dealing with employees of different social backgrounds or role differentiation. However, experience shows that there are often tensions among these legitimation mechanisms; the quest to act effectively might come up against legal and fairness requirements (see Bottoms and Tankebe 2017). How those tensions, even conflicts, are resolved can often make the difference between a scandal that threatens the survival of corporations and the legitimacy health of corporations. The financial crisis of 2008 and Cambridge Analytical show what can happen when officials put narrowly-defined effectiveness targets ahead of ethical obligations.

Second, a key implication of the above and the dialogue view of legitimacy is that the legitimacy of compliance officers is never a given, never a settled phenomenon (Dunn 2013). It is always work in progress, and it is work that is never always smooth and uncontested; it is, as Loader and Sparks (2013) put it an "unfinished business". This means compliance officers cannot engage in what we might term *legitimacy fracking*. By legitimacy fracking, we mean the attempt to secure recognition one's authority through moments of intensive pursuit of legitimation mechanisms. For example, growing evidence that procedural justice builds legitimacy, which, in turn, encourages compliance and cooperation has led some police departments to offer procedural justice training to frontline officers (see Skogan et al. 2015). However, the approach appears entirely managerialist in mindset, with street-level officers and senior officials expecting procedural justice training to yield immediate legitimacy dividends. Such an approach is not true to the nature of legitimacy and neglects the historical processes that have produced the current fraught legitimacy relationships that are the target of the fracking. It is, therefore, important that compliance officers avoid a managerialist mentality when they seek to build or to repair legitimacy. Legitimacy requires a long-term strategy that is fully conscious of the complex and ceaseless nature of legitimacy.

Third, it is tempting but wrong to assume that individual experiences of effective, fair, and lawful exercise of authority by compliance officers can translate seamlessly into favourable judgments of the overall legitimacy of the organisation the officers represent. The reason is that

there is a problem of induction in legitimation, a problem of moving from particular positive experiences to general institutional legitimacy perceptions. In a brilliant paper, Bell (2016) shows how people make exceptions about individual power-holders ("officer exceptionalism"); sometimes, people find officers effective in handling particular problems ("domain specificity"), or they foresee some beneficial outcome in a given situation ("therapeutic consequences"), while, other times, it is in search of protection or to secure leverage with other power-holders ("institutional navigation"). The challenge in building organisational legitimacy is, therefore, the challenge of making individual experiences with compliance officers count for general legitimacy perceptions.

However, these caveats which emphasise the complexity of building legitimacy do not imply resignation; indeed, they rather reinforce the centrality of legitimacy in all spheres of a compliance officer's day-to-day activities. What can corporate managers do to build a legitimacy culture? Tyler (2011) has outlined a number of strategies. First, *the attitude of leaders—tone from the top*. It is indubitable that leaders play a crucial role in shaping the culture within corporations. Therefore, leadership can create a moral climate within corporations that emphasise the principles of legitimacy in all aspect of work, including the work of compliance officers. This may start by the example from leadership at all levels in terms of how they treat ordinary employees. The available research evidence shows that such treatment can affect employee compliance with organisational directives.

A second strategy involves *designing new operational guidelines* (Tyler 2011). Managers could start by mapping out sites of legitimacy deficits; for example, are there particular aspects of work practices—such as promotions and complaints handling—or are there employees in certain departments that are associated with high concentrations of illegitimacy. Operating procedures can be developed for supervisors that mimic the legitimation mechanisms discussed. Third, *employee reward structures* can be restructured to in order to build legitimacy among employees (Tyler 2011). In the specific context of policing, Tyler rightly argues that "if officers believe that their opportunities for advancement, their compensation, and the respect that they will have in the eyes of their leadership are linked to their ability to create legitimacy and motivate cooperation, then they are more likely to engage in procedurally just behavior when on the street". The same might be true for all institutions that aim to establish and maintain the legitimacy of compliance officers.

## Notes

1. Sentencing Remarks by Mr. Justice Keith, 20 November 2012. https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/kweku-adoboli-sentencing-remarks-20112012.pdf, accessed 2 January 2019.
2. Chattam House. 2010. https://www.chathamhouse.org/expert/comment/lasting-effects-financial-crisis-have-yet-be-felt, accessed 3 January 2019.
3. Taleb uses the term via *negativa* to mean the same thing; as he defines it, via negativa is "the philosophical principle that we know what is wrong with more clarity than what is right, and that knowledge grows by subtraction" (Taleb 2018, p. 15fn).

## References

Allan, T. (2001). *Constitutional Justice: A Liberal Theory of the Rule of Law*. Oxford, UK: Oxford University Press.

Allred, B. B., Findley, M. G., Nielson, D., and Sharman, J. C. (2017). Anonymous Shell Companies: A Global Audit Study and Field Experiment in 176 Countries. *Journal of International Business Studies, 48*(5), 596–619.

Ariel, B. (2012). Deterrence and Moral Persuasion Effects on Corporate Tax Compliance: Findings from a Randomized Controlled Trial. *Criminology, 50*(1), 27–69.

Arsovska, J., and Verduyn, P. (2007). Globalization, Conduct Norms and 'Culture Conflict' Perceptions of Violence and Crime in an Ethnic Albanian Context. *The British Journal of Criminology, 48*(2), 226–246.

Beetham, D. (1991). *The Legitimation of Power*. London: Macmillan.

Beetham, D. (2013). Revisiting Legitimacy, Twenty Years on. In J. Tankebe and A. Liebling (Eds.), *Legitimacy and Criminal Justice: An International Exploration* (pp. 19–36). Oxford: Oxford University Press.

Bell, M. C. (2016). Situational Trust: How Disadvantaged Mothers Reconceive Legal Cynicism. *Law and Society Review, 50*(2), 314–347.

Bottoms, A. E. (this volume) Understanding Compliance with Laws and Regulations: A Mechanism-Based Approach. In M. Krambia-Kapardis, *Financial Compliance: Issues, Concerns and Future Directions*. Palgrave Macmillan.

Bottoms, A. E. (2002). Morality, Crime, Compliance and Public Policy. In A. E. Bottoms and M. Tonry (Eds.), *Ideology, Crime and Criminal Justice: A Symposium in Honour of Sir Leon Radzinowicz*. Cullompton: Willan.

Bottoms, A. E., and Tankebe, J. (2012). Beyond Procedural Justice: A Dialogic Approach to Legitimacy in Criminal Justice. *The Journal of Criminal Law and Criminology, 102*(1), 119–170.

Bottoms, A. E., and Tankebe, J. (2013). Voice Within: Powerholders' Perspectives on Authority and Legitimacy. In J. Tankebe and A. Liebling

(Eds.), *Legitimacy and Criminal Justice: An International Exploration*. Oxford: Oxford University of Press.

Bottoms, A. E., and Tankebe, J. (2017). Police Legitimacy and the Authority of The State. In A. Du Bois-Pedain, M. Ulväng, and P. Asp (Eds.), *Criminal Law and the Authority of the State*. Oxford: Hart Publishing.

Boulding, K. E. (1967). The Legitimacy of Economics. *Economic Inquiry, 5*(4), 299–307.

Bradford, B., and Quinton, P. (2014). Self-Legitimacy, Police Culture and Support for Democratic Policing in an English Constabulary. *British Journal of Criminology, 54*(6), 1023–1046.

Bradford, B., Quinton, P., Myhill, A., and Porter, G. (2014). Why Do 'the Law' Comply? Procedural Justice, Group Identification and Officer Motivation in Police Organizations. *European Journal of Criminology, 11*(1), 110–131.

Brownlee, K. (2011). *Offender's Part in the Dialogue*. In Rowan Cruft, Matthew H. Kramer, and Mark R. Reiff (Eds.), *Crime, Punishment, and Responsibility: The Jurisprudence of Antony Duff*. Oxford: Oxford University Press.

Carroll, A. B. (1991). The Pyramid of Corporate Social Responsibility: Toward the Moral Management of Organizational Stakeholders. *Business Horizons, 34*, 39–48.

Coicaud, J.-M. (2002). *Legitimacy and Politics: A Contribution to the Study of Political Right and Political Responsibility*. Cambridge: Cambridge University Press.

Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O., and Ng, K. Y. (2001). Justice at the Millennium: A Meta-Analytic Review of 25 Years of Organizational Justice Research. *Journal of Applied Psychology*, *86*(3), 425–445.

DiMaggio, P., and Powell, W. W. (1983). The Iron Cage Revisited: Collective Rationality and Institutional Isomorphism in Organizational Fields. *American Sociological Review, 48*(2), 147–160.

Dunn, J. (2013). Legitimacy and Democracy in the World Today. In J. Tankebe and A. Liebling (Eds.), *Legitimacy and Criminal Justice: An International Exploration*. Oxford: Oxford University Press.

Feldman, Y., and Tyler, T. R. (2012). Mandated Justice: The Potential Promise and Possible Pitfalls of Mandating Procedural Justice in the Workplace. *Regulation and Governance, 6*(1), 46–65.

Ferran, E. (2012). The New Mandate for the Supervision of Financial Services Conduct. *Current Legal Problems, 65*(1), 411–453.

Gobena, L. B., and Van Dijke, M. (2016). Power, Justice, and Trust: A Moderated Mediation Analysis of Tax Compliance Among Ethiopian Business Owners. *Journal of Economic Psychology, 52*, 24–37.

Gouldner, A. W. (1954). *Patterns of Industrial Bureaucracy*. New York: The Free Press.

Hirschi, T. (1969). *Causes of Delinquency*. Berkeley: University of California Press.

Honneth, A. (1996). *The Struggle for Recognition: The Moral Grammar of Social Conflicts*. Cambridge: Polity Press.

Johnston, D. (2011). *A Brief History of Justice*. Chichester: Wiley.
Kogler, C., Batrancea, L., Nichita, A., Pantya, J., Belianin, A., and Kirchler, E. (2013). Trust and Power as Determinants of Tax Compliance: Testing the Assumptions of the Slippery Slope Framework in Austria, Hungary, Romania and Russia. *Journal of Economic Psychology, 34*, 169–180.
Lerner, M. J., and Clayton, S. (2011). *Justice and Self-Interest*. Cambridge, UK: Cambridge University Press.
Loader, I., and Sparks, R. (2013). Unfinished Business: Legitimacy, Crime Control and Democratic Politics. In J. Tankebe and A. Liebling (Eds.), *Legitimacy and Criminal Justice: An International Exploration*. Oxford: Oxford University Press.
MacCormick, N. (2007). *Institutions of Law*. Oxford: Oxford University Press.
Mathiesen, T. (1965). *The Defences of the Weak: A Sociological Study of a Norwegian Correctional Institution*. London: Routledge.
Mazerolle, L., Antrobus, E., Bennett, S., and Tyler, T. R. (2013). Shaping Citizen Perceptions of Police Legitimacy: A Randomized Field Trial of Procedural Justice. *Criminology, 51*(1), 33–63.
Mbembe, J. A. (2001). *On the Postcolony*. Berkeley: University of California Press.
Reus-Smit, C. (2007). International Crises of Legitimacy. *International Politics, 44*(2–3), 157–174.
Rosanvallon, P. (2011). *Democratic Legitimacy: Impartiality, Reflexivity, Proximity*. Princeton: Princeton University Press.
Rothstein, B. (2011). Anti-corruption: The Indirect 'Big Bang' Approach. *Review of International Political Economy, 18*(2), 228–250.
Sherman, L. W. (1978). *Scandal and Reform: Controlling Police Corruption*. Berkeley: University of California Press.
Skogan, W. G., Van Craen, M., and Hennessy, C. (2015). Training Police for Procedural Justice. *Journal of Experimental Criminology, 11*(3), 319–334.
Sparks, R. (1994). Can Prisons Be Legitimate? "Penal Politics, Privatization, and the Timeliness of an Old Idea". *The British Journal of Criminology, 34*, 14–28.
Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review, 20*(3), 571–610.
Sunshine, J., and Tyler, T. R. (2003). The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing. *Law and Society Review, 37*(3), 513–548.
Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. New York: Random House.
Taleb, N. N. (2018). *Skin in the Game: Hidden Asymmetries in Daily Life*. London: Allen Lane.
Tamanaha, B. (2001). *A General Jurisprudence of Law and Society*. Oxford, UK: Oxford University Press.
Tamanaha, B. (2004). *On the Rule of Law: History, Politics, Theory*. Cambridge, UK: Cambridge University Press.

Tankebe, J. (2009). Policing, Procedural Fairness and Public Behaviour: A Review and Critique. *International Journal of Police Science and Management, 11*(1), 8–19.

Tankebe, J., and Meško, G. (2015). Police Self-Legitimacy, Use of Force, and Pro-Organizational Behaviour in Slovenia. In *Trust and Legitimacy in Criminal Justice: European Perspectives* (pp. 261–277). London: Springer.

Tyler, T. R. (2003). Procedural Justice, Legitimacy and the Effective Rule of Law. In M. Tonry (Ed.), *Crime and Justice: Review of Research* (Vol. 30, pp. 283–357). Chicago: University of Chicago Press.

Tyler, T. R. (2006). *Why People Obey the Law*. Princeton: Princeton University Press.

Tyler, T. R. (2011). Trust and Legitimacy: Policing in the USA and Europe. *European Journal of Criminology, 8*(4), 254–266.

Tyler, T. R., and Fagan, J. (2008). Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities. *Ohio State Journal Criminal Law, 6*, 231–275.

Tyler, T. R., and Huo, Y. (2002). *Trust in the Law: Encouraging Public Cooperation with the Police and Courts Through*. New York: Russell Sage Foundation.

Tyler, T. R., Callahan, P., and Frost, J. (2007). Armed, and Dangerous(?): Motivating Rule Adherence Among Agents of Social Control. *Law and Society Review, 41*, 457–492.

Ullmann-Margalit, E. (2017). *Normal Rationality: Decisions and Social Order*. Oxford: Oxford University Press.

Watson, G. (forthcoming). *Respect and Criminal Justice*. Oxford: Clarendon Press.

Weber, M. (1978). *Economy and Society: An Outline of Interpretive Sociology* (2 vols, ed. G. Roth and C. Wittich). Berkeley: University of California Press.

Wikström, P. O. H., Oberwittler, D., Treiber, K., and Hardie, B. (2012). *Breaking Rules: The Social and Situational Dynamics of Young People's Urban Crime*. Oxford: Oxford University Press.

Wrong, D. (1994). *Problem of Order*. New York: Simon and Schuster.

**Justice Tankebe** is a University Lecturer in Criminology and a Fellow at St. Edmund's College, University of Cambridge. He holds MPhil degree in Criminological Research and a Ph.D. in Criminology from the University of Cambridge. He was a teaching associate on the Police Executive Programme at the Institute of Criminology, Cambridge. Justice's interests include policing, legitimation and legitimacy, organisational justice, and corruption. His current research projects include legitimacy and counter-terrorism policing, corruption among prospective elites, sentencing decision-making in Ghana, the death penalty in Africa, and police self-legitimacy.


CHAPTER 3

# The Uncertain Professional Status of Compliance

*James A. Fanto*

## 1 Introduction

For the past two decades, the story of compliance has been one of progress, even triumph, in business firms and other organizations. Yet compliance officers face persistent challenges, at least in the USA. The contention in this chapter will be that these challenges arise from the uncertain professional status of compliance. This uncertainty owes much to the ambivalence that the legal profession shows toward compliance: At times, it claims that legal authorities should assert control over compliance practice, while at other times it appears indifferent to the activities of compliance officers. Among other reasons, this ambivalent relationship with the law has made it difficult for compliance to acquire full professional status.

This chapter proceeds as follows. Section 2 describes the triumph of compliance within US organizations. After briefly identifying the nature of compliance, it discusses its origins in law and regulation governing different industries. It then observes that compliance has become an accepted organizational function—this is its triumph—as one of the systems of

J. A. Fanto (✉)
Brooklyn Law School, New York City, NY, USA
e-mail: james.fanto@brooklaw.edu



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_3

internal control and that there is now an accepted model of compliance and its governance. The Part also explains that a particular sign of the institutionalization of compliance in organizations is the prevalence of the position of the chief compliance officer (CCO), who is a specialist in compliance and directs the compliance department and program.

Section 3 discusses the ways in which compliance has progressed along the path to achieving professional status. It explains that compliance has become a recognized occupation, with certain knowledge and skills that its practitioners must obtain and exhibit. Moreover, it observes that, as in the case of other professions, institutions of higher learning increasingly impart this knowledge to aspiring compliance officers through courses of study. It discusses how compliance practitioners have a group identity of engaging in a common mission that is exemplified by their membership in professional organizations. The Part explains, however, that they do not possess a defining feature of professional status, which is their control over the practice of compliance (i.e., a monopoly of practice), which is usually granted to a field by the government, as exemplified by medicine and the law.

Section 4 identifies several negative effects or consequences of compliance's uncertain or incomplete professional status. The first is compliance officer liability, where a compliance officer is held responsible when a major legal violation occurs in an organization. The Part explains that this liability is imposed on compliance officers because they are not seen as independent professionals offering advice to executives, but as part of executive teams. The second negative effect is weak employment protection for compliance officers in circumstances where they try to prevent or detect organizational misconduct. Here courts fail to accord them protection provided to members of other professions because they fail to acknowledge the public mission fulfilled by compliance officers. The third consequence is the uncertain organizational status of compliance officers, particularly the CCO, who may work in a compliance department but may be subject to the control of diverse executives. The uncertain organizational status of compliance allows organizations to place compliance officers and the compliance department where they see fit in their structures.

Section 5 offers several reasons for the incomplete professional status of compliance. It explains that the most significant reason is the ambivalent relationship between compliance and the established legal profession. It explains how, in its origins, compliance was part of or under the

authority of legal departments. Moreover, it observes how, from time to time, legal authorities and practitioners assert control over it as if it were in their domain of influence. It points out, however, that at other times the legal profession has been passive or complacent with respect to compliance practitioners (including those trained as lawyers), even allowing them to engage in legally related activities. The Part offers reasons for this ambivalence, including that the legal profession has acceded to the demands of its organizational clients that need compliance but that wish to have control over it. The Part also explains how the government through regulators favors having compliance separated from the legal profession and having a weaker professional status because compliance officers can be more easily enlisted to serve government purposes. Finally, the Part observes that the uncertain professional status of compliance is due to other disciplines, such as organizational and management studies, claiming that compliance should be under their theoretical control and to the fact that technological developments in compliance suggest sources of information and training for compliance officers other than the law.

Section 6 offers thoughts on the future of compliance as a profession. It discusses how the legal profession may continue to influence compliance's professional identity, particularly because one of compliance's main tasks is instructing organizational actors on how to conduct their affairs in line with law and regulation. It suggests that the law may retain compliance as a "satellite" activity or subprofession, which may be in the interest of compliance practitioners because of the status associated with the legal profession. It also observes that law's influence over compliance is reinforced by how regulators, their enforcement officials and prosecutors control the structure of compliance programs. However, the Part acknowledges that compliance is a "young" occupation and that a different professional outcome may thus emerge. It notes that, as compliance develops outside the USA, there may be other sources of professional inspiration for it that are not legally focused.

Finally, Sect. 7 concludes.

## 2 The Triumph of Compliance

The last two decades have witnessed the establishment, and even triumph, of compliance in organizations throughout the USA. Compliance is the function in an organization that helps to ensure

that the organization, its employees and agents conduct their affairs in accordance with law, regulation and ethical standards (Miller 2017, p. 3). In this respect, it is part of the internal control systems of organizations (COSO 2013, p. 2). In the modern era, the government, through regulators and prosecutors, supplements its own enforcement of laws and regulation, which constitute "external control," with the "internal control" conducted by the organizations themselves (Miller 2017, pp. 157–158). This internal control function is necessary because the government does not have the resources to make sure that the many organizations existing in the private sector are in fact following the law.

There is a rich literature on the origins of compliance. Some point to the growth of the administrative state in the twentieth century, which began to regulate in detail organizations operating in various sectors (Miller 2017, p. 160). The affected organizations needed a firm function to keep track of all the pertinent regulations and to make sure that employees were complying with them. The basic legal reason for the existence of a compliance function in an organization is an organization's liability for the acts of its employees and agents. This liability, which existed in common law, has found its way into criminal law and has been further imposed directly upon organizations by statutory law and regulation. If an organization is criminally or civilly liable for misconduct by its employees and agents, it has an incentive to prevent this misconduct. It thus makes sense for an organization to have a function to keep track of the laws and regulations governing the organization's activities, particularly if they are detailed and complex, to instruct employees on how to do their work in compliance with them and to prevent and to detect legal violations. This became the compliance function (Griffith 2016, pp. 2082–2083).

In certain industries, Congress and regulators directly or indirectly imposed a compliance function on the organizations regulated by them. For example, in the brokerage industry, Congress imposed a duty of supervision on broker-dealers, which made them liable for a supervisory violation if a brokerage employee violated the law. Congress also provided firms with defenses to this liability if a firm had an effective and comprehensive system of supervision of the employees, which system required that the employees be trained and monitored. A firm function was needed to create and administer this system, which was

the compliance department. Years later, the delegated self-regulator of broker-dealers required them by rule to have a CCO to establish and direct the compliance department and to guide the broker-dealer's board and management in compliance matters (Fanto 2014, pp. 1130–1143). A similar story about the development of compliance departments could be told for other regulated industries, such as health care, commercial banking, investment advisors and companies operating in the defense industry, to name a few.

Many attribute the growth of compliance for US organizations in general to the guidelines of the US Sentencing Commission that set out guidance for punishment of organizations in which criminal conduct under federal law had occurred. These guidelines recommended that an organization receive favorable sentencing treatment if it had an effective compliance program (Griffith 2016, pp. 2084–2086). The guidelines also laid out the features of an effective program, which included having a CCO who would be responsible for the day-to-day operations of the compliance function (US Sentencing Commission 2016, § 8B2.1 (b), pp. 534–535). In an amendment, the guidelines expanded the definition of an effective compliance program to include compliance with ethical standards, in addition to law and regulation (Hess 2016, p. 335). The guidelines have become a powerful incentive for an organization to have a compliance program because nearly every organization could be subject to criminal liability under federal law for the misconduct of its employees.

Whatever their exact genealogy, compliance, compliance programs and compliance officers are now part of the US organizational landscape. Moreover, there is now a standard "model" for the functions or features of a compliance program, which Congress and regulators follow when they impose compliance requirements on firms in another industry (Langevoort 2002, pp. 81–83). The first task of a compliance program is to identify the compliance and legal risks (as well as ethical risks) in the organization, ideally determining those with the greatest probability of occurring and the greatest consequences. It then promulgates compliance policies and procedures to address these risks: The policies set out general principles of conduct for organizational actors while the procedures instruct them on how to conduct their affairs and business in accordance with the law, regulations and the organization's code of ethics. As part of the compliance program, compliance

officers train organizational actors in these policies and procedures and, significantly, advise them on how to conduct themselves in accordance with these guidelines, as well as on how to deal with new or unusual situations falling outside them. Compliance officers monitor organizational actors to ensure that they are following the policies and procedures and to detect any violations of them, which might indicate a legal or ethical violation. Under the compliance program, compliance officers may be required to investigate potential instances of noncompliance, or the organization's legal department may have this duty. Finally, one of the features of a compliance program is to audit it to make sure that it is functioning appropriately and to update it to take account of any legal or other developments affecting the organization.

Another important and accepted part of a compliance program, which is generally found in an organization's compliance policies and procedures, is the governance of compliance (The American Law Institute 2017, § 3.01, p. 19). This means that the compliance program assigns compliance responsibilities to the various organizational actors. As in the case of the other compliance program features, compliance governance has become standardized through law, regulation and practice. Typical compliance governance has the governing body of the organization, such as a board of directors, approving, and periodically reviewing, the compliance program, which is the responsibility of senior executives to formulate and propose. These executives turn to the CCO, the specialist of compliance, for its design (DeMott 2013, p. 64). The CCO (in some organizations, the "CECO" (chief ethics and compliance officer)) administers and manages the compliance program on a day-to-day basis with attendant compliance officers (together, they make up the compliance department). The CCO also reports and advises the governing body and senior executives on compliance issues and, depending upon the industry, may report on the performance of the compliance function to the organization's regulator.

An overview of compliance over the past twenty or so years reveals an organizational function that has become established and standardized: thus, the characterization of the story of compliance as one of "triumph." Moreover, the occupation of compliance has itself progressed along the path of achieving recognition as a profession. It is to this subject that the chapter now turns.

## 3 Compliance's Incomplete Professional Status

Scholars of professions propose that an occupation achieves professional status when it possesses certain features (Freidson 2001, p. 127). A practitioner of the occupation must acquire a certain body of knowledge and related skills that are necessary to conduct the activity in question and that are distinct from those used by people engaged in other occupations. The application of the knowledge and the exercise of the skills require discretion and judgment. In this application and exercise, the professional activity is distinguished from a technical one, which requires specialization but which involves routines and less judgment. Another important professional feature is that the acquisition of the required body of knowledge and the basic skills takes place in universities outside the labor market. Professional schools within universities act as a required gateway or passage for aspiring members of a profession, because in the institutions professionals devoted to research and education train the students for their future occupation. Yet another professional feature is a consciousness by its practitioners that they engage in a common occupation and a shared social identity associated with it. The consciousness and identity often emerge from the shared professional formation and are evidenced by societies and organizations devoted to standardizing, advancing and sharing professional knowledge and practices. The most important professional feature is that the government accords to the occupation official recognition by giving its practitioners a monopoly of practice and exclusive control of the activity. The government, thus, makes it illegal for anyone to engage in the activity unless the practitioner is an authorized member of the profession. This exclusive control, however, is given only to occupations that can establish that the control is necessary for the public benefit; a profession justifies its special status on the grounds of public service.

The occupation of compliance has some of these professional features (Walsh 2015, pp. 776–788). As discussed in the preceding Part, compliance is a recognized practice of specific activities. There are accepted and proper ways of conducting these activities, which demand certain knowledge and skills. Moreover, this knowledge has become "theorized" and is embodied in standardized format (International Standard 2014). Practitioners and scholars are enhancing the theoretical and practical knowledge about compliance, which is evidenced by a growing number of articles and books on the subject.

Moreover, the teaching of compliance knowledge and skills has become part of the university curriculum. These institutions, particularly through their law and business schools, are offering students courses of study and degrees in compliance, with the promise and understanding that they are preparing the students for careers in compliance (Fanto 2015, pp. 760–763). Certainly, this university activity is in its embryonic form and is not at the level of established professions (e.g., there are no "compliance schools" like law and medical schools). Moreover, as noted above, the teaching of compliance often takes place in another professional school, like a law school. Because compliance is a relatively new occupation, it would not be expected to have a complete university setting at this stage of its development. However and significantly, unlike in established professions, the passage through specific university studies, with its generalist and theoretical training, is not a requirement for compliance practice; a person can enter the compliance field in many ways, including by "on the job" training, which is more characteristic of technical fields, rather than professions (Freidson 2001, p. 90).

Moreover, compliance officers and practitioners demonstrate that they are aware of engaging in and furthering their common occupation. This awareness is best evidenced by the fact that there exist in the USA "professional" groups or societies that a compliance officer can join (e.g., Society of Corporate Compliance & Ethics, National Society of Compliance Professionals). Not only do these societies have journals and other publications that promote standard compliance practices and codes of ethics and develop theoretical and practical knowledge, but they also have conventions and other meetings where compliance practitioners can gather to become acquainted and to share their knowledge and skills. These meetings also foster the collective identity of compliance practitioners. In addition, in these societies, compliance positions are advertised, which shows that compliance practitioners can have a professional career where they move horizontally from firm to firm, including to firms of only compliance practitioners, rather than having their work identity defined solely by their organization (Freidson 2001, p. 76).

Despite this attainment of professional features, compliance still lacks the ultimate one: Authority given by the government to compliance practitioners to control their occupation, particularly to determine who can engage in it, and to separate it from other occupations. There has been no sustained movement to have compliance receive this power, which, again, would be closely related to an exclusive formation

for compliance practitioners through university training (Walsh 2015, pp. 794–795). This leads to the subject of how the failure to possess all professional features and to achieve full professional status has hurt compliance practice, to which the next Part is devoted.

## 4 The Negative Effects of Compliance's Incomplete Professionalism

Despite its successes and its steps toward achieving full professional status, compliance faces persistent challenges. The contention here is that these challenges all relate to the incomplete or uncertain professional situation of compliance. The challenges are: (i) compliance officer liability, (ii) problematic employment protection for compliance officers who report organizational problems, and (iii) the varying organizational position of the CCO and the compliance department.

Compliance officer liability occurs when a compliance officer is held responsible for misconduct in the organization (Golumbic 2017, p. 49). Compliance officers can be liable in different circumstances, some of which do not implicate, or pose a challenge to, compliance's professional status. Like any other employee, a compliance officer can participate, directly or indirectly, in the misconduct, and his or her liability in such circumstances has no implication for the professional position. Moreover, a compliance officer may be liable if the misconduct occurred in the organization because of the officer's neglect of, or failure to perform, his or her compliance duties. For example, if the officer is responsible for drafting policies and procedures to direct appropriate conduct for a given activity, but fails to do so, and employees engage in the activity in violation of the law, the officer may be held liable for the violation, in additional to the perpetrators. This is not problematic from a professional perspective, because the compliance officer is liable for not adequately performing his or her organizational role.

The troubling situations are those where misconduct has occurred in the organization, but where compliance officers have not been involved in it or negligent in the performance of their duties. Rather, in many of these situations, compliance officers detected the misconduct and warned executives about its risk, but were ignored. When enforcement officials identify those who are vicariously responsible for the misconduct, in addition to the primary liability of the violator, they include the

compliance officer in this group of executives as someone who had control or supervisory authority over the violator or the activities in which the violator was engaged. Needless to say, this kind of prosecution of compliance officers has produced consternation among them (Urban 2015). He contends that, as part of an organization's internal control system, they are only advising executives on the existence of the misconduct and leaving it to the executives, who are in the organization's chain of command to decide what steps to take in response to it. To lump compliance officers with managers and executives, supporters of compliance would argue, is to fail to understand the distinction between the organizational roles of the different parties.

Although compliance officer liability raises a number of issues depending upon the industry in question, it is clearly due to the incomplete professional status of compliance. In imposing supervisory liability upon compliance officers, enforcement officials are viewing them as just part of the organization's executive team responsible for managing and controlling organizational actors. They do not consider compliance officers as independent professionals, who have an organizational role but who, like inside counsel, occupy a special advisory position in light of their professional status. A clear and strong professional identity for compliance officers would make it much more difficult (although not impossible) for enforcement officials to impose this kind of liability upon them. For compliance officers could claim that they were fulfilling a public service duty in advising the executives on the misconduct, which duty the government itself has recognized.

Another related challenge to the position of compliance officers is weak employment protection for them when they identify, and report in the organizational chain, misconduct (Walsh 2015, pp. 773–776). In these situations, senior executives rebuff compliance officers and do not acknowledge the misconduct, sometimes because it implicates them in it. They fire the compliance officer in question, which is allowed under the "at will" nature of most employment relationships. However, an important exception to the "at will" doctrine provides that a professional cannot be fired for acting in accordance with his or her recognized professional duty, the exercise of which serves the public interest. In a notable New York case, a court declined to extend this exception to compliance officers, concluding, among other things, that they did not have the professional status entitling them to it (Sullivan v. Harnisch, p. 761). This judicial treatment of compliance officers in the employment area plainly reflects

the fact that the government has not recognized their "public interest" mission and thus granted them professional status. This lack of recognition is ironic because, as noted above, the government uses compliance officers to help accomplish a government function, enforcement of the law.

A third professionalism-related challenge facing compliance officers is their organizational position, particularly that of the CCO. In the scenario that would best reflect the professional status of compliance officers operating within an organization, the CCO would be in charge of a compliance department composed of compliance officers and would report directly to the chief executive officer, who would hire and fire this officer and determines the officer's conditions of employment (American Law Institute 2017, § 3.16 and Comment, pp. 96–105). The CCO would thus sit at the highest executive level, much in the way as does the general counsel, who is a member of an established profession. In addition, the CCO would have an informational reporting relationship with the highest governing authority of the organization, like a board of directors, which would also ensure that the CCO is not fired inappropriately and has the resources and authority to fulfill the position's responsibilities. This scenario would recognize both the organizational importance of compliance and the independence to which this professional internal control function is entitled.

Yet this scenario is not the universal or even the dominant model of the position of compliance officers and the CCO in organizations (LRN 2015, pp. 7–8). Once again, this is no doubt due to the uncertain professional status of compliance, which allows organizations to situate compliance and compliance officers as they would any other organizational function and actors. In many organizations, the CCO reports to the general counsel and the compliance department is a part of the legal department for cost and other reasons (Bird and Park 2016, pp. 204–205; Rostain 2008, p. 481). In others, the reporting may be to the chief risk officer or to the chief financial officer. While the law requires the governing authority to oversee the operation of compliance in the organization, the actual reporting relationship between CCOs and boards can vary greatly, and there may even be no regular reporting of CCOs to them. The organization's positioning of the CCO and the compliance department thus can undermine the claim by compliance officers that they are professionals operating within organizations but with a recognized independence accorded to them by their professional status.

In many cases, their occupation is characterized by bureaucratic, rather than professional, control (Freidson 2001, pp. 48–50).

While the above are not the only challenges facing compliance, they are persistent ones that point to its uncertain professional status. It is thus worthwhile exploring the reasons for and causes of these impediments to compliance's realization of a full professional status. This is the subject of the following part.

## 5 Reasons for the Uncertain Professional Status of Compliance

The primary cause of the uncertain or ambiguous professional status of compliance is its ambivalent relationship with an established profession, the law. That there are close connections between compliance and the law is not surprising because in its origins the compliance function emerged out of the legal department. Historically, a major task of inside counsel in organizations was "preventive law," the process designed to ensure that organizational actors complied with law and regulation in conducting organizational activities (Rosen 1989, p. 522). However, preventive law is simply another name for compliance. Indeed, an early codification of compliance was done by the National Center for Preventive Law, which was composed of inside and general counsel (National Center for Preventive Law 1996). Indeed, the close connection between law and compliance is evidenced in many organizations by the fact that the general counsel also serves as the CCO or is the person to whom the CCO directly reports.

Moreover, because compliance is related to and perhaps even a part of legal activities, the legal profession has occasionally asserted its authority over the compliance function (Remus 2014, p. 1259). Associations of general counsel and their intellectual supporters assert that compliance should be subject to the legal department in organizations and that the CCO should report to the general counsel (if there is a standalone CCO position) (DeStefano 2013–2014). They justify this assertion by the argument that, while compliance officers apply the law, their interpretation of it is subject to the judgment of the general counsel and the organization's legal staff, which judgment is part of the latter's professional activities. Indeed, the American Law Institute project on compliance, mentioned above, represents a recent example of the legal

profession's exercise of its authority over compliance. In the project, that Institute, an authoritative organization on the standardization of the law, sets forth the "principles" of compliance for organizations. This act makes professional sense only if the subject matter falls within the domain, or under the authority, of the legal profession.

At other times, the legal profession has distanced itself from or has been passive with respect to compliance and compliance practitioners (Rostain 2006, p. 1407). Although the practice of compliance, as it occurs in organizations today and as discussed above, could be seen to constitute a law practice, the legal profession does not explicitly address compliance in its Model Rules of Professional Conduct. Moreover, it has often taken a "hands off" approach to compliance by allowing lawyers to engage in compliance activities, so long as they do not advertise themselves as being involved in legal practice. However, compliance officers, many of whom are lawyers, may be viewed as offering legal advice to organizational actors whether through the policies and procedures or through their interpretation of them in particular circumstances.

There are explanations for the above ambivalence of the legal profession toward compliance. One explanation is that the legal profession is uncertain about how much to assert its authority in situations where organizations need legal advice that must be given in complex organizational contexts and that, as occurs in the case of compliance, draw upon both legal expertise and learning from other disciplines (e.g., accounting, intellectual technology) (Rostain 2006, pp. 1420–1423). A critical perspective on the legal profession's passivity in these situations is that it allows lawyers acting as compliance officers to serve purely organizational interests without professional oversight and thus without a profession's focus on the public interest (Remus 2014, p. 1270). This view is related to the claim that organizations (particularly large ones) increasingly limit the power of professionals whose services they need by incorporating them into the organization's hierarchy (Freidson 2001, p. 210). Thus, the legal profession has limited authority over compliance just as it may have lost full control over inside counsel (Rosen 1989, p. 542). Another explanation is that, well established as it is, the legal profession has little incentive to assert more than a general control over a law-related, subsidiary occupation like compliance (Freidson 2001, p. 154). For example, doctors have the ultimate authority over nurses and nurse practitioners, but they do not control those occupations.

The government has not pushed the legal profession to assert more control over compliance (or for compliance to become a standalone profession) because it has an interest in maintaining the uncertain professional status of compliance officers. Again, as noted earlier, compliance is part of internal control, which is an internalization of external (or government) control. Compliance officers are private actors who have been "deputized" to act for regulators and enforcement officials in their organizations. In this, they serve the interests of both their organizations and the regulators. The undefined professional status of compliance officers allows the government more leeway to use them for its own purposes than would be the case if compliance officers were clearly subject to the authority of the legal profession. If a compliance officer were part of a strong profession, or clearly part of the legal profession, they would serve the government's interests, but they would ultimately be subject to the canons or guidelines of their profession, which would lessen the government's control over them. For example, while a lawyer serves the public interest, the lawyer's professional relationship with and loyalty to his or her organization generally outweigh his or her obligations to the government. This is no doubt why it is reported anecdotally that regulators prefer that compliance officers not be lawyers. In other words, not unlike the organizations themselves, the government wants to subsume compliance officers within an organizational hierarchy, rather than allow them to act as professionals, although in its case the hierarchy is that of the government. This control allows the government to use compliance officers for specific, and changing, government purposes.

Not only has the legal profession been ambivalent about compliance—with government acquiescence in this ambivalence—but those in other intellectual disciplines, and even compliance practitioners, argue against the alignment of compliance with the law. There has been a sustained criticism of the involvement of lawyers in compliance (Parker et al. 2009). Organizational, managerial and business ethics scholars promote compliance as an occupation that has a different orientation from the legal profession (Weaver and Trevino 1999; Parker and Nielsen 2011). In this, they emphasize that the role of compliance is to promote ethical decision-making and an ethical culture in an organization (Tenbrunsel et al. 2003, pp. 293–296). This assertion is echoed by some practicing compliance officers who insist upon using the CECO title and who emphasize this aspect of their job, which they see as the foundation for a compliant organization (Murphy 2017, p. 425).

The overall message from these scholars and practitioners is that the focus on legal compliance can crowd out the mission of promoting ethical conduct, which allows destructive cultures to flourish in the organization and which ultimately leads to noncompliance and organizational problems.

This resistance to a legal orientation for compliance also reflects a different professional vision for it. The study of compliance would be situated in business, not law, schools and would be considered another managerial discipline. Its intellectual foundation would be in disciplines like organizational studies, business ethics and social psychology, rather than the law.

The uncertain professional status of compliance may also reflect developments in compliance practice today. Compliance was originally a "back office," almost technical function in industries like finance. Compliance practitioners knew how an organization's processes worked and made sure that they were done in accordance with basic policies and procedures. Today, many organizational operations are increasingly automated and guidance and monitoring with respect to them also demand technical expertise. Indeed, increasingly compliance practitioners should be skilled in or conversant with the technology enabling this automation and associated data analysis (Fanto 2016). Therefore, an alternative vision of compliance may be developing, which is within the domain of neither the legal practitioner nor the ethics specialist. However, this view of a compliance practitioner as a technical specialist would be at odds with professional status because it does not embrace the judgment and discretion that are typical of professionals.

It is thus clear from the above that there are many reasons for compliance's uncertain professional status. The importance of its professional outcome and predictions on what it might be will be the subject of the next part.

## 6 The Future of Compliance as a Profession

The outcome of the debate about the professional status of compliance and about the intellectual foundations of that organizational activity is not just an academic matter but has real-world consequences. It deals with, among other things, the importance given to this important internal control function in organizations. Because compliance is intended to prevent and to detect organizational misconduct, the resolution of the debate

could shape compliance practice in organizations and thus potentially result in effective, or ineffective, compliance and thus in less or more misconduct.

One potential outcome is that the legal profession continues to exert its authority over compliance, even if it does not draw this occupation entirely within its control as a designated legal practice (although that, too, represents a possibility). In this scenario, compliance would not achieve full professional status, but compliance practitioners would operate at the periphery of the legal profession as a related, somewhat technical occupation or "semi-profession," much in the way that various medical practices function under the authority of doctors (Freidson 2001, p. 90). There are a number of factors suggesting that this might well be the outcome. In many regulated industries (e.g., finance and health care), "legal" compliance is dominant because law and regulation influence the conduct of many activities and because regulators insist upon an organization's complete compliance with the law. The importance of law and regulation in these industries means that a compliance officer must possess legal knowledge and training. Thus, here compliance officers are recruited from law schools or law programs or have legal training (Fanto 2015, pp. 756–758). Although compliance officers also focus on ethical issues in these industries, they have less time to devote to them, given the sheer—and growing—number of laws and regulations.

Although this "legalization" of compliance appears in regulated industries, these industries are significant ones in the economy, such as finance, defense contracting and health care. Moreover, the governance and internal conduct of regulated firms often ends up serving as a model for nonregulated organizations, as practices in the former get taken up by the latter organizations. Thus, the focus on legal compliance and the use of lawyers in compliance programs may become widespread in nonregulated domains.

Moreover, prosecutors and other enforcement officials, who are all lawyers, have considerable influence over compliance in organizations that are not subject to special regulation. They evaluate the efficacy of organizations' compliance programs in their decisions whether to prosecute organizations when violations occur in them. As one of the elements of different kinds of settlements with organizations, such as "no prosecution" agreements and deferred prosecution agreements, prosecutors compel the organizations to modify their compliance programs and their compliance governance. The US Department of Justice even

had a compliance expert on its staff to assist in this evaluation of compliance programs and in the recommendations for modifications of them (US Department of Justice 2017). Prosecutors and enforcement officials guard their influence over compliance and show no inclination to relinquish it (Haugh 2017, p. 1239). Indeed, the American Law Institute project discussed earlier has a section devoted to Enforcement that, among other things, offers principles to guide enforcement officials in their evaluation of compliance programs.

There is no doubt that ethical conduct and the culture of compliance in organizations matter to the prosecutors and officials, and their settlements treat these issues. However, the emphasis in the settlements with respect to compliance programs is on legal compliance. This is understandable because, when they are crafting the settlement, prosecutors are responding to the revelation of significant legal violations in an organization and pushing organizations to reform the programs to ensure that the legal violations do not recur. The effect of this prosecutorial activity is to reinforce in all organizations that they need organizational actors with legal expertise, i.e., lawyers, as CCOs and compliance officers.

Therefore, much of what is occurring in compliance today argues for the continuation of the legal profession's influence over the field, which could continue the uncertain professional status of compliance, again unless that profession absorbs compliance within it. No doubt other disciplines, as discussed above, will continue to contest law's influence. However, they are in a weaker position than the legal profession, simply given the pressures for organizations to show their legal compliance. Moreover, there may be a social status story that also supports the continued, and even growing, influence of the legal profession in compliance. As more lawyers enter the compliance field, like inside counsel from a previous time, they may advocate that they be recognized as an important part of the legal profession. Clearly aligning themselves with that profession may bring compliance practitioners a higher organizational position and a benefit that usually accompanies a strong professional identity—more control over their working conditions.

As also discussed earlier, the government has its own reasons to resist the professionalization of compliance. However, it hardly speaks with a unified voice; after all, prosecutors and enforcement officials are part of the government. Moreover, its goal of the "internalization" of enforcement that produced compliance is achieving comprehensive legal compliance in organizations, which demands that compliance officers have legal

expertise. Yet, if one considers how other professions achieved their professional status, practitioners in the incipient profession had to take the lead to lobby government officials to grant them the monopoly of control over their occupation. In other words, the government will only be reactive to a movement for the professionalization of compliance, which will emerge from outside it.

The professional outcome for compliance thus remains uncertain, even if many of the signs point to its remaining within the sphere of influence of the legal profession. Compliance is a relatively new occupation, with about 25 years of sustained activity, that is "growing up" in a time of significant technological and organizational transformation. It should be no surprise then that its professional status and identity remain undefined and unclear. Moreover, as it becomes widespread in countries outside the USA, which often have a less powerful legal profession, it may offer models of compliance that are not as "law centric" as the US one (Parker et al. 2009) and that may support another professional identity for compliance. The story of compliance's professional journey has not yet reached its end.

## 7 Conclusion

This chapter examined the professional status of compliance in the USA. Section 2 first discussed the origins of compliance as a response to organizational liability and its triumph as an internal control function that has become an accepted and necessary part of organizations. Section 3 then turned to an explanation of compliance practitioners' attainment of features of professional status, chiefly the development of a body of compliance knowledge and skills, the acceptance of compliance as a course of study in universities and other institutions of higher learning, and the consciousness by these practitioners of engaging in a common occupation. It observed, however, that a necessary feature of professional status is still absent: that the government grants compliance practitioners monopoly of and control over their occupation. Section 4 discussed three important negative consequences of compliance's incomplete professionalism: (i) compliance officer liability arising from the failure of regulators to consider the officer as a professional advisor to executives; (ii) the lack of the kind of employment protection typically given to professionals for compliance officers when they report misconduct in the organization; and (iii) the uncertain organizational position of the CCO and the compliance department, which position is subject to organization preference.

Section 5 next explored the reasons for the uncertain or incomplete professional position of compliance. It identified as the primary reason the ambivalent relationship that compliance has with the legal profession, which historically controlled compliance and at times assumes authority over it but at other times does not influence the practice of compliance. It discussed possible explanations for this ambivalence, including that the law allows compliance to operate as a subsidiary technical occupation under its oversight. The chapter also highlighted other reasons for compliance's incomplete professionalism, including that the government considers compliance officers to serve better the government's purposes if they are not in a strong profession and that other disciplines contest law's influence over compliance.

Finally, Sect. 6 speculated on the outcome of compliance's professional quest. It explained why the legal profession is likely to exert continuing influence over compliance, which would lead the latter to remain a satellite occupation, given the legalization of compliance in regulated areas and the overall influence of prosecutors and enforcement officials on organizational compliance. It discussed why the government or other disciplines will or cannot likely counter the law's influence on compliance. It also emphasized that compliance practitioners must themselves be the ones pushing for professional status. It concluded by observing that compliance practice outside the USA may offer professional alternatives to the legally influenced US perspective.

The debate about compliance's professional status is likely to continue because compliance is an important organizational function and because it is a relatively new occupation. Compliance is attracting more academic attention throughout the world, as scholars seek to understand it and propose ways to make it more effective, as is evidenced by the international compliance conference that was the inspiration for this book. It is thus likely that, through this intellectual activity, there will be more insight about the outcome of the professionalization of compliance.

## References

The American Law Institute. (Sept 22, 2017). *Principles of the Law: Compliance, Enforcement and Risk Management for Corporations, Nonprofits, and Other Organizations, Preliminary Draft No. 3.*

Bird, R. C., and Park, S. K. (2016). The Domains of Corporate Counsel in an Era of Compliance. *American Business Law Journal, 53*(2), 203–249.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (May 2013). *Internal Control—Integrated Framework: Framework and Appendices.*

DeMott, D. A. (2013). The Crucial but (Potentially) Precarious Position of the Chief Compliance Officer. *Brooklyn Journal of Corporate, Financial & Commercial Law, 8*(1), 56–79.

DeStefano, M. (2013–2014). Creating a Culture of Compliance: Why Departmentalization May Not Be the Answer. *Hastings Business Law Journal, 10,* 71–182.

Fanto, J. A. (2014). Surveillant and Counselor: A Reorientation in Compliance for Broker-Dealers. *Brigham Young University Law Review, 2014*(5), 1121–1184.

Fanto, J. A. (2015). Preparing to Become a Compliance Officer, and the Academy. In David H. Lui and John H. Walsh (Eds.), *Modern Compliance: Best Practices for Securities & Finance* (pp. 755–764). Alphen aan den Rijn, the Netherlands: Wolters Kluwer Financial Services.

Fanto, J. A. (2016). Dashboard Compliance: Benefit, Threat, or Both? *Brooklyn Journal of Corporate, Financial & Commercial Law, 11*(1), 1–24.

Freidson, E. (2001). *Professionalism: The Third Logic.* Chicago: The University of Chicago Press.

Golumbic, C. E. (2017). "The Big Chill": Personal Liability and the Targeting of Financial Sector Compliance Officers. *Hastings Law Journal, 69,* 45–94.

Griffith, S. J. (2016). Corporate Governance in an Era of Compliance. *William & Mary Law Review, 57,* 2075–2140.

Haugh, T. (2017). The Criminalization of Compliance. *Notre Dame Law Review, 92*(3), 1215–1269.

Hess, D. (2016). Ethical Infrastructures and Evidence-Based Corporate Compliance and Ethics Programs: Policy Implications from the Empirical Evidence. *New York University Journal of Law & Business, 12*(2), 318–368.

International Standard. (2014). *Compliance Management Systems—Guidelines, ISO 19600.* Geneva: International Organization for Standardization.

Langevoort, D. C. (2002). The Behavioral Economics of Corporate Compliance with Law. *Columbia Business Law Review, 2002,* 71–118.

LRN. (2015). *The 2015 Ethics and Compliance Effectiveness Report.* https://lrn.com. Accessed 8 October 2018.

Miller, G. P. (2017). *The Law of Governance, Risk Management, and Compliance.* New York: Wolters Kluwer.

Murphy, J. E. (2017). Policies in Conflict: Undermining Corporate Self-Policing. *Rutgers University Law Review, 62,* 421–496.

National Center for Preventive Law. (1996). *Corporate Compliance Principles.*

National Society of Compliance Professionals. (2018). https://nscp.org. Accessed 8 October 2018.

Parker, C., and Nielsen, V. L. (2011). Introduction: From Regulation to Compliance. In C. Parker and V. L. Nielsen (Eds.), *Explaining Compliance: Business Responses to Regulation* (pp. 1–33). Cheltenham, UK: Edward Elgar.

Parker, C. E., Rosen, R. E., and Nielsen, V. L. (2009). The Two Faces of Lawyers: Professional Ethics and Business Compliance with Regulation. *Georgetown Journal of Legal Ethics, 22,* 201–248.

Remus, D. A. (2014). Out of Practice: The Twenty-First-Century Legal Profession. *Duke Law Journal, 63,* 1243–1286.

Rosen, R. E. (1989). The Inside Counsel Movement, Professional Judgement and Organizational Representation. *Indiana Law Journal, 64,* 479–553.

Rostain, T. (2006). The Emergence of "Law Consultants." *Fordham Law Review, 75,* 1397–1428.

Rostain, T. (2008). General Counsel in the Age of Compliance: Preliminary Findings and New Research Questions. *Georgetown Journal of Legal Ethics, 21,* 465–490.

Society of Corporate Compliance and Ethics. (2018). https://www.corporatecompliance.org. Accessed 8 October 2018.

Sullivan v. Harnisch. (2012). 969 North Eastern Reporter 2d Series, 758–765.

Tenbrunsel, A. E., Smith-Crowe, K., and Umphress, E. E. (2003). Building Houses on Rocks: The Role of the Ethical Infrastructure in Organizations. *Social Justice Research, 16*(3), 285–307.

Urban, T. (2015). Avoiding Supervisory Liability. In David H. Lui and John H. Walsh (Eds.), *Modern Compliance: Best Practices for Securities & Finance* (pp. 703–732). Alphen aan den Rijn, the Netherlands: Wolters Kluwer Financial Services.

U.S. Department of Justice, Criminal Division, Fraud Section. (2017). *Evaluation of Corporate Compliance Programs.* https://www.justice.gov/criminal-fraud/page/file/937501/download. Accessed 8 October 2018.

U.S. Sentencing Commission. (Nov 2016). *Guidelines Manual.* https://www.ussc.gov. Accessed 8 October 2018.

Walsh, J. H. (2015). Compliance as a Profession. In David H. Lui and John H. Walsh (Eds.), *Modern Compliance: Best Practices for Securities & Finance* (pp. 765–795). Alphen aan den Rijn, the Netherlands: Wolters Kluwer Financial Services.

Weaver, G. R., and Trevino, L. K. (1999). Compliance and Values Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior. *Business Ethics Quarterly, 9*(2), 315–335.

**James A. Fanto (JD, PhD)** is the Gerald Baylin Professor of Law at Brooklyn Law School and Co-Director of the school's Center for the Study of Business Law & Regulation. He teaches courses on banking, compliance, corporate, and

securities law, and corporate finance. He writes and speaks on, among other things, the law relating to corporate boards, broker-dealer law and compliance, and compliance. He is the author of Directors' and Officers' Liability (2005) and Corporate Governance in French and American Law (1997), and is the co-author (with Professors Jill Gross and Norman Poser) of Broker-Dealer Law and Regulation (5th ed., 2019, annually updated). He is an editor of an electronic journal in the Social Science Research Network, Corporate and Financial Law: Interdisciplinary Approaches, and a co-editor in chief of Practical Compliance & Risk Management for the Securities Industry. He is also an Associate Reporter for the American Law Institute's project on Principles of the Law, Compliance, Enforcement, and Risk Management. Before becoming a law professor, he practiced banking, corporate and securities law with the firm of Davis Polk & Wardwell in Washington, Paris and New York. Professor Fanto received his B.A. from the University of Notre Dame, his M.A. and Ph.D. from the University of Michigan and J.D. from the University of Pennsylvania. He was a law clerk to Judge Louis H. Pollak of the United States District Court for the Eastern District of Pennsylvania and to Justice Harry A. Blackmun of the United States Supreme Court.

CHAPTER 4

# Compliance: From Soft Law to Hard Law—A View from France

*Maria Lancri*

## 1 Soft Compliance

According to US Legal (2018), it can prove difficult to define what soft law is. It is suggested that soft law is defined as "rules that are neither strictly binding in nature nor completely lacking legal significance but do have in common that they are directed at and have as effect that they influence the conduct of undertakings and individuals, however without containing rights and obligations." In a report a few years ago on Corporate Social Responsibility ("CSR") soft law, writers (Croquet et al. 2009, p. 2) praised soft law as being more tailored to the needs of a company and thereby more efficient by noting that "it is often said that the importance of CSR soft law developments lies in how they influence, rather than control, the behavior of corporations. It is in this way that soft law is distinguished from more traditional domestic legislative instruments or hard law, such as Acts and statutes, which are legally binding on corporations. Within this 'soft touch' approach is the promise of a more tailored and efficient route to ensuring corporate respect for human rights."

M. Lancri (✉)
GGV Grützmacher Gravert Viegener, Paris, France
e-mail: lancri@gg-v.net



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_4

### *Non-legally Binding Instruments*

Lawyers are involved in soft law as they have always valued what soft power can bring rather than waiting for a never satisfying law. Hence, different soft law tools can be used at the international level: international conventions or non-binding interstate agreements. For instance, the 2015 Paris Agreement on Climate change (United Nations 2015) was adopted during the Conference of the Parties (COP 21) and it aims to strengthen the global response to the threat of climate change. It is mostly non-binding for the States; actually, one recalls how the signature was almost derailed at the last minute when the word "shall" was mentioned instead of a "should" in one of the provisions detailing the commitments of the states to continue emission reductions (Vidal 2015). At the same time, when the USA decided to leave the agreement, it was seen as a strong setback against the capacities of the other signatories to get it enforced. One year later, analysts have not seen any impact of this decision in the USA while all nations have maintained in the agreement (*Washington Post* 2018).

Another example which is of interest to companies is the United Nations (2018a) Global Compact. It is noted in their Web site that "is a voluntary initiative based on CEO commitments to implement universal sustainability principles and to take steps to support UN goals." Yet, around 13,000 entities are now participating and publishing annually their efforts to conform to the Ten Principles of the UN (2018b) Global Compact on human rights, labor, environment, and anti-corruption.

The signatories publish on the UN (2018a) Global Compact Web site their annual Communication on Progress and use the opportunity to communicate their achievements on their own Web sites. Co-contractors tend to look at Global Compact commitments to evaluate their counterparts; it is then understandable that they take good care in declaring them.

At the level of the European Union, directives and regulations are the legally binding instruments, but the European bodies may use other tools: opinions, recommendations, or interpretative communications or guidelines. These non-binding instruments are particularly important in a currently rapidly evolving field of compliance such as data protection.

Until May 25, 2018, the main document regulating the matter was the Directive 95/46 (European Parliament and Council 1995). It set up the Working Party of Article 29 ("WP29"), composed of supervisory

authorities' representatives of each member state. It was making recommendations on matters of personal data in the EU. On this basis, it issued several opinions and guidelines which were of its own view. It also issued guidelines to interpret the new regulation, on the Guidelines of Data Protection Regulation (GDPR) (European Parliament and Council 2016) which was fully adopted by May 25, 2018. Now, under the GDPR, this task of ensuring consistent application of data protection rules throughout the EU and providing general guidance has been taken over by the European Data Protection Board ("EDPB").

Safety of products provides the same types of examples. For instance, to interpret the directive on safety of toys, several documents are issued by the European Commission. For instance, Guidance Document No. 4 (European Commission 2009, p. 1) states clearly that it is non-binding, "this Guidance document is a non-binding document intended to provide guidelines to help Member States and stakeholders to decide whether or not different kinds of products are covered by the Toy Safety Directive 2009/48/EC." Yet, companies tend to abide by those guidance documents because they are the most detailed documentation to assist in the understanding, if not completely, of the matter and, also, because if any controls are conducted by the authorities, they expect to see how companies implement the European regulation in view of these guidelines.

It can be seen that although none of these documents are binding, they are an essential part of the whole spectrum as they are the texts that give the most details on how a field of law should be understood. In technical matters, laws cannot provide sufficient details or cannot be updated rapidly enough. Those guidelines are therefore a good compromise because they help both the authorities who provide details on how they may intervene and they give companies sufficient detail to get organized, for instance, to proceed to the collection of personal data or to determine a process of manufacturing. Soft law also allows exchanges with the authorities as they often organize consultations to release new guidance documents or adapt existing ones. It is probably clear by now that the authorities are also becoming experts in using soft law. This is evident at the level of companies or federations of companies, guidelines, policy declarations, or codes of conduct are adopted, either directly by companies as a self-regulation or because regulations themselves tend to favor regulation of the sector through professional guidelines.

Codes of conduct prepared by trade associations or professional bodies (International Ethics Standards Board of Accountants [IESBA] 2018) can also be suggested by law. Such codes of conduct are assisting the professional associations and their members to implement high-quality ethics standards when serving their clients with public interest safeguarded. In fact, the IESBA's long-term objective is convergence of the Code's ethical standards for professional accountants, with those issued by regulators and national standard setters because by doing so the quality and consistency of services provided by professional accountants throughout the world and can improve and enhance the efficiency of global capital markets.

On a different note, the much talked about GDPR (European Parliament and Council 2016) in its Article 40(1) states that, "the Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises." Thus, the European Parliament through its Guidelines is recommending the use of soft law to enhance the implementation of the particular regulation.

National Data Protection authorities, such as the Information Commissioner's Office ("ICO") in the UK, favor the adoption of such codes of conduct by trade associations, also because these codes can provide for the implementation of an independent monitoring body. The data protection authorities see an advantage to internal regulation: Although the code has to be approved by the authority, the code is prepared by pairs and therefore should suit the needs of the sector more easily and for that same reason; they are more likely to be accepted by companies or professionals. On its Web site, the ICO insists on the advantages for a company to adhere to a code of conduct, which, inter alia, allows to follow data protection requirements, it helps to be more transparent and accountable on these issues, it gives a competitive advantage as one can advertise their participation, or it improves standards by establishing best practice. On a Brexit standpoint, it is important to see that the ICO is fully implementing the GDPR, no matter what. They are taking steps to ensure that "UK data protection continues to be recognized as a globally leading standard" (Information Commissioner's Office 2017, p. 6) and for that in their strategic plan, they identified collaboration as a priority, by stating that "we will collaborate with the

international business community and other stakeholders to support work to turn the GDPR's accountability principles into a robust but flexible global solution. We will continue to take part in international work to promote global data protection standards and the long-term aim of a global data protection and privacy agreement or treaty." Furthermore, the ICO decided to also continue to engage with leading international privacy networks. Here again, what cannot be achieved by law can be reached by negotiation and soft law.

The reaction from US companies following the entry into force of the GDPR is also interesting. It is expected some companies will try to limit its implementation to the pure scope of the EU regulation while others will move decisively on implementing GDPR and see the entire process as a journey rather than a destination (Silber 2018). Others, however (Clark 2018), noted that some of the world's biggest tech and telecoms companies have come out in favor of Federal US data protection legislation but have warned against bringing in a "burdensome" GDPR-style law and giving the Federal Trade Commission more powers. Interestingly, according to Serrato et al. (2018) several US states (Alabama, Arizona, Colorado, Iowa, Luisiana, Nebraska, Oregon, South Carolina, South Dakota, Vermont, Virginia) have recently introduced and passed legislation to expand data breach notification rules and to mirror some of the protections provided by Europe's newly-enacted "GDPR". In fact, California's recently enacted California Consumer Privacy Act of 2018 is similar to the EU's GDPR (Patrizio 2018). However, this outcome was not favorably accepted by Tech giants who are calling for Federal Regulation in an effort to subvert California's GDPR-style laws (GDPR Report 2018). As this book goes to print, it is worth noting that on September 26, 2018, the Senate Committee on Commerce, Science, and Transportation held a hearing on data privacy, focusing in part on the potential for federal privacy regulation. The discussion centered on two issues: (1) the potential for Congress to pass a federal privacy law, including the scope and model for any such law and (2) the role of the Federal Trade Commission ("FTC") in regulating data privacy practices (Inside Privacy 2018). Representatives from Apple, Amazon, AT&T, Charter Communications, Google, and Twitter testified.

Furthermore, it is worth noting that the recently adopted USA-Mexico-Canada Agreement (Office of the United States Trade Representative [2018]) introduced in Chapter 19, Article 19.8(3) the

processing principles of the GDPR by noting that "the Parties recognize that these key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented." Companies tend to adopt their own codes of conduct and to use them as an instrument of communication on their values. For instance, certain companies decide to communicate to the Business and Human Rights Resource Centre their policy on human rights. A company like Adidas provided detailed answers to the Centre on their internal policies and on the supply chain due diligence processes they apply (Adidas Group 2016).

It is evident therefore from the above discussion that soft law can influence legal systems and vice versa. Furthermore, soft law may have emerged in the last decades because of the change of paradigm, since companies are not viewed any more as having to be solely efficient and earning money, but all the stakeholders believe in companies that carry a message, have values, either environmental or to fight against corruption.

As a matter of fact, companies are now communicating on these issues, using all the tools provided by new technologies, in particular their Web site. When anyone needs to make a first appraisal of the commitments and values of a company, they should first refer to the corporate Web site of a company where official corporate documentation is accessible but, also, where companies decide on their achievements of plans of actions.

## 2 The Role of the NGOs

The evolution of the role of companies can be seen in context with Non-Governmental Organizations (NGOs). For instance, a company may decide to communicate on its commitment to CSR law while another may opt to detail its actual achievements on improving CSR issues and to publish reports they have conducted themselves or with the help of consultants or even NGOs, as the values exposed in these reports matter both to the company and to its stakeholders. NGOs are often talked about because they aim at revealing, together with journalists, bad behaviors from companies or even suspected violation of the laws.

This practice of revealing such information may on the one hand act as a deterrent for companies, and on the other it may prompt them to be more transparent.

For instance, several NGOs (i.e., Publish What you Pay, One, Oxfam, and Sherpa) have published a report (Alliot et al. 2017) on transparency in the extractive industries where they analyze what is being paid to governments by the companies of this industry. Their conclusions aim at influencing changes in the law, whether at the European level or the French law. Cognizant of the value of their work and of its dissemination, the NGOs understand that their "recommendations" would be more powerful if these were transformed into actual law.

Another example of NGOs participating in petitions to encourage companies to improve their processes is the work of Amnesty International. In fact, Amnesty International UK (2018) published a petition to ask Microsoft to conduct a thorough investigation of their supply chain in cobalt, considering the violations of human rights that have been witnessed mainly in Democratic Republic of Congo.

NGOs also work in assisting companies in their conformity programs, because some of them have become quite specialized in investigating certain issues and also to ensure impartiality of the results. For instance, as cocoa is one of the most important ingredients used in so many of Nestlé products, Nestlé believes that the way their sourcing of cocoa is organized is strongly linked to both their business success and their impact on society. As a consequence, Nestlé has been working on child labor issues in growing cocoa, with the help of the International Cocoa Initiative ("ICI"), which is a non-profit organization that promotes child protection in cocoa-growing communities. Nestlé produced a report in 2017 where it declares that "child labor has no place in [their] supply chain" (p. 9) and they aim to "improve the lives of cocoa farmers and the quality of their products. This includes tackling child labor. With ICI, [they] have introduced a Child Labor Monitoring and Remediation System to help address this complex issue" (Nestle Cocoa Plan 2017, p. 21).

As illustrated above, NGOs are strongly lobbying to improve and enhance the legal system and raise awareness on compliance issues, rather than only encourage CSR initiatives. This is further illustrated with the encouragement of the NGO "Sherpa" to the French legislator to propose a law on corporate impunity. As illustrated (see Peychaud 2016), a number of EU member States (e.g., Austria, France, Germany, Italy) are in the process or have already enacted legislation in an effort to

recognize human rights, or issuing a human trafficking statement, or imposing administrative liability against a legal person for the offense of foreign bribery, an initiative prompted by Danielle Auroi, a member of the French Parliament (European Coalition for Corporate Justice 2016). As Peychaud (2016, p. 7) notes, eight European Parliaments back in 2016 launched a "Green Card" initiative in "order to ask the European Commission to legislate on a duty of care for European Companies." Following a four year "legislative marathon", France has legislated on the duty of care requirements for multinationals, in an effort to "strengthen the responsibility of parent companies for their subcontractors, particularly in the developing world" (Barbiére 2017, p. 1).

On another note, in an effort to combat corporate capture and enhance transparency in lobbying of multinationals toward the politicians, legislatures etc. the European Union has implemented the Transparency Register, a move encouraged by Transparency International for a number of years. As Nesterovych (2015, p. 103) notes, implementing the Register had come across difficult consultations between the European Commission and lobbyist. In fact, in order to be able to conduct any lobbying activities with the European institutions, any entity falling within the scope has to appear on the Transparency Register. This Register was set up to ensure "balanced representation and avoid undue pressure and illegitimate or privileged access to information or to decision-makers" (Europa 2018). The Transparency Register is maintained in an effort for the lobbyist and lobbied to enhance transparency by answering questions such as what interests are being pursued, by whom and with what budgets. Furthermore, the Register displays as of October 2018, the list of meetings registrants had with Commissioners and their closest advisors. Some organizations listed in the Register are Transparency International, Amnesty International European Association, and British Institute of International and Comparative Law.

How lobbying is regulated across Europe varies as some member states (Austria, France, Poland, Slovenia) have enacted legislation while others (Belgium, Denmark, Greece, Estonia, Cyprus etc.) have no legislation, code of conduct, or register of lobbyists (European Parliament 2016). Krambia-Kapardis and Neophytidou (2017, p. 99) have argued that the enhancement of transparency in lobbying is not achieved only through legislative measures but through implementation of legislative footprint, minimizing the practice of revolving doors, and robust "codes of conduct for elected and appointed officials".

## 3 When Soft Law Prompts Hard Law

Often NGOs may be successful in encouraging companies and professional associations to issue codes of conduct or enact relevant legislative measures to combat corruption as can be seen by the accomplishments of Transparency Cyprus (see Krambia-Kapardis 2013) in prompting the Cypriot government and legislatures to enact legislative and other measures to combat corruption.

As already noted, codes of conduct are not stand-alone documents; they need to be implemented by the company if they want them to have an actual impact. The first stage is generally for companies to recommend to their business partners to follow the same principles. The second one is to make the codes of conduct a prerequisite to business negotiations and/or a part of the contractual documentation. Obviously, this second stage is more easily implemented by companies with a bargaining power.

Furthermore, the companies who started to request the application of codes of conduct to their business partners are the ones who are at the end of the supply chain and which are the most visible and, perhaps, the most vulnerable because they are selling to the end-customer. To apply codes of conduct to business partners enhances the protection of the image, brand, and reputation of a company, especially when the company is active in exposed or high-risk business fields.

Oil and gas are considered as being one of the most exposed to corruption and conflicts of interest due to the fact that the natural resources are often from developing countries (see OECD 2016). Often, revenues are not publically available and payments may even be made to governments or government officials to obtain authorization or be granted access to exploit resources. More specifically, Osborne (2018) noted that big names in Houston's energy world, "suddenly were having to explain how they came to win drilling rights and contracts worth billions of dollars in countries such as Nigeria, Angola and Brazil," and this was not an isolated incident as there were cases in Europe, Australia etc.

In an interesting move, Petroleos Mexicanos ("Pemex"), the Mexican state-owned company, recently published its new contractual general conditions whereby it requires from its co-contractors to have implemented compliance programs. This obligation applies to any supplier or subcontractor. They are required to know and to

adopt Pemex compliance program. Whenever co-contractors, subcontractors, or suppliers do not have their own compliance program, they have to implement Pemex program until they can implement their own (Petroleos Mexicanos 2018, see Article 43). This move was required by law to render Pemex contractual system public and transparent (Pemex 2018). This example illustrates that soft and hard law can be interconnected and one can encourage the implementation of the other.

A company which has consistently developed its sustainability requirements over the years is 3M. They not only distribute the "3M Supplier Responsibility Code" which outlines 3M's basic expectations for their supplies 3M Supplier Direct (2018), but they request that their co-contractors apply the same obligations to their subcontractors and monitor their level of compliance. These controls can lead up to termination in case the supplier does not implement corrections to its compliance plan.

It is evident that there is a move away from soft law. When it comes to the anti-corruption compliance program for instance, this last requirement is actually frequently a requirement of the authorities as it is considered that if a company remains in a business relationship although they know their contractor is not sufficiently diligent it may mean that they are not applying seriously enough the principle of zero tolerance. When public opinion is ready, codes of conduct or recommendations may become law.

It is interesting to see the path followed at the EU level on CSR and how soft and hard law are now intrinsically linked. The European Commission (2001) moved from promoting the green paper whose objective was to invite all stakeholders (international organizations, NGOs, and companies) to express their views on the development of a new framework for the promotion of CSR, to a resolution of the European Parliament (2013) based on all the documentation issued in between both by the Commission and the Parliament. However, the resolution lacked any binding authority for it and stressed that CSR should remain primarily a voluntary policy, leaving room to regulatory measures whenever appropriate. It is on this basis that a directive was adopted in 2014 (European Parliament 2014) to render mandatory publication of certain non-financial information by large undertakings. This text has now transposed into laws by member states, and in France, companies are starting in 2018 to publish their reports.

## 4 The Transition to Hard Law

Corruption offenses have been detailed in the criminal code for a number of years. More specifically, France applies a different provision to other Member Stated on whether the corruption is active or passive or if it concerns private or public persons or concerns a relationship between two and three persons or if it is "influence peddling."

However, in its two latest reports on the implementation of the Anti-Bribery Convention, OECD (2011) strongly criticized the French anti-corruption framework for its lack of efficacy in combating corruption of foreign public officials. A first step toward a meaningful reform was made with the law on the 6th of December 2013 (Legifrance 2013) which increased significantly the sanctions for corruption offenses. In its Phase 3 report, OECD (2014) deemed the measure insufficient. In particular, the OECD pointed not to the system of law but to the fact that an insufficient number of cases pursued and to the requirement under French law for a certain number of obstacles to legal actions, such as the requirement of reciprocity of criminalization contained in Articles 113–6 of the *Code penal*. Actually, when one studies the cases carefully, they see that considering how difficult corruption is to demonstrate in Court, oftentimes, people are convicted on the basis of other offenses such as misappropriation of corporate assets.

In any event, it is in this context that the previous French government introduced the text of the Sapin II Law (Law on Transparency in an effort to Fight against Corruption and for the Modernization of Economic Life) (the "Law") in an effort to update the French law to bring it in line with international standards and to increase its credibility in the fight against corruption. These initiatives open up the gateway for French businesses to be prosecuted abroad and to invoke the principle of *non bis in idem* (i.e., not punishing twice for the same crime) with reasonable chances of success.

What is original in the Law (Legifrance 2016) is that it introduces the French Deferred prosecution agreement, the *convention judiciaire d'intérêt public*. It is an innovation for France where it is traditionally considered that the judicial authority should not settle on criminal law issues. On the basis of this provision, the case of the settlement with the French bank, Société Générale is interesting both because it applies the *convention judiciaire d'intérêt public* mechanism in a major corruption case and because it is the first time ever the US Department of Justice

(Ministére De La Justice 2018) has agreed to split half and half an award of 500 million USD with a French authority. However, what is truly original in the French law is that it is one of the first times that a law describes what a compliance program should be made of. Generally, such information appears only in guidelines. In fact, Article 17 of the Sapin II law states that companies in the scope have to implement "measures and procedures" that form a compliance program very similar to what is already stated in other systems of law.

As Whisler et al. (2016) have noted, this Law came about due to international pressure against the French government for its perceived laissez-faire enforcement toward corruption and in an effort to respond to separate sanctions imposed by the US Department of Justice. Whisler et al. (2016) go on to note that the Law has been nicknamed "Sapin II" after the French Minister of Finance, Michel Sapin. The law provides for the setting up of the new French anti-corruption agency ("AFA" in French) which, among others, has the mission to make recommendations to enhance public and private bodies to prevent and detect corruption (recommendations adapted to the size of the entities and the nature of the risks identified).

The Sapin II law came up with 8 steps: (a) the code of conduct, (b) the whistleblowing scheme, (c) the risk mapping, (d) the evaluation of third parties, (e) accounting controls procedures, (f) a training program, (g) disciplinary measures, and (h) internal audit and evaluation mechanism. It is also worth noting that this law applies to French companies or French groups of foreign companies and to their subsidiaries either in France or abroad, companies or group of companies with a turnover of 100 million Euros and 500 employees at least. The recommendations or guidelines, also available in English, were issued (Agence Française Anticorruption [AFA] 2017) in an effort to reflect the highest international standards on the subject. They do echo the same issues as the ones expressed by other bodies (e.g., the US Department of Justice, Criminal Division, Fraud Section 2017), the UKBA Guidance or the World Bank Group (2017). Thus, they provide the same principles and obligations with a difference in the wording: In the French system of law, obligations are often more detailed as French people believe that if something is not stated it does not apply.

*The eight steps set out by Sapin II are:*

Firstly, the code of conduct should define and detail the different types of behaviors that are forbidden, because they may be qualified as

corruption or influence-peddling acts. Note that in order to ensure the enforcement of this code, the law also specifies the code should be an annex to the work rules of procedure. As such, it shall be subject to a process of consulting the works council. Secondly, the whistleblowing scheme should aim at gathering information from employees regarding misconduct or situations that are contrary to the company's code of conduct. Thirdly, the risk mapping should take into account the economic sector and geographical zone. The documentation should be regularly updated and should identify, analyze, and prioritize the risk exposure of the company to external solicitations of a corrupt nature. Fourthly, third-parties due diligence should be used to evaluate the situations of clients and first-tier suppliers as well as intermediaries with reference to the risk mapping. To comply with the obligation, corporations may have to collect sensitive personal data on the said third parties. It is going to be necessary that the authorities clearly state what kind of personal information corporations are allowed to retain, maybe through a modification of the Data Protection law. Fifthly, accounting control procedures should aim to ensure that the books, records, and accounts are not used to mask corruption or influence peddling. The controls could be carried out by the company's own accounting and financial oversight services or by an external auditor. Sixthly, a training program with a general application ought to be implement but it should aim at training employees who are exposed most to risks of corruption and influence peddling. Seventh, the disciplinary system implemented ought to enable the sanctioning of company employees in the case of a violation of the company code of conduct and should actually be applied in case of a violation. Finally, the internal audit and evaluation mechanism should aim at controlling the implementation of the rules, which is the very sign of an efficient program.

It is worth noting that despite the fact that the above requirements are expected of certain size companies, the AFA is in fact advising companies that fall outside the scope of Article 17 that in effort to remain in the market and ensure they are not held liable for corruption offenses they should consider implementing a compliance program.

### *The Duty of Care*

Finally, the chapter considers the duty of care obligations applying in France only to large companies (5000 employees), as well as

the obligations set by the law to conduct due diligence on suppliers and clients on CSR issues, thus requesting from their co-contractors (below the threshold of the law) to comply, by contract, with the same obligations.

This duty of care law (Legifrance 2017a) was adopted in France after the Rana Plaza collapsed which killed thousands of workers of garment workshops. It provides for wider obligations than the compliance program as it requires companies to identify (a) the risks and foresee serious attacks against human rights, (b) observe the fundamental liberties of humans including health and security of people, and (c) issues relating to climate change and the environment. Similarly to France, the UK adopted in 2015 the Modern Slavery Act Legislation. Article 54 of this Act requires on companies providing of goods and services, with a realized turnover of £36 million and activity carried out on UK soil, to declare the controls carried out on their supply chain. California, too, had already adopted a similar text to limit supply chains (see Senate Bill No. 657 Chapter 556).

The French Law provides for the adoption of a compliance program entitled "plan de vigilance," designed to "identify the risks and to foresee serious attacks against human rights and fundamental liberties, health and security of people, as well as of the environment." This identification is as important as regards the activities of companies subjected to the obligation as it is to those which the company controls, directly or indirectly, as well as to activities of subcontractors or suppliers with which a commercial relationship is established. This duty of care plan, which is intended to be prepared with the stakeholders of the company, must comprise several measures among which a risk assessment and evaluation procedures of subcontractors and supplies. Contrary to the French tradition, no authority was set up to follow the implementation of this law or to issue guidelines to help in the determination of efficient duty of care programs.

As stated by the International Labor Organization ("ILO"), the Coordination Committee announced two years following the accident that it had managed to raise $30m and has paid out the awards promised to the 2800 claimants. Following the Rana Plaza incident in Bangladesh, approximately 190 companies have signed the "Accord on Fire and Building Safety in Bangladesh" (Industriall 2018), covering 1600 factories employing a total of 2.5 million workers. Despite the positive outcome of this initiative, some consider that the evolution is slow

and that it is also impeded by what is called the "fast fashion" or the disposable fashion of very cheap products. Potier (2016), the Member of the French Parliament who introduced the Bill on duty of care, now enacted, explained that such laws are needed at EU and international level because they provide a 360° vigilance on human rights, environment, and corruption and strengthen access to justice and remedy for victims by enhancing the chain of causality.

Although the law provides for the legal liability of businesses when there is any failure to comply with the duty of care obligation, it also imposes a responsibility on the businesses to repair the harm caused. In addition, the proper execution of the business's obligations is considered and whether necessary actions were undertaken to avoid unpleasant outcomes and to prevent action being filed by any person with interest in the matter. It also worth noting that the legislation provides for decision taken by the authorities to be made publically available and also judicial procedures can be taken. As with the Rana Plaza, it is most certainly the NGOs and the information network (both journalists and social networks) enhanced transparency and shed light on any violation of the law.

### *Other Fields of Law*

These days, discussions about compliance are often centered on corruption and sanction issues because of high sanctions imposed on companies. However, for people who started compliance with competition law and safety of products, they know that in these fields of law:

- High sanctions have been applied in antitrust cases for many years not only in the USA, but also in the EU and elsewhere;
- The consumption authorities may decide that a product be withdrawn from the market in case of a health and safety hazards of the product for the public.

But more importantly, compliance programs have been implemented in these fields either directly by the entrepreneurs or with the incentive given by the legislator.

For instance, in France, the French competition authority, the *Autorité de la concurrence ("ADLC")*, disclosed a guidance document in 2012 whereby it explains how useful antitrust compliance programs are

as they show that the governance of a company is determined to comply with the law. After having described what an efficient program is like, the ADLC explains that such programs may benefit from a lower sanction, as this is authorized by Article 464-2-III of the French *code de commerce (Legifrance* 2017b*)*. However, the ADLC, in the same document, recalls that the mere fact that a compliance program should not be considered as a mitigating factor when determining the amount of the sanction, when the program did not prevent the violation at stake.

Nowadays, authorities tend to consider compliance as regular business. When soft law becomes binding, it is not an innovation any longer and it does not help. As a matter of fact, the ADLC went even further in 2017 when in a cartel settlement decision they decided that they were not going to take into account the propositions that were made by the undertakings to improve their compliance programs. They went further to consider that

> …the development and implementation of compliance programs are intended to be integrated into the day-to-day management of companies, particularly when those are of significant size. Implementation commitments of such compliance programs are therefore not intended to, in general, to justify a reduction in the penalties incurred for breaches of competition law.

Is that the future for any compliance program? No matter whether it is existing in application of a soft or a hard law, it is now an absolute need for companies, in particular to preserve their reputation. They need to show that they care, and if they fail, they need to show that they took the appropriate measures to limit the consequences.

## 5 Conclusion

Undoubtedly, the experience worldwide has shown that there is a limit to how much human behavior can be regulated by enacted legislation and, as the preceding discussion shows, the usefulness of soft law, both at the international (e.g., conventions, non-binding interstate agreements) and national level (e.g., self-regulation, codes of conduct), cannot be underestimated when addressing the issue of compliance. The United Nations (2018a) Global Compact with its ten principles

is a good example of what can be achieved internationally in getting CEO's to commit to implementing universal sustainability principles. Another such example would be the GDPR adopted by the European Parliament earlier in May 2018. Despite not being binding, the two instruments mentioned have already proved effective in enhancing compliance with their provisions. At the national level, the experience, for example, of the UK's Information Commission Office reiterates the importance of a company's code of conduct in complying with data protection requirements. In addition, there is a dynamic interaction between soft and hard law as soft law can influence legal systems and vice versa.

The prominent role of soft law in the context under consideration can be attributed to the increased role played by NGOs in helping to formulate, implement, and effectively monitor conformity to stipulated principles and procedures. A good example here would be the Transparency Register recommended by Transparency International which has been adopted by the European Union. NGOs, of course, can and have played a crucial role in the introduction of codes of conduct for companies and their partners to combat corruption and other undesirable phenomena such as child labor, as the experience of anti-corruption NGOs in the Republic of Cyprus attests, especially when we have an interaction effect of both hard law and soft law. In considering the utility of soft law in compliance, one should not forget the vital importance of the concept of duty of care. In France, for example, it was adopted in the wake of the Rana Plaza collapse in Bangladesh and it applies to large companies which have to request their co-contractors (suppliers or clients) to comply (by contract) with the same obligations as the company itself.

Finally, drawing on the French experience with anti-corruption legislation, the preceding discussion has documented the transition to hard law in the form of the Sapin II Law (with its eight steps to anti-corruption effectiveness that has mandated compliance programs for companies and the 2016 Law on Transparency that provides for the establishment of a new French Anti-corruption Agency [AFA]). It is comforting to conclude that today compliance programs are an absolute must for companies wishing to preserve their reputation and, thus, profits. The success in establishing compliance on its throne is owed both to the work of NGOs as well as to both hard law and soft law.

## References

Adidas Group. (2016). Adidas Group Response to KnowTheChain. *Apparel & Footwear Benchmark*. https://www.business-humanrights.org/en/adidas-0. Accessed 15 October 2018.

Agence Française Anticorruption. (2017). *Guidelines to Help Private and Public Sector Entities Prevent and Detect Corruption, Influence Peddling, Extortion by Public Officials, Unlawful Taking of Interest, Misappropriation of Public Funds and Favouritism*. https://www.economie.gouv.fr/files/files/directions_services/afa/French_Anticorruption_Agency_Guidelines.pdf. Accessed 15 October 2018.

Alliot, C., Cortin, M., Kurkjian, M., Lemaître, S., Ly, S., and Parrinello, Q. (2017). *Beyond Transparency: Investigating the New Extractive Industry Disclosures, Publish What You Pay*. ONE, OXFAM, Sherpa. https://www.oxfamamerica.org/static/media/files/BeyondTransparency-_Investigating_the_New_Extractive_Industry_Disclousures.pdf. Accessed 15 October 2018.

Amnesty International UK. (2018). *Microsoft Moves on Child Labour Claims*. https://www.amnesty.org.uk/microsoft-moves-child-labour-claims. Accessed 10 October 2018; https://www.amnesty.fr/responsabilite-des-entreprises/petitions/microsoft. Accessed 15 October 2018.

Autorité de la concurrence. (2012). *Document-Cadre Du 10 Février 2012 Sur Les Programmes De Conformité Aux Règles De Concurrence*. http://www.autoritedelaconcurrence.fr/doc/document_cadre_conformite_10_fevrier_2012.pdf. Accessed 1 September 2018.

Barbiére, C. (2017). *France Leads EU on Duty of Care Requirements for Multinationals*. Euractive. https://www.euractiv.com/section/global-europe/news/france-leads-eu-on-duty-of-care-requirements-for-multinationals/. Accessed 15 October 2018.

Clark, S. (2018). *Tech Companies Call For US Federal Data Protection Law*. https://globaldatareview.com/article/1174906/tech-companies-call-for-us-federal-data-protection-law. Accessed 31 October 2018.

Croquet, N., Hammed, A., and Yalkin, T. R. (2009). *Corporate Social Responsibility Soft Law Developments in the European Union*. Oxford Pro Bono Publico. https://www.business-humanrights.org/sites/default/files/reports-and-materials/CSR-soft-law-in-EU-Oxford-Pro-Bono-Publico-for-Ruggie-30-Jul-2009.pdf. Accessed 26 October 2018.

Europa. (2018). *Transparency Regist*er. http://ec.europa.eu/transparencyregister/public/homePage.do?redir=false&locale=en; http://ec.europa.eu/transparencyregister/public/consultation/searchControllerPager.do?declaration=amnestry+international&search=search. Accessed 15 October 2018.

European Coalition for Corporate Justice. (2016). *Members of 8 European Parliaments Support Duty of Care Legislation for EU Corporations*, 31 May

2016. http://corporatejustice.org/news/132-members-of-8-european-parliaments-support-duty-of-care-legislation-for-eu-corporations. Accessed 15 October 2018.

European Commission. (2001). Green Papaer: Promoting a European framework for Corporate Social Responsibility. http://europa.eu/rapid/press-release_DOC-01-9_en.htm. Accessed 25 October 2018.

European Commission. (2009). *Guidance Document No 4 on the Application of Directive 2009/48/EC on the Safety of Toys—Grey Zone Problem: Is a Specific Product Covered by the Toy Safety Directive 2009/48/EC or Not?* http://ec.europa.eu/DocsRoom/documents/13253/attachments/1/translations. Accessed 10 October 2018.

European Parliament. (2013). *Corporate Social Responsibility: Accountable, Transparent and Responsible Business Behaviour and Sustainable Growth.* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0049+0+DOC+XML+V0//EN. Accessed 5 October 2018.

European Parliament. (2016). *Regulation of Lobbying Across the EU.* http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/595830/EPRS_ATA(2016)595830_EN.pdf. Accessed 31 October 2018.

European Parliament and of the Council. (1995). Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. *Official Journal L* 281, 23/11/1995 P. 0031 – 0050. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=FR. Accessed 15 October 2018.

European Parliament and of the Council. (2014). *Amending Directive 2013/34/EU as Regards Disclosure of Non-financial and Diversity Information by Certain Large Undertakings and Groups.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0095&from=FR. Accessed 15 October 2018.

European Parliament and of the Council. (2016). *Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR. Accessed 15 October 2018.

GDPR Report. (2018). *Tech Giants Call for National Data Regulations That Subvert California's GDPR-Style Laws.* https://gdpr.report/news/2018/10/01/tech-giants-call-for-national-data-regulations-that-subvert-californias-gdpr-style-laws/. Accessed 31 October 2018.

Industriall. (2018). *Signatories to the 2018 Accord.* http://www.industriall-union.org/signatories-to-the-2018-accord. Accessed 15 October 2018.

Information Commissioner's Office. (2017). *International Strategy 2017–2021*. https://ico.org.uk/media/about-the-ico/documents/2014356/international-strategy-03.pdf. Accessed 15 October 2018.

Information Commissioner's Office (ICO). (2018). *Codes of Conduct*. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/. Accessed 15 October 2018.

Inside Privacy. (2018). *Senate Examines Potential for Federal Data Privacy Legislation*. https://www.insideprivacy.com/uncategorized/senate-examines-potential-for-federal-data-privacy-legislation/. Accessed 31 October 2018.

International Cocoa Initiative. (2017). *Putting Children First 2017 Annual Report*. https://annualreport2017.cocoainitiative.org/. Accessed 15 October 2018.

International Ethics Standards Board of Accountants. (2018). *Handbook of the International Code of Ethics for Professional Accountants*. https://www.icpac.org.cy/selk/en/ethicscode.aspx. Accessed 31 October 2018.

International Labor Organization. (2015). *Rana Plaza Victims' Compensation Scheme Secures Funds Needed to Make Final Payments*. http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_374239/lang--en/index.htm. Accessed 5 October 2018.

Krambia-Kapardis, M. (2013). *Anti-corruption Measures in Cyprus*. http://cyprusintegrityforum.org/wp-content/uploads/2013/04/TIC_Suggestions_Anticorruption-Measures_english_March-13.pdf. Accessed 31 October 2018.

Krambia-Kapardis, M., and Neophytidou, C. (2017). Lobbying in Cyprus. In A. Bitonti and P. Harris (Eds.), *Lobbying in Europe* (pp. 89–102). Chester, UK: Palgrave Macmillan.

Legifrance. (2013). *Loi n° 2013-1117, 6 déc. 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière: JO 7 déc. 2013, p. 19941, Dispositions Renforçant La Poursuite Et La Répression Des Infractions En Matière De Délinquance Économique, Financière Et Fiscale*. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028278976. Accessed 15 October 2018.

Legifrance. (2016). *OI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (1) De La Lutte Contre Les Manquements À La Probité*. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528&dateTexte=&categorieLien=id. Accessed 15 October 2018.

Legifrance. (2017a). *OI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (1)*. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034290626&dateTexte=&categorieLien=id. Accessed 15 October 2018.

Legifrance. (2017b). *Article L464-2 Modifié par Ordonnance n°2017-303 du 9 mars 2017 - art. 7.* https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=0FE90B1213A9C2981B500782AD27B373.tplgfr21s_1?idArticle=LEGIARTI000034164359&cidTexte=LEGITEXT000005634379&categorieLien=id&dateTexte. Accessed 15 October 2018.

Ministére De La Justice. (2018). *Convention judiciaire d'intérêt public conclue entre le Procureur de la République financier et la Société Générale SA.* https://www.economie.gouv.fr/files/files/directions_services/afa/24.05.18_-_CJIP.pdf. Accessed 15 October 2018.

Nesterovych, V. (2015). EU Standards for the Regulation of Lobbying. *Prawa Człowieka*, nr 1, 97–107. https://www.academia.edu/37339449/EU_standards_for_the_regulation_of_lobbying. Accessed 15 October 2018.

Nestle Cocoa Plan. (2017). Tackling Child Labour 2017 Report. http://www.nestle.com/asset-library/documents/creating-shared-value/responsible-sourcing/nestle-cocoa-plan-child-labour-2017-report.pdf. Accessed 15 October 2018.

OECD. (2011). *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents.* http://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf. Accessed 15 October 2018.

OECD. (2014). *France: Follow-up to the Phase 3 Report & Recommendations.* https://www.oecd.org/daf/anti-bribery/France-Phase-3-Written-Follow-up-ENG.pdf. Accessed 15 October 2018.

OECD. (2016). *Corruption in the Extractive Value Chain.* http://www.oecd.org/dev/Corruption-in-the-extractive-value-chain.pdf. Accessed 31 October 2018.

Office of the United States Trade Representative. (2018). *United States-Mexico-Canada Trade Agreement.* https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/united-states-mexico; Chapter 19, Digital Trade, Article 19.8(3). https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/19%20Digital%20Trade.pd. Accessed 15 October 2018.

Osborne, J. (2018). Oil Industry Rocked by Global Corruption Scandals. *The Star Business Journal*, 2 February 2018. https://www.thestar.com/business/2018/02/02/oil-industry-rocked-by-global-corruption-scandals.html. Accessed 15 October 2018.

Patrizio, A. (2018). *While No One Was Looking, California Passed Its Own GDPR.* https://www.networkworld.com/article/3286611/data-center/while-no-one-was-looking-california-passed-its-own-gdpr.html. Accessed 31 October 2018.

Pemex. (2018). *Sistema de información pública de proveedores y contratistas.* http://www.pemex.com/procura/relacion-con-proveedores/Paginas/info-proveedores-contratistas.aspx. Accessed 15 October 2018.

Petroleos Mexicanos. (2018). *Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias*, 18 May 2018. http://www.pemex.com/procura/procedimientos-de-contratacion/marco-legal/Documents/DISPOSICIONES%20Generales%20de%20Contratación%20para%20PM%20y%20sus%20EPS%202018_05_18.pdf. Accessed 15 October 2018.

Peychaud, C. (2016). *In the Face of Corporate Impunity, Progress in Europe, Forum Citoyen pour la Responsabilité Sociale des Entreprises*. https://www.asso-sherpa.org/wp-content/uploads/2013/03/Corporate_impunity-progress-in-Europe.pdf. Accessed 15 October 2018.

Potier, D. (2016). *Towards the Adoption of A Duty of Vigilance Law for Transnational Corporations: Putting an End to Modern Slavery*. Presentation 11 May 2016 at "The EU Roadmap to Business and Human Rights Conference" Plenary session: Human Rights Due Diligence: The Role of States, Amsterdam. http://eu-roadmap.nl/background-information/plenary-session-human-rights-due-dilligence-the-role-of-states/. Accessed 15 October 2018.

Serrato, J. K., Cwalina, C., Rudawski, A., Coughlin, T., and Fardelmann, K. (2018). US States Pass Data Protection Laws on the Heels of the GDPR. *Compliance and Risk Management, Regulatory Response*. https://www.data-protectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/. Accessed 26 October 2018.

Silber, T. (2018). *Some Media Companies Moving Decisively on GDPR, Others Not So Much, Forbes 31/3/2018*. https://www.forbes.com/sites/tonysilber/2018/04/03/some-media-companies-moving-decisively-on-gdpr-others-not-so-much/#61f02c955e25. Accessed 31 October 2018.

3M Supplier Direct. (2018). *Global Supplier Responsibility Code*. https://www.3m.co.uk/3M/en_GB/suppliers-direct/supplier-requirements/global-supplier-responsibility-code/. Accessed 15 October 2018.

U.S. Department of Justice, Criminal Division, Fraud Section. (2017). *Evaluation of Corporate Compliance Programs*. https://www.economie.gouv.fr/files/files/directions_services/afa/French_Anticorruption_Agency_Guidelines.pdf. Accessed 15 October 2018.

US Legal. (2018). *Soft Law and Legal Definition*. https://definitions.uslegal.com/s/soft-law. Accessed 26 October 2018.

UKBA Guidance, The Bribery Act. 2010. https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf. Accessed 6 November 2018.

United Nations. (2015). *Paris Agreement*. https://unfccc.int/files/essential_background/convention/application/pdf/english_paris_agreement.pdf. Accessed 10 October 2018.

United Nations. (2018a). *Global Compact*. https://www.unglobalcompact.org/about. Accessed 20 October 2018.

United Nations. (2018b). *Global Compact the Ten Principles of the UN Global Compact*. https://www.unglobalcompact.org/what-is-gc/mission/principle. Accessed 26 October 2018.

Vidal, J. (2015). How A 'Typo' Nearly Derailed the Paris Climate Deal. *The Guardian*, 16 December 2015. https://www.theguardian.com/environment/blog/2015/dec/16/how-a-typo-nearly-derailed-the-paris-climate-deal. Accessed 5 October 2018.

*Washington Post*. (2018). *Trump Withdrew From the Paris Climate Deal a Year Ago*. https://www.washingtonpost.com/news/energy-environment/wp/2018/06/01/trump-withdrew-from-the-paris-climate-plan-a-year-ago-heres-what-has-changed/?noredirect=on&utm_term=.067bdb06633b. Accessed 1 October 2018.

Whisler, B., Norrant-Eyme, J., Lasry, E., and Koski, S. (2016). New French Anti-corruption Law: France Strengthens Its Legislation to Combat Bribery and Corruption and Adopts U.S.-Style Anti-corruption System. *Global Compliance News*, 15 November 2016. https://globalcompliancenews.com/new-french-anti-corruption-law-20161123/. Accessed 15 October 2018.

World Bank Group. (2017). *Integrity Compliance Guidelines*. http://wallensteinlawgroup.com/wp-content/uploads/2017/12/WBG-Integrity-Compliance-Guidelines-full.pdf. Accessed 15 October 2018.

### *Legislation*

*Modern Slavery Act*, 2015, UK. http://www.legislation.gov.uk/ukpga/2015/30/pdfs/ukpga_20150030_en.pdf. Accessed 31 October 2018.

Senate Bill No. 657 Chapter 556, The California Transparency in Supply Chains Act, Senate Bill No. 657, Chapter 556. https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersafety/sb_657_bill_ch556.pdf. Accessed 31 October 2018.

**Maria Lancri** is a French lawyer practicing as a Counsel with GGV Avocats à la Cour—Rechtsanwälte since 2015. She assists and advises international companies in French, English, and Spanish in business law and in compliance matters: data protection, corruption, product safety, distribution, and competition law. She has been involved in the discussion of the new French Sapin II law as part of the team proposed, as a member of the ACE's International Section, amendments to the Parliament on behalf of the ACE. The ACE (Association des avocats conseils d'entreprises) is a prominent French association of business lawyers. These last months she has been advising companies on the implementation of the Sapin II law as well as the obligations of the GDPR. Prior to joining GGV, Maria Lancri was in-house with Hachette Livre (one of the largest publishers in the world), acting as Deputy General Counsel and Compliance Manager.

CHAPTER 5

# Living with the New General Data Protection Regulation (GDPR)

*Mark Foulsham*

## 1 Introduction

This chapter discusses the General Data Protection Regulation (GDPR) (European Parliament 2016) which came into enforcement in May 2018. The chapter addresses the following themes:

a. how businesses have attempted to comply with GDPR; addressing various sectors, countries and methods;
b. how regulators are enforcing the Regulation; specifically in relation to financial penalties;
c. how businesses should ensure compliance that is practical;
d. what does the future hold for data compliance; extrapolating from May 2018 forwards.

Although the following sections relate to GDPR from a global perspective, particular attention has been given to:

M. Foulsham (✉)
CEO and Founder of Keyenable Ltd, London, UK
e-mail: markfoulsham@keyenable.com



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_5

- SMEs (Small and Medium Size) organisations: as these companies form a major part of the global economy and have been more significantly affected by GDPR readiness and compliance due to higher size/resource ratios.
- The European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB) as well as the UK Regulator (the Information Commissioners Office—ICO). The EDPS provided good oversight and encouragement to GDPR and the ICO was one of the most effective national regulators in readying organisations for GDPR; consequently, the UK was the most prepared country globally heading into May 2017.

## 2 Background to the GDPR

Throughout the 1990s and 2000s, as countries developed their data privacy rules, Europe started to coalesce its views around the need for a unified data privacy standard for its citizens. Consequently, a number of European-centric Regulations were introduced to standardise the way that personal data was treated.

As far back as 1995, the European Union (EU) decided to create a single Regulation that would apply to all member states and also to any company or country that wanted to store or process data that belonged to any citizen of the EU. This was memorably entitled "EU Directive 95/46/EC" (European Parliament 1995)—a Data Protection Directive with the primary objective requiring that "…Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data". This was clearly a precursor to the current GDPR. For further historical evolution of EU data protection standards, the EDPS provides a timeline history from 1995 to current day on its website (European Data Protection Supervisor 2018a).

With the launch of GDPR, the old Article 29 Working Party (established by Directive 95/46/EC), whose members were the EU's national supervisory authorities, the "EDPS" and the European Commission, has been transformed into the "European Data Protection Board" ("EDPB"), with similar membership but an independent Secretariat (provided by the EDPS). The EDPB has the status of an EU body with legal presence and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification (Lexicology 2018).

The concept of a "One Stop Shop" for data protection rules meant that the whole EU would present a unified front to the world and produce a set of rules that went beyond protecting data that was being processed by a company and defined what would happen to data as it moved around the world. The EDPB continues to state its ambitions to maintain GDPR as a gold standard globally.

## 3 A High-Level Overview of the GDPR

The GDPR contains 99 Articles followed by 173 Recitals. The Articles state the main requirements of the Regulation and the Recitals provide further clarification and refinement to the intent of the Articles.

The Articles are only likely to change when there is a review of the Regulation; however, the Recitals may be updated and expanded as cases are taken to court; essential providing a proxy to legal precedent until such time as case law is established. Consequently, in referencing GDPR, it is important to check the precise wording of the Regulation in the writing of a contract (or otherwise need a precise understanding of what the Regulation specifically states) (see European Parliament 2016).

The GDPR is more specific than previous incarnations of regulations; for example, putting the onus on the data processor to ensure that they have the correct permissions before they use consented for information. The GDPR applies to "controllers" and "processors"—these definitions are very similar to the standards that it replaces. The new Regulation provides for a person's right to have their data deleted, which is more limited than the earlier "right to be forgotten". As widely reported in the press in 2006, it was not until 2014 that the European Court of Justice recognised this as a human right (BBC News 2014).

GDPR represents considerable challenges to any company that has not prepared. People will have the right to ask for their data in a "common format" to allow them to move their data from one processor to another. While this may seem like a simple data extract, the requirement for the data to be presented in a "common format" will present many companies with technical difficulties while they decide what will be acceptable (something we shall discuss further later in this chapter). Many bespoke database systems will not easily produce a file that meets the requirements of the Regulation.

There are a number of new responsibilities in the Regulation and any company that wants to deal with the personal data of any citizen of the EU must understand what the Regulation requires of them.

As more countries started to recognise, the data protection Acts within Europe as giving their citizens' rights over large multi-national data brokers, so they started to introduce their own laws and interpretations. As the EU expands (or contracts as countries leave) the influence that the GDPR has will also develop.

### *Scope*

The GDPR applies to all personal data, just as previous regulations did but it gives a more detailed definition of what this means, so that, for example, an online identifier, such as an IP address, is deemed personal and identifiable information.

The definition of "sensitive personal data" has also been expanded so that genetic and biometric data (such as a DNA profile or a fingerprint) are included. Personal data relating to criminal convictions are not included but additional safeguards have been put in place.

Article 3 (European Parliament 2016; ICO 2018e) provides the territorial scope of the GDPR (and is far-reaching).

> 1. This Regulation applies to the processing of personal data in the context of activities of an establishment of a controller or a processor in the [European] Union.
>
> 2. …. applies to the processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union, where the processing activities are related to:
> the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the [European] Union; or,
> the monitoring of their behaviour, as far as their behaviour takes place in the European Union.
>
> 3. …. applies to the processing of personal data by a controller not established in the [European] Union, but in a place where the national law of a Member State applies by virtue of international law.

The reach of GDPR has effectively created a global reach for the protection of people's privacy rights.

## 4 How Businesses Have Attempted to Comply with GDPR

### *Approach Through 2016–2018*

As a reminder, on the 14 April 2016, the GDPR was ratified by all 28 countries of the EU and came into force 20 days later. A two-year transition period to give organisations time to comply with the requirements was allowed for.

In the lead up to the initial release of GDPR adoption requirements in May 2016, public and industry awareness was low. Indeed, there was limited publicity from regulators, the EU or news agencies: Data Protection compliance was not newsworthy. The two-year grace period from May 2016 to May 2018 was taken by many to be a period of gradual readiness, with most organisation interpreting the Regulation as another version of the softer requirements that had come before. Those in the compliance and data privacy field had already realised what an impact GDPR would have and were dismayed by the lack of ownership around promoting what would be a major undertaking.

The situation on 2016 was therefore one of idle complacency and sowed the seeds for the struggles company's had in subsequent years to address the complex and far-reaching changes required of them. An earlier engagement and commencing of work would have also meant that the noticeable data breaches that occurred between 2016 and early 2018 may have had a lesser impact on those suffering the consequences. TalkTalk (Decision Marketing 2016) stands out as an example here. Business confidence during this period would often include subjects entitled "What is GDPR and why it matters to you"; they were ill-attended.

Nevertheless, momentum of commitment built through 2017 as realisation seeped into industry and public consciousness and regulators actively geared up their PR engines to promote the need to be ready. Even as the realities and lack of time left became all too apparent, there was a significant number of businesses leaders who believed the Regulation would be delayed. In the UK, the consequence of the 2016 Brexit referendum muddied the waters and provided excuses to prevaricate. In mid-2017 many organisations had not started a GDPR project—or not even come to the conclusion that a project was needed. Lack of understanding meant that preparations were assigned to IT Directors or Heads of Governance rather than establishing company-wide programmes and addressing the Regulation as a Board-related matter.

### *Early 2018*

The period from late 2017 through to early 2018 was one of frenetic activity with Boards, CEOs and Chief Risk Officers (CROs) realising that the Regulation was actually going to be applied. Companies woke up to the realisation that an umbrella Business Project Manager, not technical or function-specific management was needed to be appointed. Debate in the business community centred around two areas in particular: risk mitigation and competitor readiness.

Most organisations began to take a risk-based approach to managing their GDPR projects; not because this was necessarily the best way to tackle their readiness but out of necessity around time constraints. In fact, as discussed later in this chapter, risk-based compliance is a highly effective means to achieve a pragmatic level of compliance. GDPR Project Managers found themselves negotiating with Heads of functions on the best way to deliver a "minimal viable compliance". Again, this is not necessarily an approach which would compromise compliance but the way in which projects were undertaken was often heavy on finding ways to exclude work rather than assessing the best ways to improve processes towards compliance.

A significant amount of focus at the time was also placed on looking across competitor landscapes. Many regulators use frameworks which are geared to identifying outliers from alignment with standards and GDPR was not an exception. No company wanted to be picked off by industry watchdogs as unready or named through the press as ill-prepared. Many seminars and network events at the time included sector-specific huddles debating how best to act as one rather than approach GDPR in a non-collegiate manner. Through 2017 and early 2018 in the UK, the ICO undertook successful sector-specific consultation which helped provide guidance in areas of compliance specifically relating to particular segments of industry.

The combination of a risk-based approach and the weighted guidance from the ICO in the UK was immensely helpful to organisations in setting the scope for their projects on a priority-led basis as May 2018 loomed. The EU and associated regulators, whilst supporting particular sectors were not as proactive and tended to allow consultants to move in this space; arguably this less centrally based approach diluted the effectiveness of readiness across the Union and beyond.

### *25 May 2018 and the Immediate Aftermath*

The deadline for GDPR was not as eventful as anticipated. In fact, the UK regulator was careful to explain to businesses that 25.05.18 was not a "deadline". The ICO Commissioner, Elizabeth Denham (see CBR Government 2018), stated:

> [GDPR is] an evolutionary process for organisations – 25 May is the date the legislation takes effect but no business stands still. You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018.

and at a Data Practitioners Conference (ICO 2018a):

> We want you to feel prepared, equipped and excited about the GDPR. I know many of you do. For those that still feel there is work to be done – and there are many of those too – I want to reassure you that there is no deadline….
>
> In fact, it's important that we all understand there is no deadline. 25 May is not the end. It is the beginning.

This pragmatic support for businesses was replicated through the EU and beyond. This was welcomed by business leaders, given the sizeable challenge to businesses, economic uncertainties being faced by many countries and the limited amount of interpretation.

In the months following May 2018 although there have been a number of data breaches, as yet GDPR has not been "weaponised" by regulators. It is unclear at this stage whether this is because case law has not been established to guide exactly how legal proceeding will be taken, setting the right level of punitive measures to adopt or the need to recognise that the first few non-compliant cases could have a more dramatic effect on company's reputation than perhaps future incidents. All of these and other reasons are interplaying currently and certainly 2019 will be an interesting time in this respect.

In September 2018, ICO Deputy Commissioner for Operations, James Dipple-Johnstone, said during a CBI Cyber Security speech (Cimpanu 2018):

> Unfortunately - or maybe fortunately - we have not issued any fines for breaches of the new regime to be able to share learning about our approach.

He continued by saying the agency is not a revenue-generating organisation, hence, the reason why they never "go for the jugular" when a company has been caught misreporting a security or privacy-related GDPR breach. Also, the intense desire from government agencies to punish companies via the new GDPR legislation is one of the myths that are currently forming around the new GDPR legislation, mainly due to a lack of information on the public's side" (Cimpanu 2018).

This is an interesting comment on a number of fronts. Most noticeably, given the clear intent of GDPR to push organisations to better compliance through where it hurts most—the bottom line—fines are not (yet) being seen as a principle part of the ICO's armoury. The idea that the public's desire to punish organisations financially was forming in September is also questionable. The public outcry from breaches such as Facebook (Keane 2018) Cambridge Analytica (*The Guardian* 2018; Valdez 2018) and British Airways (Bloomberg 2018) demonstrated the increasing concern many had (and indeed still have) over the poor way in which companies take data protection seriously. Cognisant of the fact that the ICO has fined a number of firms (ICO 2018f), it seems for the present that the ICO are using carrots rather than sticks. It is likely that this strategy will not continue for a significant amount of time.

From just one perspective, the amount of cyber-related attacks and fraudulent activity has increased significantly through 2018, as it has done in previous years. The public will only tolerate so many short failings by companies before they demand what benefit the GDPR has. From another perspective, civil action may be the route through which individuals and companies create a greater momentum in the months ahead—which in turn may force the Regulators hand. Either way, the pragmatic approach, may seem to be now a soft approach rather than in the spirit of compelling organisations to address issues.

### *A Project Approach (or Not?)*

Many businesses have taken the approach to achieving compliance through a project-based method. Typically, this has been a "waterfall" approach rather than agile although due to the changing nature of guidance and interpretation, an iterative dynamic approach was often the most useful for certain work streams. Certainly, when a solution has been needed, for example, a website refresh, agile methodologies have been deployed as part of wider programmes of work. In the view of the author, the best approach has been to:

- Treat GDPR compliance as a business-wide initiative with Board-level engagement.
- Govern the programme by appointing a business (not technology) lead; a background in general project management, compliance or law is healthy.
- Divide the programme into work streams, either by GDPR component (such as privacy by design or individual right processing) or business function (such as HR, IT and Legal teams). The most common approach was the latter, which required the programme lead to ensure that cross-functional coordination was effective.
- Engage with (or create) a Data Protection Office (DPO).
- Ensure the Executive Leadership Team (ELT) and Risk Committee of the Board (or equivalent) is kept informed regularly.

Given the degree of transformation programmes being undertaken by businesses currently and the impactive nature of GDPR, many organisations have embedded their GDPR projects squarely within their overall business change portfolios.

As companies have worked to transfer GDPR activities into operational (or Business as Usual, BAU) areas and processes of their organisations, they have found challenges in the running of the Regulation that were not as apparent during the change element of readying for compliance. These challenges are discussed later within the section on how companies are aiming to achieve practical compliance.

The resourcing of projects through 2017–2018 has been challenging as demand far outstripped supply for GDPR specialists. This deficit created a vacuum which was filled with individuals and organisations who overnight became compliance and privacy specialists. Some organisations fell into the trap of appointing anyone who imprecisely matched the job requirements and has since suffered from the realities of a credible GDPR specialist, uncovering poorly executed projects post-peak-demand. It is worth noting that a GDPR programme may have been declared "achieved" only for a BAU team to discover the situation required significant additional budget to remediate.

The wide availability of qualified GDPR practitioners also caused—and continues to cause—confusion. Although the EU is considering accreditation schemes, there is no official GDPR certification currently (Froud 2018). However, alignment with standards including

ISO SO/IEC 17024 (International Organisation for Standardisation 2018) does at least provide a degree of credibility.

In budgeting for GDPR, industry was polarised between those companies who prepared and budgeted early (typically large international companies) and those who either left financial concerns too late or not provided for at all.

Cross-referencing and comparison of approaches was significant during 2017 but reduced through 2018 as organisations "knuckled down". Interestingly, this also appeared to be a factor of business leaders realising that GDPR could also be a competitive differentiator. The need for suppliers and service providers to ensure they were GDPR compliant during prequalification and tendering process has sharpened their general approach to providing information to prospective clients on Information Security provisions, data strategy and historic incidents. In one difficult scenario, the current chapter contributor came across in late 2017, a housing management company removed a potential supplier from its long list after it transpired the supplier had not yet considered GDPR, let alone made provisions towards compliance.

Across vertical markets and sectors, the approach to achieving GDPR has not varied materially. The nuances of each industry are of course important and Regulators such as the ICO have helped guide sectors through working with industry bodies and represent organisations. An example is in the not-for-profit sector in the UK where the ICO engaged strongly with charities to ensure that areas such as consent and vulnerable individuals were accommodated thoroughly (ICO 2018b). The ICO also undertook a survey of eight selected charities in which it found a combination of good practices, but also noticeable improvements needed (ICO 2018c). Worryingly some basic business governance and operational practices which ought to have been in place regardless of GDPR were found to be lacking. A finding on incident reporting concludes:

> Whilst there was mostly good awareness among staff of how to report an incident and who to report it to; most charities visited did not have documented reporting procedures in place. (ICO 2018c, p. 7)

GDPR adoption by country remains too early to firmly track but can be assessed through action taken by national regulators—and the severity of response to breaches. Adoption has been varied and in line with typical approaches nations have had to deploy similar legislative changes.

Germany and the UK have led the way in complying with both the intent and specifics of the Regulation. The USA remains behind on both measures despite the international reach of US organisations and the regular warnings provided through news on large corporate breaches (Facebook in particular). Ironically, it is likely the battle over data rights and setting of international case law may well be fought within the litigious landscape of US industry rather than entirely through European courts.

Interpretation of GDPR by country and within sector is hugely varied and often relies heavily on Article 6 (see European Parliament 2016, par. (47), Legitimate Interests)

> The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Most organisations have assessed the basis for legitimate processing thoroughly but as interpretation could be undermined through a high-profile incident or new case coming to court, the capture and documentation of their particular interpretation has needed to be well noted within the company-specific Governance framework.

As we approach 2019, it is clear that many companies still have "gaps and tails" in their completion of GDPR compliance. Some have declared compliance only to discover through, for example, new contracts their approach was flawed or ineffective. Based on the author's personal experience in working with many companies in this area, as at May 2018, the average length of a GDPR projects tail was 6 months; many have extended this further. There are principally two reasons for this extension. Firstly, work has purely taken longer than expected in the final stages of compliance but more worryingly, as compliance accountable is divested into "BAU" the ability and willingness of business functions to absorb the overhead has come under scrutiny—and caused both a delay and compromise to compliance effectiveness. As an example in September 2018, ITPro (2018), it was reported that the majority of companies around the world are failing to fulfil subject access requests (SARs) in time—contravening one of the most important provisions boosted under GDPR. This is not just a function of a volume increase in SARs; companies should have been ready.

## 5 How Regulators Are Enforcing the Regulation

The European Information regulator is the EDPS and acts as the EU's independent data protection authority. Their stated mission (European Data Processing Supervisor 2018b) is to:

- monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals;
- advise EU institutions and bodies on all matters relating to the processing of personal information. We are consulted by the EU legislator on proposals for legislation and new policy developments that may affect privacy;
- monitor new technology that may affect the protection of personal information;
- intervene before the Court of Justice of the EU to provide expert advice on interpreting data protection law;
- cooperate with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information.

The EDPS has provided authoritative advice on navigating the GDPR and the website is an effective reference to the Regulation details. Surprisingly, searching for the Articles and Recitals is not straightforward and support on their interpretation is thin from the EDPS. In some respect, this is not unusual given that each member state has (or working towards) reflecting its own interpretation. In the UK, this has been legislated through the Data Protection Act 2018 (Government UK 2018) whose stated aims are to:

- make "data protection laws fit for the digital age in which an ever-increasing amount of data is being processed;
- empowers people to take control of their data;
- supports UK businesses and organisations through the change;
- ensures that the UK is prepared for the future after we have left the EU".

Understandably, the aims of the Act are heavy on "readying for the future" given that Brexit is looming on the horizon. The DPA will be a stand-alone piece of legislation post-Brexit. Interpretation of the GDPR in the UK by the ICO has been thorough. This has included:

- sector-specific consultations;
- business conferences presentations;
- working groups with representative organisation;
- publicity campaigns for the general public.

In Germany, only five days after the GDPR became applicable, the Regional Court in Bonn, issued a ruling on the practical application of the GDPR. This was the first GDPR court decision worldwide, and the decision addressed the issue of public availability of ICANN "WHOIS data" (Spittka and Mirzaei 2018). Germany has kept a momentum of action since this time, including notably the intention of its antitrust agency (the Federal Cartel Office) to take enforcement action against Facebook for its data breaches in 2018 (Today NG 2018).

In France, the data regulator, CNIL (Hunton 2018) reported in late September 2018 that it has received over 3767 data protection complaints, showing a "64 percent increase compared to the same period last year. CNIL also reported that it has received 600 data breach notifications during the same period" (Pearce 2018).

Enforcement objectives across the EU appear to be similar with no regulatory body standing out as taking more severe action than other national bodies. Actions (ICO 2018d) have taken against Facebook and those organisations associated with Cambridge Analytica and their misappropriation of 87m users' data. In the UK, the ICO issuing a £500,000 fine with the Commission stating (see Sky News 2018):

> We are at a crossroads. Trust and confidence in the integrity of our democratic processes risk being disrupted because the average voter has little idea of what is going on behind the scenes….New technologies that use data analytics to micro-target people give campaign groups the ability to connect with individual voters. But this cannot be at the expense of transparency, fairness and compliance with the law…. Fines and prosecutions punish the bad actors, but my real goal is to effect change and restore trust and confidence in our democratic system.

This is strong comment but when added to the fact that the £500,000 fine represents just 15 minutes of Facebook profits (Heaphy 2018), the financial penalty seems somewhat low. The reputational damage is, however, likely to have more of an impact on revenues.

Going forward, regulators will need to balance their strength of enforcement against business oversight and public pressure. GDPR has

amplified public awareness on data privacy with each incident receiving front-page headlines, notably Under Amour (Robinson 2018), British Airways (Butterworth 2018), Google (Townsend 2017) and Equifax (Osborne 2018). From a public perspective, people are realising that daily data privacy infringements remain commonplace.

## 6 How Businesses Should Ensure Compliance That Is Practical

### *A Risk-Based Approach*

A risk-based approach has been common among companies and "practical GDPR compliance" has been a phrase deployed to indicate a sensible rather than idealistic approach. However, for practical read "inexpensive". As covered earlier, budgeting for GDPR has been difficult for businesses and as the true extent of effort was realised, practical ways were geared to match effort to both risk (of financial penalties) and value (for example, improved customer centricity). Risk appetite statement has duly been considered by Boards and ELTs as defining the level of compliance that would be palatable—and this means assessing the likelihood of a breach and the impact on brand, the cost base and reputation.

### *Examples of GDPR Challenges and Navigation*

There are a number of examples which highlight how companies are having to navigate the new Regulation—balancing risks and early interpretation—as well as dealing with some unintended consequences of the new rules:

- **Marketers**. The marketing industry, already challenged by new Digital technology, has been hit hard by GDPR. Legitimate business interest has been deployed widely as has the legal right to processing, including data suppression: individual's basic data being removed in order to allow for decisions on content to be upheld. This highlights the dichotomy of how to balance a purist view on the right to be forgotten against a mistake in re-marketing an individual who had not supplied consent information.
- **Affiliates**. A data analytics firm "harvested millions of Facebook profiles and used them to build a powerful software program to predict and influence choices at the ballot box" (Cadwalladr and

Graham-Harrison 2018; Valdez 2018). The Facebook data leak scandal is a perfect example of the reason why we need the GDPR when it comes to protecting data subjects' rights. While steps are being taken in the right direction for the individual, there are impacts on businesses and marketers which should be considered. Anyone who does business in Europe or even tangentially collects data from EU Citizens needs to be aware of the GDPR. It affects all industries from e-commerce to horse breeders. Marketers and advertisers who use affiliate networks also must be aware of the GDPR's impact on their industry. With this sudden shift in privacy laws, affiliate marketers have their own set of questions that they need answered to properly adapt (Bachmann 2018).

- **Recruiters**. The right to be forgotten has limited the ability for organisations (both recruiting companies and clients) to store and reuse information on perspective candidates. This means the pool of knowledge on talent has shrunk. Many recruitment organisations have argued legitimate business interest in their approach to ensuring they do not drain down their databases. A few—and not a large proportion—have gained explicit consent. Client organisations are less able to do this, meaning that resources such as LinkedIn have benefited greatly.

### *Organisations Dealing with Minors*

Another challenge for some companies is Article 8, "Conditions applicable to child's consent in relation to information society services" (European Parliament 2016). Point 1 states:

> … the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

For any child below the age of 13 it will be up to the data controller to:

> make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child taking into account available technology.

Organisations are finding it difficult to navigate through the various requirements (Foulsham and Hitchen 2017) and legislation associated

with protecting vulnerable adults and children. This is a blessing in that it provides extra checks and balances for those in our society who are least able to protect themselves. Conversely, the barriers to a free-flow of supportive data (e.g. to ensure effective social care and services) could mean these individuals are deemed to be "too difficult to engage with" from a data perspective.

*Subscription-Based Organisations and Publishers*

In the UK, The Guardian newspaper provides an example of clear wording when allowing users to delete their account, stating "deleting your account removes personal information from our database. Your email address becomes permanently reserved and the same email address cannot be re-used to register a new account" (Davis 2017).

GDPR required, for example, as part of SRAs, for companies to provide all information to individuals promptly (within one month). Organisations have in many cases moved to a "single customer view" or ensured that a user can see all the information on their account readily. However, as is so common in applying practical compliance, the balance between guarding data and providing transparency continues to be a battlefield.

*Cookies*

The number of 3rd party tracking cookies fell by 22% between April and July 2018 as GDPR came into affect; in the UK this was as high as 45%. Historically, the right to refuse cookies was introduced by the EU in May 2011 and had many similarities associated with the wider privacy intent of GDPR. A user agreement for a site to use cookies continues to be part of our everyday web journeys. However, many organisations with web presence have not moved to an improved, clear, defaulted-on explicit consent acceptance for their site. For many companies then, cookies are part of the post-May 2018 sweep up work.

A variety of residual risks and questions remain with organisations currently, such as:

- Interpretation—has the Regulation been embedded within their organisation in line with the original wording, guidance from regulators and in comparison with competitors' approaches?
- Adaption—with new incidents, cases and punitive actions being taken, is the businesses able to monitor these successfully to correlate with their compliance framework?

- Risk appetite levels—have these been set appropriately, balancing the risk of compliance failure against the running of the organisation and individuals' rights?
- Oversight—now that data privacy, information security and compliance has a strengthened position with a business, can this be maintained with all the other competing legislative overheads, initiatives and budgetary pressures?

Legal judgment and case law will help to refine some of the above questions, as will high-profiles incidents and public opinion. Furthermore, political and societal shifts could "move the needle" in either direction; aspects of the consideration are covered in the final section below.

## 7 What Does the Future Hold for Data Compliance?

Certainly, a new international data protection benchmark has been set with the introduction of GDPR. The Regulation has taken many years in its development and addresses many of the concerns that individuals have about the widespread (mis)use of data. It ought to be remembered though that GDPR was originally conceived over ten years ago in response to the rise of pervasive social media. Technology, data dissemination, access and fraud have all increased significantly since this time and the new Regulation may not be able to address the future world, we will live in. As an example, the roll-out of 5G technology will provide a transformative and amplifying effect on the ability of users to access data and systems—but also the opportunity for fraudsters to hack the complex architecture and gain access (quickly and deeply) to information. Certainly, vulnerabilities that already exist with 3G and 4G (and not yet resolved) will become significantly more damaging in the context of 5G—which relies on a complex interconnecting set of standards, hardware and organisations. The new mobile network standard is just one example of new technology that may test the adequacy of compliance rules and certainly others such as Artificial Intelligence (AI) and Internet of Things (IoT) will potentially exacerbate the situation.

When it comes to large fines, businesses being closed down and highly damaging reputational issues, the pre-GDPR hype has not been borne out by reality. Some organisations used the level of potential fines to warrant a large-scale investment in GDPR and scaremongering was shamefully rife amongst consultants. This isn't to say that the impact on

non-compliant businesses will not come to be felt—it is that regulators have not hit their stride yet. As discussed earlier, they are taking a prudent and encouraging approach first. This will not continue.

Although GDPR is now firmly embedded in the Board room and corporate risk framework rather than sat in the province of back-office functions, it needs to remain there. This is not just the responsibility of businesses leaders and their oversight committees, it the responsibility of regulators, courts and the public. Data protection legislation has now generated a new paradigm, one that is high profile, has the ammunition to enforce its intent and the international reach for a globalised marketplace.

In the opinion of the author, the highest risk to its effectiveness is likely to come from two areas: complexity and affordability.

The proliferation of technology, in particular AI, machine learning and complex analytical platforms means that as the underlying systems we rely upon become more unfathomable, our ability to control them reduces. Impenetrable logic, complex code and nebulous architecture have the potential to surpass the control we put in place. As it evolves so must our oversight and governance. Most importantly, the context of personal information that relates to an individual, rather than a "profile", "demographic category" or "user type" must be preserved. GDPR is based on the human, not corporate or system's right to privacy.

In terms of the overhead that GDPR places on organisations, the jury is out. Progressive businesses see the legislation has beneficial to treating their customers fairly, placing them squarely at the centre of their strategies and providing a positive competitive differentiator. Others remain of the opinion it is an unnecessary block to business effectiveness and creating another barrier to innovation. Industry needs to accept GDPR is here to stay and build its principles into concept and design stages of planning. In the same way, Information Security should be ingrained "by design" so must data privacy—the sooner this is achieved the quicker citizens will feel that they are protected intrinsically and not as an afterthought.

### *Financial Crime: An Example of Improving Standards*

Just as the Payment Card Industry Data Security Standards were seen by some companies as a threat to business, it turned out that they simply forced a higher standard of security on companies that took payments over the Internet. While there were some highly publicised breaches,

most companies embraced the rules and upped their game. The criminals have had to look for other personal data to exploit.

As the credit and debit card providers saw a rapid growth in online fraud and criminal hacking, there was a danger that the general public would see the Internet as a dangerous place to do business. The result was the banks and card providers had to start protecting their customers against card-based fraud. Some people then saw the growth of online fraud as a "soft" crime, where there were no real victims. Many people thought of credit-card fraud as a lesser crime than "real" theft. The people who investigated financial crime saw a very different picture with serious and organised criminals making millions of pounds or dollars without running much risk of being caught and even when they were, the sentences were very lenient. Drug-dealers, people traffickers and new terrorist groups saw the Internet as a place where they could fund their activities with very little risk: eventually, Governments and the courts started to take notice.

The GDPR has taken these higher standards and moved the bar up several notches. It is likely that most companies that are forced to improve their security will find that they are not at a competitive disadvantage since their competitors are having to work just as hard as them. If the Payment Card Security Standards (PCI 2018) and GDPR (European Parliament 2016) makes the job of the cyber-criminal harder and therefore protect the innocent Internet user this must be a good thing.

Formal certification will arrive in 2019. The EDPB which replaced the Article 29 of the Working Party (European Commission 2018), includes representatives from the data protection authorities of each EU member state, adopts guidelines for complying with the requirements of the GDPR. The EDPB (2018) published for consultation draft guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 on 30 May 2018. The consultation ended on 12 July 2018 and the responses are currently being considered.

## 8 Conclusions

Although six months into a live GDPR context is too early to tell the deeper ramifications of its effect, there are some clear trends that have emerged, and we should be optimistic about. The "beating stick" of penalties will eventually be wielded and this will add further impetus for improved compliance. GDPR is perceived as the gold standard for

privacy and data protection compliance and its comprehensive nature, broad adoption has ensured a critical-mass driving change globally.

Does the world feel a better place in respect of privacy and data protection since May 25, 2018? In the opinion of the author, it does. Companies are being held to account and responding promptly (British Airways may have announced a data breach as quickly as they did in a pre-May environment, but the current author suspects they would have not publicised the issue in depth quite as promptly). We only have to go back to the incident surrounding the TalkTalk breach of October 2015 (discussed earlier in the chapter) to see how things have moved forward. Last year when the current author asked the former, CEO Dido Harding what she felt the single biggest lessons learned was she replied "…not informing my customers soon enough". GDPR drives us all to provide prompt, transparent and clear disclosure. Dido's concluding wish has now perhaps been codified for all individuals to benefit.

## References

Bachmann, A. (2018). *GDPR: The New European Data Protection Law and Its Impacts On Affiliate Marketers*. https://www.itproportal.com/features/gdpr-the-new-european-data-protection-law-and-its-impacts-on-affiliate-marketers/. Accessed 27 November 2018.

BBC News. (2014). *EU Court Backs 'Right to Be Forgotten' in Google Case*, 13 May 2014. https://www.bbc.co.uk/news/world-europe-27388289. Accessed 19 November 2018.

Bloomberg. (2018). *British Airways Facing Massive Fine Under GDPR After Data Breach*, 7 September 2018. https://www.insurancebusinessmag.com/uk/business-news/british-airways-facing-massive-fine-under-gdpr-after-data-breach-110711.aspx. Accessed 19 November 2018.

Butterworth, B. (2018). *British Airways Faces £500m Fine Over Data Breach That Saw Thousands of Customers' Card Details Stolen*. https://inews.co.uk/news/british-airways-data-attack-record-fine-threat/. Accessed 19 November 2018.

Cadwalladr, C., and Graham-Harrison, E. (2018). Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian*, 17 March. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed 26 November 2018.

CBR Government. (2018). *No 'Fixed Point' for GDPR Compliance, Says ICO Chief*, 4 January 2018. https://www.cbrgovernment.com/policy/no-fixed-point-for-gdpr-compliance-says-ico-chief/. Accessed 19 November 2018.

Cimpanu, C. (2018). *UK Watchdog Has Not Issued Any GDPR Data Breach-Related Fines Yet*, 18 September 2018. https://www.zdnet.com/article/uk-watchdog-

has-not-issued-any-gdpr-data-breach-related-fines-yet/. Accessed 19 November 2018.

Davis, B. (2017). *GDPR for Marketers: Five Examples of 'Legitimate Interests'*. https://econsultancy.com/gdpr-for-marketers-five-examples-of-legitimate-interests/.

Decision Marketing. (2016). *TalkTalk Could Have Faced £70m Fine Under GDPR*, 6 October 2016. https://www.decisionmarketing.co.uk/news/talk-talk-could-have-faced-70m-fine-under-gdpr. Accessed 19 November 2018.

European Commission. (2018). *The Article 29 Working Party Ceased to Exist as of 25 May 2018*. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492. Accessed 19 November 2018.

European Data Protection Board. (2018). *Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation 2016/679*. https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_en. Accessed 19 November 2018.

European Data Protection Supervisor. (2018a). *The History of the General Data Protection Regulation*. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Accessed 19 November 2018.

European Data Protection Supervisor. (2018b). *Mission*. https://edps.europa.eu/about-edps_en. Accessed 19 November 2018.

European Parliament and of the Council. (1995). *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Date of End of Validity: 24/05/2018; Repealed by 32016R0679*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046. Accessed 19 November 2018.

European Parliament and of the Council. (2016). *Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed 19 November 2018.

Foulsham, M., and Hitchen, B. (2017). *GDPR: Guiding Your Business to Compliance: A Practical Guide to Meeting GDPR Regulations* (Edition 2). London: Independent Publishers.

Froud, D. (2018). *There Is No Such Thing as GDPR Certification …Yet! April 2018*. http://www.davidfroud.com/there-is-no-such-thing-as-gdpr-certification-yet/. Accessed 19 November 2018.

Government UK. (2018). *Data Protection Act 2018*. https://www.gov.uk/government/collections/data-protection-act-2018. Accessed 19 November 2018.

Heaphy, E. (2018). *Facebook's Fine for Mishandling the Data of 87 Million People Is Worth 15 Minutes of Its Profit*, 11 July 2018. https://qz.com/1325687/

facebooks-cambridge-analytica-fine-is-worth-15-minutes-of-profit/. Accessed 19 November 2018.

Hunton Privacy Blog. (2018). *CNIL Publishes Initial Assessment of GDPR Implementation*, 25 September 2018. https://www.huntonprivacyblog.com/2018/09/25/cnil-publishes-initial-assessment-gdpr-implementation/; https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application (in French). Accessed 21 November 2018.

ICO. (2018a). *Data Protection Practitioners' Conference 2018*, 9 April 2018. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/04/data-protection-practitioners-conference-2018-ed/. Accessed 18 November 2018.

ICO. (2018b). *Charity*, 25 May 2018. https://ico.org.uk/for-organisations/charity/. Accessed 18 November 2018.

ICO. (2018c). *Findings from ICO Information Risk Reviews at Eight Charities*, April 2018. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2259675/charities-audit-201808.pdf. Accessed 19 November 2018.

ICO. (2018d). *ICO Issues Maximum £500,000 Fine to Facebook for Failing to Protect Users' Personal Information*, October 2018. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/; https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit. Accessed 19 November 2018.

ICO. (2018e). *Guide to General Data Protection Regulation*. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Accessed 27 November 2018.

ICO. (2018f). *News, Blogs and Speeches*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/. Accessed 27 November 2018.

International Organization for Standardization. (2018). *Iso/Iec 17024:2012 Preview Conformity Assessment—General Requirements for Bodies Operating Certification of Persons*. https://www.iso.org/standard/52993.html. Accessed 19 November 2018.

ITPro. (2018). *GDPR News: Portuguese Hospital Hit with €400,000 Fine for Two GDPR Violations*. https://www.itpro.co.uk/data-protection/28029/latest-gdpr-news-uk?tpid=189842655. Accessed 19 November 2018.

Keane, S. (2018). *GDPR: Google and Facebook Face Up To $9.3B in Fines on First Day of New Privacy Law*, 25 May 2018. https://www.cnet.com/news/gdpr-google-and-facebook-face-up-to-9-3-billion-in-fines-on-first-day-of-new-privacy-law/. Accessed 19 November 2018.

Lexicology. (2018). *Guide to the General Data Protection Regulation*. https://www.lexology.com/library/detail.aspx?g=fe64fbad-d514-492f-b4b2-2b6b-204da0da%2F. Accessed 27 November 2018.

Osborne, C. (2018). *Equifax Fined £500,000 Over Customer Data Breach*. https://www.zdnet.com/article/equifax-fined-500000-over-customer-data-breach/. Accessed 20 November 2018.

PCI (2018). *Payment Card Security Standards*. https://www.pcisecuritystandards.org/. Accessed 19 November 2018.

Pearce, S. M. (2018). Dramatic Increase in French Privacy Complaints since GDPR. *The National Law Review*, 8 October. https://www.natlawreview.com/article/dramatic-increase-french-privacy-complaints-gdpr. Accessed 27 November 2018.

Robinson, T. (2018). *Under Armour Deftly Manages Breach, Dodges GDPR Scrutiny*. https://www.scmagazine.com/home/security-news/data-breach/under-armour-deftly-manages-breach-dodges-gdpr-scrutiny/. Accessed 19 November 2018.

Sky News. (2018). *Facebook, Worth £445bn, Fined £500,000 For Data Breach*, July 2018. https://news.sky.com/story/facebook-to-be-fined-500000-over-data-breaches-11432749. Accessed 19 November 2018.

Spittka, J., and Mirzaei, K. (2018). *Germany: First Court Decision on GDPR*. https://blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-gdpr/. Accessed 19 November 2018.

*The Guardian*. (2018). *Facebook Fined for Data Breaches in Cambridge Analytica Scandal*. https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal. Accessed 19 November 2018.

Today NG. (2018). *German Antitrust Authorities Prepare Sanctions Against Facebook*, 8 January 2018. https://www.today.ng/technology/social/german-antitrust-authorities-prepare-sanctions-facebook-51800. Accessed 19 November 2018.

Townsend, K. (2017). *Google's $2.73 Billion Fine Demonstrates Importance of GDPR Compliance*. https://www.securityweek.com/googles-273-billion-fine-demonstrates-importance-gdpr-compliance. Accessed 15 November 2018.

Valdez, A. (2018). *Everything You Need to Know About Facebook and Cambridge Analytica*. https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/. Accessed 26 November 2018.

**Mark Foulsham (BEng (Hons), MBCS, MIoD)** has experience spanning over thirty years leading both business and technology disciplines within broad types of organisations. During this time, he has spent his career at the "sharp end" of what it means to provide safe, reliable systems to high-transaction businesses. These include start-ups, recently merged and divested entities and newly listed companies. In addition, he has worked with small and medium enterprises (SMEs) to ensure that confidentiality and security provisions are effective

at the right level of investment and are not a throttle to an organisation's productivity. Mark has a strong presence in his industry peer group and has been a finalist in the INSEAD European CIO of the Year Award. From 2004 to 2016, Mark was CIO for the Insurance Group (including the comparison site GoCompare)—one of the fastest growing Internet insurers of recent times. In his 12-year tenure, there were no serious data breaches or cyber-attacks—he puts this down to placing security at the centre of every aspect of business thinking. During this time, Mark was also a Non-Executive Director for Europe's largest Microsoft Exchange cloud hosting business, cobweb and Chaired the Advisory Board of CIO Connect. In 2017, Mark co-authored a book on GDPR readiness which became an international best-selling edition on Amazon within six months. A new book was published in January 2019 that addresses data privacy post-May 2018 and the international context of GDPR as it beds in. Between 2016 and 2019 as part of a portfolio of engagements, Mark has worked with businesses from the Financial Services, the wider commercial sector, universities and social enterprises in achieving their GDPR compliance and data strategy programmes. He also gives industry seminar presentations focusing on the practicality of GDPR-alignment and how these can fit within the risk appetite levels of businesses. Mark also provides coaching to CIOs and other senior technology leaders.

CHAPTER 6

# Risk-Based Financial Regulation and Compliance Officer Liability

*Stuart Bazley*

## 1 Introduction

This chapter addresses two facets of the UK's regime for regulating the financial services industry. First, it considers in outline how the law and regulation in the UK intervenes to require that risk in the financial services sector is controlled and managed. In so doing, it will explore a variety of regulatory and statutory provisions that require risk in financial services to be identified, assessed and managed. Secondly, the chapter provides an overview of how those persons that work within the compliance function of a regulated firm can be held accountable for their professional activities, including when they may be exposed to personal liability.

## 2 Risk and Financial Services Regulation

The cause and impact of the global financial crisis in 2007/2008 is often partly blamed on failings in the financial services sector's ability to effectively identify and manage its risks. The UK Parliamentary Commission

S. Bazley (✉)
BPP University, Law School, London, UK
e-mail: srbazley@icloud.com



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_6

on Banking Standards commented on weakness in regulation to make judgements about risks in banking, it stated,

> Serious regulatory failure has contributed to the failings in banking standards. The misjudgment of the risks in the pre-crisis period was reinforced by a regulatory approach focused on detailed rules and process which all but guaranteed that the big risks would be missed….[1]

Although it is not be fair to say that risk-based regulation and compliance did not operate prior to the financial crisis, since 2007 considerable enhancement has been made. The Basel Core Principles for Effective Banking Supervision[2] include a variety of provisions underlining the inherent nature of risk management within banking supervision, for instance, Basel Core Principle 15 addressing risk management provides:

> '…that banks have a comprehensive risk management process (including effective Board and senior management oversight) to identify, measure, evaluate, monitor, report and control or mitigate all material risks on a timely basis and to assess the adequacy of their capital and liquidity in relation to their risk profile and market and macroeconomic conditions…' and at Principle 16 in relation to capital adequacy that 'The supervisor sets prudent and appropriate capital adequacy requirements for banks that reflect the risks undertaken by, and presented by, a bank in the context of the markets and macroeconomic conditions in which it operates…'.

Moreover, in relation to the regulation of securities markets the International Organization of Securities Commissions (IOSCO) also stresses the imperative of risk management within regulator supervision stating at Principle 6 of the IOSCO Objectives and principles of securities regulation that, 'The Regulator should have or contribute to a process to identify, monitor, mitigate and manage systemic risk, appropriate to its mandate'.[3]

At a fundamental level, risk management is concerned with the identification and response to risk probability and risk impact. Indeed the UK Financial Conduct Authority (FCA) describes risk as follows: 'We consider risk to be the combination of impact (the potential harm that could be caused) and the probability (the likelihood of the particular issue or event occurring)'.[4] Effective risk identification of course requires methodology and management process and it will be seen from the examination of regulation in this chapter, that the law and regulation often requires

financial services firms to establish organisational controls to allow for processes of risk management, often referred to by risk managers as 'enterprise risk management'. The Committee of Sponsoring Organisations of the Treadway Commission define enterprise risk management as:

> … a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.[5]

It will be seen that risk-based regulation, in addition to requiring regulated financial firms to identify and manage the risk of threats to their business, also allows for a firm to design risk management controls, internal systems and compliance procedures with the firm's own unique risks in mind, rather than requiring a firm to adopt and meet generic controls.

It is perhaps important to stress that the current regulatory regime does not operate risk-based regulatory obligations in a compartmentalised fashion. One can only acquire an appreciation for the full risk-based nature of the financial services system by considering firm-specific obligations holistically. That said, one might consider how risk-based obligations apply by analysing the cascade of risk-focused regulations, starting with risk-based duties, imposed on regulatory agencies, then by considering the governance and control obligations taken into account when considering whether a firm meets requirements for authorisation, the risk-based nature of the capital requirement rules, through to activity and conduct focused risk-based compliance.

## 3 Financial Services Regulatory Agencies and Risk-Based Regulation

The reforms to the UK system of financial regulation that followed the financial crisis through amendments to the Financial Services and Markets Act 2000 (which throughout this chapter is referred to as FSMA) included the formation of two regulatory agencies—The Prudential Regulation Authority (PRA) and FCA—whereby in general terms a division of responsibility now exists between prudential (capital) regulation and conduct regulation for banks and insurers. Such division is however not always applicable in regard to many other types of

financial institutions (regardless of their size) where the FCA has responsibility for both prudential and conduct regulation.

Other amendments to FSMA set out a series of revised measures that help to ensure both the PRA and FCA can be held to account. Included within such measures are provisions that set out objectives for each agency. The FCA for instance is subject to a consumer protection objective at S1C Financial Services and Markets Act 2000, which upon analysis incorporates reference to risk, stating,

> S1C… (2) In considering what degree of protection for consumers may be appropriate, the FCA must have regard to—
> (a) the differing degrees of risk involved in different kinds of investment or other transaction;…
> (e) the general principle that those providing regulated financial services should be expected to provide consumers with a level of care that is appropriate having regard to the degree of risk involved in relation the investment or other transaction and the capabilities of the consumers in question;….

In addition, both the PRA and FCA must undertake their respective activities in line with defined regulatory principles (see S3B Financial Services and Markets Act 2000) and it is possible to infer from the regulatory principles concepts of risk-based regulation. For instance and perhaps recognising that neither the PRA or FCA have limitless resource, as a result, the agency's resources should be focused on what is most important, S3B (1) (a) FSMA provides, 'the need to use the resources of each regulator in the most efficient and economic way'. Indeed in its publication 'Our Mission 2017', the FCA outlines its risk-based approach to supervision and states,

> …We use our risk tolerance framework to inform our prioritisation by understanding trends in the risk of harm and therefore threats to our statutory objectives. The risk framework thus underpins the decision-making framework by enabling the FCA to focus on potential harm, through analysis of trends and emerging risks to our objectives.[6]

### *Authorisation, Threshold Conditions and Risk*

Persons carrying on regulated activity by way of business in the UK are required under the Financial Services and Markets Act 2000 to be authorised by either the PRA or FCA depending of the business they

carry on (unless they are exempt). To obtain authorisation, a person must meet relevant statutory threshold conditions set out at Sch. 6 FSMA and with the FSMA (Threshold Conditions) Order 2013/555. For example, in relation to FCA authorisation, the Threshold Conditions include provisions relating to whether an applicant for FCA authorisation is 'suitable', has sufficient financial and non-financial resources and the suitability of its 'business model' (defined as its 'strategy for doing business'). Upon further analysis, a number of the Threshold Conditions draw upon issues relating to risk in regulation. For instance, in regard to the business model condition, the FCA states in its Condition sourcebook[7] at COND 2.7.8G (7) that it will consider amongst other things a firm's '…growth strategy and any risks arising from it' and in its rule guidance an expectation that firms should undertake a risk assessment including scenario testing of their business model, by stating at COND 2.7.10G

> Firms should consider scenarios which may negatively impact on the firm's business model with a view to ensuring the sustainability of the firm and, further, to consider the vulnerability of the business model to specific events and the risks and consequences that might arise. … A firm should put in place a credible plan to minimise the risks that it identifies from, or in relation to, its business model and a contingency plan for dealing with risks that have crystallised.

The Threshold Condition requires consideration of both financial and non-financial resources. Consideration will be given below to some of the more detailed risk-related provisions relating to capital, solvency and liquidity, but it is useful to highlight that the FCA conditions guidance within its COND sourcebook is provided also in the context of the adequacy of non-financial resources. Sch6 para 2D (2) (b) FSMA requires firms to be able to meet risks to 'the continuity of the services provided…'. In its sourcebook guidance on the application of such requirement, the FCA sets out that it will consider issues such as the 'means of managing [the firms] resources' including the 'means by which to manage risk' and at COND 2.4.4G (2) (d) 'whether the firm has taken reasonable steps to identify and measure any risks of regulatory concern that it may encounter in conducting its business' and at COND 2.4.4G (2) (f) 'whether the resources of the firm are commensurate with the likely risks it will face'.

### *Capital Regulation and Risk*

A variety of discrete EU Directives operate to regulate financial services firms' capital, solvency and liquidity. Although this chapter does not provide an opportunity to identify and examine all of such EU regulation, it is worth mentioning the following regulations: (a) the EU Capital Requirements Directive[8] (referred to as CRD) which applies to banking and other investment firms, (b) the EU Second Solvency Directive for Insurance,[9] plus (c) UK specific regulation, which set out series of measures addressing both obligations for organisation-wide management of risk specific to solvency and liquidity, and which reveal upon analysis an inherent relationship between risk management and capital and solvency requirements.

In many areas, such regulation is drafted by reference to high-level principles. That is a series of objective standards designed to ensure that an authorised financial institution devises a compliance response suited to its own circumstances. For instance, the FCA high-level principle of businesses 4 requires that its authorised firms 'must maintain adequate financial resources'.

Furthermore, amplifying the Principle 4 obligation in respect of authorised firms defined as BIPRU firms, the FCA's General Prudential rules (GENPRU) at GENPRU 1.2.11 (G) confirm that the 'Adequacy of a firms financial resources needs to be assessed in relation to all the activities of a firm and the risks to which they give rise…'[10] and at GENPRU 1.2.26R that 'A firm must maintain financial resources including capital resources and liquidity resources which are adequate both as to amount and quality to ensure that there is no significant risk that its liabilities cannot be met as they fall due'.[11]

Much of the law relating to regulatory capital, solvency and liquidity provides detailed and complex provisions relating to the amounts and quality of capital that a firm must maintain and it's fair to say that a thorough analysis of such complex provisions is beyond the word limit of this chapter. It may be observed however that central to capital requirement regulation is the necessity to link the calculation of regulatory capital with risk. For instance, the CRD along with measures implemented by the FCA in it sourcebooks GENPRU, BIPRU and IFPRU[12] require firms within the scope of such provisions to carry out an assessment of their capital in accordance with an 'Internal Capital Adequacy Assessment Process' (ICAAP). The rules make it clear that a firm's ICAAP must be 'an

integral part of the firm's management process…' be supported with procedures systems and a strategy and (see IFPRU 2.2.7R), be documented (IFPRU 2.2.16 and 2.2.43R) and that its Board is responsible for it. The rules at IFPRU 2.2.7R require assessment of major risk from identified and defined categories, including 'credit risk', 'market risk', 'operational risk', 'interest rate risk' and 'business risk'.[13]

Key features of a firm's ICAAP, which evidence that the regulatory requirements embrace concepts of risk management, include:

- Regularly carrying out 'assessments of the amounts, types and distribution of financial resources, own funds and internal capital that it considers adequate to cover the nature and level of the risks to which it is or might be exposed…' (IFPRU 2.2.7R)
- To 'identify the major sources of risk to its ability to meet its liabilities as they fall due' (at IFPRU 2.2.7R)
- To 'conduct stress and scenario tests' (for firms defined as 'significant IFPRU firms' at IFPRU 2.2.37R, and also in GENPRU 1.2.42R).

### *Risk, Governance and Management*

It is perhaps fair to suggest that effective risk control requires sound internal systems and organisation-wide controls. The regulatory provisions applicable to various sectors of financial services include detailed provisions addressing requirements imposed on firms to operate systems of governance where many of such provisions are typically drafted drawing on objective standards using words such as 'appropriate' and 'reasonable'.

Once again, relevant rules relating to governance and risk might be considered to cascade through an organisation. Analysis of the EU second Markets in Financial Instruments Directive[14] as implemented in the UK reveals obligations which operate generally to the firm and its governance, specific rules dealing with risk management and more discrete provisions relating to risk and compliance functions. For instance rules within the FCA's Senior Management Arrangements, Systems and Controls sourcebook at SYSC 4.1.1R (1)[15] imposes generic governance and business control obligations, albeit making clear that such obligations asked include provision for risk management. SYSC 4.1.1R provides, 'A firm must have robust governance arrangements, which

include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems'. Furthermore, SYSC 4.1.2R makes clear that the firm's governance arrangements must be designed to meet the regulated firm's own circumstances and risks, in that sense the rules are designed to 'flex' in order to create firm-specific obligations. SYSC 4.1.2R provides, 'For a common platform firm, the arrangements, processes and mechanisms referred to in SYSC 4.1.1 R must be comprehensive and proportionate to the nature, scale and complexity of the risks inherent in the business model and of the common platform firm's activities …'.

It is of course important to consider risk from the standpoint of a threat to or failure to meet all of the firm's regulatory obligations and in that sense it is evident that regulatory risk management, in addition to being concerned with risk to capital, market, credit, operational matters and the like, is also concerned with risks in relation to more general regulatory obligations. In a number of respects, it may be observed that risk management is concerned with the utilisation of internal processes to guard against risk, although it can be seen from the relevant regulation that the risk identification and assessment must be performed in order to design appropriate systems of control. For instance and in relation to broader questions of compliance, The EU second Markets in Financial Instruments Directive (MiFID II) supplementing regulation[16] at Article 22 provides that,

> Investment firms shall establish, implement and maintain adequate policies and procedures designed to detect any risk of failure by the firm to comply with its obligations under Directive 2014/65/EU, as well as the associated risks, and put in place adequate measures and procedures designed to minimise such risk and to enable the competent authorities to exercise their powers effectively under that Directive.

Similarly the FCA rules at SYSC 6.1.1R (1) provide,

> a firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents)

with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.[17]

## 4 Governance and Risk Management

Regulation provides for more specific risk management obligations in relation to the establishment and maintenance of internal risk management arrangements. For instance, in relation to investment firms MiFID II at Article 16 (5) begins by imposing a generic obligation relating risk that, 'An investment firm shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment …'. The MiFID II supplementing regulation at Article 23[18] goes on to provide more specific obligations relating to nature and extent of the risk management arrangements that must be adopted by a firm. Once again and upon analysis of Article 23 these risk management obligations are based on objective standards to be met by individual firms. Article 23 (1) provides as follows,

> Investment firms shall take the following actions relating to risk management:
>
> a) establish, implement and maintain adequate risk management policies and procedures which identify the risks relating to the firm's activities, processes and systems, and where appropriate, set the level of risk tolerated by the firm;
>
> b) adopt effective arrangements, processes and mechanisms to manage the risks relating to the firm's activities, processes and systems, in light of that level of risk tolerance;
>
> c) monitor the following:
>
> (i) the adequacy and effectiveness of the investment firm's risk management policies and procedures;
>
> (ii) the level of compliance by the investment firm and its relevant persons with the arrangements, processes and mechanisms adopted in accordance with point (b);
>
> (iii) the adequacy and effectiveness of measures taken to address any deficiencies in those policies, procedures, arrangements, processes and mechanisms, including failures by the relevant persons to comply with such arrangements, processes and mechanisms or follow such policies and procedures.

In addition to requiring firms to operate internal risk management processes, the MiFID II supplementing regulations also require firms where it is 'appropriate and proportionate' to do so, to establish an

operationally independent internal risk management function, meeting prescribed tasks under Article 23 (1). The MiFID II supplementing regulation Article 23 (2) provides,

> Investment firms shall, where appropriate and proportionate in view of the nature, scale and complexity of their business and the nature and range of the investment services and activities undertaken in the course of that business, establish and maintain a risk management function that operates independently and carries out the following tasks:
>
> (a) implementation of the policy and procedures referred to in paragraph 1;
>
> (b) provision of reports and advice to senior management in accordance with Article 25(2).
>
> Where an investment firm does not establish and maintain a risk management function under the first sub-paragraph, it shall be able to demonstrate upon request that the policies and procedures which it is has adopted in accordance with paragraph 1 satisfy the requirements therein.

## 5 Risk, Investment Products, Conduct and Activity

Hitherto, this chapter has considered examples of regulation that address fundamental and broad risk management and risk control obligations. It has been shown that many of these are designed to shape authorised firms general approaches to its internal governance arrangements and more specifically set and control its capital and liquidity. It is, however, important to have regard for examples of regulation that set risk-based compliance obligations in relation to specific areas of a firm's transaction activities or in relation to financial products manufactured or sells to customers.

### *Product Governance*

MiFID II introduced obligations for relevant firms to operate controls to guard against certain risks associated with financial products. For instance in relation to firms that are regarded as manufacturers of financial products, Article 9 (10) of the MiFID Delegated Directive[19] requires such firms by way of scenario testing to assess risk when products may present 'poor outcomes' for clients. Article 9 (10) provides, 'Member States shall require investment firms to undertake a scenario analysis of their financial instruments which shall assess the risks of poor outcomes for end clients posed by the product and in which circumstances these outcomes may occur'.

### *Risk and Financial Crime*

Provisions setting out a risk-based approach to regulation are evident in the law relating financial crime. More specifically, provisions operate that establish a framework for control to guard against the threat that the financial system or individual authorised firms may be exposed to criminal activity. Such provisions set out requirements to ensure that compliance arrangements are designed with specific financial crime risk in mind. Indeed earlier in this chapter when considering a firm's general risk management, it was seen that under FCA rules at SYSC 6.1.1R, firms are obliged to establish financial crime specific internal controls, that is controls, '…for countering the risk that the firm might be used to further financial crime'.

### *Anti-Money Laundering (AML)*

The EU 4th Money Laundering Directive[20] (which will be referred to as the ML Directive) approaches risk-based compliance from the standpoint of risks faced by individual jurisdictions, those faced by individual firms from the markets and services they provide and those presented by the individual customers (whether arising from their characteristics or the transactions they undertake).

EU member states are required to undertake a risk assessment of the money laundering threats presented to their jurisdictions. Article 7 (1) of the ML Directive as implemented in the UK by Regulation 16 of the UK Money Laundering Regulations 2017[21] (which are referred to throughout this chapter as the Money Laundering Regulations 2017) requires that 'Each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. It shall keep that risk assessment up to date' (and pursuant to regulation 16 (9) ensure the risk assessment is kept up to date).[22]

Regulation 19 (2) of the Money Laundering Regulations 2017 goes on to prescribe the core components of the national risk assessment, which must include an assessment of such matters as,

> (2) The risk assessment must, among other things—
>
> (a) identify any areas where relevant persons should apply enhanced customer due diligence measures, and where appropriate, specify the measures to be taken;

> (b) identify, where appropriate, the sectors or areas of lower and greater risk of money laundering and terrorist financing;
>
> (c) consider whether any rules on money laundering and terrorist financing made by a supervisory authority applying in relation to the sector it supervises are appropriate in the light of the risks of money laundering and terrorist financing applying to that sector;
>
> (d) provide the information and analysis necessary to enable it to be used for the purposes set out in paragraph (3)….

In its first assessment published in October 2015, the UK Government stressed the risk-based nature of the money laundering law and regulation and indicated the benefit that its risk assessment might provide. It stated that:

> The objective of the NRA is to better understand the UK's money laundering and terrorist financing risks, inform the efficient allocation of resources and mitigate those risks. While this assessment should not be relied upon in isolation, the improved understanding it provides should assist the government, law enforcement agencies, supervisors and the private sector in targeting their resources at the areas of highest risk, ensuring that the UK's approach to preventing financial crime is risk-based and proportionate.[23]

Similarly, risk assessment obligations are also extended to supervisory authorities in relation to their regulatory jurisdiction (The FCA for the financial services sector regulated under FSMA). Regulation 17 requires that 'Each supervisory authority must identify and assess the international and domestic risks of money laundering and terrorist financing to which those relevant persons for which it is the supervisory authority ("its own sector") are subject'.

## 6 Money Laundering Risk and the Regulated Entity Standpoint

The ML Directive along with its UK implementation under the Money Laundering Regulations 2017 set out a series of measures designed to require firms to undertake a risk assessment of the extent to which their business might be exposed to the threat of money laundering, whether from customers, the jurisdictions in which they operate or their products and services, as well as to design internal systems of control to address identified risk. It is once again evident from the regulation that

the risk-based nature of the law requires firms to design appropriate responses to the risk that are specific to the firm's business. One may analyse the ML Directive and Money Laundering Regulations 2017 firm-specific risk assessment obligations as operating in a way that further adds to authorised firms overall internal controls obligations. Thus Article 8 (1) of the ML Directive provides that 'Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels…'. similarly regulation 18(1) of the Money Laundering Regulations 2017 requires, that 'a relevant person must take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject'. Regulation 18 (2) of the regulations also identifies the risk factors that a firm must take into account and where it should draw its risk research data from by requiring as follows,

> '(2) In carrying out the risk assessment required under paragraph (1), a relevant person must take into account—
>
> (a) information made available to them by the supervisory authority under regulations 17(9) and 47, and
>
> (b) risk factors including factors relating to— (i) its customers; (ii) the countries or geographic areas in which it operates; (iii) its products or services; (iv) its transactions; and (v) its delivery channels'. The extent of the work that the firm should undertake to risk assess (i.e. the steps it should take) may under the regulations be taken from the perspective of the size and characteristics of the individual firm, regulation 18 (3) providing, 'In deciding what steps are appropriate under paragraph (1), the relevant person must take into account the size and nature of its business'.

Furthermore, the extent of the work that the firm should undertake to risk assess (i.e. the steps it should take) may under the regulations be taken with regard the size and characteristics of the individual firm, with regulation 18 (3) of the Money Laundering Regulations 2017 providing, 'In deciding what steps are appropriate under paragraph (1), the relevant person must take into account the size and nature of its business.' Thus, recognising that the risk control requirements for a small firm (perhaps with a lower risk customer exposure) may be different to a larger and more complex firm, dealing with higher risk customers or operating in higher risk jurisdictions.

In keeping with the standardised approach to risk management, having identified money laundering risk, the ML Directive and Money Laundering Regulations 2017 require firms to establish internal controls to address such risks. Article 8 (3) of the ML Directive provides that 'Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities'. In addition, Regulation 19 (1) of the Money Laundering Regulations 2017 requires that a firm must '(a) establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment undertaken by the relevant person under regulation 18(1);..'

### *Customer Due Diligence*

The ML Directive at Article 13 (1) and the Money Laundering Regulations 2017 go on to set out obligations for firms to identify their customer and understand the nature of their customers business activities, referred to in the law as customer due diligence. The ML Directive and Money Laundering Regulations 2017 once again approach the requirement for due diligence by allowing a risk-based approach to compliance in terms of an overall acknowledgement of the risk-sensitive nature of internal customer due diligence by providing at ML Directive Article 13 (2) 'Member States shall ensure that obliged entities apply each of the customer due diligence requirements laid down in paragraph 1. However, obliged entities may determine the extent of such measures on a risk-sensitive basis'. Additionally the ML Directive and Money Laundering Regulations 2017 draw a clear distinction between lower risk customers where more simplified due diligence may be undertaken (as provided by Article 15) and enhanced due diligence that must be undertaken where a firm is dealing with high-risk customers or has activities in higher risk jurisdictions. In this regard, the ML Directive Article 18 provides 'Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately' and further to assist classification and assessment of customers sets out in with its annex I–III a series of 'risk factors' to be taken into account in assessing the risk profile of customers.

Considering generally the ML Directive and UK's Money Laundering Regulations 2017 approach to enforcing compliance with the various internal control requirements, the regulations provide power to the relevant regulatory agency (which includes the FCA for firms authorised under FSMA) at Regulation 76 to take civil enforcement action such as the imposition of a financial penalty, or under Regulation 77 to remove or suspend authorisation, in the event of a breach of compliance where there is a breach of compliance with obligations described in those regulations. Furthermore, it is noteworthy that it is a criminal offence under Regulation 86 of the Money Laundering Regulations 2017 for a person to '…contravene[s] a relevant requirement imposed on that person…'. Relevant requirements are defined in Regulation 75 as having the meaning set out in Schedule 6 of the Money Laundering Regulations 2017 regulations and includes amongst other items, matters such as (a) Regulation 18 (risk assessment by relevant persons); (b) Regulation 19 (policies, controls and procedures); (c) Regulation 21 (internal controls); (d) Regulation 27 (customer due diligence); (e) Regulation 28 (customer due diligence measures); (f) Regulation 33(1) and (4) to (6) (obligation to apply enhanced customer due diligence); (g) Regulation 35 (enhanced customer due diligence: politically exposed persons); and (h) Regulation 37 (application of simplified due diligence). It is noteworthy that such an offence when committed by the corporate body can also be committed by its directors and officers under the provisions of regulation 92 of the 2017 regulations.

### *Compliance at Risk—Failings in Risk-Based AML Systems and Controls*

The UK FCA has for some time been concerned with the extent to which individual firm's anti-money laundering procedures appropriately focus on high risks within the organisations business. To understand the extent of the concerns it can be helpful to consider relevant enforcement action undertaken by the Authority. Although relating to the law and regulation prior the 4th EU Money Laundering Directive and the Money Laundering Regulations 2017, the FCA's final notice to Deutsche Bank AG on 30 January 2017[24] provides assistance in understanding the nature and extent of the FCA's concerns about the risk-sensitive nature of money laundering compliance. In the Deutsche Bank matter the FCA imposed a financial penalty of £163,076,224 (inclusive of a £9,076,224 disgorgement) arising from the bank breaching FCA principle for

business 3 (that 'A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'[25]) and SYSC rules 6.1.1 R and 6.3.1 R. Many of the failings identified by the FCA related to weaknesses in the bank's risk management obligations, including those relevant to customer due diligence and enhance due diligence. In the Final Notice, the FCA stated,[26]

> (1) its CDD and EDD was inadequate in that it failed to obtain sufficient information about its customers to inform the risk assessment process and to provide a basis for transaction monitoring;
> (2) its culture failed to instill a sense of responsibility in the front office business for the identification and management of non-financial risks, particularly in the London Front Office, which failed to appreciate that it was ultimately responsible for Deutsche Bank's KYC obligations (in accordance with London Front Office's role as the first line of defence);
> (3) it used flawed AML customer and country risk rating methodologies which meant that customers were assigned inappropriate risk ratings;
> (4) its AML policies and procedures were deficient;
> (5) its AML IT infrastructure was inadequate and failed to provide a single authoritative repository of KYC information;
> (6) it lacked automated AML systems for detecting suspicious trades and lacked an effective system for monitoring money flows associated with transactions; and
> (7) it failed to provide adequate oversight of trades booked in the UK by Moscow Front Office as well as other non-UK locations.
> ..Because of the inadequacies in Deutsche Bank's AML control framework, it was unable to identify, assess, monitor, or manage its money laundering risk. As a result, Deutsche Bank engaged in suspicious transactions that enabled its customers to transfer approximately USD10 billion from Russia, via Deutsche Bank's UK trading books, to overseas bank accounts including in Cyprus, Estonia and Latvia without detection.[27]

### *Compliance Officer Responsibility and Liability*

In this section of the chapter, consideration is given to the responsibility of those persons working in the UK within an authorised firm's compliance function or money laundering reporting function, together with an assessment of the extent to which compliance officers may incur liability arising from their activities.[28] The section will initially consider the issue regarding general liability under the law, then consider in outline accountability

as relevant to the compliance officer under the provisions of Part V the Financial Services and Markets Act 2000, (in relation to 'Controlled Functions' including Approved Persons and the Senior Managers and Certified Persons regime) along with providing an overview of the characteristics of a compliance function as defined by the EU 2nd Markets in Financial Instruments Directive[29] and conclude with an outline of a number of regulatory enforcement actions against compliance officers or other persons where the case raises issues of importance and relevance.

It is a incontrovertible that the criminal law can apply to the activities of compliance officers and Money Laundering Reporting Officers (MLRO) whether arising from what may be considered to be special regulatory offences as well as aspects of general criminal law that might apply to financial services. For instance, the offence of misleading a regulatory agency as set out in Ss398 and 399 FSMA, and Regulation 88 of the Money Laundering Regulations 2017 might be offences relevant and applicable to the work undertaken by a compliance officer or MLRO when in communication with a relevant regulator. Offences under the Proceeds of Crime Act 2000 (POCA), such as failure to disclose (S330 and 331, 332 POCA), tipping off (S333 POCA), prejudicing an investigation (S342 POCA) as well as specified AML internal control requirements offence in regulation 86 and regulation 92 Money Laundering Regulations 2017, might also be relevant the work undertaken by a Money Laundering Reporting Officer. Furthermore, senior compliance officers and MLROs might have regard to the extent to which they can be liable under s 400 Financial Services and Markets Act or Regulation 92 Money Laundering Regulations 2017 (if they are a company director or 'member of the committee of management') for a relevant corporate offence committed by way of their 'consent', 'connivance' or 'attributable to their neglect'.

Other offences impacting financial services which might create criminal liability for the rogue compliance officer or MLROs include: offences relating to fraud under s1 Fraud Act 2006, theft under s1 Theft Act 1967, Insider Dealing under Part V Criminal Justice Act 1993, market manipulation or making misleading statements to the market under Part 7 Financial Services Act 2012.

### *The UK Approved Persons and the Senior Managers and Certified Persons Regime*

Since the coming into force of the Financial Services and Markets Act 2000, persons working in defined 'Controlled Functions' at regulated firms

have been subject to a statutory Approved Persons regime, set out in Ss60 and 61 of the Act requiring such persons to be fit and proper in order to be approved by UK's FCA (and in appropriate cases PRA). Under that regime, Approved Persons are subject to an Approved Person's Code. Controlled Functions include Directors and partners along with other prescribed senior roles, such as the person with responsibility for compliance oversight (i.e. a firm's nominated senior compliance officer) and its MLRO.

The FCA's Approved Person's Code[30] sets out regulatory obligations applying to that conduct. Breaches of the Code expose the Approved Person to the potential of regulatory enforcement action. As will be illustrated below, compliance officers and MLRO can be exposed to such enforcement liability. The Code is drafted by reference to regulatory principles rather than detailed and descriptive regulatory obligations. That is, it is based on descriptions of objective standards such as 'due skill' 'proper standards' and 'appropriately'. These are all terms and standards which arguably can flex to meet the circumstances of persons responsibilities and activities and indeed the activities of the firm for whom they work. The Code is also divided between more general principles applying to all types of controlled function and obligations at Principles 4–6 only applying to those persons performing a significant influence function including those persons holding the compliance oversight or money laundering reporting functions. Those principles impose obligations relating to the persons responsibilities for managing compliance. The FCA Approved Person Code principles are as follows[31]:

**Statement of Principle 1**
An Approved Person must act with integrity in carrying out his accountable functions.
**Statement of Principle 2**
An Approved Person must act with due skill, care and diligence in carrying out his accountable functions.
**Statement of Principle 3**
An Approved Person must observe proper standards of market conduct in carrying out his accountable functions.
**Statement of Principle 4**
An Approved Person must deal with the FCA, the PRA and other regulators in an open and cooperative way and must disclose appropriately any information of which the FCA or the PRA would reasonably expect notice.
**Statement of Principle 5**
An Approved Person performing an accountable significant-influence function must take reasonable steps to ensure that the business of the firm for

which he is responsible in his accountable function is organised so that it can be controlled effectively.

**Statement of Principle 6**

An Approved Person performing an accountable significant-influence function must exercise due skill, care and
diligence in managing the business of the firm for which he is responsible in his accountable function.

**Statement of Principle 7**

An Approved Person performing an accountable significant-influence function must take reasonable steps to ensure that the business of the firm for which he is responsible in his accountable function complies with the relevant requirements and standards of the regulatory system.

Following the 2007/2008 financial crisis, a UK Parliamentary Commission on Banking Standards reviewed culture and behaviour in the banking sector. The Commission made a number of observations regarding the extent to which Senior Managers within banks were held to account for their decision-making, including that 'Too many bankers, especially at the most senior levels, have operated in an environment with insufficient personal responsibility. Top bankers dodged accountability for failings on their watch by claiming ignorance or hiding behind collective decision-making…'.[32] The Parliamentary commission was also critical of the extent to which the Approved Person regime had been effective at holding Senior Managers to account, stating 'The Approved Persons Regime has created a largely illusory impression of regulatory control over individuals, while meaningful responsibilities were not in practice attributed to anyone…'.[33]

In response, Parliament established a revised approach to accountability for Senior Managers, introducing a series of measures in Pt 4 Financial Services (Banking Reform) Act 2013 by way of amendments to the FSMA, to reform and strengthen the responsibilities and accountability of senior persons working UK banking sector. A new Senior Manager's regime was brought into force in March 2016 for Banks, Building societies and PRA designated investment firms and is now being extended to practically all sectors UK financial services industry by December 2019.

The division of responsibility for firms' authorisation between PRA and FCA complicates a simple overview of the new regime, in that not all provisions apply to PRA firms or may dealt with by the FCA for PRA authorisation matters. The following overview however is approached on the basis of the regime as applicable to the FCA. The new regime

identifies three main categories applicable persons—the Senior Manager, the Certified Person and other persons to whom conduct rules will apply. It is likely that even where a compliance officer is not holding one of the senior management compliance relevant functions, they will still be subject to some of the 'Individual Conduct rules' (see below). The Senior Manager's regime is applicable to 17 defined senior management functions, which included the compliance oversight function and Money Laundering Reporting function. All persons holding a Senior Manager function must be approved by the PRA or FCA (based on the business undertaken by their firm). In addition to support the notion of responsibility, the law requires that authorised firms must ensure that where relevant, 30 prescribed responsibilities[34] are allocated to a nominated Senior Manager and that person must be provided with a statement of responsibility.[35] Indeed to assist the allocation of responsibility, firms must develop and maintain a 'responsibility map'.[36] Prescribed responsibilities of relevance to the Compliance Officer or MLRO include:

- In relation to financial crime and thus of relevance to the MLRO at FCA rules SYSC 24.2.6R (3) 'Responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime'
- In relation to compliance function independence at FCA rules SYSC 24.2.6R '*(8) which the FCA expects will be allocated to a non-executive director. Responsibility for:*
  - *safeguarding the independence of; and*
  - *oversight of the performance of;*
  - *the compliance function in accordance with the compliance requirements for SMCR firms*'.
- In relation to responsibility for compliance with the FCA's Safe custody asset rules as to SYSC 24.2.6R (11) 'Responsibility for the firm's compliance with CASS'
- Relevant to Third Country firms SYSC 24.2.6R (16) 'Responsibility for the firm's compliance with the UK regulatory system applicable to the firm'
- Relevant to Third Country firms SYSC 24.2.6R (17) 'Responsibility for the escalation of correspondence from the PRA, FCA and other regulators in respect of the firm to each of the governing body or the management body of the firm and, as appropriate, of the firm's parent undertaking and the ultimate parent undertaking of the firm's group'.

The regime provides for 9 conduct rules as set out below, all of which apply to the approved Senior Manager, with only principles 1–5 applying to certified persons and other persons (subject to defined exceptions) working for an authorised firm.

FCA rules at COCON 2.1.1R to 2.1.5R[37]

Individual Conduct Rules

Rule 1: You must act with integrity.

Rule 2: You must act with due skill, care and diligence.

Rule 3: You must be open and cooperative with the FCA, the PRA and other regulators.

Rule 4: You must pay due regard to the interests of customers and treat them fairly.

Rule 5: You must observe proper standards of market conduct.

FCA rules at COCON 2.2.1R to 2.2.4R[38]

Senior Manager conduct rules

SC1: You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively

SC2: You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system

SC3: You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.

SC4: You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.

A key component of the regime is the 'assumption of responsibility' applicable to Senior Managers set out at S66B (5) FSMA. That is a person is guilty of misconduct under the regime if the authorised financial institution is in breach of an obligation under FSMA, EU provision and 'the Senior Manager was at that time responsible for the management of any of the authorized person's activities in relation to which the contravention occurred'. Unless pursuant to S66B(6) the person can satisfy the regulator [they] '…had taken such steps as a person in [their] position could reasonably be expected to take to avoid the contravention occurring (or continuing)'.

The FCA provides guidance in its Conduct rules sourcebook of the types of behaviour or failures that might result in liability, some of which is relevant to the Compliance Officer or MLRO. For instance at COCON 4.2.16G (7) in regard to a breach of senior management

principle SC2 on compliance with relevant requirements 'For a money laundering reporting officer, failing to discharge the responsibilities imposed on them by the firm for oversight of its compliance with the FCA's rules on systems and controls against money laundering'. And for a senior compliance officer, which might include matters relevant to the characteristics of a compliance function (which will be examined later in this chapter) the FCA states at COCON 4.2.16G (8):

> For a *senior conduct rules staff member* who is responsible for the compliance function, failing to ensure that:
>
> (a) the compliance function has the necessary authority, resources, expertise and access to all relevant information; or
>
> (b) a compliance officer is appointed and is responsible for the compliance function and for any reporting as to compliance; or
>
> (c) the persons involved in the compliance functions are not involved in the performance of services or activities they monitor; or
>
> (d) the method of determining the remuneration of the persons involved in the compliance function does not compromise their objectivity;….

### *The Markets in Financial Instruments Directive and the Compliance Officer*

The Second EU Markets in Financial Instruments Directive[39] describe pursuant to Article 22 of its supplementing regulation[40] key characteristics of a compliance function and sets out the activities that must be performed by that function. It requires that a firm subject to the Directive establishes a compliance function which:

- Is 'Permanent',
- Is 'Effective'
- and 'Operates independently'.[41]

Article 22 (3) goes on to require that the Compliance function must:

- have '…necessary authority, resource expertise, expertise and access to all relevant information' (Art 22 (3) (a)
- have appointed compliance officer (who can only be replaced by firms management body) (Art 22 (3) (b)

- report ad hoc to management body if it detects significant risk of failure (Art 22 (3) (c)
- not be involved in performance of services they monitor (Art 22 (3) (d)
- not be remuneration in a way that compromises 'their objectivity' (Art 22 (3) (e).[42]

Article 22 (2) also sets out the compliance functions key responsibilities which cover:

- Monitoring how adequate the firm's compliance procedures are (Art 22 (2) (a). In regard to monitoring Article 22 outlines the need for the monitoring programme to be risk based and pre-determined from a compliance risk assessment, stating,

> …, the compliance function shall conduct an assessment on the basis of which it shall establish a risk-based monitoring programme that takes into consideration all areas of the investment firm's investment services, activities and any relevant ancillary services, including relevant information gathered in relation to the monitoring of complaints handling. The monitoring programme shall establish priorities determined by the compliance risk assessment ensuring that compliance risk is comprehensively monitored.

- Advising the firm of its obligations under the Directive (Art 22 (2) (b)
- Reporting to management body on effectiveness of its compliance arrangements, risk identified and complaints handling (Art 22 (2) (c)
- Monitor operations of complaints handling (Art 22 (2) (d).

It is also important to note that separately under Article 9 and Article 10 of the MiFID delegate directive[43] the compliance function has also specific product governance oversight obligations.

### *Example Civil Regulatory Enforcement Cases*

Compliance Officers and Money Laundering Officers where occupying a Controlled Function can carry liability for civil enforcement action under the Approved Persons Code (and Senior Managers Code). To provide insight into how liability can arise, it can be helpful to consider examples of regulatory civil enforcement action against compliance officers and MLROs. It should be noted that the decisions outlined below arise the

regime relating to Approved Persons and Controlled Functions and not under the new Senior Managers regime.

The FCA will take civil enforcement against senior management, including those involved in Compliance where there are issues concerning a person's integrity. For instance, in the FCA's Final Notice to Niall O'Kelly[44] Mr. O'Kelly, who was the Chief Financial Officer, and a Director, at a spread betting firm named Worldspreads Limited and who also held controlled functions for Systems and Controls and Client Asset Oversight (the Client Asset Oversight function referred to as CF10 (a) might be regarded as a quasi-compliance function) was prohibited and subject to a financial penalty of £11,900 (being reduced due to personal hardship) arising from his activities concerning WorldSpread's parent, Worldspreads Group plc along with failings in client money oversight. The FCA set out various findings in its final notice to Mr. O'Kelly, including that he knew that Worldspreads Group plc admission document for flotation on the UK Alternative Investment Market (AIM), contained certain materially misleading information and in relation to his responsibility in client asset compliance, that he had effected or had oversight of improper use of client money.[45]

It is also important to consider the extent to which question of integrity in personal life might impact upon a compliance officer's fitness and propriety to hold a controlled function. Examples of issues with personal integrity can be found in historical FCA civil enforcement notices to Approved Persons albeit not in relation to compliance or MLRO functions. Nonetheless, these cases serve to illustrate the importance of maintaining personal integrity. For instance, Mr. Jonathan Burrows[46] was prohibited by the FCA following his evasion of purchasing the correct train fare failure on a number of occasions and Paul Flowers[47] the Cooperative Bank Chairperson was prohibited as a result of his conduct in using a work phone for a premium rate chat line, work email for 'sexually explicit' and other 'inappropriate messages' and a drugs possession conviction after he had left the bank.

The Authority has taken action against Compliance Officers in connection with failings to have regard to or report suspicions of market abuse by other persons whether their employers, clients or colleagues. For instance, the Financial Services Authority's (the Financial Services Authority being the name of the regulatory agency prior to the FCA) civil enforcement decision against Alexander Ten-Holter[48] a Trader, Compliance Officer and MLRO for a company named Greenlight Capital

in UK, for breaching APER Principle 6 arose from his failure '…to question and to make reasonable enquiries prior to his effecting an order to sell…' certain securities. The Authority identified in its Final Notice that Mr. Ten-Holter had been informed at the time of being given the order that the issuer of the securities in question would have told Greenlight 'secret bad things' if Greenlight Capital had signed a 'non-disclosure agreement'; 'other shareholders had signed the NDA and in Greenlight's opinion would want to sell'; and 'Greenlight potentially had a window of a week to sell before the stock plummets, although that might be a 'lie''.

Similarly in the matter of David Davis,[49] who held a senior management position and was responsible for compliance oversight at a firm named Schweder Miller, Mr. Davis was subject to a financial penalty and prohibition following the Financial Services Authority's decision that he had failed to act with due skill, care and diligence (in breach of Principle 6) in that he did not '…challenge and make reasonable enquiries before authorising…' a customer orders (the customer was engaging in market abuse).[50] The Authority stated in its press release concerning the Final Notice that it 'makes it clear that every individual involved in a chain that leads to trading must proactively challenge suspicious behaviour and ensure it is reported', adding that 'all Approved Persons have a duty to help the FCA in its fight against market abuse'.[51]

Many senior staff involved in the management of firm's compliance and money laundering functions have responsibility for the establishment and effectiveness of elements of a firm's systems of control. Examples can be found of enforcement action against compliance officers whether they have failed to meet their regulatory responsibilities in relation to such systems of control. For instance, in the civil enforcement decision concerning David Watters in which he was subject to a financial penalty of £75,000,[52] Mr. Watters held the Compliance Oversight Controlled function at a firm involved in enhanced transfer value pensions business (referred to as ETV business) and was responsible for oversight of the firm's compliance with the FCA's Conduct of Business rules. The FCA found that in breach of Approved Person Principle 6 'due skill, care and diligence' Mr. Watters 'failed to':

1. 'take reasonable steps adequately to inform himself about his obligations in performing the CF10 controlled function and about the specific nature and risks of the ETV advice business';

2. 'take reasonable steps to ensure that the ETV advice process was compliant and capable of providing compliant advice…'
3. 'identify obvious ways in which the ETV advice process failed to comply with certain of the COB/COBS rules…'
4. 'take reasonable steps to monitor the ETV advice process to ensure that it was compliant with the rules in COB/COBS and that compliant advice was being given…'
5. 'take reasonable steps to identify and manage adequately [certain] …potential conflicts of interest…'
6. 'undertake any review of the Partnership's processes and documentation in light of the impending implementation of MiFID in the form of the COBS rules….'

Similarly but in relation to banks anti-money laundering systems of controls, the FCA took civil enforcement action against Steven Smith the MLRO at Sonali Bank UK.[53] The Authority had also take action against the bank for breaches of its obligations under Principles for Businesses 3 and 11, stating in its Final Notice to the Bank (in relation to principle 3) that,

> 'SBUK failed to take such steps in relation to its AML governance and control systems. The weaknesses in these controls were serious and systemic, and affected almost all levels of its business and governance structure, including its senior management team, MLRO function, oversight of its branches, and policies and procedures in relation to AML'. and in relation to principle 11, that, 'SBUK breached Principle 11 by failing to notify the Authority for at least seven weeks that it had become aware of a potentially significant fraud which had occurred at SBUK'.[54]

Confirming the nature of its findings against Sonali Bank UK, the FCA subsequently stated in its publication 'Enforcement performance account for 2016/17' that

> We found serious weaknesses affected almost all levels of SBUK's AML controls. This meant that the firm failed to comply with its operational obligations in respect of customer due diligence, the identification and treatment of politically exposed persons, transaction and customer monitoring and making suspicious activity reports….[55]

In regard to Mr. Smith who was subject to a financial penalty of £17,900 and prohibited from performing Money Laundering and Compliance oversight functions, the Authority in particular stated,[56] 'Mr Smith failed to put in place compliance monitoring plans which were appropriately focussed on the risks faced by SBUK and which adequately demonstrated that SBUK's AML systems were working effectively'. And further subsequently stated in its publication enforcement performance account for 2016/2017, 'We also found that Mr. Smith failed to oversee the day-to-day operation of, and ensure the effectiveness of, SBUK's AML systems and controls. We considered that Mr. Smith demonstrated a serious lack of competence and capability'.[57]

In keeping with all applications for Controlled Functions, the person to be appointed for the Compliance Oversight or Money Laundering Reporting function needs to have demonstrable competence. Issues regarding competence arose in the FCA's decision regarding a controlled function application by Goldenway Global Investments (UK) Ltd for Gregory Nathan to perform Compliance Oversight (CF10), MLRO (CF11), Director (CF1) and Customer Function (CF30).[58] The matter concerned a firm offering online trading services for over the counter securities (such as foreign exchange and commodity contracts for differences CFDs). It appears that the majority of the firm's customers were retail clients based in and nationals of China. Mr. Nathan had prior experience as head of compliance with a CFD firm. The FCA however, following a written application for authorisation, an interview, written and oral representations, and supplemental statements refused the CF10 and CF11 applications including on grounds that Mr. Nathan '…failed to demonstrate detailed knowledge and understanding of the implications of the firm's operating mode the money laundering and financial crime risks faced by the firm…'[59] and '…did not convey an adequate understanding of the difficulties in assessing the appropriateness of transactions for customers inherent in the firm's business model…'.[60]

## 7 Concluding Remarks

The measures outlined above show that the UK regulatory regime for financial services facilitates the holding to account of senior management including those that hold responsibility for compliance oversight and money laundering reporting. Indeed the selected number of historical civil enforcement cases show that the FCA is ready to exercise its civil

enforcement powers in appropriate cases. It can be expected that civil enforcement as a way of securing accountability of Senior Managers will continue as both a deterrent and mechanism for maintaining regulatory standards under the UK's new Senior Managers and Certified Persons regime. In the first part of the chapter, an overview of aspects of financial services regulation and law was used to illustrate the risk-based nature of the regime for regulating the financial sector and the importance placed on the obligation for firms to identify, assess and manage risks to their business—whether that is through the provision of capital or systems of control. Aside from the question of accountability and liability for those working in senior compliance roles, it is the case that in providing for a risk-based approach to compliance with regulation, the regulatory regime has established a necessary connection between, regulation, risk and a compliance function. Indeed when reflecting on the characteristics and requirements for a Compliance Function within MiFID regulated firms as set out Sect. 7 above, it is evident that the Compliance Function, in providing advice and undertaking monitoring, is regarded as an inherent part of a firm's overall risk control framework.

## Notes

1. Parliamentary Commission on Banking Standards. Changing Banking for Good. Vlm 1. HC 175 -I 12 June 2013 [11].
2. Basel Committee on banking Supervision. Core principles for Banking Supervision. Bank for International Settlements. September 2012. https://www.bis.org/publ/bcbs230.pdf. Accessed 16 January 2019.
3. OICU-IOSCO. Objectives and principles of Securities Regulation. International Organization of Securities Commissions. May 2017. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf. Accessed 16 January 2019.
4. The Financial Conduct Authority. Risk Management. The FCA website. 21 September 2017. https://www.fca.org.uk/about/supervision/risk-management. Accessed 16 January 2019.
5. Committee of Sponsoring Organisations of the Treadway Commission '*Enterprise Risk Management—Integrated Framework*' Executive Summary. September 2004 [2].
6. The Financial Conduct Authority. Our Mission 2017, How we regulate financial services. https://www.fca.org.uk/publication/corporate/our-mission-2017.pdf. Accessed 16 January 2019.

7. FCA Handbook of rules. Conditions sourcebook (COND). In force as at 8 January 2019. https://www.handbook.fca.org.uk/handbook/COND/1/?view=chapter. Accessed 16 January 2019.
8. Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending directive 2002/87/EC and repealing directives 2006/48/EC and 2006/49/EC.
9. Directive 2009/138/EC of the European Parliament and of the council of 25 November 2009 on the taking-up and pursuit of the business of insurance and reinsurance (solvency ii). See also the European Insurance and occupational Pensions Authority web site https://eiopa.europa.eu/Pages/Supervision/Insurance/Solvency-II-Going-Live.aspx. Accessed 16 January 2019.
10. FCA handbook of rules, General Prudential rules (GENPRU) sourcebook. In force as at 16 January 2019. https://www.handbook.fca.org.uk/handbook/GENPRU/1/?view=chapter. Accessed 16 January 2019.
11. n10.
12. n11, GENPRU, FCA handbook of rules BIPRU sourcebook https://www.handbook.fca.org.uk/handbook/BIPRU/1/?view=chapter and IFRPU sourcebooks https://www.handbook.fca.org.uk/handbook/IFPRU/1/?view=chapter. In force as at 16 January 2019. Accessed 16 January 2019.
13. See FCA handbook of rules. Sourcebook IFPRU 2.2.17R to 2.2.35R for definitions of certain risk categories. In force 8 January 2019. https://www.handbook.fca.org.uk/handbook/IFPRU/2/?view=chapter. Accessed 16 January 2019.
14. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.
15. FCA handbook of rules. Senior Management Arrangements Systems and Controls sourcebook (SYSC). In force as at 16 January 2019. https://www.handbook.fca.org.uk/handbook/SYSC/1/?view=chapter. Accessed 16 January 2019.
16. Commission delegated regulation (EU) of 25.4.2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.
17. n15. SYSC 6. In force as at 16 January 2019. https://www.handbook.fca.org.uk/handbook/SYSC/6/?view=chapter. Accessed 16 January 2019.
18. n16.
19. Article 9 (10) Commission Delegated Directive (EU) 2017/593 of 7 April 2016.
20. Directive (EU) 2015/849 of the European Parliament and of the council of 20 May 2015.

21. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692).
22. For the most recent The UK National Risk Assessment, see: National risk assessment of money laundering and terrorist financing 2017. HM Treasury and HM Home Office. October 2017. https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017. Accessed 16 January 2016.
23. National Risk assessment of money laundering and terrorist financing 2015. HM Treasury and HM Home Office. October 2015. https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing. Accessed 16 January 2019.
24. FCA Final Notice to Deutsch Bank AG 30 January 2017. https://www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf. Accessed 16 January 2019.
25. FCA handbook of rules. High-level principles for businesses Sourcebook PRIN 2.1. In force as at 16 January 2019. https://www.handbook.fca.org.uk/handbook/PRIN/2/?view=chapter. Accessed 16 January 2019.
26. n24 para 5.4 page 24.
27. n24 para 5.5 page 25.
28. For further reading see Rider, Alexander, Bazley and Bryant, Insider Dealing and Market Abuse 3rd edition, Bloomsbury Professional in particular Chapter 13.
29. n14.
30. The FCA handbook of rules, Approved Persons Code (APER). In force as at 16 January 2019. https://www.handbook.fca.org.uk/handbook/APER/1/?view=chapter. Accessed 16 January 2019.
31. n30 at APER 2.1A. https://www.handbook.fca.org.uk/handbook/APER/2/?view=chapter. Accessed 6 January 2019.
32. Parliamentary Commission on Banking Standards. Changing Banking for Good. Vlm 1. HC 175 -I 12 June 2013 [8].
33. Parliamentary Commission on Banking Standards. Changing Banking for Good. Vlm 1. HC 175 -I 12 June 2013 [8].
34. FCA Handbook of rules. Senior Management Arrangements, Systems and Controls sourcebook (SYSC) at SYSC 24 in force as at 16 January 2019. https://www.handbook.fca.org.uk/handbook/SYSC/24/?view=chapter. Accessed 16 January 2019.
35. S60 (2A) Financial Services and Markets Act 2000.
36. FCA rules at SYSC 25.1.1R https://www.handbook.fca.org.uk/handbook/SYSC/25/?view=chapter. Accessed 16 January 2019.
37. FCA rules Code of Conduct sourcebook COCON. In force 16 January 2019. https://www.handbook.fca.org.uk/handbook/COCON/1/?view=chapter. Accessed 16 January 2019.

38. n37.
39. n14.
40. (EU)Commission delegated regulation of 25.4.2016 supplementing Directive 2014/65/EU.
41. The European Securities Markets Authority (ESMA) provides guidance on a compliance function in, Guidelines on certain aspects of the MiFID Compliance Function requirements. 28 September 2012 ESMA/2012/388. https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-388_en.pdf. Accessed 6 January 2019.
42. n40 MiFIR The Compliance function performance and remuneration requirements are subject to a proportionality opt out at MiFIR Art 22 (4).
43. Commission delegated directive (EU) 7.4.2016 supplementing directive 2014/65/EU of the European Parliament and of the council with regard to safeguarding of financial instruments and funds belonging to clients, product governance obligations and the rules applicable to the provision or reception of fees, commissions or any monetary or non-monetary benefits.
44. Niall O'Kelly. FCA Final Notice 7 April 2017. https://www.fca.org.uk/publication/final-notices/niall-okelly.pdf. Accessed 16 January 2019.
45. n44 para 2.2 to para 2.6 pages 2 and 3.
46. John Burrows FCA Final Notice 15 December 2014. https://www.fca.org.uk/publication/final-notices/jonathan-paul-burrows.pdf. Accessed 16 January 2019.
47. Paul Flowers FCA Final Notice 1 March 2018. https://www.fca.org.uk/publication/final-notices/paul-john-flowers-2018.pdf. Accessed 16 January 2019.
48. Financial Services Authority Final Notice Alexander Ten-Holter 26 January 2012. https://www.fca.org.uk/publication/final-notices/ten-holter-greenlight.pdf. Accessed 16 January 2019.
49. FCA Final Notice David Davis 5 July 2012. https://www.fca.org.uk/publication/final-notices/david-thomas-davis.pdf. Accessed 16 January 2019. See also FCA Press release, 'FCA Fines Compliance Officer and broker whose actions enabled market abuse to be committed in October 2010.' 8 August 2013. https://www.fca.org.uk/news/press-releases/fca-fines-compliance-officer-and-broker-whose-actions-enabled-market-abuse-be. Accessed 16 January 2019.
50. FSA Final Notice to Rameskumar Satyanarayan Goenka 17 October 2011. https://www.fca.org.uk/publication/final-notices/rameshkumar_goenka.pdf. Accessed 16 January 2019.
51. FCA Press release, 'FCA fines compliance officer and broker whose actions enabled market abuse to be committed in October 2010,' 8 August 2013. https://www.fca.org.uk/news/press-releases/fca-fines-

compliance-officer-and-broker-whose-actions-enabled-market-abuse-be. Accessed 16 January 2019.
52. FCA Final Notice David Watters 10 July 2017. https://www.fca.org.uk/publication/final-notices/david-samuel-watters.pdf. Accessed 16 January 2019.
53. FCA Final Notice to Steven Smith 12 October 2016. https://www.fca.org.uk/publication/final-notices/steven-smith-2016.pdf. Accessed 16 January 2019.
54. See FCA Final Notice to Sonali Bank (UK) Limited 12 October 2016. https://www.fca.org.uk/publication/final-notices/sonali-bank-uk-limited-2016.pdf. Accessed 16 January 2019 para 2.3 page 2.
55. FCA enforcement annual performance account 2016/17 [10]. https://www.fca.org.uk/publication/annual-reports/enforcement-annual-performance-account-2016-17.pdf. Accessed 16 January 2019.
56. n 54 para 2.4 page 2.
57. n 55 page 11.
58. FCA Final Notice Goldenway Global Investments (UK) Ltd re Gregory Nathan 21 August 2017. https://www.fca.org.uk/publication/final-notices/goldenway-global-investments-uk-limited.pdf. Accessed 16 January 2019.
59. n 58 para 6 page 2.
60. n 58 para 7 page 2.

**Stuart Bazley** is Visiting Professor in Financial Regulation and Compliance Law at BPP University Law School, London, where he is co-leader of an LL.M. programme in financial regulation and compliance law and programme leader for an LL.M. in commercial law. Stuart has over 30 years' experience working in the financial services industry, including senior roles as in-house lawyer, compliance officer, head of compliance, money laundering reporting officer and regulatory consultant. He has a wide range of practical and academic experience in financial markets regulation, sales practice compliance, regulatory misconduct and enforcement. Stuart has particular academic interests in the interplay between the law of regulation, risk management, internal systems of control, and the role of the internal compliance function. Stuart has lectured on the law relating to financial regulation and compliance since 1998 and is a regular speaker on financial services compliance matters at the annual International Symposium on Economic Crime at Jesus College, Cambridge. Stuart's published works include: Rider, Alexander, Bazley and Bryant, *Insider Dealing and Market Abuse*, 3rd edition, Bloomsbury Professional (2016); and Bazley, *Market Abuse Enforcement Practice and Procedure*, Bloomsbury Professional (2013).

CHAPTER 7

# Whistleblowing: The Neglected Facilitator of Compliance

*Eva Tsahuridu*

## 1 Introduction

Corporate scandals are commonly the result of exposed illegal and/or unethical activities. Their proliferation, extensive publicity and the harm they create has increased the focus on compliance and compliance programmes in organizations, particularly in the corporate but also in the government and not for profit sectors. Some, like Griffith (2015, p. 2077), argue that we cannot seriously doubt "that we now live in an era of compliance".

Compliance is defined as "the processes by which an organization seeks to ensure that employees and other constituents conform to applicable norms which can include either the requirements of laws or regulations or the internal rules of the organization" (Miller 2017, p. 3). Miller describes compliance as the processes that an organization uses to police its own conduct. Importantly, compliance is not only concerned with laws and regulations but also with organizational policies and standards that may or may not have been developed in relation to externally imposed requirements, such as corporate governance codes. Compliance

E. Tsahuridu (✉)
School of Accounting, RMIT University, Melbourne, VIC, Australia
e-mail: eva.tsahuridu@rmit.edu.au



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_7

has increased in prominence and influence in corporations, so much so it has been called "the new corporate governance" (Griffith 2015, p. 2075).

This chapter is not evaluating the effectiveness of compliance in promoting ethical and legal conduct by organizations and their people. It defines compliance in the broad sense, as described by Miller (2017), to include internal and external expectations of appropriate conduct, as reflected in organizational codes of ethics and other standards or behaviour expressed in internal policies, as well as organizational legal and regulatory obligations. It explores the role whistleblowing plays as a fundamental element of compliance and reports on some of the initial findings of the *Whistling While They Work 2*[1] research project conducted across Australia and New Zealand, as reported in Brown (2018).

## 2 Compliance

The increased emphasis on compliance has several bases. Griffith (2015, p. 2078) perceives compliance as a new way of exercising government power "a de facto government mandate imposed upon firms by means of ex ante incentives, ex post enforcement tactics, and formal signalling efforts… through compliance, the government dictates how firms must comply, imposing specific governance structures expressly designed to change how the firm conducts its business".

The most frequently employed elements of compliance programmes are described by Stöber et al. (2018) as consisting of codes of conduct, compliance training and whistleblowing policies and their effectiveness should be associated with reduced illegal and/or unethical activities. Treviño et al. (1999) call for employees to be at the centre of compliance programmes since they know the most about existing misconduct and they are an "organization's first line of defence against ethical or legal problems because they are most likely to know about violations of the law or of ethical guidelines" (p. 134). It is thus necessary for compliance

[1]The *Whistling While They Work 2: Improving Managerial Responses to Whistleblowing in Public and Private Sector Organizations* was funded by the Australian Research Council and 23 partner and supporter organizations. The author of this chapter is a member of its research team. Details at: www.whistlingwhiletheywork.edu.au. It builds and extends research undertake in the project *Whistling While They Work 1: Enhancing the Theory and Practice of Internal Witness Management in the Australian Public Sector*.

to "engage critically with both flows of information, through the reporting function and through training. Through the reporting function, compliance ensures that lower-level employees can safely report concerns to their managers and that information concerning potential violations is quickly related to the appropriate level in the organization" (Griffith 2015, p. 2095). Training should focus not only on how people should report suspected illegal or unethical activities but importantly how the recipients of such reports should ensure that they keep the reporter safe and also efficiently and effectively deal with the reported misconduct. Whistleblowing and its effective management plays a key role in enabling valuable information to flow through the organization so that incidents of non-compliance are identified and addressed in a timely manner. Ensuring that whistleblowers are safe and recognized for their valuable contribution sends a powerful signal to employees who have blown the whistle and others in the organization who may be aware of incidents of non-compliance that they will be heard and protected.

## 3 Whistleblowing

Over the last two decades, we have seen a shift in how whistleblowing is seen by organizations. "Whistleblowing as a threat to an organization's authority, cohesiveness and public image that leads to the need to protect whistleblowers from retaliation, is slowly being replaced with a perception of whistleblowing as a means of organizational protection" (Tsahuridu 2011, p. 60). Indeed, the fact that whistleblowing policies are considered one of the three key elements of the compliance function is indicative of this shift, at least at the policy level, even if not yet fully appreciated and effectively practised in many organizations.

The most common definition of whistleblowing is that provided by Near and Miceli (1985, p. 4), which describes it as "the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to affect action". In essence, the "whistleblower attempts to exert power to change the behaviour of some members of the organization" (Near and Miceli 1995, p. 686) to address non-compliance with laws, regulations or organizational ethical standards, as reflected in the organization's code of ethics and policies. Internal whistleblowing refers to reporting channels inside the organization (to people such as compliance officers) while external

whistleblowing typically refers to reporting channels outside the organization (such as media or regulators) (Miceli et al. 2008).

While a lot of legislative attention has developed over the years on the protection of whistleblowers, in many instances it has not been effective in protecting whistleblowers or encouraging whistleblowing. This is likely a consequence of the perception of whistleblowing by management as disloyal and costly, despite research evidence that shows the benefits of whistleblowing and its appropriate management (Miceli et al. 2009). Near and Miceli (2008) find that "policy actions by lawmakers aimed at increasing the penalties for wrongdoing … and increasing sensitivity to wrongdoing may have more impact on the incidence of whistleblowing than laws aimed at reducing retaliation against whistleblowers. If executives terminate wrongdoing when informed about it, then observers of wrongdoing may be more likely to blow the whistle" (p. 278). They further speculate that a clear understanding by executives of what constitutes wrongdoing (by societal, legal or organizational standards) and the penalties they will incur if wrongdoing continues is likely to result in them being more receptive to whistleblower disclosures and more willing to terminate reported wrongdoing. Furthermore, Near and Miceli (2008) find that "initial evidence suggests that policy would be better served to focus on penalties for wrongdoing, as a way to increase reporting of organizational wrongdoing" (p. 278).

In the whistleblowing literature, the organization is commonly assumed to be the respondent to the whistleblower but the whistleblower experiences a range of responses from colleagues, superiors, whistleblowing report recipients, etc. The organizational response is unlikely to be a consistent and explicit response. Further, the different actors within the organization may respond to the whistleblower or the wrongdoing, and those responses are likely to differ in focus and content. Retaliation against the whistleblower may occur at the same time as the wrongdoing is addressed or terminated; or the whistleblower may not be harmed but the wrongdoing may be allowed to continue and not addressed.

Similar to the multiple responses that the whistleblower, the wrongdoing and those perpetrating it are likely to encounter, the responses of the whistleblower may vary too, something the literature also does not adequately address as it is generally assumed that "the individual either reports the behaviour/incident/practice or does not" (Knapp et al. 1997, p. 697).

Near and Miceli (1995, p. 681) describe effective whistleblowing as the "extent to which the questionable or wrongful practice (or omission) is terminated at least partly because of whistleblowing and within a reasonable time frame". This definition addresses the motivations and objectives of whistleblowing. More recently, Vandekerckhove et al. (2014) include the consequences to the whistleblower in what constitutes effective whistleblowing and describe it as leading to the cessation of the wrongdoing while at the same time keeping the whistleblower safe and unharmed.

### *Whistleblowing and Compliance*

"The assertion that whistleblowers are 'rats' or 'sneaks' has been refuted by empirical research on the psychological and sociological dimensions of whistleblowing" (Tsahuridu and Vandekerckhove 2008, p. 109). At the same time, internal whistleblowing is increasingly and more consistently seen as a critical means of identifying wrongdoing in organizations (Kaptein 2011) and a key element of compliance.

Brown and Donkin (2008) in the *Whistling While They Work 1* research project found that while several methods of discovery of identifying wrongdoing ranked as important "'reporting by employees' ranked overall as the single most important trigger for the uncovering of wrongdoing in the view of these respondents" (p. 44). Significantly, employee reporting was seen as more important than routine controls, internal audits or external investigations, confirming that "on the whole, whistleblowing is not only regular, but is recognised within organizations as highly important for uncovering organizational wrongdoing" (p. 44).

In the recently released initial findings of *Whistling While They Work 2* project (Brown 2018) reporting by employees was again considered the most important means for employees, managers and governance professionals to bring to light wrongdoing in, or by, organizations in the public and private sectors (Brown et al. 2018).

Often, whistleblowing expresses an act of loyalty to the organization that reflects organizational citizenship and prosocial behaviour and not disloyalty or negative deviance (Lewis 2011). However, Lewis argues that given the serious risks to the whistleblower that remain present in many organizations, employers and the courts should not impose a duty to report misconduct. Instead, organizations "should promote trust and confidence in the whistleblowing process through the provision of and adherence to codes of ethics, the negotiation and maintenance of

effective whistleblowing procedures and the promotion of a general culture of openness at the workplace" (Lewis 2011, pp. 71–72).

Similarly, Vandekerckhove and Tsahuridu (2010) call for the imposition of a general duty to blow the whistle on employees to only be considered when all three of the following conditions are satisfied:

- Ability to attribute responsibility for whistleblowing based on the capacity to identify who should know of the organizational wrongdoing.
- Ability to offer effective protection to whistleblowers.
- Ability to effectively prevent erroneous whistleblowing.

The mere presence of formal codes of ethics and compliance programmes is not an adequate defence against fraud and misconduct. Rather, "the more important and effective deterrent to fraud is managers who are ethical and enforce ethical standards" (Blount and Markel 2012, pp. 1045–1046).

Research consistently confirms that internal disclosures generally precede external disclosures (Jubb 1999; Vandekerckhove and Phillips 2017). In multiple prior studies, most employees who report perceived wrongdoing externally (e.g. to a government regulator or the media) also reported it to an internal complaint recipient (see reviews in Brown 2008; Miceli et al. 2008). More recently, Vandekerckhove and Phillips (2017) found that the whistleblowing process generally involves two or even three internal attempts to raise a concern before an external attempt is made, if it is made at all.

Difficulties have been expressed with what have been called bounty programmes where regulators encourage, through rewards, the disclosure of information of illegal activities to them instead of encouraging, initially at least, an internal disclosure. Ebersole (2011) in discussing the US Dodd-Frank bounty programme lists the following costs it incurs on business compliance and agency administration:

1. "cause a flood of poor quality tips;
2. encourage employees to report fraud externally rather than internally;
3. develop an inflexible SEC fraud enforcement strategy;
4. not be cost-effective; and
5. result in excessive and unnecessary litigation" (p. 135).

Given the rewards offered to employees who provide new information to the SEC and the substantial rewards they stand to gain if they report fraud directly to the SEC rather than internally, Ebersole (2011) argues that "external reporting undermines the effectiveness of internal corporate compliance systems, which are often responsive and effective in stemming fraud. Further, internal compliance systems can be more efficient than external reporting in avoiding delay in correcting financial misstatements and increasing the accuracy of management's assessment of internal controls. It is also efficient for internal systems to screen tips to reduce the volume of agency tips, preserve the SEC's limited resources, and ease the SEC's recent difficulty managing tips" (p. 137). Ebersole also contends that the incentive to report externally also has a negative effect on organizational culture because it undermines management's efforts to foster an ethical culture. "By undermining management's efforts to internally handle fraud and foster an ethical culture, Dodd-Frank is concurrently harming the organizational culture. Deteriorating organizational culture has a cascading effect on internal compliance because employees are more likely to report fraud internally in organizations with an ethical culture, in which case there is less fear of retaliation. More broadly, as organizational culture affects organizational performance, Dodd-Frank is harming the bottom line" (p. 139).

### *Inaction and the Silent Observers*

Overall, the characteristics of the whistleblower are less predictive of whistleblowing than the characteristics of the wrongdoing and the organization. Mesmer-Magnus and Viswesvaran (2005) provide a summary of some research evidence on the characteristics of the wrongdoing and their impact on the decisions to blow the whistle, which indicates that the perceived severity of the wrongdoing and its materiality, as well as convincing evidence of wrongdoing are related to the decision to blow the whistle, as is wrongdoing that is harmful to the organization and co-workers.

However, not all people who see wrongdoing, even if it is severe or material and they have convincing evidence and it is harmful to the organization or colleagues, will blow the whistle. Whistleblowing inaction rates refer to the proportion of employees who have perceived wrongdoing but appear to take no action, that is raise a concern or report it. The inaction rate is considered a key measure of the whistleblowing reporting climate by Brown and Donkin (2008). The *Whistling While They Work*

1 project was conducted in 2005–2007 across a wide cross section of Australian public agencies from the Commonwealth, New South Wales, Queensland and West Australian governments and examined the incidence, outcomes and management of whistleblowing (Brown and Donkin 2008). Significant differences in reporting and inaction rates across organizations were identified in that research project (Wortley et al. 2008). What seems to influence the occurrence of whistleblowing includes:

- the employee believes that the identified wrongdoing is serious and frequent;
- there is sufficient information or basis on which to make a report;
- the employee believes that effective management action will follow as a result; and
- reprisal risk.

Wortley et al. (2008, p. 78) find that "for those who do not report, lack of confidence in management action and the fear of management reaction, in circumstances in which management is involved or perhaps complicit, represent the major disincentives to reporting. When employees do go ahead and report, it is usually because these risks are less present or because the perceived seriousness outweighs the risks and the employee is willing to take their chances". Brown and Donkin (2008) found that the average inaction rate across all organizations was 28.6%, with differences at the organizational rather than jurisdictional levels even though there existed substantial differences in the legislative whistleblowing regimes between the jurisdictions and sectors. This finding indicates the influence of the culture and whistleblowing reporting climate of the organization on the decision to act and report misconduct when it is identified, rather than the importance of regulatory regimes. It also highlights the non-compliance that goes unreported in organizations because people do not believe that management will take action to deal with the non-compliance and that it will not react harmfully towards the whistleblower.

## 4 How Can Whistleblowing Facilitate Compliance?

Employee reporting of actual or suspected misconduct is one of the most effective ways to identify wrongdoing and can thus play a key role in the identification of compliance risks and their management. The way many

employees are still treated after they disclosed wrongdoing, and the way disclosures are managed, indicates that we still have a lot of work to do to realize the benefits of internal whistleblowing. Employees' awareness of illegal or unethical activities is insufficient to instigate whistleblowing, as research indicates that ethical judgement is related to the intention to blow the whistle but not to actual whistleblowing (Mesmer-Magnus and Viswesvaran 2005). "It is crucial that organizations stimulate employees who suspect or observe wrongdoing not to 'look the other way' or 'stick their head in the sand'" (Kaptein 2011, p. 513) but to respond in a manner that will enable the wrongdoing to be stopped. That is why the "U.S. Federal Sentencing Guidelines and Sarbanes-Oxley Act … advise organizations to create sufficient opportunity for employees to report wrongdoing internally" (p. 514).

The *Ethics at Work: 2018 Survey of Employees—Europe* undertaken by the Institute of Business Ethics (2018) involved 6119 interviews conducted in February 2018. It reveals that 30% of European employees have been aware of conduct by their employer or colleagues, which they thought violated either the law or their organization's ethical standards in the last 12 months. However, only 54% of European employees aware of legal or ethical misconduct in the last year raised their concerns.

The *2018 Report to the Nations* is based on the results of the 2017 Global Fraud Survey, an online survey opened to 41,573 Certified Fraud Examiners (CFEs) from July 2017 to October 2017 (Association of Certified Fraud Examiners 2018). It reports that tips, internal audit and management review have been the three most common means of detecting occupational fraud every edition of the report since 2010. In the 2018 report, these three detection methods were cited in 68% of the cases. Tips represented 40% of the cases and were the most common means of detection, while internal audit represented 15% and management review 13%. Employees provided 53% of the tips to the organizations. It is noteworthy that 32% of the tips that led to fraud detection came from customers, vendors and competitors who are placed outside the organization. Additionally, 14% of the tips came from an anonymous source, demonstrating that a significant portion of those who reported fraud did not want their identities known.

Albrecht et al. (2018) explored empirically the relationship between whistleblowing and fraud prevention and detection. While controlling for multiple variables, they found that of the 4943 frauds for which

they had data, 1774 or 35.9% were detected through whistleblowing, followed by internal controls, with 1057 cases or 21.4%, again supporting the role whistleblowing can play in the fight against fraud and corruption. Albrecht et al. also found that as the number of perpetrators increased so did the likelihood that whistleblowing will be the detection method. Similarly, the more anti-fraud measures an organization has the more likely that whistleblowing will be the detection method, indicating that anti-fraud measures increase awareness and responsiveness to identified fraud.

### *Whistling While They Work 2*

The recently published initial findings of the *Whistling While They Work 2* project (Brown 2018) provide new insights into whistleblowing processes and experiences of 17,778 individuals in 46 organizations based in Australia and New Zealand. They shed a new and extensive light on issues and practices relating to observing and reporting of wrongdoing, as well as management responses to the wrongdoing and to the whistleblower. This research demonstrates "how any type of organization – public or private, big or small – should approach the task of making whistleblower protection 'real' as part of their integrity, compliance and governance systems" (p. iii).

In this research Dozo et al. (2018) report that a total of 7391 or 41.6% of respondents had observed wrongdoing. Of those 5509 respondents observed wrongdoing in their current organization and 1881 in their previous organization. However, while over two-fifths of respondents observed wrongdoing, 29.5% of them did not report the most serious wrongdoing they observed in their current organization. Of those who did not report wrongdoing, 17.2% said that they dealt with the wrongdoing or someone else reported it, while 12.3% said that they were not aware of any action being taken in relation to the wrongdoing. This finding confirms previous research on the incidence of observers of wrongdoing who do not take any action to address or report it and confirms the need for better management of whistleblowing processes and compliance systems to encourage employees to report wrongdoing.

Dozo et al. (2018) also report on the outcomes of whistleblowing in relation to changes and reforms. The most common outcomes reported were:

- wrongdoers were disciplined;
- mistakes, failures or bad decisions were addressed;
- organizational policies/procedures were improved; and
- management or other personnel changes were made.

While the least common outcomes were:

- wrongdoers were rewarded;
- compensation was issued to people affected;
- apologies were issued to people affected; and
- outcomes or lessons were officially shared across the organization.

While the important role whistleblowing can, and does, play in compliance by assisting organizations to become aware and address risks is appreciated by managers and governance professionals, whistleblowers continue to report mistreatment due to raising concerns of non-compliance. In this research, Brown et al. (2018) show that 23% of the people who reported concerns were treated badly by management or colleagues, (17% reported they were treated badly by management, 8% treated badly by colleagues, with 6% treated badly by both). Importantly, this finding reveals the frequency and extend of negative repercussions towards those who raised concerns about wrongdoing. While the existence of direct reprisals in terms of harassment and employment-related mistreatment was reported by 50% of people who reported wrongdoing, indirect negative repercussions such as stress, reduced work performance, isolation and ostracism were reported by about 80% of reporters. These indirect or "collateral" repercussions were present in almost all cases of reprisals, indicating that what is considered direct mistreatment is almost always accompanied by indirect or collateral repercussions that affect individual and organizational well-being and performance.

Overall, a minority of respondents (17.6%) felt no adverse repercussions at all after they reported wrongdoing, with most (82.4%) experiencing at least some type of negative outcome (Smith 2018). Most respondents (81.6%) experienced at least one type of informal repercussion, compared with almost one in two (48.8%) who experienced at least one type of formal repercussion. A very small number of respondents (0.8%) experienced formal repercussions but not informal ones, while (32.6%) experienced informal but not formal repercussions and half

experienced both types. The data also reveal that informal repercussions are more intense, as well as more common.

The existence of formal organizational whistleblowing policies and procedures has been found to have little effect on the types of support whistleblowers receive or the extent of the negative repercussions that they face (Smith 2018). Smith explains that this finding may be understood by the fact that given the increased focus on formal whistleblowing policies, many organizations have introduced them but they have not yet operationalized and supported them adequately to affect actual practices. Or it may be that even organizations that have not developed formal policies pay more attention to the management of whistleblowing due to the increased attention it receives from governments and other external stakeholders. Either way, what is evident is that the introduction of a formal whistleblowing policy is in itself inadequate, if it is not supported and implemented in a manner that affects organizational practices and culture.

What has been found to lead to positive outcomes in the management of whistleblowing was a manager's emotion towards the reporting, a manager's provision of support and work level, as well as the broader organizational ethical culture (Brough 2018). Further, the findings indicate that detrimental outcomes for whistleblowers are not inevitable. When proactive management and risk assessment of detrimental actions towards the whistleblower occur, particularly as soon as a whistleblower has reported a concern rather than after problems arise, the detrimental outcomes fall by at least half (Olsen and Brown 2018).

Overall, the findings of the *Whistling While They Work 2* research project indicate that whistleblowing can be managed effectively so that wrongdoing can be identified and addressed in organizations in all sectors and that is happening in some organizations. What is important is for the formal policies to be supported by practices that are proactive in assessing risk and providing active and extensive support to address direct and indirect harm to whistleblowers.

## 5 Conclusion

Whistleblowing is a fundamental element of compliance programmes, as described earlier. "The theoretical case for the compliance-increasing effect of whistleblowing is strong: it increases the chance of

getting caught by installing a peer-surveillance" (Stöber et al. 2018, p. 7). However, observing misconduct does not mean that misconduct is reported, as found in several research findings reported earlier. Many people observe non-compliance but remain inactive observers. Whistleblower protection laws were based on the assumption that people that observe wrongdoing would be more likely to report it if the law afforded them protection from retaliation (Near and Miceli 2008; Near et al. 2004). This, however, has not been the case, as survey data suggest that not only whistleblowing but retaliation increased as legal protection increased (Miceli et al. 1999; Near et al. 2004), indicating that the law on its own has not been effective in protecting whistleblowers from retaliation but also that the fear of retaliation does not necessarily deter whistleblowing. It is also an unflattering outcome for organizational compliance, which failed to effectively use one of its key defences, that of whistleblowing, and in doing so also failed to comply with laws that require organizations to protect whistleblowers from retaliation.

For whistleblowing to be an effective element of compliance, as well as ensure compliance with whistleblowing laws, it is important that people feel that they will be, and are in fact, heard, as well as protected from direct and indirect forms of retaliation and harm. We ought to remember that people who see wrongdoing do not report it primarily because they think that nothing will be done if they speak up (Near et al. 2004; Brown et al. 2008).

Laws need to focus not only on the protection of whistleblowers but they should also impose obligations on organizations and their compliance function to effectively manage whistleblowing by responding to the report and the reporter in a timely and effective manner.

The initial findings from the *Whistling While They Work 2* project, reported in this chapter, indicate the continuing existence of direct retaliation but also the prominence and harm that indirect retaliation or collateral repercussions have on those who blow the whistle. They also indicate that organizations irrespective of sectors or industry can and do manage whistleblowing effectively by proactively identifying risks to the whistleblower and addressing them, while at the same time responding to the report and addressing the wrongdoing.

Compliance that only focuses on the inputs of policies, codes and training is in danger of becoming what has been termed cosmetic compliance "where an entity sets up formal internal compliance controls

that are largely ineffective or unenforced, and instead act as mere window dressing for the purposes of obtaining leniency in case of regulatory enforcement" (Blount and Markel 2012, p. 1046).

The existence of whistleblowing policies, codes of ethics or conduct and training will not in themselves lead to organizations that are behaving ethically and legally. What is going to make the difference is the practices.

## References

Albrecht, C. O., Holland, D. V., Skousen, B. R., and Skousen, C. J. (2018). The Significance of Whistleblowing as an Anti-fraud Measure. *Journal of Forensic & Investigative Accounting, 10*(1), 1–13.

Association of Certified Fraud Examiners. (2018). *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf. Accessed 19 December 2018.

Blount, J., and Markel, S. (2012). The End of the Internal Compliance World as We Know It, or an Enhancement of the Effectiveness of Securities Law Enforcement? Bounty Hunting Under the Dodd-Frank Act's Whistleblower Provisions. *Fordham Journal of Corporate & Financial Law, 17,* 1023–1062.

Brough, P. (2018). Managerial Support—Why It's Important, Where It Comes from, and What Enables or Prevents It. In A. J. Brown (Ed.), *Whistleblowing: New Rules, New Policies, New Vision (Work-in-Progress Results from the Whistling While They Work 2 Project)* (pp. 81–88). Brisbane: Griffith University.

Brown, A. J. (2008). *Whistleblowing in the Australian Public Sector: Enhancing the Theory and Practice of Internal Witness Management in Public Sector Organizations*. Canberra: ANU Press.

Brown, A. J. (Ed.). (2018). *Whistleblowing: New Rules, New Policies, New Vision (Work-in-Progress Results from the Whistling While They Work 2 Project)*. Brisbane: Griffith University.

Brown, A. J., and Donkin, M. (2008). Introduction. In A. J. Brown (Ed.), *Whistleblowing in the Australian Public Sector* (pp. 1–22). Canberra: ANU Press.

Brown, A. J., Mazurski, E., and Olsen, J. (2008). The Incidence and Significance of Whistleblowing. In A. J. Brown (Ed.), *Whistleblowing in the Australian Public Sector* (pp. 25–52). Canberra: ANU Press.

Brown, A. J., Olsen, J., and Lawrence, S. (2018). Why Protect Whistleblowers? Importance Versus Treatment in the Public & Private Sectors. In A. J. Brown (Ed.), *Whistleblowing: New Rules, New Policies, New Vision (Work-in-Progress*

*Results from the Whistling While They Work 2 Project)* (pp. 27–52). Brisbane: Griffith University.

Dozo, N., Brown, A. J., and Lawrence, S. A. (2018). Whistleblowing in Public & Private Organizations: Types, Incidence, Variations. In A. J. Brown (Ed.), *Whistleblowing: New Rules, New Policies, New Vision (Work-in-Progress Results from the Whistling While They Work 2 Project)* (pp. 1–26). Brisbane: Griffith University.

Ebersole, D. (2011). Blowing the Whistle on the Dodd-Frank Whistleblower Provisions. *Ohio State Entrepreneurial Business Law Journal, 6,* 123–174.

Institute of Business Ethics. (2018). *Ethics at Work 2018 Survey of Employees (Europe)*. www.comresglobal.com/polls/institute-of-business-ethics-ethics-at-work-2018-survey-of-employees-europe/. Accessed 19 December 2018.

Griffith, S. J. (2015). Corporate Governance in an Era of Compliance. *William & Mary Law Review, 57,* 2075–2140.

Jubb, P. (1999). Whistleblowing: A Restrictive Definition and Interpretation. *Journal of Business Ethics, 21*(1), 77–94.

Kaptein, M. (2011). From Inaction to External Whistleblowing: The Influence of the Ethical Culture of Organizations on Employee Responses to Observed Wrongdoing. *Journal of Business Ethics, 98*(3), 513–530.

Knapp, D. E., Faley, R. H., Ekeberg, S. E., and Dubois, C. L. Z. (1997). Determinants of Target Responses to Sexual Harassment: A Conceptual Framework. *The Academy of Management Review, 22*(3), 687–729.

Lewis, D. (2011). Whistleblowing in a Changing Legal Climate: Is It Time to Revisit Our Approach to Trust and Loyalty at the Workplace? *Business Ethics: A European Review, 20*(1), 71–87.

Mesmer-Magnus, J., and Viswesvaran, C. (2005). Whistleblowing in Organizations: An Examination of Correlates of Whistleblowing Intentions, Actions, and Retaliation. *Journal of Business Ethics, 62*(3), 277–297.

Miceli, M. P., Near, J. P., and Dworkin, T. M. (2008). *Whistle-Blowing in Organizations.* New York: Routledge.

Miceli, M. P., Near, J. P., and Dworkin, T. M. (2009). A Word to the Wise: How Managers and Policy-Makers Can Encourage Employees to Report Wrongdoing. *Journal of Business Ethics, 86*(3), 379–396.

Miceli, M. P., Rehg, M., Near, J. P., and Ryan, K. (1999). Can Laws Protect Whistle-Blowers? *Work and Occupations, 26*(1), 129–151.

Miller, G. P. (2017). *The Law of Governance, Risk Management, and Compliance.* New York: Wolters Kluwer Law & Business.

Near, J. P., and Miceli, M. P. (1985). Organizational Dissidence: The Case of Whistle-Blowing. *Journal of Business Ethics, 4*(1), 1–16.

Near, J. P., and Miceli, M. P. (1995). Effective Whistle-Blowing. *The Academy of Management Review, 20*(3), 679–708.

Near, J. P., and Miceli, M. P. (2008). Wrongdoing, Whistle-Blowing, and Retaliation in the U.S. Government: What Have Researchers Learned from the Merit Systems Protection Board (MSPB) Survey Results? *Review of Public Personnel Administration, 28*(3), 263–281.

Near, J. P., Rehg, M. T., Van Scotter, J. R., and Miceli, M. P. (2004). Does Type of Wrongdoing Affect the Whistle-Blowing Process? *Business Ethics Quarterly, 14*(2), 219–242.

Olsen, J., and Brown, A. J. (2018). Preventing Detrimental Whistleblowing Outcomes: The Value of Risk Assessment and Proactive Management. In A. J. Brown (Ed.), *Whistleblowing: New Rules, New Policies, New Vision (Work-in-Progress Results from the Whistling While They Work 2 Project)* (pp. 89–108). Brisbane: Griffith University.

Smith, R. (2018). Processes & Procedures: Are Current Organizational Policies Linked to Better Reporter Treatment? In A. J. Brown (Ed.), *Whistleblowing: New Rules, New Policies, New Vision (Work-in-Progress Results from the Whistling While They Work 2 Project)* (pp. 67–80). Brisbane: Griffith University.

Stöber, T., Kotzian, P., & Weißenberger, B. E. (2018). Design Matters: On the Impact of Compliance Program Design on Corporate Ethics. *Business Research*, 1–42, https://doi.org/10.1007/s40685-018-0075-1.

Treviño, L., K., Weaver, G. R., Gibson, D., and Toffler, G. (1999). Managing Ethics and Legal Compliance: What Works and What Hurts. *California Management Review, 41*(2), 131–151.

Tsahuridu, E. (2011). Whistleblowing Management Is Risk Management. In D. Lewis and W. Vandekerckhove (Eds.), *Whistleblowing and Democratic Values* (pp. 56–69). International Whistleblowing Research Network. http://whistleblowers.dk/ArkivPDF/whistleblowing_and_democratic_values_3rd_jan(1).pdf. Accessed 17 December 2018.

Tsahuridu, E. E., and Vandekerckhove, W. (2008). Organizational Whistleblowing Policies: Making Employees Responsible or Liable? *Journal of Business Ethics, 82*(1), 107–118.

Vandekerckhove, W., Brown, A. J., and Tsahuridu, E. E. (2014). Managerial Responsiveness to Whistleblowing: Expanding the Research Horizon. In A. J. Brown, D. Lewis, R. Moberly, and W. Vandekerckhove (Eds.), *International Handbook on Whistleblowing Research* (pp. 298–327). Cheltenham: Edward Elgar.

Vandekerckhove, W., and Phillips, A. (2017). Whistleblowing as a Protracted Process: A Study of UK Whistleblower Journeys. *Journal of Business Ethics*, 1–19. https://doi.org/10.1007/s10551-017-3727-8.

Vandekerckhove, W., and Tsahuridu, E. (2010). Risky Rescues and the Duty to Blow the Whistle. *Journal of Business Ethics, 97*(3), 365–380.

Wortley, R., Cassematis, P., and Donkin, M. (2008). Who Blows the Whistle, Who Doesn't and Why? In A. J. Brown (Ed.), *Whistleblowing in the Australian Public Sector* (pp. 53–82). Canberra: ANU Press.

**Eva Tsahuridu (PhD, MBA, BBus)** is Associate Professor and Industry Fellow at the School of Accounting, RMIT University, Melbourne, Australia. Eva has been researching and teaching business and professional ethics for over two decades. She previously held academic roles in Australian and European Universities and most recently was the Manager of Accounting Policy and the Professional Standards & Governance Policy Adviser at CPA Australia; a Technical Adviser at the International Ethics Standards Board for Accountants and represented CPA Australia at the Australian Securities Exchange Corporate Governance Council. Eva's research interests include personal and organizational ethical conduct, whistleblowing, ethical and professional standards and anomie. She is the Section Editor of Practice in Business Ethics of the *Journal of Business Ethics* and the Convener of the Accounting Ethics Special Interest Group of the Australasian Business Ethics Network (ABEN).

CHAPTER 8

# The Skillset of an Effective Compliance Officer

*Maria Krambia-Kapardis*

## 1 Introduction

As Ramirez (2017) asserts, around the turn of the twenty-first century Congress acted aggressively in an attempt to empower attorneys and others to blow the whistle on wrongdoing. Many jurisdictions have enacted hard law in an effort to address wrongdoings, protect shareholders and act in the public interest. While effective legislation is necessary for preventing security risk corporations may face, the legislations (hard law) are becoming complex "making it difficult for regulatory authorities …to better understand the factors that challenge compliance" (Pok et al. 2014, p. 395). Compliance officers (CO) have expressed the view that a "clear set of guidelines or industry benchmark best practices could help" (p. 396) them in fulfilling their duties; however, adding to the complexity of regulation is the difficulty to assess human quality and culture (Goodhart 2005).

Despite the fact governments enacted hard law and, as Lancri argues in Chapter 4, soft law also gained momentum, financial crimes and corporate

M. Krambia-Kapardis (✉)
School of Management and Economics, Cyprus University of Technology, Limassol, Cyprus
e-mail: maria.kapardis@cut.ac.cy



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_8

collapses have continued to strike and affect countries, particularly in Europe. Pok et al. (2014) recommend that corporations establish a strong compliance culture which implies seriousness "on the part of officers while filling reports and the timely submission thereof… mitigating the problem of 'crying wolf'" (p. 399). It is apparent, therefore, that "rule observation has a tendency to improve with the degree of support, trust and fairness built into the organisation" (Engdahl 2014, p. 346) and, thus, the corporate culture has a major role to play in the field of compliance.

## 2 Corporate Culture

The corporate culture ought to be based on a code of compliance and ethics. DeGroot (2005) asserts that compliance effectiveness depends on ethical behavior, governance and legal compliance. Schlichting and Sutherland Cornett (2006) are in agreement with DeGroot who cite the "COSO Framework" developed by the Committee on Sponsoring Organizations of the Treadway Commission in an effort to argue that the foundations of the control environment of an entity begin with the "tone or overall attitude toward legal and regulatory compliance and ethics set by the CEO" (p. 33) and the governing body.

An ethical corporate culture can be empowered with diversity in an effort to "enhance sound risk management" (Ramirez 2017, p. 475), encourage heterogeneous work groups to resist groupthink and affinity bias (Levine et al. 2014) in an effort for superior compliance and ethics outcomes to be achieved (Phillips 2014) because social barriers will be broken down and enable speaking out against unlawful and unethical conduct (Ramirez 2017, p. 480). More specifically, cultural diversity in a corporation and in the field of compliance is important according to Ramirez in empowering diverse voices to be heard. Having diverse groups from different ethnic groups, gender, age build stronger relationships with key stakeholders, make better firm level decisions (Pandey et al. 2005) and will operate to positively influence compliance and ethics (Weeks et al. 1999). In fact, Dawson (1997) theorized that women approach ethics differently based upon gender socialization, thus Ramirez (2017, p. 471) goes on to assert that the "different approach women and minorities take to issues relating to risks also leads to more ethical behaviour and legal compliance… [which] lead to higher levels of corporate transparency." Given these findings in "ethical sensibilities and risk sensitivities," Ramirez suggests that business ought to consider

to "diversify in order to assure that its behaviour conforms to the ethical expectations of all its key constituencies" (p. 472). It is worth highlighting, however, that diversity will not ensure that the different voices will be heard if tokenism is in place, i.e., when only one female or minority employee is appointed the chances the diverse voice will not be empowered to give voice to his/her diverse perspectives and experiences. Thus, it is suggested a critical mass is needed to ensure diverse voices are heard so that diversity is embraced at the highest level of the firm.

As Brown and Treviño (2006) maintain, given that virtually every type of organization around the globe has encountered ethical scandals, the importance of an ethical dimension of leadership appears to exist. While research over the years has indicated that "personal traits such as integrity" (p. 597), linked to honesty, integrity and trustworthiness as well as cognitive trust have been associated with effective styles of leadership, Brown and Trevino argue that ethical leaders need to be credible role models, and demonstrate authentic, spiritual and transformational leadership. Once COs prove they are ethical leaders, they are likely to win the social exchange relationship (Blau 1964) and will gain legitimacy in the eyes of their constituents (Treviño et al. 2014, p. 186).

However, it is not enough to have an ethical corporate culture if the compliance department lacks the leadership skills and the ability to influence others, including the governing body. Thus, COs require not only the relevant knowledge and academic background, they also need interpersonal skills and the ability to understand the business as well as what motivates the people in the business in becoming an effective CO (Snell 2016). In an effort, therefore, for the COs to gain the skills required to become effective in achieving their and their company's goal, the next section will suggest a number of strategies.

## 3 Road Map to Being an Effective Compliance Officer

It is suggested by Grant-Hart (2016a, b) that in order for the CO to becoming effective strategic COs, they need to follow a number of strategies starting from the general corporate stage and moving onto specific individual empowering skills.

The *first strategy* goal in becoming an effective CO, one needs to utilize what Grant-Hart (2016a) refers to as four primary motivators which will enable the CO to gain effective training and communication skills.

These four primary motivators are: (a) fear for self; (b) fear for the business; (c) noble cause; and (d) competitive edge.

*Fear for self* relates to the avoidance of personal pain or difficulty. According to Henning (2015), Lanny A. Breuer, the former assistant attorney general in charge of the criminal division of the department of justice, noted that: "the strongest deterrent against corporate crime is the prospect of prison time for individual employees." Most people in the corporate world consider themselves unlikely to be involved in criminality. They think big fines happen to someone else, and even if the company is fined, nothing will happen to them. Many people are primarily motivated by fear for self. Since the science of persuasion asserts that people are most affected by stories of individuals most similar to themselves, when dealing with those motivated by fear for self, it is critical to engage them using stories of someone similar to themselves. Grant-Hart (2016a) recommends using whenever possible, a story of someone of the same age, gender, position in the company (manager, regular employee, board member, etc.), or in the same industry. She also suggested that telling real and specific stories brings home the risk to the individual. Similarly, in using big number fines and trends in jail time—which always seem to be increasing, not decreasing—intensifies the impact of one's stories, particularly when the trainer deliberately looks people in the eye during training and addresses the potential of imprisonment. By making the threat real and personal, employees are much more focused on policies because they understand the personal cost of failure. Another suggestion is to warn people that they can be personally extradited for trial and imprisonment in other countries for violations of bribery and competition laws. For many, the shock is palpable because they didn't know that, but once they do, they will always be aware of the personal risk. Furthermore, people connect with compliance when they internalize the answer to "What's in it for me?" Does it affect their: (1) job, (2) freedom, and (3) future at the organization.

The second primary motivator is *fear for the business*. This motivation centers on avoidance of problems in the business. Most business leaders love the business in which they work. Top executives, creators, owners and board members do not want to see the reputation of their company sullied by news reports of illegal conduct. More importantly, they don't want to slash the budget and their bonuses so they can pay huge fines to the government for corporate wrongdoing. Like fear for self, people motivated by fear for the business are best reached by stories

of businesses similar to the one in which they work. To be most effective, one will want to find stories of businesses in serious trouble that are related to their business. Fines can be very expensive, increasingly in the billions for serious violations. Fear for the business can really be ramped up when CO describes to the employees the multiple types of sanctions that can be applied. For instance, the CO can describe the difference between criminal fines and civil fines, class action lawsuits and private plaintiff lawsuits, etc. If the CO is in a publicly traded business, and his/her country allows shareholder derivative suits, the CO can explain the devastation a multiyear battle with the shareholders can cause. COs can also describe the knock-on effect many laws have if a multinational operation is involved. For instance, knowledge that activities in another jurisdiction can implicate the company in bribery or corruption allegations can scare even the most hardened CEO. In addition, if the CO works for a company that has government contracts, explaining that the company could be debarred or not allowed to bid on government contracts in the future, can be a great incentive to create buy-into the compliance program from the business.

Fear for the business and fear for self can interrelate even though they touch different motivations thus, one can use many stories for both purposes. If there is a case about a business that has gotten in trouble, by digging deeper, one will find a story or two about individuals in the business who suffered at the same time as the company and there will be individual penalties. Stories like these emotionally connect to people with fear-based motivations, which can help the CO to be wildly effective when presenting solutions to the problems faced by the company.

The third motivation relates to the *noble cause of the corporation* such as pride in corporate social responsibility, and/or in being the most ethical company possible. The noble cause of corporations is also highlighted by Krambia-Kapardis (2016) in her holistic model for preventing fraud and corruption who asserts that: (a) the individuals require ethics and moral fiber, (b) the corporation ought to introduce ethical programs, be corporate socially responsible and implement the governance principles, and (c) the community should encourage civil society participation, the government and politicians ought to be politically accountable and, finally, ethics should be incorporated in the curriculum of primary, secondary and tertiary education.

For some companies in the business community, connecting to the ideals of corporate social responsibility and ethical business is a strategic

goal. Many companies, such as Starbucks (2018) or TOMS Shoes (Fritz 2018), use their ethical business credentials or the fact that they are members of the United Nations Global Compact, as a mandate and a marketing element. By working for a company with corporate social responsibility or ethical business as part of its identity or marketing, things may be easier in selling compliance as part of the corporate mission. A company with an espoused ethos of positive governance is much more likely to be compelled to protect its reputation and the reputations of its employees, by complying with all laws and regulations. Likewise, by working with individuals or business leaders who hold themselves to high ethical standards and believe that complying with the law is simply the right thing to do make compliance achievable. If one is employed in a company or with people who are motivated by a noble cause, he/she should work to inspire them to be their best selves when it comes to complying with the law and to instill in them the sense of purpose that can change the world. People motivated by noble cause will respond most strongly to stories where the company is put in the spotlight as one to emulate and admire. Compliance professionals should focus on finding storylines where the business is seen to be doing more for the world, or being at the forefront of the most ethical business within the industry, country or environment in which the business operates. People motivated by noble cause like to imagine their company is a shining beacon on the hill. They want their company to be the benchmark against which other companies compare themselves. By using this motivator, CO can illustrate how much better the company could be with continued compliance investment and improvement.

The fourth primary motivator is the *competitive edge* which centers on winning business through the use of compliance as a business advantage. Many sales people can be lured onto the side of compliance when motivated by winning business through the use of competitive edge. Compliance, good governance and proper procedures can be a business advantage. If there hasn't yet been a scandal in the relevant industry or region of the world, there will be eventually. Because multinational corporations are frequently the ones concerned with compliance and procedures, CO can inform business units that ethical business and a good compliance program is the best way to position one's business to win large contracts. Additionally, world governments are more and more frequently requiring compliance programs and supply chain compliance as part of their criteria for awarding contracts. In the USA, for instance,

government contracts must have compliance provisions throughout the supply chain to ensure that no forced labor is utilized. If a company has a powerful compliance program in place, new regulations are less likely to disrupt business. In order to effectively use competitive edge, CO should tell stories of similar companies in the same industry or aligned industries that won contracts or business because of the strength of their compliance program.

Once the CO identifies the primary motivators of the company he/she works in, he/she would need to then identify the power sources in an effort to use them effectively. Grant-Hart (2016a) advocates that in every business, family, group of friends or NGOs, there are two sources of power—the named power and the covert power. The named power is the obvious source of authority. In business, the named power is almost always the manager, Chair of the Board, the chief executive officer (CEO) and the members of the Board of Directors. The second source of power is the covert power. Covert power tends to come from people who are highly charismatic, well-connected or long-established within the company. Whenever one is in a room with the business managers, it is suggested he/she looks around to see who has covert power. By observing the responses of the listeners to the person who is talking, identifying the source of power is easy. The comments of some people are quickly dismissed or ignored, while those of others are carefully considered. One can also determine who has covert power by noting the people who are consistently chosen to lead important projects. People with covert power are incredibly important resources. By connecting with those with covert power so that they become compliance believers, one will have a much better likelihood of success.

In becoming an effective CO, it is suggested one connects with and obtains buy-in from both the people with named power and covert power. People with covert power who believe in the compliance mission will carry compliance ideas into their meetings and processes since they are natural leaders, others will follow their lead. It is also suggested CO establish their role so that they can have a direct line of reporting to the top power sources, usually including both the CEO and the Board of Directors. Having direct access will allow CO to perform their job at the highest possible level, without interference or screening by the business or the general counsel.

Once the CO has identified the primary motivators and the power of sources he/she ought to leverage the primary motivator with the

power sources. Each company will have a dominant primary motivator, and each individual within a company will also have a primary motivator. Companies tend to attract people with similar primary motivators. To be most effective, one must leverage both the primary motivator of the company and the primary motivator of each individual power source. In doing so, however, it is required that one finds the primary motivator of the business, firstly by looking at how the company portrays itself in its marketing. One may start by reviewing the company's Web site. Does the company promote its ethical credentials and sustainable business objectives? If so, it implies that the company probably has an overriding primary motivator of noble cause. If, for instance, the company's press releases are dominated by sales figures and descriptions of how they beat the competition, then the company's primary motivator is probably competitive edge.

A company's choice of values can also give a strong indication of the primary motivator of the business. Does the company espouse collaboration and integrity as its values? Or does it value cutting-edge technology and maintaining shareholder profitability? Another way to determine the primary motivator of one's company is to review what they publish or write, both in internal and external communications. What is the story behind the company? What is the story the company is trying to sell? Some companies position themselves as the most ecological in the business, or the most "green." Companies with this sensibility are more likely to have power sources that respond to noble cause as their primary motivator.

Once the primary motivators are identified and applied to the business, it is feasible to identify the primary motivator to favor in the CO's training. Given people tend to join a company that speaks to their own personal values and motivations; the primary motivator of the company is likely to be reflected in the majority of the people working at the company. To get to the next level, however, one will need to reach each power source individually with their individual primary motivator.

Thus, the next step (according to Grant-Hart 2016a, b) relates to finding the primary motivator of each power source. The Chair of the Board of the company may have a different primary motivator than the members of the Board. Although many boards have a group primary motivator, if one is able to spend time with each member of the Board, one may find that each has a different primary motivator. Therefore, how does one figure out the primary motivator for each power source? The first way is to

watch carefully during training sessions to see which slides or stories seem to have the greatest effect on each power source. Some power sources visibly wince when stories are told of executives being indicted or extradited to face trial. Others will become engaged when the CO speaks of competitive edge in his/her training. A primary reason to include slides with all four primary motivators in the CO training is so that one can study the power sources to see what they respond to by watching carefully when the trainer tells stories of executives going to jail or losing their jobs during your training. Does the leader fidget, look down, sigh or roll his or her eyes? As more and more compliance investigations and scandals strip executives of their jobs, more executives are motivated by fear for self. Fear for self can be a major motivator to get the leader to buy into the CO's vision.

Once the CO has figured out the primary motivators for the power sources of his/her entity, it is suggested by Grant-Hart (2016b), he/she moves on to *strategy two* which relates to knowing were the company's program *really* is on the compliance wave. The CO with some years' experience in compliance will notice that there is a trend whereby the investment in ethics and compliance fluctuates and follows a cycle. Understanding that cyclic nature helps one to understand the stage at which their organization is at and predict the next phase. According to Grant-Hart (2016b), the compliance cycle comprises four phases:

1. Phase one refers to an investment period during which a corporation has ceased investing in compliance or has never had such a program, often because the need for compliance is not appreciated or is not considered a serious one.
2. Phase two describes the crisis phase which unavoidably comes about because of the lack of investment and insufficient attention paid to compliance. In such cases, company management is shocked at the discovery of an unethical behavior, or a serious fraud or an allegation of bribery by an employee or a partner or a third party which comes to their attention. In response, companies start to invest heavily in compliance utilizing consultants and legal firms, largely out of a fear of the likely consequences if the media discover the "story."
3. Phase three is the stability phase, whereby with the crisis now behind it, a stable compliance budget is provided and additional such budget is carefully examined to the satisfaction of COs. This is the best time to be in a compliance department.

4. Phase four is when the crisis experienced is a distant memory; in otherworld's it is the forgetting phase where there may have been a change of management and employees are tired with compliance. Consequently, there is hardly any budget or investment in compliance.

As Grant-Hart (2016a) reminds her readers the four-phase cycle begins again as phase four is succeeded by phase one. Understanding the cycle helps one to maintain a consistent positive approach to compliance and to address crisis periods.

Having become well acquainted with the power sources, power motivators in strategy one and knowing where the company's program really is in strategy two, it is time to move on to *strategy three* which relates to the actual work of the CO. The compliance industry has an unusually high level of burnout. Many conferences showcase experts giving information about stress relief, work-life balance and how to counteract the negative experiences that working in compliance can bring. Some of these emotions may be feeling defeated, blamed, misunderstood, unappreciated, hostile and bored. There will unquestionably be days in the life of a CO where the skies are gray and the tide is against him/her. According to Grant-Hart (2016a), many COs experience setbacks like the following:

- *Defeat*: Compliance officers frequently need to fight for resources and support from the business. Sometimes an initiative will not be backed, or a policy decision will go the wrong way. It is easy to feel defeated when this occurs.
- *Blame*: The job of a CO was once described to Grant-Hart as, "You're the person who makes sure the trains run on time. No one notices when the train is on time, but when it is late, people throw a fit!" When executives, managers or employees go through disciplinary actions for violating the rules, they often blame the compliance department or the CO specifically, for their problems. The CO may experience shame or regret, even when he/she was doing the right thing.
- *Feeling Misunderstood*: As Fanto notes in Chapter 3 of this book, in many countries and industries, compliance is a brand new profession. People within the CO's family, social or even work circle may not know what the CO's work duties and responsibilities are. Being misunderstood can lead to feeling unimportant.

- *Under-appreciated*: Many projects completed by a CO are not outwardly appreciated. Registering and implementing a whistle-blower hotline throughout Europe is a major feat, yet it is unlikely to be met with enthusiasm because businesses rarely think about celebrating compliance successes.
- *Hostility*: When a new regulation or program is implemented, some business leaders may openly object to the controls the CO puts in place. Stories abound of COs trying to do the right thing and being suppressed or even fired.
- *Boredom*: When a compliance program is up and running, it can feel like every day is the same. Boredom can set in, and burnout may follow.

When these emotions take over from time to time, it is helpful to step back and remember the CO and his/her department's mission. When feeling really down, it is important to take the global view and remind oneself that the compliance professional makes the world a better place. COs are leveling the playing field for the small businessman or woman in an emerging market, because due diligence procedures are making corruption less rampant and rewarding companies with a reputation for fair dealing. COs are making the world a better place by ensuring that a company abides by fair labor standards, and that supply chain audits occur to eliminate any possibility of the company engaging in modern-day slavery, or working with companies that employ forced labor.

When a CO feels defeated, it may be worth remembering that each tiny action in the compliance space alters the corporate landscape in a way that is changing the world. The tiny little actions a company takes are made in concert with the actions of millions of other companies throughout the world. Companies, NGOs and governments are changing the world, and the CO is on the front lines of this change. It is up to the CO to create the mechanisms, policies and procedures that protect his/her company from prosecution, but these same mechanisms, policies and procedures make the world a better place to live in for millions. When it all feels like it is going wrong, it may be worth remembering that COs are making a difference by being on the side of law and ethics. Connecting to the underlying mission is critical.

*Strategy four* relates to the specific skills the CO ought to possess in order to make him/her effective. These skills are:

- COs must "hear and be heard" (Grant-Hart 2016a, p. 59). It is critical for a CO to be heard by the Board and by his/her co-workers and other employees in the entity, otherwise his/her legitimacy may be questioned. At the same time, a CO ought to acquire the skills of being a good listener and ought to invite people to talk to him/her. Grant-Hart (2016a, p. 61) suggests when employees wish to talk to the CO "let them talk 70% of the time" because doing so will create a desire in that person to listen back to the CO. A final point on the issue of talking and listening is knowing when to stop talking says Grant-Hart, 2016a.
- Establish goals and expectations and frequently re-evaluate the progress made in meeting them. Grant-Hart (2017) alerts that at the end of the year, COs will be measured against their progress and the goals they have agreed to achieve. However, it is normal that during the year one forgets the goals articulated at the beginning of the year as he/she is inundated with other things. Therefore, in ensuring the CO does not lose the trust of the management he/she ought to set his/her expectations and goals, communicate them to management and set a plan for accomplishing them even when a crisis strikes.
- Empathy and compassion are often required in humanizing oneself with the business (Rakel 2018). A CO ought to learn to connect to the businesses on a human level (Grant-Hart 2018). Brown (2013) reminds us that by showing vulnerability and learning to be compassionate with the employee's concerns, it will create a connection with them on a human level and they are likely to seek advice and acknowledge the work of the CO as legitimate. In an effort to be a relationship person, Lafferty (2010) recommends that the CO: (a) tries to see the mutual benefit in situations by thinking and promoting "win-to-win," (b) seeks to understand before he is understood, and (c) creates synergies with other employees to accomplish the corporate goals.
- Particular attention ought to be paid to the "critical role that gullibility, loyalty and dependency relations among employees" play in ensuring that COs do not become too close to one another which will prevent them from fulfilling their watchdog role and responsibility to review, approve and overall ensure compliance of employees (Engdahl 2014, p. 332).
- DeGroot (2005) suggests that the CO: (a) ought to be one who has the ability to deliver "bad news" to the Board and not be an

introvert who may refrain from delivering unwanted news or one who is a boisterous person and creates toxicity and controversy; establishes; (b) sets boundaries and says no effectively and is respectful of employees regardless which level they are; and (c) has the ability to analyze the big picture, understand the regulations and be able to foresee the consequences based on action or lack of action.

Over and above the skills and knowledge required of COs, Lafferty (2010) argues that COs ought to "focus first in [their] personal values and then [their behavior]" (p. 11). In an effort to achieve this, Lafferty argues that COs ought to:

1. value values and understand that they ought to *see the "iceberg"* before it sinks the Titanic. As Lafferty (2010) asserts, it was not the iceberg that sunk the Titanic but the mere fact that the iceberg was not seen early enough to prevent the catastrophic outcome, thus CO ought to be able to identify the red flags or the iceberg before it is too late;
2. begin with the end in mind by understanding the basic framework of compliance and ethics program and how to adapt it to fit any organization "as part of the overall goal of promoting a culture of ethics and compliance with the law" (p. 12);
3. focus on the small stuff, on the "broken window" in the organization before it becomes "big stuff" (p. 14);
4. be always prepared in mind by having disciplined yourself to be obedient to every order and, situation that may occur thus develop written policies and procedures on critical aspects of compliance and ethics and empower the employees to do the same; and
5. learn to live on less than earned and learn to seek advice from competent experts because this will provide the ability and courage to apply Socrates famous word "I know one thing, and that is that I know nothing."

However, there is a limit to how much a competent, effective CO can achieve and the full support of the Board is imperative in this context. The Board ought to demonstrate it possess the political will to provide the necessary resources, support and overall appreciation for the work carried out by the compliance department.

## 4 Corporate Commitment to Compliance

While the corporate culture may empower the compliance culture of the entity to thrive and the CO may have the skills, knowledge and ability to empower compliance and be an effective CO, there is one more ingredient needed to ensure the success of compliance. The Board ought to have the political will to provide the necessary resources to the compliance department. Engdahl (2014) argues that the primary issue is "whether the organisation provides enough support, resources and incentives for the individuals concerned to ensure their proper functioning in the everyday" (p. 333). Brown (2010) recommends that an executive compliance committee charter is introduced where a strong message is sent by the governing body that the organization is "committed to compliance with laws, regulations, and ethical corporate and individual conduct" (p. 38). The corporate commitment to compliance ought to be evident, clear, transparent and apparent in theory and practice. The governing body ought to align compliance initiatives with organizational priorities by "walk the talk" in an effort to establish trust, credibility and affect change. This is also confirmed by Schlichting and Sutherland Cornett (2006) who suggest that the corporation illustrates its commitment to compliance thorough clear and visible communication and involvement.

## 5 Conclusion

The major role corporate culture has to play in the field of compliance cannot be overemphasized. At the same time, it is acknowledged that a CO needs to possess certain skills in order to be effective and strategic. Drawing on Grant-Hart (2016a), attention has focused on four interconnected strategies to that end. The first strategy evolves around four primary motivators—fear for self (i.e., avoidance of personal pain or difficulty), fear for the business (i.e., avoidance of problems in the business by learning from the mistakes of similar business to the one in question), noble cause (i.e., pride in corporate social responsibility and/or in being the most ethical company possible) and competitive edge (i.e., winning business through the use of compliance as a business advantage). Once the CO has figured out the primary motivators for the power sources (both named and covert) of his/her entity, he/she would need to identify the power sources in an effort to use them effectively.

Embracing next the second strategy means knowing where the company's program really is on the four stages of the compliance wave, i.e., low investment stage, crisis stage, stability and forgetting stage. The reality is, of course, that the actual work of an effective CO is a mixed blessing, hence the third strategy equips the CO to deal with the experience of defeat, blame, feeling misunderstood, under-appreciated, hostility and boredom. In addition, a number of specific skills the CO ought to possess in order to be effective as well as the importance of focusing first on one's personal values and behavior have been discussed. Finally, it is emphasized that there is a limit to how much an effective CO can achieve in a company and it is absolutely essential that the Board has the political will to provide the necessary resources to the compliance department.

**Acknowledgements** The author would like to thank Kristy Grant-Hart for her invaluable contribution to the International Conference on Compliance in Cyprus in June 2018 as well as for her approval to make use of some of her publicly available work in the area.

## References

Blau, P. M. (1964). *Exchange and Power in Social Life*. New York: Wiley.

Brown, J. (2010). Compliance Effectiveness: How Do We Get There? *Journal of Health Care Compliance, 12*(4), 37–38 and 63.

Brown, B. (2013). *The Power of Vulnerability: Teachings of Authenticity, Connection and Courage*. Louisville: Sounds True Inc.

Brown, M. E., and Treviño, L. K. (2006). Ethical Leadership: A Review and Future Directions. *The Leadership Quarterly, 17*(6), 595–616.

Dawson, L. (1997). Ethical Differences Between Men and Women in the Sales Profession. *Journal of Business Ethics, 16* (11), 1143–1152.

DeGroot, S. Y. (2005). What Makes an Effective Compliance Officer? *Journal of Health Care Compliance, 7*(3), 55–56.

Engdahl, O. (2014). Ensuring Regulatory Compliance in Banking and Finance Through Effective Controls: The Principle of Duality in the Segregation of Duties. *Regulation and Governance, 8*, 332–349.

Fritz, J. (2018). *Lessons in Corporate Social Responsibility from TOMS* (Shoes). https://www.thebalancesmb.com/lessons-from-toms-shoes-2502511. Accessed 14 November 2018.

Goodhart, C. (2005). An Incentive Structure for Financial Regulation. In C. Goodhart (Ed.), *The Emerging Framework of Financial Regulation*. London: Central Banking Publications.

Grant-Hart, K. (2016a). *How to Be a Wildly Effective Compliance Officer*. London: Brentham House Publishing Company.

Grant-Hart, K. (2016b). *Writing the Compliance Way*. https://www.compliancekristy.com/blog/2016/10/16/riding-the-compliance-wave. Accessed 24 November 2018.

Grant-Hart, K. (2017). *The Secret to a Long & Successful Career as a Compliance Officer*. https://www.navexglobal.com/blog/article/secret-long-and-successful-career-compliance-officer/. Accessed 14 November 2018.

Grant-Hart, K. (2018). *10 Top Ways to Be a Wildly Effective Compliance Officer*. https://www.navexglobal.com/blog/article/10-top-ways-be-wildly-effective-compliance-officer/. Accessed 10 November 2018.

Henning, P. J. (2015). The Prospects for Pursuing Corporate Executives. *The New York Times*, 14 September 2015. https://www.nytimes.com/2015/09/15/business/dealbook/theprospects-for-pursuing-corporate-executives.html. Accessed 14 November 2018.

Krambia-Kapardis, M. (2016). *Corporate Fraud and Corruption: A Holistic Approach to Preventing Financial Crisis*. London: Palgrave Macmillan.

Lafferty, L. T. (2010). The Habits of Highly Effective Compliance Officers. *Journal of Health Care Compliance, 12*(6), 11–16.

Levine, S., Evan, P., Apfelbaum, M. B., Valerie, L. B., Edward, J. Z., and David, S. (2014). Ethnic Diversity Deflates Price Bubbles. *PNAS, 111*(52), 18524–18529, 30 December 2014. https://doi.org/10.1073/pnas.1407301111. Accessed 14 November 2018.

Pandey, V. K., Shanahan, K. J., and Hansen, S. W. (2005). The Relationship Between Shareholder Wealth Effects, Diversity and Publicity as a Marketing Strategy. *Journal Academy Marketing Science, 33*, 423. https://doi.org/10.1177/0092070305277384.

Phillips, K. W. (2014). How Diversity Makes Us Smarter. *Scientific American, 311*(4). https://www.scientificamerican.com/article/how-diversity. Accessed 10 November 2018.

Pok, W. C., Omar, N., and Sathye, M. (2014). An Evaluation of the Effectiveness of Anti-money Laundering and Anti-terrorism Financial Legislation: Perceptions of Bank Compliance Officers in Malaysia. *Australian Accounting Review, 71*(4), 394–401.

Rakel, D. (2018). *The Compassionate Connection: The Healing Power of Empathy and Mindful Listening*. New York: W. W. Norton & Co.

Ramirez, S. A. (2017). Diversity, Compliance, Ethics and In-House Counsel. *University of Toledo Law Review, 48*(3), 465–483.

Schlichting, N. M., and Sutherland Cornett, B. (2006). Tone at the Top: The Foundation of an Effective Compliance Program. *Journal of Health Care Compliance, 8*(4), 33–34; 70–71.

Snell, R. (2016). It is Difficult to Be a Highly Effective Compliance Professional Without Interpersonal Skills. *Journal of Health Care Compliance, 18*(1), 31–34.

Starbucks. (2018). *What Is the Role and Responsibility of a For-Profit, Public Company*? https://www.starbucks.com/responsibility. Accessed 11 November 2018.

Treviño, L. K., de Nieuwenboer, N. A., Kreiner, G. E., and Bishop, D. G. (2014). Legitimating the Legitimate: A Grounded Theory Study of Legitimacy Work Among Ethics and Compliance Officers. *Organizational Behavior and Human Decision Process, 123*(2), 186–205.

Weeks, W. A, Moore, C. W., McKinney, J. A., and Longenecker, J. G. (1999). The Effects of Gender and Career Stage on Ethical Judgement. *Journal of Business Ethics, 20*(4), 301–313.

**Maria Krambia-Kapardis (PhD, MBus, BEc, CFE, FCA)** is an Associate Professor of Accounting, Cyprus University of Technology, a fellow member of the Chartered Accountants of Australia and New Zealand and a Certified Fraud Examiner. For a number of years, she was a university academic in Australia, has been a Visiting Scholar at Cambridge University; Girona University, Spain; and Visiting Professor at Victoria University, Melbourne, Australia. She was the founder and first Chair of Transparency International-Cyprus (2010–2017), for a number of years served as the country corruption correspondent for the European Commission, was the founder and first president of the Economic Crime and Forensic Accounting Committee of the Institute of Certified Public Accountants of Cyprus (2010–2014) and she is a member of the disciplinary body of the Institute of Certified Public Accountants of Cyprus. She has authored a number of books, articles in peer-reviewed journals and presented her work at international conferences. Her research interests include: fraud detection, investigation and prevention; anti-corruption; corporate responsibility; corporate governance; gender issues in business; and ethical behavior. She has been the local coordinator for a number of EU–funded projects. In 2015, she was awarded two best paper awards by Emerald for her articles on corruption. Krambia-Kapardis is on the editorial board of a number of peer-reviewed journals, has been the examiner of a number of PhDs overseas and in 2017 was commissioned by the Cyprus Ministry of Justice and Public Order to author a Report on Anti-Corruption Agencies. Finally, in 2017 the Gold Business Magazine named her one of the 100 most powerful and influential women in Cyprus and was also awarded the ACFE's 2019 Achievement in Outreach/Community Service Award for being an active contributor to her community and for being committed to helping improve the quality of life where she lives and works.

CHAPTER 9

# Disentangling the Expectation Gap for Compliance Officers

*Maria Krambia-Kapardis, Salomi Dimitriou and Ioanna Stylianou*

## 1 Introduction

Regulation, compliance, and control are terms currently employed and highlighted in the "audit society" (Power 1997), rooted in the newly founded focus on compliance displayed by various companies as well as the current view of public administration as a "regulatory state" (Perezts and Picard 2015). Even though it is now recognized by most, if not all, as an essential requirement of today's business, compliance was previously almost regarded as a dirty word (Edwards and Wolfe 2005).

Treviño et al. (2014, p. 190) state that the first ethics and compliance officers (COs) emerged in the defense industry in the mid-1980s

M. Krambia-Kapardis (✉) · S. Dimitriou
Cyprus University of Technology, Limassol, Cyprus
e-mail: maria.kapardis@cut.ac.cy

S. Dimitriou · I. Stylianou
University of Central Lancashire Cyprus (UCLan), Pyla, Cyprus
e-mail: IStylianou@uclan.ac.uk



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8_9

following a loss of confidence in its integrity. However, Snell (2015) asserts there were some "compliance activities" by the early 1990s, but there were very few organization-wide, comprehensive compliance programs established prior to that. Irrespective of whether the compliance profession emerged in the 1980s or 1990s, it is safe to say there was a general resistance to implementing compliance programs. Weber and Fortun (2005) noted that compliance is "coming of age as a field of legal practice, as a subject taught in law schools, and as a field of research and analysis by academics" (Miller 2017, p. 437).

The 1980s experienced a "wave of deregulation and privatization" which paradoxically led to even more regulation than before, both by the State but, also, by independent, self-regulatory initiatives (Parker and Nielsen 2011). Today, there seems to be a strong emphasis on legal compliance emerging from a strong standardized or ethical motivation that leads to the creation and maintenance of an organization's ethics and or compliance program (Weber and Wasieleski 2012). A "control of control" is currently in operation where supra-surveillance is employed (Power 1997). As a result, states and governments are increasingly relying on insider help from organizations and businesses in the form of "internal responsibility, accountability, and risk management control" (Perezts and Picard 2015, p. 834), to fight criminal activity, while highlighting the benefits that compliance can bring to the organization. The idea found behind this widespread acceptance and acknowledgment of "compliance" is the realization that "good people do bad things if they are put in an environment that does not value values" (Lafferty 2010, p. 12). Therefore, compliance aims to create business environments that are resistant to misconduct and, most importantly, to criminal behavior and activity.

The existence of unethical activity continues to exert a heavy toll on organizations (Schminke et al. 2014). These effects range from reputational damage, loss of public confidence or even financial and material damages. Compliance has added greatly to the awareness of these risks by both management and other employees and can now be seen as an important way to manage and minimize the above-mentioned risks of a financial institution (Verhage 2009). Governments all around the world have responded to the increase of financial crimes, including money laundering and the financing of terrorism, through the implementation of the expansion of various regulations and the development of compliance departments (De Dios 2016).

Compliance programs carry a strong sense of ethical responsibility which is coupled with a keen awareness of the importance of complying with internal and external laws and regulations to allow for the smooth and effective operation of the organization (Weber and Wasieleski 2012). Studies present the following, as the two most important goals of compliance:

1. To prevent the organization from getting involved in criminal activities, and
2. To protect the organization against reputational damage (Verhage 2009).

Furthermore, the impact of compliance programs includes being legal or compliant, avoiding financial costs (through fining and fraud) and creating and maintaining an ethical organizational culture. Some of the challenges faced by the COs concern criminal activities and more specifically in reference to anti-money laundering and corruption.

Nowadays, there seems to be a blurring of the line of normal and corrupt activity (Harvey 2004). Corruption, as a widespread issue, seems to be affecting all societies in varying degrees and at different times (Baldock 2016). Corporations currently aware of the extent of this issue implement compliance programs and departments which aim, among other things, to ensure that the company's actions and transactions remain legal and legitimate and do not in themselves contribute or are exploited for criminal activity (De Dios 2016). Among the most significant criminal activities that can be caused by an organization's lack of compliance is that of money laundering.

Money laundering, which is defined as the "process in which assets obtained or generated by criminal activity are moved or concealed to obscure their link with the crime" (Verhage 2009, p. 9), has increasingly received attention during the last two decades, both from policymakers as well as national and international organizations. This criminal phenomenon is depicted as a major criminal threat to society and its economy. However, it is not possible to measure accurately the volume and extent of money laundering activity that is taking place (Harvey 2004), nor is the purpose of the paper, yet it is worth noting that the United Office on Drugs and Crime (UNODC 2018) has estimated that laundered money globally in one year is 2–5% of global GDP, or 800 billion—2 trillion in current US dollars.

The battle against money laundering has become an international priority. Private institutions are now entering the global struggle against crime, through the employment of inspectors, the COs, whose duty is to enable the institution to comply with anti-money laundering regulation (Verhage 2009). This employment position which has evolved over the years is now considered globally a legal obligation. Financial institutions, accounting, and legal firms as well as those providing administrative services are required to have a compliance department. The CO is now responsible to supervise compliance of the organization he/she is working in, in an effort to ensure that management and employees comply with the rules, regulations, and codes of conduct applicable to that particular sector and entity. COs are expected to report suspicious transactions as well as "develop programs to fight money laundering…. [including] employee training" (Gibeaut 2002, p. 50).

While some suggest that the threat for money laundering is being exploited to serve as a convenient motive for policymakers to implement far-reaching regulations and guidelines without raising opposition (Verhage 2009), others argue that "the main aims of combating money-laundering is to maintain the integrity of [the] financial institutions" (Van Duyne 1998, p. 370). In 2001, anti-money laundering entered the top of the list as one of the most important tasks of the CO's mandate (Verhage 2009) but another very significant job responsibility for CO is that of creating an ethical culture and climate that will allow for the field of compliance to develop and flourish within a business (Greenberg 2009). Others argue that due to the complex regulation and guidance, the focus has shifted from money laundering prevention towards compliance (Harvey 2004), integrity and ethics (Aznar and Vaccaro 2015).

## 2 The Compliance Program

Compliance is considered to be a relatively young profession (Mills 2008), that has exploded in the first decade of the twenty-first century. Miller (2017) has argued that while COs "tended to work in cubicles and performed a sort of glorified bookkeeping task, making sure that forms were filled out and boxes checked" (p. 437) today compliance is a "vibrant field for hiring and a desirable career option" (p. 438). The "Compliance Officer" (CO) is now listed as the No. 20 best business job according to some sources (Grant-Hart 2016) while the predictions demonstrate a rise of 4.6% of the occupation by 2022 (ibid.). Even though the average department size for a compliance department is six employees (Weber and

Fortun 2005), compliance is considered to be everyone's job. Businesses have been currently investing a lot of money in formal compliance and ethics programs, having realized the significance of such programs (Weaver et al. 1999). For compliance to work, it needs to be part of a united effort, starting from the highest stratum of the organization all the way to the frontline personnel; it needs to be part of the organizational culture. The compliance team can offer its guidance and advice, but in order to work, the program needs to be understood and accepted by all.

Considering next the concept of compliance is the "adherence by the regulated to rules and regulations laid down by those in authority" (Edwards and Wolfe 2005, p. 48). Yet, compliance is not only about adhering to the letter of the law but also adhering to the spirit of the law, which leads to the creation of an ethical and compliant organizational culture. The term compliance includes concepts of "obedience, observance, deference, governability, amenability, passiveness, non-resistance and submission" (ibid.). Furthermore, Edwards and Wolfe assert that compliance includes aspects of duty, of doing the right thing versus doing the wrong thing, of moral obligation and accountability, of acting morally and ethically. Thus, compliance programs foster a control orientation within a corporation through the focus on rules, discipline, and monitoring (Weaver et al. 1999). Therefore, compliance personnel need to ensure that all aspects of organizational requirements and regulations are being managed properly, consequently making compliance an oversight function (Gnazzo 2011; Mills 2008).

Martin (2015, p. 171) suggests that compliance is a procedure of going beyond "developing and implementing processes and procedures" but one addressing the business model risk. Thus, COs' work requires:

1. Sufficient **accountability to be provided** to the CO to enable him/her to carry out his/her responsibilities;
2. Adequate **independence** to allow the CO to point toward areas of concern without worrying about conflict of interests or the fear of reprisal;
3. **Connection to company operations** to assist for the execution of an ethical culture that advances the overall objectives of the business; and, finally,
4. Ample **authority** to empower the CO to make decisions and recommendations that will be acknowledged at all organizational levels (Kavanagh 2008).

On the other hand, non-compliance behavior can be defined as "risk taking behavior, deliberate or not-deliberate, by insiders or employees who ignore an organization's (security) policies and guidelines" (Dols and Silvius 2010, p. 12).

Thus, compliance is being seen as a social construction, where formal compliance systems and management of an organization interact with individual beliefs and attitudes to create what we now recognize to be a "compliance culture" (Parker and Gilad 2011). Generally, compliance programs are expected to enhance an organization's reputational capital, promote an ethical workplace for all employees, contribute to the delivery of high-quality services (Brown 2010; Martin 2015) and provide a solution for preventing fraud and abuse (Snell 2009). It is suggested that for compliance to be perceived as legitimate it ought to be proactive rather than reactive (Weaver et al. 1999). Thus, in enhancing their legitimacy, compliance personnel are expected to prevent and anticipate and not to act as crime-fighters (Van Duyne 1998).

Duszak (2008) suggested that the CO's primary task is to keep the organization out of trouble. Furthermore, the CO is described to be the single individual in the organization whose sole purpose is to create and maintain an environment that supports legal and ethical behavior (Treviño et al. 2014), which also makes it his/her initial job responsibility. More specifically, Kavanagh (2008, p. 27) presented the following as tasks of the CO:

1. Creation, revision, distribution, and enforcement of the code of conduct;
2. Training of the board, employees, and vendors on organizational standards, risks, compliance, and resources;
3. Operation of the reporting helpline (or oversight of vendors responsible for the function);
4. Auditing and monitoring;
5. Investigation of misconduct reports; and
6. Provision of guidance and support for enforcement of organizational standards at all levels. Furthermore, compliance personnel put together inspection criteria, they make checklists for what needs to be improved, and they set deadlines for the submission of reports (Jones and Bird 2008).

## 3 The Impact of Non-compliance

### *Reputational Damages*

Non-compliance can have detrimental effects on reputation (Verhage 2009). Furthermore, the loss of reputation stemming from non-compliance can result in various financial costs that will be explored on the next subsection. On the other hand, being "legal" or "compliant" creates the image of integrity which serves as good advertisement and adds value to the business (Morf et al. 1999). Therefore, it is essential to note that ethics and compliance initiatives and programs become the focal point for restoring public trust in the financial industry (Treviño et al. 2014).

Furthermore, organizations use compliance personnel as their "agents" in communicating with stakeholders "assurances about the quality of the firm's compliance systems and controls" (DeMott 2013, p. 66). Thus, an effective compliance program with good internal controls minimizes the possibility of disciplinary action against the company in case of isolated instances of misconduct (Martin 2015) and therefore protects the company's reputation. Failure to comply will have dire consequences for a company.

### *Financial Damages*

Financial damages caused by non-compliance can take three forms. The first is the result of direct costs (loss of income and money) to an organization in the form of fines and sanctions, imposed by the government and various other regulatory institutions when organizational non-compliance is detected. In fact, avoiding penalty and the fear of sanctions is ranked as the principal driver of complying with rules and regulations (Verhage 2009). The second financial cost stemming out of a company's non-compliance is that of "indirect costs (clients withdrawal or legal costs) and opportunity costs (forgone business opportunities) all of which will reduce the overall profitability of the firm" (Harvey 2004, p. 336). Finally, a corporation can suffer financial damages due to non-compliance, through losing money as a result of fraud and other criminal activity (De Dios 2016). Consequently, the present authors advocate that a successful compliance program ought to be based on ethical culture and internal legitimacy.

## 4 Ethical Culture/Internal Coherence

The compliance program in itself should be "values-based, motivating employees to aspire to ethical conduct, encouraging them to question authority when ethics are at stake, and holding them accountable for rule violations" (Treviño et al. 1999, p. 149). When such a program is implemented, it can produce highly committed employees who are aware of ethics and compliance issues and are thus more likely to avoid unethical behavior, seek advice when confronted with ethical dilemmas, have a greater commitment to the organization, and who are willing or likely to report ethical/legal violations. Furthermore, effective compliance programs can result in less unethical/illegal behavior in the organization and better decision-making.

Highly effective COs are capable of recognizing social trends within the organization that are counterproductive to the overall compliance/ethics program and thus, target these behaviors and attitudes (Lafferty 2010). The compliance function includes the detection and discontinuation of the compromise of legal or ethical standards and the replacement of those with an ethical organizational culture (Perrone 2014). After detecting compliance issues, COs are expected to inform senior management, which will proceed with handling those issues (Belton 2009). Thus, compliance programs provide significant internal benefits by enhancing internal organizational systems through providing guidelines for employee conduct, establishing a strong ethical culture and improving managerial decisions (Weaver and Treviño 1999). This strong ethical culture is expected to encourage whistleblowing which will be protected and aid the corporation in detecting and addressing internal issues (Baldock 2016; Grant-Hart 2016).

Weber and Wasieleski (2012) assert that ethics and compliance are at the core of their organizations' values and culture and that only programs consistent with a strong ethical culture are likely to work to dissuade unethical and illegal behavior within an organization. Furthermore, it is widely recognized that what is perceived to be corrupt behavior in one culture may not be totally accepted as such in another (Baldock 2016). It is thus imperative for corporations to make sure that the internal culture is one that recognized and dissuaded criminal or corrupt behavior by its employees.

Another benefit of compliance is that of attaining internal legitimacy because when people see authorities as legitimate, "it leads them to feel personally obligated to defer to those authorities, institutions, and social arrangements" (Tyler 2006, p. 376). On the other hand, "employees

who witness an ethical failure" will have low respect for the organization and will perhaps not hesitate to violate legal or ethical guidelines (Schminke et al. 2014, p. 217).

COs serve as "referential anchor" through their role in interpreting laws and regulations that have been enacted by the organization (Perezts and Picard 2015, p. 848). Thus, poor quality of a compliance program can potentially hamper effective implementation of the regulation (Pok et al. 2014) and have a multiplying effect on corruption, cheating, bribing and failure to comply with regulation (Méndez 2012, p. 189).

It follows from the literature, and advocated by the present authors, that COs are therefore expected to be both a "watchdog" and a "bloodhound." Such a high expectation could create a future credibility crisis for the financial sector generally and the profession specifically. Thus, the present authors decided to carry out a research on COs by adapting the expectation gap model developed for the accounting profession.

## 5 Expectation Gap: A Model and an Empirical Study

Liggio (1974) was the first to use the phrase "expectation gap," while Porter (1988, 1993) developed a model and tested it on the accounting profession (Porter and Gowthorpe 2004). Utilizing Porter's model, the identifiable components of the expectation gap are:

1. The difference between what society expects the professional to achieve and what they can reasonably be expected to accomplish (designated as "reasonableness gap").
2. A difference between what society can reasonably expect of the professional to accomplish and what they actually achieve (designated as the "performance gap"). This component is further divided into:

   (a) The gap between what duties can reasonably be expected of the professional as defined by the standards, legislation, codes of conduct, rules and regulations ("deficient regulations gap"); and
   (b) The gap between the duties as defined by professional standards/legal obligations and the actual performance ("deficient performance gap").

The expectation gap has been extensively studied for the audit profession (Krambia-Kapardis 2001; Gherai 2011; Idris and Ojemen 2012; Ruhnke

and Schmidt 2014; Füredi-Fülöp 2015), and the accounting profession (Nadana and Kim 2014). Other studies disentangling the expectation gap are in the context of: (a) stress and educational aspiration of mothers (Bravo et al. 2016); (b) graduate's and the role of employers (Islam et al. 2015); (c) restaurants in London (Madichie 2007); (d) gender differences (Perry et al. 2009); and (e) directors and officers of US Multinationals (Brooks 2010).

In order to study if there is an expectation gap in the CO's profession, the current authors have had extensive discussions with stakeholders (regulators, COs, legal officers of companies, academics, and professional associations) in an effort to ascertain the state-of-practice. The study was carried out, in the months of April and May 2018 in Cyprus, which is a Member State of the EU.

The Cypriot legislators have enacted a legislation Law 188(I)/2007 which creates the obligation and responsibilities for implementation by professionals including lawyers, accountants, auditors, financial companies, and those providing administrative services to prevent and report anti-money laundering and anti-terrorist financial activities. Under S. 59 of the above law, the following five entities have been assigned as supervisory authorities: (a) The Central Bank of Cyprus; (b) The Cyprus Securities Commission (CySEC); (c) The Institute of Certified Public Accountants of Cyprus (ICPAC); (d) The Cyprus Bar Association; and (e) The Cyprus Insurance Commissioner.

Following the unstructured discussions/interviews held late 2017 with COs, the management of those who appoint COs and regulators, it had become apparent to the authors of the paper that there is disparity (a) between the role, duties, and responsibilities of CO as expressed by each stakeholder; and (b) in the understanding of what are the CO's duties as prescribed by the law and as perceived by management and the regulators.

Figure 1 outlines the model as adapted from Porter (1988) and Porter and Gowthorpe (2004) in an effort to study if there is such an expectation gap and how each component can be bridged before the compliance profession reaches a credibility crisis.

## *Methodology*

The study aimed to identify if there is an expectation gap and the type of gap in an effort to reduce it. Thus, the following research questions were developed:

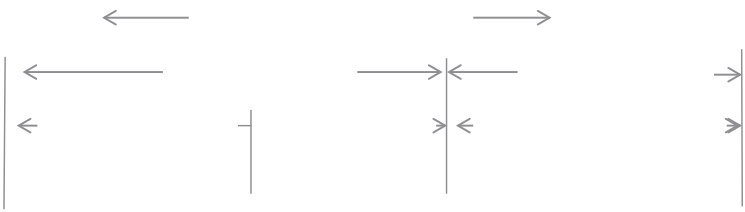

**Fig. 1** The structure of the expectation gap. *Source* Adapted from Porter (1988)

1. Is there a reasonableness gap?
2. Is there a deficient regulation gap?
3. Is there a deficient performance gap?
4. Is there an expectation/performance gap between the CO and the Board and Regulators as far as the duties, role, and responsibilities of the CO?

In addition, this study moves beyond Porter's (1988, 1993) expectation–performance gap analysis and examines the level of knowledge of COs and managers about responsibilities COs are legally expected to perform, in an attempt to also ascertain if there is a knowledge gap. Consequently, the following research question is also examined:

5. Is there a knowledge gap?

A questionnaire was prepared following the literature review and was pilot tested by the regulators of the Cyprus Bar Association, the ICPAC, and the CySEC. The survey instrument was separated in three parts. Part A covered the demographics of the respondents, Part B had a list of general questions about the compliance profession and compliance department of the respondent, and Part C addressed the CO's duties and responsibilities. The questionnaire was set up on survey monkey and was e-mailed to COs, regulators, and board members of the entities that by law ought to appoint a CO. A similar study (Treviño et al. 2014) on COs, carried out in the USA, had surveyed 40 COs. Thus, the current researchers, given the small size of the country and the four different categories of COs (i.e., legal, accounting, banking, and financial sector) it was considered that it ought to aim to receive 100 responses to enable detail statistical analysis to be carried out. A total of 119 valid responses were received and analyzed.

The respondents of the current study were mainly males (58%) who were predominantly qualified Lawyers (15%) or Accountants (39%). Most held a Bachelors Degree in one of the following: (a) Banking (3%), (b) Finance (10%), (c) Accounting (14%), (d) Business Administration (10%), (e) Law (10%), (f) Economics (10%), (g) Quantitative Methods (1%). Some of the respondents also had postgraduate qualifications such as a Master's Degree (38%) or other qualification (18%). A mere 54% had 1–5 years' experience in the field of compliance (see Table 1, below).

The current chapter will discuss the findings of Part C of the questionnaire.

A list of 36 duties and responsibilities were provided to the respondents. The 18 duties were derived from the responsibilities as outlined in Article 9 of the Directive (CySEC 2015), 12 were listed as duties provided in March 2017 to the first author by the International Compliance Association (ICA) to be included in the questionnaire (these roles are reproduced and are also highlighted in ICA [2016, pp. 171 and 172]), and the remaining 6 were drawn from the literature search (Forman 2013; Martin 2015; Treviño et al. 1999). Table 4 in Appendix presents the responsibilities together with the source of authority. The respondents asked to identify which duties were:

1. Duties Performed by COs,
2. Duties Expected of COs by the relevant regulations,
3. Duties which are cost-beneficial for the CO, to perform, and
4. Duties expected of COs by Board/Management[1]

The data was analyzed using SPSS.

**Table 1** Respondents' details

| | *Total responses* | | *CO* | | *Board/ Management/ Regulators* | |
|---|---|---|---|---|---|---|
| *Regulated by* | *≠No* | *%* | *≠No* | *%* | *≠No* | *%* |
| Insurance | 1 | 0.8 | 0 | 0 | 1 | 4 |
| CySEC | 52 | 43.7 | 44 | 46.8 | 8 | 32 |
| Accounting | 39 | 32.8 | 28 | 29.8 | 11 | 44 |
| Legal | 13 | 10.9 | 11 | 11.7 | 2 | 8 |
| Banking | 14 | 11.8 | 11 | 11.7 | 3 | 12 |
| **Total** | **119** | **100** | **94** | **100** | **25** | **100** |

*Source* Authors based on their survey

## 6 Findings

***Reasonableness Gap: Compliance Officer Expectation–Performance Gap***

The responsibilities falling into the reasonableness gap are those that are unreasonably expected of COs by board and management.[2] As shown in Table 2, from the 12 responsibilities expected of COs by board and management, seven are unreasonably expected, as they are not prescribed by statute law, case law, regulations, and professional promulgations, neither were they perceived by COs to be cost-beneficial to perform them. Consequently, the seven responsibilities comprise the reasonableness gap.

- Identifying the requirements of legislation and regulations that should be conducted by the organization, and gathering and disseminating information about compliance requirements in the organization (Responsibility 1).
- Providing guidance on the proper application and interpretation of laws, regulations, and policies applicable to the firm (rules, guidance documents, codes of conduct, and internal policies) (Responsibility 2).
- Providing managers with guidance in the development, implementation, and maintenance of robust policies, procedures, and practices for regulated activities (Responsibility 3).
- Setting policies and procedures and proposing improvements in the event that the monitoring program identifies weaknesses (Responsibility 6).
- Providing regular and accurate reports to management (and where necessary to the board of directors) on regulatory and compliance matters (Responsibility 7).
- Assisting in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct (Responsibility 10).
- Ensuring the employees and management do not violate any unwritten moral and ethical values (Responsibility 18).

Reviewing the responsibilities falling into the "reasonableness gap," it is observed that duties expected by board and management to be performed by the CO have a broad focus of dealing with the overall compliance process within organizations. These duties vary from identifying the legislation and standards that a company should follow, providing

**Table 2** Contribution of responsibilities to components of the COs expectation–performance gap

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 1 | Identifies the requirements of legislation and regulations for the business conducted by the organization; gathers and disseminates information about compliance requirements in the organization | | | | | RG | S |
| 2 | Provides guidance on the proper application and interpretation of laws, regulations, and policies applicable to the firm. Such regulation may include rules, guidance documents, codes of conduct, and internal policies designed to meet regulatory compliance | | | | | RG | S |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 3 | Provides managers with guidance in the development, implementation, and maintenance of robust policies, procedures, and practices for regulated activities | | | B | | RG | S |
| 4 | Creates a program of activities to educate and encourage both managers and staff to operate in compliance with relevant laws and regulations. This should include providing training on key compliance and regulatory matters such as complaints, money laundering, conflicts, and personal account dealing | | | B | | | |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 5 | Facilitates implementation and maintenance of a compliance-monitoring program, which provides management with assurance that key regulatory risks are being adequately managed within the business areas | | | B | | | |
| 6 | Sets policies and procedures and proposes improvements in the event that the monitoring program identifies weaknesses | | | | | RG | S |
| 7 | Provides regular and accurate reports to management (and where necessary to the board of directors) on regulatory and compliance matters. This should include the raising of significant issues, concerns, or regulatory breaches | | | | | RG | S |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 8 | Coordinates and assists other control and risk functions in order to comprehensively identify, assess, and manage regulatory risk | | | | | | |
| 9 | Supports senior management in establishing and maintaining good relationships with the regulators. This includes acting as the main point of contact between the institution and the relevant regulators | | | | | | |
| 10 | Assists in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct | | | | | RG | S |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 11 | Maintains relationships with regulators, including the coordination of responses to consultative papers or other regulatory pronouncements | | | | | | |
| 12 | Develops and maintains a relevant internal manual for compliance within an organization | | | | | | |
| 13 | Prepares and submits to the regulator the monthly prevention statement | | D | | RE | | |
| 14 | Prepares an annual report which assesses the firm's level of compliance with its obligation laid down in the law, and the money laundering and terrorist financing preventive issues | | D | | RE | | |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 15 | Responds to all requests and queries from MOKAS[a] and the appropriate regulator (e.g., Cyprus Bar Association, CySEC, ICPAC, Central Bank) | | D | | RE | | S |
| 16 | Ensure the employees and management do not violate any regulations and legislations | | | | | | |
| 17 | Ensure the employees and management do not violate any written ethical codes of conduct | | | | | | |
| 18 | Ensure the employees and management do not violate any unwritten moral and ethical values | | | | | RG | S |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 19 | Designs the internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing and describes and explicitly allocates the appropriateness and the limits of responsibility of each relevant department | | D | | RE | | |
| 20 | Develops and establishes the firm's AML policy, and submits it to the board of directors for consideration and approval | | D | | RE | | |
| 21 | Prepares a risk management and procedures manual regarding money laundering and terrorist financing | | D | | RE | | |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 22 | Monitors and assesses the correct and effective implementation of the policy principles in relation to money laundering and terrorist financings | | D | | RE | | |
| 23 | Receives from the employees, information which is considered by the latter to be knowledge/suspicion of money laundering or terrorist financing activities | | D | | RE | | |
| 24 | Validates/evaluate information received regarding the suspicion or the knowledge of money laundering or terrorist financing activities | | D | | RE | | S |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 25 | Notifies MOKAS through online submission system of any actual or suspicious money laundering or terrorist financing activities following the evaluation of information | | D | | RE | | |
| 26 | CO has a duty to fully explain the reasons of not notifying MOKAS in the Internal Evaluation Report | | D | | RE | | S |
| 27 | Acts as a first point of contact with MOKAS upon commencement of and during investigation as a result of filing a report to MOKAS | | D | | RE | | |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 28 | Ensures the preparation and maintenance of the lists of customers categorized following a risk based approach | | D | | RE | | S |
| 29 | Based on customer risk evaluation, detects, records and evaluates, annually or bi annually all risks arising from new customers and existing customers | | D | | RE | | |
| 30 | Ensures that the branches of the firm that operate in countries outside the EEA have taken all necessary measures in relation to customer identification, due diligence and record keeping procedures as per the EEA legal framework | | D | | RE | | |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 31 | Provides advice and guidance to other employees on money laundering and terrorist financing matters | | D | | RE | | |
| 32 | Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing | | D | | RE | | |
| 33 | Develops and maintains a relevant internal manual for compliance within an organization which is submitted to the board of directors for approval | | | | | | |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| 34 | Evaluates the systems and procedures applied by a third person on whom the compliance officer relies upon for customer identification and due diligence purposes | | D | | RE | | S |
| 35 | Incorporates compliance and ethics messaging into broad communications to employees and in day-to-day interactions with employees | | | | | | |
| 36 | Regularly reminds employees of the importance of ethical and compliant behavior, raising concerns and the company's non-retaliation policy | | | | | | |
| | Number of responsibilities | | 18 | 3 | 18 | 7 | 12 |

(continued)

**Table 2** (continued)

| *Resp. no.* | *Duties* | *Deficient performance gap duties* | *Existing duties of CO* | *Deficient regulations gap duties* | *Duties reasonably expected of CO* | *Reasonableness gap duties* | *Duties expected of CO* |
|---|---|---|---|---|---|---|---|
| **D** | Existing responsibility of compliance officers, identified by reference to statute law, case law, regulations and professional promulgations | | | | | | |
| **RE** | Responsibilities reasonably expected of compliance officers—responsibilities that are cost-beneficial for compliance officers to perform | | | | | | |
| **S** | Responsibility identified by board and management as a responsibility compliance officers should perform | | | | | | |
| **B** | Responsibility identified by the banking sector as falling in the deficient regulations gap | | | | | | |
| **RG** | Responsibility falling into the reasonableness gap | | | | | | |

*Source* Authors, based on their survey

[a]MOKAS is the national unit for combating money laundering

guidance to managers and dealing with the application of policies and procedures, to reporting and creating internal compliance culture.

It is surprising that some of these responsibilities did not meet the cost-beneficial test as they fall within the role of a CO. Responsibility 1 "Identifies the requirements of legislation and regulations for the business conducted by the organization; gathers and disseminates information about compliance requirements in the organization" was identified by COs as not cost-beneficial. It is interesting that COs find the process of identifying legislations and regulations that their business should follow resulting in important costs, as such information is freely available online for them to review. Additionally, complying with governmental requirements results in avoiding possible financial and reputational sanctions. Hence, the benefits of identifying the regulations and standards an organization is obliged to follow outweigh the costs of having to pay penalties for not complying with them.

Other responsibilities that interestingly are considered to be unreasonably expected of CO by board and management are:

- Responsibility 2 "Provides guidance on the proper application and interpretation of laws, regulations and policies applicable to the firm. Such regulation may include rules, guidance documents, codes of conduct and internal policies designed to meet regulatory compliance."
- Responsibility 3 "Provides managers with guidance in the development, implementation and maintenance of robust policies, procedures and practices for regulated activities," and
- Responsibility 6 "Sets policies and procedures and proposes improvements in the event that the monitoring programme identifies weaknesses."

It is not readily explainable why providing guidance and setting policies is considered to result in more costs than benefits for an organization. It is generally accepted that management is responsible for establishing internal control processes within organizations, however, guidance from COs who are assumed to be knowledgeable of legislation and standards would probably help managers to choose effective processes that would minimize any possible risks.

Also, it is not readily explainable as well why COs perceive Responsibility 7 "Provides regular and accurate reports to management

(and where necessary to the board of directors) on regulatory and compliance matters. This should include the raising of significant issues, concerns or regulatory breaches," as not being cost-beneficial. This could only be expected where board and management are distant from the compliance process and they do not acknowledge the impact of non-compliance for their business. Therefore, reporting regulatory and compliance issues could be considered as not offering any benefits.

Responsibility 10 "Assists in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct" and Responsibility 18 "Ensure the employees and management do not violate any unwritten moral and ethical values" are dealing with setting the ethics and values within organizations. This responsibility could be considered to be over and above COs' duties taking into consideration the overall role of a CO as described by existing law. Duties according to law expect COs to advice employees on compliance issues along with processing and evaluating information received regarding suspicious money laundering or terrorist financing. Therefore, setting the culture of internal legitimacy and compliance within an organization could be considered by COs as a responsibility of the management team.

Studying individually the responses of each sector, no additional responsibilities were found qualifying for the reasonableness gap for the accounting, legal and administrative services. Going through the responses of COs from the banking sector, we observe that three responsibilities were identified by them as cost-beneficial, namely:

- Providing managers with guidance in the development, implementation, and maintenance of robust policies, procedures, and practices for regulated activities (R.3).
- Creating a program of activities to educate and encourage both managers and staff to operate in compliance with relevant laws and regulations (R.4).
- Facilitating implementation and maintenance of a compliance-monitoring program (R.5).

Responsibilities 4 and 5 fail to qualify as responsibilities board and management expect of COs. Therefore, they are not further considered for the *reasonableness gap*. Responsibility 3 a duty identified previously as expected by board and management is considered to be reasonably expected of COs. Consequently, it should not be included in the reasonableness gap of the banking sector.

Thus, the findings according to the first research question reveal the existence of a reasonableness gap. The reasonableness gap is derived from the unreasonable expectations placed upon COs and could be bridged by raising awareness and building capacity for both the CO and board and management. This will enable both COs and board and management to become better acquainted with the CO's responsibilities as required by statute law, case law, regulations, and professional promulgations, and to accept COs' role within organizations. In addition, board and management will acknowledge the possible risks of non-compliance. In addition, companies are legally liable to the national Financial Intelligence Units (FIUs), in Cyprus the FIU is called the Unit for Combating Money Laundering (MOKAS). Their non-compliance to MOKAS' requirements will result in paying sanctions, while meeting their obligations will enhance public confidence and reputation on the company's compliance.

Furthermore, no statistical significant difference was found between those respondents with greater than 5 years' experience than those with 1–5 years' experience, or those who hold a postgraduate qualification. The findings emphasize the importance of education and training for the overall group of COs and board and managers, as the level of experience in the field and qualifications appear not to influence the level of knowledge of existing regulations and standards.

Thus, in responding to the first research question, a reasonableness gap has been identified as far as seven duties are concerned.

### *Deficient Regulation Gap: Compliance Officer Expectation–Performance Gap*

The *deficient regulations component* of expectation–performance gap examines the gap between responsibilities, which are reasonably expected of COs by board, management, and regulators, but are not required by statute law, case law, regulations, and professional promulgations. The aim is to identify duties, which are considered by COs to generate important benefits for organizations, in an attempt to expand and enrich their current responsibilities obliged by law.

Table 2 shows that for the overall group of COs, there are 18 responsibilities, which are reasonably expected. All of them are responsibilities that arise from the relevant legislation. Consequently, in responding to the second research question, there is not a deficient regulations gap as there are no responsibilities which are reasonably expected but not enforced by existing legislation.

Studying individually each sector, it was found that there is no deficient regulations gap for the accounting, legal and administrative services. However, a deficient regulations gap was found for the banking sector. The responsibilities comprising the deficient regulations gap for the banking sector are:

- To provide managers with guidance for developing, implementing, and maintaining policies, procedures, and practices for regulated activities (Responsibility 3).
- To educate and encourage through training managers and staff compliance with relevant laws and regulations (Responsibility 4).[3]
- To implement and maintain a compliance-monitoring program for minimizing organizations' key regulatory risks (Responsibility 5).

Going through the responsibilities, it can be argued that COs in the banking sector acknowledge the importance of creating a compliance culture within organizations. Even though existing laws do not anticipate COs to provide training and guidance to managers and staff, the banking sector recognizes the benefits resulting through such measures for ensuring organizations' compliance with rules, regulations, and legislation. Concerning the compliance-monitoring program, COs are expected by law, according to Responsibility 22, to monitor and implement policies relating to money laundering and terrorist financings. Therefore, standard and policy developments could concentrate on expanding the focus of law, on monitoring organizations' compliance to the overall rules and regulations that are applicable for them, than concentrating on specific issues.

Thus, in responding to the second research question, it can be stated that the researchers did not find a deficient regulations gap as far as the CO working in the accounting, legal and CySEC regulated entities. However, there is a deficient regulations gap for the banking sector. It seems that the bankers association should consider to extend the legal duties of COs within the banking sector to include: (a) COs ought to provide managers with guidance for developing, implementing, and maintaining policies, procedures, and practices for regulated activities; (b) COs ought to educate and encourage through training, managers' and staffs' compliance with relevant laws and regulations; and (c) COs ought to implement and maintain a compliance-monitoring program for minimizing organizations' key regulatory risks.

### *Deficient Performance: Compliance Officer Expectation–Performance Gap*

*Deficient performance* examines whether COs perform their responsibilities prescribed by statute law, case law, and other regulations. As discussed in previous sections, 18 responsibilities included in the questionnaire were adopted from existing law. COs responses revealed that, they perform all duties required by law. Consequently, as shown in Table 2, there is no responsibility falling within the deficient performance gap for the overall group of COs. Examining each sector individually it was found that there is no deficient performance gap for any of the sectors either. Thus, it could be concluded that in responding to the third research question, there is no performance gap as the COs carry out their duties as prescribed by law and other regulations.

Finally, in responding to the fourth research question, given there is only reasonableness gap for all COs irrespective of the sector they operate in and a deficient regulations gap only for the COs in the banking sector, it could be argued that the COs are not facing an expectation gap, similar to the one the accounting profession faced in the late 1990s.

### *Knowledge Gap*

Going beyond Porter's (1988, 1993) expectation–performance gap analysis, the current authors examined the existence of a knowledge gap for COs and managers. The purpose was to examine the level of knowledge of COs and managers regarding the responsibilities COs are legally expected to perform. Table 3 shows the responsibilities identified by the respondent COs and managers as duties expected of COs by the relevant regulations. The table does not represent the absolute numbers of COs' and managers' responses, but the positive and negative mean values calculated, taking into consideration the responses of each interest group.[4] For example managers identified responsibilities 1, 2, 24, 25, 26, 29, 32 as duties expected of COs by regulations. Analyzing the responses, it was found that there is a knowledge gap for all interested groups, as they were not able to identify which duties are prescribed by legislation or other regulation. This is best illustrated in Table 3.

The lack of knowledge found for the overall group of COs should be of concern for the supervisory authorities of Cyprus and should be addressed as it shows how well COs understand their role within

**Table 3** Duties expected of CO by the relevant regulations

| *Resp no.* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| | ***Duties prescribed by legislation*** | | | | | | |
| 13 | Prepares and submits to the regulator the monthly prevention statement | | √ | | √ | √ | |
| 14 | Prepares an annual report which assesses the firm's level of compliance with its obligation laid down in the law, and the money laundering and terrorist financing preventive issues | | √ | | √ | √ | |
| 15 | Responds to all requests and queries from MOKAS and the appropriate regulator (e.g., Cyprus Bar Association, CySEC, ICPAC, Central Bank) | | √ | | √ | √ | |
| 19 | Designs the internal practice, measures, procedures, and controls relevant to the prevention of money laundering and terrorist financing and describes and explicitly allocates the appropriateness and the limits of responsibility of each relevant department | | √ | | √ | √ | |
| 20 | Develops and establishes the firm's AML policy, and submits it to the board of directors for consideration and approval | | √ | | √ | √ | |
| 21 | Prepares a risk management and procedures manual regarding money laundering and terrorist financing | | √ | | √ | √ | |
| 22 | Monitors and assesses the correct and effective implementation of the policy principles in relation to money laundering and terrorist financings | | √ | | √ | √ | |
| 23 | Receives from the employees, information which is considered by the latter to be knowledge/suspicion of money laundering or terrorist financing activities | | √ | | √ | √ | |

(continued)

**Table 3** (continued)

| *Resp no.* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 24 | Validates/evaluates information received regarding the suspicion or the knowledge of money laundering or terrorist financing activities | √ | √ | | √ | √ | |
| 25 | Notifies MOKAS through online submission system of any actual or suspicious money laundering or terrorist financing activities following the evaluation of information | √ | √ | | √ | √ | |
| 26 | CO has a duty to fully explain the reasons of not notifying MOKAS in the Internal Evaluation Report | √ | √ | | √ | √ | |
| 27 | Acts as a first point of contact with MOKAS upon commencement of and during investigation as a result of filing a report to MOKAS | | √ | √ | √ | √ | |
| 28 | Ensures the preparation and maintenance of the lists of customers categorized following a risk-based approach | | √ | | √ | √ | |
| 29 | Based on customer risk evaluation, detects, records, and evaluates, annually or bi annually all risks arising from new customers and existing customers | √ | √ | | √ | √ | |
| 30 | Ensures that the branches of the firm that operate in countries outside the EEA have taken all necessary measures in relation to customer identification, due diligence, and record keeping procedures as per the EEA legal framework | | √ | | √ | √ | |
| 31 | Provides advice and guidance to other employees on money laundering and terrorist financing matters | | √ | | √ | √ | |
| 32 | Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing | √ | √ | | √ | √ | |

(continued)

**Table 3** (continued)

| *Resp no.* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 34 | Evaluates the systems and procedures applied by a third person on whom the compliance officer relies upon for customer identification and due diligence purposes | | √ | | √ | √ | |
| | ***Duties not derived by legislation*** | | | | | | |
| 1 | Identifies the requirements of legislation and regulations for the business conducted by the organization; gathers and disseminates information about compliance requirements in the organization | √ | √ | | √ | √ | |
| 2 | Provides guidance on the proper application and interpretation of laws, regulations, and policies applicable to the firm. Such regulation may include rules, guidance documents, codes of conduct, and internal policies designed to meet regulatory compliance | √ | √ | √ | √ | √ | |
| 3 | Provides managers with guidance in the development, implementation, and maintenance of robust policies, procedures, and practices for regulated activities | | | | √ | √ | |
| 4 | Creates a program of activities to educate and encourage both managers and staff to operate in compliance with relevant laws and regulations. This should include providing training on key compliance and regulatory matters such as complaints, money laundering, conflicts, and personal account dealing | | √ | √ | √ | √ | |
| 5 | Facilitates implementation and maintenance of a compliance-monitoring program, which provides management with assurance that key regulatory risks are being adequately managed within the business areas | | √ | | √ | √ | |

(continued)

**Table 3** (continued)

| *Resp no.* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 6 | Sets policies and procedures and proposes improvements in the event that the monitoring program identifies weaknesses | | √ | | √ | √ | |
| 7 | Provides regular and accurate reports to management (and where necessary to the board of directors) on regulatory and compliance matters. This should include the raising of significant issues, concerns, or regulatory breaches | | √ | | √ | √ | |
| 8 | Coordinates and assists other control and risk functions in order to comprehensively identify, assess, and manage regulatory risk | | | | √ | √ | |
| 9 | Supports senior management in establishing and maintaining good relationships with the regulators. This includes acting as the main point of contact between the institution and the relevant regulators | | | | √ | | |
| 10 | Assists in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct | | | | √ | | |
| 11 | Maintains relationships with regulators, including the coordination of responses to consultative papers or other regulatory pronouncements | | | | √ | | |
| 12 | Develops and maintains a relevant internal manual for compliance within an organization | | | | √ | √ | |
| 16 | Ensure the employees and management do not violate any regulations and legislations | | √ | | √ | √ | |
| 17 | Ensure the employees and management do not violate any written ethical codes of conduct | | | | | | |
| 18 | Ensure the employees and management do not violate any unwritten moral and ethical values | | | | √ | | |

(continued)

**Table 3** (continued)

| *Resp no.* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 33 | Develops and maintains a relevant internal manual for compliance within an organization which is submitted to the board of directors for approval | | √ | | √ | √ | |
| 35 | Incorporates compliance and ethics messaging into broad communications to employees and in day-to-day interactions with employees | | | | √ | | |
| 36 | Regularly reminds employees of the importance of ethical and compliant behavior, raising concerns and the company's non-retaliation policy | | | | √ | | |

*Source* Authors, based on their survey

organizations. Even though, a knowledge gap was found in all sectors, it was surprising to discover that an important number of participants from the CySEC regulated sector are not aware of their duties as prescribed by law. The finding is of particular interest, as COs from this sector, unlike the other three sectors, are at the time of writing expected to pass qualifying examinations, which include the relevant legislation before they qualify to work in a CySEC regulated entity.

Another issue of concern is the knowledge gap found for managers. The manager's knowledge gap reflects their lack of understanding of COs' role that could jeopardize the development of compliance within a business. In addition, knowledge gap is an important component contributing to the reasonableness gap, as the expectations of management do not reflect the responsibilities of the profession as set by law.

Thus, the findings pertaining to the responses to the first and fifth research question illustrate that the component contributing to the performance-expectation gap is reasonableness gap and in addition, both the COs and Managers/Board are also facing a knowledge gap as they do not know what are the legal duties expected of COs.

Thus, in adapting the Porter (1988, 1993) and Porter and Gowthorpe (2004) model to allow for the findings relating to COs, and as shown in Fig. 2, the gaps identified relate to the reasonableness gap (i.e., the non-CO has unreasonable expectations of the CO) and a new founded knowledge gap (i.e., the CO and non-CO do not have the sufficient knowledge of what is expected by legislation even though the COs perform the work but do not know they are required to do so by law).

In disentangling the expectation gap for COs, only the first and fifth research questions are answered as there are only two components in the expectation gap, the reasonableness gap and knowledge gap. The reasonableness gap is a result of the unreasonable expectations of boards and management, as they are expecting COs to perform responsibilities that are not prescribed by statute law, case law, regulations, and professional promulgations, and that are not cost-beneficial to be performed. In addition, the second component of the expectation gap as illustrated in Fig. 2 is the knowledge gap. The lack of knowledge of responsibilities COs are legally expected to perform, further enhances the reasonableness gap as COs, board, and management are not familiar with existing and standards' requirements and expecting COs to perform duties outside their legal obligations.

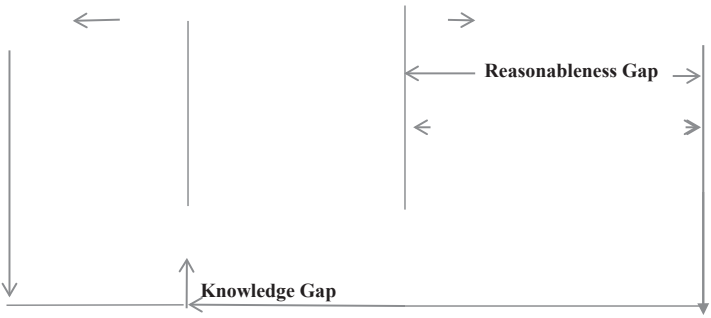


**Fig. 2** The expectation gap. *Source* Adapted from Porter (1988)

## 7 Conclusion

The field of compliance has been evolving over the last three decades and the evolution has comprised of the implementation of new ethics/compliance initiatives and amplified support of these programs from senior management (Weber and Fortun 2005). The compliance industry is also being strengthened by current legislation, obliging financial institutions to implement such programs (Verhage 2009).

Compliance should be about the protection of the client: "managing one's business as to ensure, as a minimum, that it is conducted in accordance with the law and with the rules relating to the conduct of business which are designed to protect the investor" (Edwards and Wolfe 2005, p. 55). While this should be the primary focus, one ought to acknowledge the challenges faced by the CO profession which is often asked to identify and blow the whistle on a wrongdoing that may have been committed by his/her supervisor and there may be retaliated against (McGreal 2017).

The current paper aimed to examine COs' expectation–performance gap in Cyprus. The findings revealed the existence of an expectation–performance gap with two components, a knowledge gap and a reasonableness gap, but no deficient regulations or performance gap. In other words, the COs appear to be performing the duties as derived by law, and the legislation appears with no major gaps or omissions based on the cost-beneficial criterion of COs. However, evidence found for a reasonableness gap, as the board's and management's expectations have a

broader focus on compliance than dealing with specific issues such as anti-money laundering (Harvey 2004) as they relate to creating a compliance culture within organizations (Greenberg 2009). The same view is reiterated by Berenbeim (2010) who claims there seems to be a shift of the focus of compliance programs "to resolution of workplace conflict rather than ethical decision making, cultural change, and employee empowerment" (p. 21).

Furthermore, the paper identified a challenge that needs to be addressed, namely which is the knowledge gap of both COs and managers about responsibilities COs are legally expected to perform. It was interesting to find that the overall group of COs were not aware of their legal responsibilities as prescribed by statute law, case law, and regulations. Thus, the policy implications of the findings relate to the importance of raising awareness and building capacity for COs and managers. While the COs in the current study were all well educated (see above demographics) and held professional qualifications, they did not appear to be well versed in their legal duties. Thus, it is suggested that COs ought to hold a postgraduate qualification in Financial Compliance or pass relevant examination(s) with continuing professional education requirements. It is essential to educate both COs and managers on the role and responsibilities of a CO to ensure that there are no misunderstandings. Compliance is a process that requires the engagement of the organization as a whole; from the highest stratum of the organization all the way to the frontline personnel. Educating COs will help in performing all responsibilities set by law and in ensuring organizations are being legal and compliant. However, it is also important to educate managers in order for them to understand and appreciate the CO's role within the organization and enable the CO to gain legitimacy.

It is surmised that given there is no major expectation gap as the one noted by Porter (1988) and Porter and Gowthorpe (2004), the CO will not be facing a credibility crisis as did the accountants and auditors in the late 1990s (Krambia-Kapardis 2001). The fact, however, that the CO profession does not have a common globally recognized professional association as the accounting and legal professions may mean that each regulatory body will raise or lower the apparatus as it sees fit. As has been noted in the literature (Verhage 2009), necessary steps ought to be taken to ensure the COs do not end up being Pygmalion or Narcissus, i.e., where a system is created and the COs are so blinded by the image they created (in the case of Pygmalion) or blinded by its own reflection (in

the case of Narcissus) that it is no longer able to critically question itself. The current authors extend this to include the Goliath risk as COs may be expected by management and the board to be unreasonably performing duties which they cannot and will thus take a small case or a David to bring them down.

**Acknowledgements** The authors would like to thank Eleana Fitidou for assisting with the literature search.

## Notes

1. The responses of participants were coded in order to conduct an analysis by using the means of groups' responses. For duties that were identified as falling into a category, the responses were coded +1, while −1 was used when a duty was not identified by the respondents. Therefore, the closer the mean to +1, the greater the agreement of that group that the responsibility falls into the specific category, while a mean closer to −1 indicates the disagreement between the group members. The tables used for the analysis are in the Appendix section.
2. A duty is considered to be reasonably expected, if it satisfies at least one of two criteria; (1) it is a responsibility according to statute law, case law, regulations, and professional promulgations; and (2) it is cost-beneficial for COs to perform the responsibility. Responsibilities that do not satisfy any of the two criteria are considered to be unreasonably expected.
3. Responsibility 4 met the cost benefit test as an important proportion of bankers identified it as a duty that is cost-beneficial for them to perform, while for responsibilities 3 and 5 bankers' responses were equally divided between those who identified them as being cost-beneficial and those who do not consider them as cost-beneficial duties. See Table 5 in Appendix for the mean values calculated.
4. A positive mean indicates the agreement of that group that the responsibility is expected of COs by the relevant regulations, while a negative mean indicates the disagreement between the group members. Therefore, in Table 3, the symbol "√" is used when the majority of interested group respondents identified a duty as expected of COs by regulations, while no symbol was used when the majority of participants did not identify it as expected. The mean values used for Table 3 are located at the Appendix section.

## Appendix

See Tables 4, 5, 6, and 7.

**Table 4** Duties as derived by legislation, ICA, and literature included in the questionnaire

| *Resp no.* | | *Authority for recognition as an existing responsibility* |
|---|---|---|
| | ***Duties accepted as existing responsibilities of compliance officers*** | |
| 13 | Prepares and submits to the regulator the monthly prevention statement | Article 9 of the Directive (CySEC 2015) |
| 14 | Prepares an annual report which assesses the firm's level of compliance with its obligation laid down in the law, and the money laundering and terrorist financing preventive issues | CySEC Law |
| 15 | Responds to all requests and queries from MOKAS and the appropriate regulator (e.g., Cyprus Bar Association, CySEC, ICPAC, Central Bank) | CySEC Law |
| 19 | Designs the internal practice, measures, procedures, and controls relevant to the prevention of money laundering and terrorist financing and describes and explicitly allocates the appropriateness and the limits of responsibility of each relevant department | CySEC Law |
| 20 | Develops and establishes the firm's AML policy and submits it to the board of directors for consideration and approval | CySEC Law |
| 21 | Prepares a risk management and procedures manual regarding money laundering and terrorist financing | CySEC Law |
| 22 | Monitors and assesses the correct and effective implementation of the policy principles in relation to money laundering and terrorist financings | CySEC Law |
| 23 | Receives from the employees, information which is considered by the latter to be knowledge/suspicion of money laundering or terrorist financing activities | CySEC Law |
| 24 | Validates/evaluate information received regarding the suspicion or the knowledge of money laundering or terrorist financing activities | CySEC Law |
| 25 | Notifies MOKAS through online submission system of any actual or suspicious money laundering or terrorist financing activities following the evaluation of information | CySEC Law |
| 26 | CO has a duty to fully explain the reasons of not notifying MOKAS in the Internal Evaluation Report | CySEC Law |

(continued)

**Table 4** (continued)

| *Resp no.* | | *Authority for recognition as an existing responsibility* |
|---|---|---|
| 27 | Acts as a first point of contact with MOKAS upon commencement of and during investigation as a result of filing a report to MOKAS | CySEC Law |
| 28 | Ensures the preparation and maintenance of the lists of customers categorized following a risk-based approach | CySEC Law |
| 29 | Based on customer risk evaluation, detects, records and evaluates, annually or biannually all risks arising from new customers and existing customers | CySEC Law |
| 30 | Ensures that the branches of the firm that operate in countries outside the EEA have taken all necessary measures in relation to customer identification, due diligence and record keeping procedures as per the EEA legal framework | CySEC Law |
| 31 | Provides advice and guidance to other employees on money laundering and terrorist financing matters | CySEC Law |
| 32 | Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing | CySEC Law |
| 34 | Evaluates the systems and procedures applied by a third person on whom the compliance officer relies upon for customer identification and due diligence purposes | CySEC Law |
| | ***Duties not accepted as existing responsibilities of compliance officers*** | |
| 1 | Identifies the requirements of legislation and regulations for the business conducted by the organization; gathers and disseminates information about compliance requirements in the organization | International Compliance Association (ICA) |
| 2 | Provides guidance on the proper application and interpretation of laws, regulations, and policies applicable to the firm. Such regulation may include rules, guidance documents, codes of conduct, and internal policies designed to meet regulatory compliance | ICA |
| 3 | Provides managers with guidance in the development, implementation, and maintenance of robust policies, procedures, and practices for regulated activities | ICA |

(continued)

**Table 4** (continued)

| *Resp no.* | | *Authority for recognition as an existing responsibility* |
|---|---|---|
| 4 | Creates a program of activities to educate and encourage both managers and staff to operate in compliance with relevant laws and regulations. This should include providing training on key compliance and regulatory matters such as complaints, money laundering, conflicts, and personal account dealing | ICA |
| 5 | Facilitates implementation and maintenance of a compliance-monitoring program, which provides management with assurance that key regulatory risks are being adequately managed within the business areas | ICA |
| 6 | Sets policies and procedures and proposes improvements in the event that the monitoring program identifies weaknesses | ICA |
| 7 | Provides regular and accurate reports to management (and where necessary to the board of directors) on regulatory and compliance matters. This should include the raising of significant issues, concerns, or regulatory breaches | ICA |
| 8 | Coordinates and assists other control and risk functions in order to comprehensively identify, assess, and manage regulatory risk | ICA |
| 9 | Supports senior management in establishing and maintaining good relationships with the regulators. This includes acting as the main point of contact between the institution and the relevant regulators | ICA |
| 10 | Assists in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct | ICA |
| 11 | Maintains relationships with regulators, including the coordination of responses to consultative papers or other regulatory pronouncements | ICA |
| 12 | Develops and maintains a relevant internal manual for compliance within an organization | ICA |
| 16 | Ensure the employees and management do not violate any regulations and legislations | Literature review |
| 17 | Ensure the employees and management do not violate any written ethical codes of conduct | Literature review |
| 18 | Ensure the employees and management do not violate any unwritten moral and ethical values | Literature review |

(continued)

**Table 4** (continued)

| *Resp no.* | | *Authority for recognition as an existing responsibility* |
|---|---|---|
| 33 | Develops and maintains a relevant internal manual for compliance within an organization which is submitted to the board of directors for approval | Literature review |
| 35 | Incorporates compliance and ethics messaging into broad communications to employees and in day-to-day interactions with employees | Literature review |
| 36 | Regularly reminds employees of the importance of ethical and compliant behavior, raising concerns and the company's non-retaliation policy | Literature review |

**Table 5** Responsibilities interest groups consider to be cost-beneficial and expected by board and management

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 1 | Identifies the requirements of legislation and regulations for the business conducted by the organization; gathers and disseminates information about compliance requirements in the organization | −0.45 | −0.54 | −0.29 | −0.5 | −0.85 | 0.12 |
| 2 | Provides guidance on the proper application and interpretation of laws, regulations, and policies applicable to the firm. Such regulation may include rules, guidance documents, codes of conduct, and internal policies designed to meet regulatory compliance | −0.47 | −0.59 | −0.29 | −0.5 | −0.85 | 0.12 |
| 3 | Provides managers with guidance in the development, implementation, and maintenance of robust policies, procedures, and practices for regulated activities | −0.34 | −0.49 | 0 | −0.42 | −0.85 | 0.04 |
| 4 | Creates a program of activities to educate and encourage both managers and staff to operate in compliance with relevant laws and regulations. This should include providing training on key compliance and regulatory matters such as complaints, money laundering, conflicts, and personal account dealing | −0.28 | −0.54 | 0.29 | −0.31 | −0.69 | −0.04 |

(continued)

**Table 5** (continued)

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 5 | Facilitates implementation and maintenance of a compliance-monitoring program, which provides management with assurance that key regulatory risks are being adequately managed within the business areas | −0.32 | −0.59 | 0 | −0.35 | −0.69 | −0.2 |
| 6 | Sets policies and procedures and proposes improvements in the event that the monitoring program identifies weaknesses | −0.40 | −0.44 | −0.14 | −0.46 | −0.69 | 0.2 |
| 7 | Provides regular and accurate reports to management (and where necessary to the board of directors) on regulatory and compliance matters. This should include the raising of significant issues, concerns, or regulatory breaches | −0.47 | −0.54 | −0.57 | −0.42 | −0.85 | 0.12 |
| 8 | Coordinates and assists other control and risk functions in order to comprehensively identify, assess, and manage regulatory risk | −0.60 | −0.64 | −0.71 | −0.54 | −0.85 | −0.2 |
| 9 | Supports senior management in establishing and maintaining good relationships with the regulators. This includes acting as the main point of contact between the institution and the relevant regulators | −0.60 | −0.69 | −0.43 | −0.62 | −0.69 | −0.12 |

(continued)

**Table 5** (continued)

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 10 | Assists in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct | −0.45 | −0.59 | −0.29 | −0.5 | −0.69 | 0.12 |
| 11 | Maintains relationships with regulators, including the coordination of responses to consultative papers or other regulatory pronouncements | −0.40 | −0.54 | −0.29 | −0.42 | −0.69 | −0.12 |
| 12 | Develops and maintains a relevant internal manual for compliance within an organization | −0.43 | −0.39 | −0.43 | −0.5 | −0.85 | −0.04 |
| 13 | Prepares and submits to the regulator the monthly prevention statement | −0.49 | −0.49 | −0.29 | −0.54 | −0.85 | −0.36 |
| 14 | Prepares an annual report which assesses the firm's level of compliance with its obligation laid down in the law, and the money laundering and terrorist financing preventive issues | −0.47 | −0.64 | −0.14 | −0.5 | −0.85 | −0.12 |
| 15 | Responds to all requests and queries from MOKAS and the appropriate regulator (e.g., Cyprus Bar Association, CySEC, ICPAC, Central Bank) | −0.53 | −0.54 | −0.43 | −0.54 | −0.85 | 0.04 |
| 16 | Ensure the employees and management do not violate any regulations and legislations | −0.47 | −0.74 | −0.14 | −0.5 | −0.69 | −0.12 |

(continued)

**Table 5** (continued)

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 17 | Ensure the employees and management do not violate any written ethical codes of conduct | −0.49 | −0.74 | −0.14 | −0.54 | −0.69 | −0.04 |
| 18 | Ensure the employees and management do not violate any unwritten moral and ethical values | −0.53 | −0.69 | −0.29 | −0.54 | −0.85 | 0.04 |
| 19 | Designs the internal practice, measures, procedures, and controls relevant to the prevention of money laundering and terrorist financing and describes and explicitly allocates the appropriateness and the limits of responsibility of each relevant department | −0.40 | −0.49 | −0.43 | −0.46 | −0.69 | −0.04 |
| 20 | Develops and establishes the firm's AML policy and submits it to the board of directors for consideration and approval | −0.49 | −0.44 | −0.43 | −0.58 | −0.85 | −0.04 |
| 21 | Prepares a risk management and procedures manual regarding money laundering and terrorist financing | −0.55 | −0.59 | −0.43 | −0.58 | −0.85 | −0.12 |
| 22 | Monitors and assesses the correct and effective implementation of the policy principles in relation to money laundering and terrorist financings | −0.45 | −0.49 | −0.29 | −0.46 | −0.85 | −0.12 |

(continued)

**Table 5** (continued)

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 23 | Receives from the employees, information which is considered by the latter to be knowledge/suspicion of money laundering or terrorist financing activities | −0.47 | −0.44 | −0.29 | −0.5 | −1 | −0.04 |
| 24 | Validates/evaluate information received regarding the suspicion or the knowledge of money laundering or terrorist financing activities | −0.49 | −0.59 | −0.29 | −0.54 | −0.85 | 0.12 |
| 25 | Notifies MOKAS through online submission system of any actual or suspicious money laundering or terrorist financing activities following the evaluation of information | −0.55 | −0.54 | −0.43 | −0.62 | −0.85 | −0.04 |
| 26 | CO has a duty to fully explain the reasons of not notifying MOKAS in the Internal Evaluation Report | −0.57 | −0.54 | −0.43 | −0.62 | −0.85 | 0.04 |
| 27 | Acts as a first point of contact with MOKAS upon commencement of and during investigation as a result of filing a report to MOKAS | −0.62 | −0.59 | −0.43 | −0.69 | −0.85 | −0.12 |
| 28 | Ensures the preparation and maintenance of the lists of customers categorized following a risk-based approach | −0.51 | −0.49 | −0.57 | −0.54 | −0.85 | 0.04 |

(continued)

**Table 5** (continued)

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 29 | Based on customer risk evaluation, detects, records and evaluates, annually or biannually all risks arising from new customers and existing customers | −0.43 | −0.44 | −0.14 | −0.54 | −0.85 | −0.04 |
| 30 | Ensures that the branches of the firm that operate in countries outside the EEA have taken all necessary measures in relation to customer identification, due diligence, and record keeping procedures as per the EEA legal framework | −0.47 | −0.54 | −0.14 | −0.58 | −0.85 | −0.04 |
| 31 | Provides advice and guidance to other employees on money laundering and terrorist financing matters | −0.40 | −0.38 | −0.29 | −0.5 | −0.85 | −0.04 |
| 32 | Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing | −0.45 | −0.49 | −0.29 | −0.5 | −0.85 | −0.04 |

(continued)

**Table 5** (continued)

| *Resp no.* | | *Duties which are cost-beneficial for the CO to perform* | | | | | *Duties expected of COs by board/ management* |
|---|---|---|---|---|---|---|---|
| | | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* | *Managers* |
| 33 | Develops and maintains a relevant internal manual for compliance within an organization which is submitted to the board of directors for approval | −0.60 | −0.59 | −0.43 | −0.62 | −0.85 | −0.12 |
| 34 | Evaluates the systems and procedures applied by a third person on whom the compliance officer relies upon for customer identification and due diligence purposes | −0.49 | −0.64 | −0.29 | −0.54 | −0.85 | 0.04 |
| 35 | Incorporates compliance and ethics messaging into broad communications to employees and in day-to-day interactions with employees | −0.49 | −0.49 | −0.43 | −0.54 | −1 | −0.04 |
| 36 | Regularly reminds employees of the importance of ethical and compliant behavior, raising concerns and the company's non-retaliation policy | −0.51 | −0.64 | −0.14 | −0.58 | −1 | −0.12 |

**Table 6** Existing duties performed by CO

| *Resp. no* | | *CO overall* |
|---|---|---|
| 13 | Prepares and submits to the regulator the monthly prevention statement | 0.66 |
| 14 | Prepares an annual report which assesses the firm's level of compliance with its obligation laid down in the law, and the money laundering and terrorist financing preventive issues | 0.81 |
| 15 | Responds to all requests and queries from MOKAS and the appropriate regulator (e.g., Cyprus Bar Association, CySEC, ICPAC, Central Bank) | 0.81 |
| 19 | Designs the internal practice, measures, procedures, and controls relevant to the prevention of money laundering and terrorist financing and describes and explicitly allocates the appropriateness and the limits of responsibility of each relevant department | 0.83 |
| 20 | Develops and establishes the firm's AML policy and submits it to the board of directors for consideration and approval | 0.77 |
| 21 | Prepares a risk management and procedures manual regarding money laundering and terrorist financing | 0.70 |
| 22 | Monitors and assesses the correct and effective implementation of the policy principles in relation to money laundering and terrorist financings | 0.83 |
| 23 | Receives from the employees, information which is considered by the latter to be knowledge/suspicion of money laundering or terrorist financing activities | 0.85 |
| 24 | Validates/evaluate information received regarding the suspicion or the knowledge of money laundering or terrorist financing activities | 0.89 |
| 25 | Notifies MOKAS through online submission system of any actual or suspicious money laundering or terrorist financing activities following the evaluation of information | 0.87 |
| 26 | CO has a duty to fully explain the reasons of not notifying MOKAS in the Internal Evaluation Report | 0.89 |
| 27 | Acts as a first point of contact with MOKAS upon commencement of and during investigation as a result of filing a report to MOKAS | 0.85 |
| 28 | Ensures the preparation and maintenance of the lists of customers categorized following a risk-based approach | 0.83 |
| 29 | Based on customer risk evaluation, detects, records and evaluates, annually or biannually all risks arising from new customers and existing customers | 0.81 |

(continued)

**Table 6** (continued)

| *Resp. no* | | *CO overall* |
|---|---|---|
| 30 | Ensures that the branches of the firm that operate in countries outside the EEA have taken all necessary measures in relation to customer identification, due diligence, and record keeping procedures as per the EEA legal framework | 0.62 |
| 31 | Provides advice and guidance to other employees on money laundering and terrorist financing matters | 0.85 |
| 32 | Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing | 0.83 |
| 34 | Evaluates the systems and procedures applied by a third person on whom the compliance officer relies upon for customer identification and due diligence purposes | 0.70 |

**Table 7** Duties expected of CO by regulations

| *Resp. no* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 1 | Identifies the requirements of legislation and regulations for the business conducted by the organization; gathers and disseminates information about compliance requirements in the organization | 0.12 | 0.15 | −0.03 | 0.43 | 0.27 | −0.23 |
| 2 | Provides guidance on the proper application and interpretation of laws, regulations, and policies applicable to the firm. Such regulation may include rules, guidance documents, codes of conduct, and internal policies designed to meet regulatory compliance | 0.2 | 0.15 | 0.18 | 0.57 | 0.12 | −0.23 |
| 3 | Provides managers with guidance in the development, implementation, and maintenance of robust policies, procedures and practices for regulated activities | −0.04 | −0.02 | −0.18 | 0.43 | 0.08 | −0.54 |
| 4 | Creates a program of activities to educate and encourage both managers and staff to operate in compliance with relevant laws and regulations. This should include providing training on key compliance and regulatory matters such as complaints, money laundering, conflicts, and personal account dealing | −0.2 | 0.17 | 0.03 | 0.14 | 0.23 | −0.38 |
| 5 | Facilitates implementation and maintenance of a compliance-monitoring program, which provides management with assurance that key regulatory risks are being adequately managed within the business areas | −0.04 | 0.09 | −0.03 | 0.43 | 0.12 | −0.38 |

(continued)

**Table 7** (continued)

| *Resp. no* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 6 | Sets policies and procedures and proposes improvements in the event that the monitoring program identifies weaknesses | −0.12 | 0.04 | −0.23 | 0.43 | 0.15 | −0.38 |
| 7 | Provides regular and accurate reports to management (and where necessary to the board of directors) on regulatory and compliance matters. This should include the raising of significant issues, concerns, or regulatory breaches | −0.04 | 0.02 | −0.18 | 0.57 | 0.12 | −0.54 |
| 8 | Coordinates and assists other control and risk functions in order to comprehensively identify, assess, and manage regulatory risk | −0.28 | −0.09 | −0.44 | 0.43 | 0.04 | −0.54 |
| 9 | Supports senior management in establishing and maintaining good relationships with the regulators. This includes acting as the main point of contact between the institution and the relevant regulators | −0.28 | −0.11 | −0.38 | 0.71 | −0.12 | −0.54 |
| 10 | Assists in the development of an effective internal compliance culture by promoting the benefits of ethical business conduct | −0.12 | −0.06 | −0.08 | 0.71 | −0.16 | −0.69 |
| 11 | Maintains relationships with regulators, including the coordination of responses to consultative papers or other regulatory pronouncements | −0.28 | −0.11 | −0.18 | 0.14 | −0.15 | −0.38 |
| 12 | Develops and maintains a relevant internal manual for compliance within an organization | −0.04 | −0.02 | −0.13 | 0.14 | 0.04 | −0.23 |
| 13 | Prepares and submits to the regulator the monthly prevention statement | −0.36 | 0.17 | −0.08 | 0.14 | 0.19 | −0.23 |

(continued)

**Table 7** (continued)

| *Resp. no* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 14 | Prepares an annual report which assesses the firm's level of compliance with its obligation laid down in the law, and the money laundering and terrorist financing preventive issues | −0.28 | 0.11 | −0.23 | 0.43 | 0.19 | −0.38 |
| 15 | Responds to all requests and queries from MOKAS and the appropriate regulator (e.g., Cyprus Bar Association, CySEC, ICPAC, Central Bank) | −0.04 | 0.17 | −0.08 | 0.57 | 0.23 | −0.23 |
| 16 | Ensure the employees and management do not violate any regulations and legislations | −0.28 | 0.06 | −0.03 | 0 | 0.08 | −0.38 |
| 17 | Ensure the employees and management do not violate any written ethical codes of conduct | −0.36 | −0.15 | −0.23 | −0.14 | −0.12 | −0.54 |
| 18 | Ensure the employees and management do not violate any unwritten moral and ethical values | −0.36 | −0.21 | −0.28 | 0 | −0.23 | −0.54 |
| 19 | Designs the internal practice, measures, procedures, and controls relevant to the prevention of money laundering and terrorist financing and describes and explicitly allocates the appropriateness and the limits of responsibility of each relevant department | −0.12 | 0.09 | −0.13 | 0.57 | 0.15 | −0.54 |
| 20 | Develops and establishes the firm's AML policy and submits it to the board of directors for consideration and approval | −0.04 | 0.15 | −0.08 | 0.71 | 0.19 | −0.38 |
| 21 | Prepares a risk management and procedures manual regarding money laundering and terrorist financing | −0.04 | 0.21 | −0.08 | 0.86 | 0.23 | −0.23 |
| 22 | Monitors and assesses the correct and effective implementation of the policy principles in relation to money laundering and terrorist financings | −0.28 | 0.11 | −0.18 | 0.57 | 0.15 | −0.38 |

(continued)

**Table 7** (continued)

| *Resp. no* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 23 | Receives from the employees, information which is considered by the latter to be knowledge/suspicion of money laundering or terrorist financing activities | −0.2 | 0.13 | −0.23 | 0.57 | 0.23 | −0.38 |
| 24 | Validates/evaluate information received regarding the suspicion or the knowledge of money laundering or terrorist financing activities | 0.04 | 0.06 | −0.08 | 0.71 | 0.12 | −0.54 |
| 25 | Notifies MOKAS through online submission system of any actual or suspicious money laundering or terrorist financing activities following the evaluation of information | 0.2 | 0.15 | −0.03 | 0.71 | 0.23 | −0.23 |
| 26 | CO has a duty to fully explain the reasons of not notifying MOKAS in the Internal Evaluation Report | 0.04 | 0.09 | −0.13 | 0.86 | 0.12 | −0.38 |
| 27 | Acts as a first point of contact with MOKAS upon commencement of and during investigation as a result of filing a report to MOKAS | −0.04 | 0.17 | 0.03 | 0.86 | 0.08 | −0.23 |
| 28 | Ensures the preparation and maintenance of the lists of customers categorized following a risk-based approach | −0.04 | 0.11 | −0.13 | 0.71 | 0.15 | −0.38 |
| 29 | Based on customer risk evaluation, detects, records and evaluates, annually or biannually all risks arising from new customers and existing customers | 0.04 | 0.11 | −0.08 | 0.71 | 0.19 | −0.54 |
| 30 | Ensures that the branches of the firm that operate in countries outside the EEA have taken all necessary measures in relation to customer identification, due diligence, and record keeping procedures as per the EEA legal framework | −0.12 | 0.15 | −0.08 | 0.57 | 0.27 | −0.54 |

(continued)

**Table 7** (continued)

| *Resp. no* | | *Managers* | *CO overall* | *Accounting* | *Banking* | *CySEC* | *Legal* |
|---|---|---|---|---|---|---|---|
| 31 | Provides advice and guidance to other employees on money laundering and terrorist financing matters | −0.04 | 0.04 | −0.13 | 0.57 | 0.08 | −0.38 |
| 32 | Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing, and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing | 0.12 | 0.09 | −0.03 | 0.71 | 0.08 | −0.23 |
| 33 | Develops and maintains a relevant internal manual for compliance within an organization which is submitted to the board of directors for approval | −0.04 | 0.04 | −0.18 | 0.57 | 0.15 | −0.54 |
| 34 | Evaluates the systems and procedures applied by a third person on whom the compliance officer relies upon for customer identification and due diligence purposes | −0.12 | 0.06 | −0.13 | 0.29 | 0.15 | −0.38 |
| 35 | Incorporates compliance and ethics messaging into broad communications to employees and in day-to-day interactions with employees | −0.44 | −0.28 | −0.59 | 0.14 | −0.12 | −0.85 |
| 36 | Regularly reminds employees of the importance of ethical and compliant behavior, raising concerns and the company's non-retaliation policy | −0.36 | −0.26 | −0.44 | 0.14 | −0.15 | −0.85 |

## References


Aznar, E., and Vaccaro, A. (2015). Make Way for the Chief Integrity Officer. *IESE Insight Fourth Quarter, 27,* 23–30.

Baldock, G. (2016). The Perception of Corruption Across Europe, Middle East and Africa. *Journal of Financial Crime, 23*(1), 119–131.

Belton, P. (2009). The Evolving Role of Compliance Officers During These Difficult Economic Times. *Journal of Health Care Compliance, 11*(4), 11–16.

Berenbeim, R. E. (2010). Utilizing HR and Ethics and Compliance Collaboration to Promote an Ethical Culture. *Employment Relations Today, 37*(1), 17–26.

Bravo, D. Y., Umaña-Taylor, A. J., Toomey, R. B., Updegraff, K. A., and Jahromi, L. B. (2016). Risky Behaviors and Educational Attainment Among Young Mexican-Origin Mothers: The Role of Acculturative Stress and the Educational Aspiration–Expectation Gap. *International Journal of Intercultural Relations, 52,* 13–26. https://doi.org/10.1016/j.ijintrel.2016.02.003. Accessed 1 November 2018.

Brooks, J. (2010). Directors and Officers of U.S. Multinationals: Minimizing Risk in an Era of Enhanced Responsibility. *Practical Lawyer, 56*(6), 49–57.

Brown, J. (2010). Compliance Effectiveness: How Do We Get There? *Journal of Health Care Compliance, 12*(4), 37–40.

De Dios, M. A. (2016). The Sixth Pillar of Anti-money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy. *Brooklyn Journal of Corporate, Financial & Commercial Law, 10.* http://brooklynworks.brooklaw.edu/bjcfcl/vol10/iss2/7. Accessed 20 October 2018.

DeMott, D. A. (2013). The Crucial but (Potentially) Precarious Position of the Chief Compliance Officer. *Brooklyn Journal of Corporate, Financial & Commercial Law, 8,* 56–79.

Dols, T., and Silvius, A. J. G. (2010). Exploring the Influence of National Cultures on Non-compliance Behavior. *Communications of the IIMA, 10*(3), 11–32.

Duszak, R. (2008). Building a Better Compliance Officer. *Journal of the American College of Radiology, 5*(11), 1106–1108.

Edwards, J., and Wolfe, S. (2005). Compliance: A Review. *Journal of Financial Regulation and Compliance, 13*(1), 48–59.

Forman, S. (2013). Compliance Program Leveraging of Audit Resources. *Journal of Health Care Compliance, 15*(4), 55–58.

Füredi-Fülöp, J. (2015). An Empirical Study of Audit Expectation Gap in Hungary. *Theory, Methodology, Practice, 11*(1), 37–46.

Gherai, Dana Simona. (2011). Audit Expectation Gap in the Public Sector in Romania. *Annals of the University of Oradea: Economic Science, 20*(2), 510–516.

Gibeaut, J. (2002). Show Them the Money: The Anti-terrorism Laws Target Money Laundering, Forcing Banks to Be More Vigilant and Compliance Officers to Take on More Tasks. *ABA Journal, 88*(1), 46–51. http://www.jstor.org/stable/27841938. Accessed 2 November 2018.

Gnazzo, P. J. (2011). The Chief Ethics and Compliance Officer: A Test of Endurance. *Business and Society Review, 116*(4), 533–553.

Grant-Hart, K. (2016). *How to Be a Wildly Effective Compliance Officer*. London: Brentham House Publishing.

Greenberg, M. D. (2009). *Perspectives of Chief Ethics and Compliance Officers on the Detection and Prevention of Corporate Misdeeds: What the Policy Community Should Know*. Santa Monica, CA: RAND Corporation. http://www.rand.org/pubs/conf_proceedings/CF258.html. Accessed 2 November 2018.

Harvey, J. (2004). Compliance and Reporting Issues Arising for Financial Institutions from Money Laundering Regulations: A Preliminary Cost Benefit Study. *Journal of Money Laundering Control, 7*(4), 333–346.

Idris, A., and Ojemen, C. (2012). Existence and Nature of Audit Expectation Gap: Nigerian Perspective. *Asian Economic and Financial Review, 2*(8), 1051.

International Compliance Association (ICA). (2016). *ICA International Diploma in Governance, Risk and Compliance*. International Compliance Training. https://www.int-comp.org/. Accessed 11 November 2018.

Islam, T., Ahmed, I., Khalifah, Z., Sadiq, M., and Faheem, M. A. (2015). Graduates' Expectation Gap: The Role of Employers and Higher Learning Institutes. *Journal of Applied Research in Higher Education, 7*(2), 372–384. https://doi.org/10.1108/jarhe-05-2014-0056. Accessed 10 October 2018.

Jones, D. S., and Bird, L. C. P. N., Jr. (2008). Are Compliance Officers Leading the Way When It Comes to Quality? *Journal of Health Care Compliance, 10*(5), 43–48.

Kavanagh, S. (2008). Paper Discusses the Role of a Chief Ethics and Compliance Officer. *Journal of Health Care Compliance, 10*(1), 25–28.

Krambia-Kapardis, M. (2001). *Enhancing the Auditor's Fraud Detection Ability*. Frankfurt: Peterlang.

Lafferty, L. T. (2010). The Habits of Highly Effective Compliance Officers from Effectiveness to Greatness in Your Program Activities. *Journal of Health Care Compliance, 12*(6), 11–18.

Liggio, C. D. (1974). The Expectation Gap: The Accountant's Legal Waterloo. *Journal of Contemporary Business, 3*(3), 27–44.

Madichie, N. O. (2007). Nigerian Restaurants in London: Bridging the Experiential Perception/Expectation Gap. *International Journal of Business and Globalisation, 1*(2), 258. https://doi.org/10.1504/IJBG.2007.014434.

Martin, S. L. (2015). Compliance Officers: More Jobs, More Responsibility, More Liability. *Notre Dame Journal of Law, Ethics & Public Policy, 29*(1), 169–198.

McGreal P. E. (2017). HorseShoes and Hand Grenades: Protecting Compliance Officers from the At-Will Employment Doctrine. *University of Toledo Law Review, 48,* 485–492.

Méndez, F. (2012). Can Corruption Foster Regulatory Compliance? *Public Choice, 158,* 189–207.

Miller, G. P. (2017). Compliance: Past, Present and Future. *University of Toledo Law Review, 48,* 437–451.

Mills, A. (2008). *Essential Strategies for Financial Service Compliance*. Chichester, New York: Wiley.

Morf, D. A., Schumacher, M. G., and Vitell, S. F. (1999). A Survey of Ethics Officers in Large Organizations. *Journal of Business Ethics, 20,* 265–271.

Nadana, A., and Kim, W. (2014). The Expectation-Performance Gap in Generic Skills in Accounting Graduates. *Asian Review of Accounting, 22*(1), 56–72.

Parker, C., and Gilad, S. (2011). Internal Corporate Compliance Management System: Structure, Culture and Agency. In C. Parker and V. L. Nielsen (Eds.), *Explaining Compliance: Business Responses to Regulation* (pp. 170–197). Cheltenham: Edward Elgar.

Parker, C., and Nielsen, V. L. (2011). *Explaining Compliance: Business Responses to Regulation*. Cheltenham: Edward Elgar.

Perezts, M., and Picard, S. (2015). Compliance or Comfort Zone? The Work of Embedded Ethics in Performing Regulation. *Journal of Business Ethics, 131,* 833–852.

Perrone, C. M. (2014). The Language of Collaboration. *Journal of Health Care Compliance, 16*(1), 22, 63–66.

Perry, J. C., Przybysz, J., and Al-Sheikh, M. (2009). Reconsidering the Aspiration–Expectation Gap and Assumed Gender Differences Among Urban Youth. *Journal of Vocational Behavior, 74*(3), 349–354.

Pok, W. C., Omar, N., and Sathye, M. (2014). An Evaluation of the Effectiveness of Anti-money Laundering and Anti-terrorism Financing Legislation: Perceptions of Bank Compliance Officers in Malaysia. *Australian Accounting Review, 24*(4), 394–401.

Porter, B. A. (1988). *Towards a Theory of the Role of the External Auditor in Society*. Research Monograph No. 1, Massey University.

Porter, B. A. (1993). An Empirical Study of the Audit Expectation–Performance Gap. *Accounting and Business Research, 24*(93), 49–68.

Porter, B. A., and Gowthorpe, C. (2004). *Audit Expectation–Performance Gap in The United Kingdom in 1999 and Comparison with the Gap in New Zealand in 1989 and in 1999*. Edinburgh: The Institute of Chartered Accountants of Scotland. https://www.icas.com/__data/assets/pdf_file/0019/7705/65-Audit-Expectation-Performance-GAP-UK-and-New-Zealand-Comparison-ICAS.pdf. Accessed 2 November 2018.

Power, M. (1997). *The Audit Society: Rituals of Verification*. New York: Oxford University Press.

Ruhnke, K., and Schmidt, M. (2014). The Audit Expectation Gap: Existence, Causes, and the Impact of Changes. *Accounting and Business Research, 44*(5), 572–601. https://doi.org/10.1080/00014788.2014.929519. Accessed 2 November 2018.

Schminke, M., Caldwell, J., Ambrose, M. L., and McMahon, S. R. (2014). Better Than Ever? Employee Reactions to Ethical Failures in Organizations, and the Ethical Recovery Paradox. *Organizational Behavior and Human Decision Processes, 123,* 206–219.

Snell, R. (2009). The Tables Are Turned as Roy Snell Offers His Insight on the Current State of Compliance. *Journal of Health Care Compliance, 11*(2), 33–36.

Snell, R. (2015). A Brief History of Time… in Compliance: Yes, Compliance Can Be Tough, but It Can Also Be Meaningful and Rewarding. *Journal of Health Care Compliance, 17*(5), 3–5.

Treviño, L. K., den Nieuwenboer, N. A., Kreiner, G. E., and Bishop, D. G. (2014). Legitimating the Legitimate: A Grounded Theory Study of Legitimacy Work Among Ethics and Compliance Officers. *Organizational Behavior and Human Decision Processes, 123,* 186–205.

Treviño, L. K., Weaver, G. R., Gibson, D. G., and Toffler, B. L. (1999). Managing Ethics and Legal Compliance: What Works and What Hurts. *California Management Review, 41*(2), 131–151.

Tyler, T. R. (2006). Psychological Perspectives on Legitimacy and Legitimation. *Annual Review of Psychology, 57,* 375–400.

United Office on Drugs and Crime (UNODC). (2018). *Money Laundering and Globalisation*. https://www.unodc.org/unodc/en/money-laundering/globalization.html. Accessed 15 September 2018.

Van Duyne, P. C. (1998). Money-Laundering: Pavlov's Dog and Beyond. *The Howard Journal, 37*(4), 359–374.

Verhage, A. (2009). Between the Hammer and the Anvil? The Anti-money Laundering-Complex and Its Interactions with the Compliance Industry. *Crime Law Society Change, 52,* 9–32.

Weaver, G. R., and Treviño, L. K. (1999). Compliance and Values Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior. *Business Ethics Quarterly, 9*(2), 315–335.

Weaver, G. R., Treviño, L. K., and Cochran, P. L. (1999). Corporate Ethics Programs as Control Systems: Influences of Executive Commitment and Environmental Factors. *Academy of Management Journal, 42*(1), 41–57.

Weber, J., and Fortun, D. (2005). Ethics and Compliance Officer Profile: Survey, Comparison and Recommendations. *Business and Society Review, 110*(2), 97–115.

Weber, J., and Wasieleski, D. M. (2012). Corporate Ethics and Compliance Programs: A Report, Analysis and Critique. *Journal of Business Ethics, 112*(4), 609–626.

**Maria Krambia-Kapardis** is an Associate Professor of Accounting, Cyprus University of Technology, a Fellow member of the Chartered Accountants of Australia and New Zealand, and a Certified Fraud Examiner. For a number of years, she was a university academic in Australia, has been a Visiting Scholar at Cambridge University; Girona University, Spain; and Visiting Professor at Victoria University, Melbourne, Australia. She was the founder and first Chair of Transparency International-Cyprus (2010–2017), for a number of years served as the country corruption correspondent for the European Commission, was the founder and first president of the Economic Crime and Forensic Accounting Committee of the Institute of Certified Public Accountants of Cyprus (2010–2014), and she is a member of the disciplinary body of the Institute of Certified Public Accountants of Cyprus. She has authored a number of books, articles in peer-reviewed journals and presented her work at international conferences. Her research interests include: fraud detection, investigation and prevention; anti-corruption; corporate responsibility; corporate governance; gender issues in business; and ethical behavior. She has been the local coordinator for a number of EU-funded projects. In 2015, she was awarded two best paper awards by Emerald for her articles on corruption. Krambia-Kapardis is on the editorial board of a number of peer-reviewed journals, has been the examiner of a number of Ph.Ds overseas and in 2017 was commissioned by the Cyprus Ministry of Justice and Public Order to author a Report on Anti-Corruption Agencies. Finally, in 2017 the *Gold Business Magazine* named her one of the 100 most powerful and influential women in Cyprus and was also awarded the ACFE's 2019 Achievement in Outreach/Community Service Award for being an active contributor to her community and being committed to helping improve the quality of life where she lives and works.

**Salomi Dimitriou** is a Lecturer in Accounting at the University of Central Lancashire and a special scientist at Cyprus University of Technology. She is the Course Leader of B.A. Accounting and Finance at the University of Central Lancashire. She previously held academic positions at the Open University of Cyprus; Unicaf, Cyprus; King's College of London and Fulham and Chelsea College, London. She holds M.Sc. in Accounting, Organisation and Institutions and a Ph.D. in Corporate Social and Environmental Responsibility. Salomi's research interests include compliance, ethics, corruption, corporate responsibility, and governance.

**Ioanna Stylianou** is a Lecturer in Statistics and Econometrics at the University of Central Lancashire Cyprus (UCLan) and research fellow at the University of Cyprus. She is the Course Leader for the Economics and Business Administration division at the University of Central Lancashire Cyprus. She previously held academic positions at the University of Cyprus (Visiting Lecturer), the Cyprus University of Technology (Special Scientist) and at the University of Wisconsin Madison, USA (research visiting scholar). Her research interests lie in the field of econometrics and macroeconomics with emphasis on the implications of model uncertainty (theory uncertainty and parameter heterogeneity) on economic growth, income inequality, social mobility, growth volatility and employment volatility through the implementation of Bayesian Model Averaging and non-linear models. Also, she is interested in short-run and long-run implications of structural changes on time series relationships. Her most recent research focuses on the relationship between income inequality and social mobility, income inequality and employment volatility in SMEs, compliance practices and the implementation of non-linear methods to model tourism demand.

# Conclusion

In its 2018 report on *Getting Ahead of the Watchdog*, PwC acknowledges that big data, analytics, artificial intelligence, the cloud, robotics, drones, blockchains, and 3-D printing have changed the business climate and how corporations operate. This increasing velocity of information is inevitably increasing the demands placed upon compliance departments and increases the pressure on compliance officers (COs) to achieve efficiency and effectiveness. Furthermore, the compliance professional of the future is required to have diverse talents, come from different disciplines, and have the mindset and behavior that will enable him/her to respond to the growing expectations from regulators, businesses, and customers. Furthermore, PwC suggests in the same report that COs "grapple with an ever-more-complicated risk landscape and ever-changing regulatory requirements" (p. 18).

In order to know where one is going, one needs to firstly contextualize the state of art and state of practice. The current edited book and more specifically each chapter provides the milestones needed by COs.

Chapters 1 and 2 of the book, by Sir Anthony Bottoms and Dr. Justice Tankebe, respectively, set the conceptual groundwork for the multifaceted and interactive complexity of compliance processes. In unraveling these complexities, they provide a set of tools with particular attention being paid to the "dissective" dimension of mechanism-based analyses and the typology of compliance mechanisms in an attempt to address some features of compliance in the field of business regulation.



M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8

Cognizant of the tensions among the legitimation mechanism and the guest to maximize profits, it is concluded that legitimacy is never given but is forever an "unfinished business" where leaders play a key role in creating a moral climate within corporations that emphasize the principles of legitimacy in all aspects of work.

Chapter 3 examines the professional status of compliance in the USA and explains why the legal profession is likely to exert continuing influence over compliance, which would lead the latter to remain a satellite occupation, given the legalization of compliance in regulated areas and the overall influence of prosecutors and enforcement officials on organizational compliance. Professor Fanto also emphasizes that compliance practitioners must themselves be the ones pushing for professional status. In addition, it is noted that by observing the compliance practice outside the USA it may offer professional alternatives to the legally influenced perspective. Furthermore, Professor Fanto concludes that the debate about compliance's professional status is likely to continue because it is both an important organizational function as well as a relatively new occupation. As is evidenced by the international compliance conference that was the inspiration for this book, compliance is attracting more academic attention throughout the world, as scholars seek to understand it and propose ways to make it more effective. It is thus likely that, through this intellectual activity, there will be more insight about the outcome of the professionalization of compliance.

Chapter 4 demonstrates that the experience worldwide has shown that there is a limit to how much human behavior can be regulated by enacted legislation given the usefulness of soft law, both at the international and national level. Mrs. Lancri discusses in this chapter the role of soft law and the increased role played by NGO's in helping to formulate, implement, and effectively monitor conformity to stipulated principles and procedures. Finally, the chapter concludes with a discussion on Sapin II Law, the establishment of a new French Anti-Corruption Agency and the significance of both hard and law in effectively establishing compliance.

Chapter 5 provides a consolidated overview of how General Data Protection Regulation (GDPR) came in to existence, its aims, and lessons learned so far. Mr. Foulsham believes after May 2018 the world and its citizens ought to feel their privacy is respected. Having discussed throughout the chapter the realities and complexities in adopting the new regulation, Mr. Foulsham concludes that companies are held to account and drives all to provide prompt, transparent, and clear disclosure.

Chapter 6 outlines that the UK regulatory regime for financial services facilitates the holding to account of senior management including those that hold responsibility for compliance oversight and money laundering reporting. Professor Bazley discussed the issue of accountability and liability for those working in senior compliance roles and concluded that in providing for a risk-based approach to compliance with regulation, the regulatory regime has established a necessary connection between regulation, risk, and a compliance function. He also noted that the compliance function, by providing advice and undertaking monitoring, is regarded as an inherent part of a firm's overall risk control framework.

Chapter 7 discusses the significance of whistleblowing as an effective element of compliance. Assoc. Prof. Tsahuridu has argued that to ensure compliance with whistleblowing laws, it is important that people feel that they will be, and are in fact, heard, as well as protected from direct and indirect forms of retaliation and harm. Laws need to focus not only on the protection of whistleblowers but they should also impose obligations on organizations and their compliance function to effectively manage whistleblowing by responding to the report and the reporter in a timely and effective manner. Compliance that only focuses on the inputs of policies, codes, and training is in danger of becoming what has been termed "cosmetic compliance."

Chapter 8 acknowledges that a CO needs to possess certain skills in order to be effective and strategic. Whilst the skill set required by a CO is discussed in order to be effective in carrying out his/her duties, it is acknowledged that the actual work of an effective CO is a mixed blessing. This is because there is a limit to how much an effective CO can achieve in a company. Finally, the chapter concludes by highlighting that it is absolutely essential that the Board demonstrates the political will to provide the necessary resources to the compliance department.

Chapter 9 places the capstone on the edited book as it attempts to disentangle the expectation gap for COs. It does so by acknowledging both the invisibility of compliance personnel and the evolution of the compliance field as well as the lack of consistency in qualifications, experience etc. and the increasing demands placed upon the COs by the Board and the regulators. Utilizing the results of a survey carried out in Cyprus of COs, the authors have found the existence of an expectation-performance gap with two components, a knowledge gap and a reasonableness gap, but no deficient regulations or performance gap.

In other words, the COs appear to be performing the duties as derived by law, and the legislation appears with no major gaps or omissions based on the cost-beneficial criterion of COs. It was found that whilst the COs in the current study were all well-educated and hold professional qualifications, they do not appear to be well versed in their legal duties. Thus, it is suggested that COs ought to hold a postgraduate qualification in Financial Compliance or pass relevant examination(s) with continuing professional education requirements. It is essential to educate both COs and managers about the role and responsibilities of a CO in order to ensure that there are no misunderstandings. Compliance is a process that requires the engagement of the organization as a whole—from the highest stratum of the organization all the way to the front-line personnel. Educating COs will help in performing all responsibilities set by law and in ensuring organizations are being legal and compliant. However, it is also important to educate managers so they understand and appreciate the work of COs.

The diverse professional background of the contributors (some are academics and others practitioners), as well the international coverage of the chapters makes this edited book a notable contribution to the field of compliance, an area of research and practice which is likely to be of interest to the financial sector for many years to come.

PwC. (2018). *Getting Ahead of the Watchdog*. https://www.pwc.ch/en/publications/2018/PwC-2018-State-of-Compliance.pdf. Accessed 10 December 2018.

# Index




M. Krambia-Kapardis (ed.), *Financial Compliance*,
https://doi.org/10.1007/978-3-030-14511-8