CONDUCT RISK — WHEN COMPLIANCE BECOMES A GAME
DR. ROGER MILES

The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of Thomson Reuters.
ABOUT THE AUTHOR
Dr. Roger Miles counsels on strategic risk and uncertainty. Leaders in corporate, professional and public sectors now use his simple interventions to transform their organizations’ collective self-awareness and to displace value-threatening behaviors. With published research and commercial interests in organizational psychologies of risk, he develops trading products and new approaches to protecting value in brands; and leads behavioral risk learning on postgraduate courses.
INTRODUCTION

Earlier papers in this series have supported regulators’ calls for a new culture of risk control. To reach further into financial markets requires a new generation of risk controls which go beyond mere financial reporting and impact directly on human behavior. Most financial services organizations are considering their own approach to conduct risk. For many, this means asking “Are we vulnerable to enforcement action, and if so, where?” Some organizations have already found – the hard way, with fines in the tens of millions – that it can be costly to ignore the significance of good conduct. More than ever, organizations want to know how behavioral factors affect people making decisions in the face of risk. This new knowledge that they are seeking does exist. Thanks to recent developments in behavioral research, we are now able to see, for example, how a regulator’s concept of risk differs from a market-maker’s. Referred to by researchers as “cognitive gaps” or “asymmetries”, these mismatches help to explain why many risk controls have historically failed, including major systemic collapses. These gaps are of deep concern to regulators and so should be to all of us – financial services organizations are starting to explore their importance.

In fact, the gaps occur from a simple enough starting-point. Much of the current nervousness around conduct risk arises from what risk cognitive analysts call input asymmetries: that is, problems arising from the differing ways that businesses and regulators define their core tasks and deploy their resources to address these. Although this paper is mainly concerned with the “compliance game” outputs found in recent research, it is worth first briefly reminding ourselves why inputs matter too. Unwanted outputs, including non-compliance and other failures of risk control, flow from poorly conceived control structures; these bad designs, in turn, are often created when organizations fail to appreciate how a new control measure will work when it’s given to real people to use – the “what actually happens” behavioral effect. A future white paper will look in more detail at the mismatch in conceptions of risk between various industrial sector cultures, governments and regulators. For now, it is helpful to be aware of how the task of framing risk controls may itself be compromised, before turning to the more colorful topic of the resulting “games”.

WHY COMPLY?

TWO CONTRASTING VIEWS OF RISK

The point is perhaps so obvious that it’s often overlooked: people who work as regulators are generally motivated by rather different things from people who work in regulated commercial sectors. One can prove this by a simple research probe, asking each of these two groups of employees “What is risk management for?” and “What does the word “risk” signify to you?” Regulatory staff - and the public sector as a whole - tend to conceive risk primarily in terms of threat. They see risk analysis as a vital tool to help them contain and prevent hazards. Commercial people, by contrast, see risk as a structured way to pursue opportunities for profit. Although these two different cultures of risk may not be exact opposites, they show a contrast in emphasis which helps to explain why there are persistent gaps between regulatory design and the reality of compliance: why, in the real world, rules are broken.

Working with many public- and private-sector practitioner groups over the years, this researcher has found a contrasting pair of visual...
metaphors, each of which speaks strongly to one or other side of the cultural divide about what “risk” really means. For public-sector people, the icon of risk engagement is a news photograph of a firefighter rescuing a child from a burning building. For the private sector, “risk” appears as a very different type of picture: that of a gold prospector in 1848, tooling up and saddling his mule to head for California.

Why do these mental pictures of risk matter? Consider this: recent research shows that our choice of career is heavily influenced by the structure of our brains and in particular by the workings of our personal neurochemical reward system. According to this research, we self-select and pursue a career in either the public service or commerce depending on whether our brains are more inclined to reward risk-taking or risk-aversion. One anti-social outcome of this effect is that people whose brain chemistry rewards risk-taking are often drawn to work in financial services. At the extreme end of the scale, some people with an elevated (gambler’s) appetite for risk find the financial sector irresistible. Should we really be surprised that a sector where money is a constant presence is skewed towards attracting thrill-seekers?

The financial services industry, then, is fated to be one type of organized activity that greatly excites the interest of chancers, despite the best efforts of HR and security departments to bar the door to these characters. The chancer’s rationale has a beautiful simplicity, perhaps best summed up by a famously reported conversation with career bank robber Willie Sutton back in 1951. When the judge asked “Why do you rob banks?”, Sutton replied “Because that’s where the money is.”

To unpack this just a little: places and commercial sectors where there are large concentrations of money naturally attract criminal enterprise as seen in historic sales frenzies in complex derivatives contracts, or simply the proximity of large quantities of cash. In passing, we might also note that this hazard is not unique to financial product providers: there’s also an “evil twin” of this effect in the public sector, where the Willie Sutton factor may be found in the business of government procurement, especially in countries where democracy is in short supply. As anti-corruption experts well know, a kleptocrat likes nothing better than to start up a big infrastructure project, such as building a dam or a highway (and preferably hidden away in the middle of nowhere), as their preferred tool for quietly siphoning the national exchequer into their own pocket.

At the heart of the problem, then, lies a clash of concepts as the phrase “risk management” has divergent meanings for different organized groups. Governments and regulators approach risk management mainly as the business of preventing hazards and enforcing compliance. Commercial firms see risk management as the art of turning a profit on risk-taking. Many commercial firms, to be fair, can point to a strong record in ethical and regulatory compliance that proves their deep commitment to good behavior and sound management. But, to oversimplify this in terms of cash flow: for as long as compliance activity takes up a lot of expensive resources, a few people will always regard that as resources displaced from the higher priority of making sales.

Where practitioners resent giving proper resources to compliance, one available (though unethical) alternative is “creative compliance” – that is, presenting a compliant public face whilst not actually changing one’s behavior to conform to what the rules require. If one’s core values include the twin beliefs that compliance is a cost to be avoided and that making profit
trumps all other considerations, then the behaviors listed in the following section of this paper may be rationalized as acceptable or even normal. For regulators – and indeed the rest of us who possess any kind of moral compass – the following behaviors would not seem to fall within our normal working definitions of “acceptable risk engagement”.

However, for as long as there remains even a small minority who cling to the Moral Vacuum school of risk management, we should all look carefully for signs of their work in progress. Among the myriad forms that creative compliance may take, several consistent patterns of behavior have been explored in recent research studies, highlighted below.

**TYPES OF CREATIVE COMPLIANCE**

As outlined in a previous white paper, games of compliance may be roughly divided into three categories: people-games; reframing; and gaming the system. Because real life is messy, there are of course some overlaps between the three sets. In any case, this grouping is only one suggestion to help to identify and group together patterns of similar phenomena. It is very much in the public interest – not to mention, quite entertaining – to find and report new examples of each of these games. The game examples in the following list are all proven to exist, as unfortunately seen in reports arriving daily from a wide range of sectors.

- **Revolving door** (including its most common variant: poachers and gamekeepers): In this game commercial organizations second their own staff to the regulator’s office, to sound out what’s going on there. In an alternate version of this game the regulators themselves, or quasi-regulatory staff such as external auditors, “go native” with in-house secondments to regulated firms. Of course, argue many players, experience on both sides of the regulatory divide is helpful for all concerned and can only improve dialogue and ultimately the framing of regulation itself. Up to a point, maybe so. But 21st century history already provides two painful warnings, at least: the implosion of Arthur Andersen, whose staff had permanent residence in two floors of Enron’s headquarters; and the hasty departure of a CEO of a major bank, who allegedly had a problem with legitimate whistleblowing.
• **Bad apple**: This is a classic blame-shift tactic used by ethically blind senior managers. The institution cynically rewards aggressive risk-taking for as long as this is profitable, but then disowns any large-loss events as the work of an unlicensed junior, acting alone – trades which “couldn’t possibly reflect our ethical values”. And yet: Isn’t there at least a grain of plausibility in the defense offered by Leeson, Kerviel, Hamanaka, The Whale and other indicted rogue traders, that they’d started to run up their huge positions because at first their employers had rewarded them for their “brave” risk-taking?

• Where a team has been caught mis-selling, there is a standard set of attempted blame-shifts which seek to implicate the victim in the crime. Our modern understanding of this game is informed by a landmark research study of criminals appearing in court. Nearly sixty years after the study, its core finding still stands up: rule-breakers use a standard set of justifications to rationalize and play down their accountability for their own bad behavior. A creative complier will displace blame anywhere as long as it’s away from himself. For example: the mis-sale is the victim’s fault (they were asking for it); it is the fault of an employer organization or society as a whole (for putting temptation in my way); it doesn’t really count (no-one was really hurt; losses are insured anyway); any unethical earnings are an entitlement, not a crime (everyone else is doing it, why shouldn’t I?).

• **“We’re special people”**: Creative compliers often excuse themselves from obedience to rules on the grounds that they are “exceptional” people: also known as the Rock Star Defense (because you enjoy what I produce, you can’t question how I live and work). Creative compliers may go one stage further, bending reality, for example, by inventing an alternative future in which there are extenuating circumstances (oh, of course that product’s losing money now – the market just hasn’t found us yet).
Games of re-framing and measurement

• Normalizing bad behavior: This is another perverse payoff from the cognitive bias known as social proof – the justification used by blame-shifters everywhere (see above) that “everyone’s doing it”. In this game, a corrupt team starts to encourage others around them at first to tolerate, and then to condone, their unlicensed risk-taking. Eventually the team’s results are reported as routine successes. This team’s first move is typically over-eager selling, moving on to aggressive plays disguised as logical arguments against honest others, such as forced teaming (if you’re not with us you’re against us) and violent innocence (accusing your accuser). The dismal record of mistreatment of whistleblowers in many sectors – even after their rebranding as “public interest disclosers” – shows how little the embedded risk cultures of self-protection have changed. Normalizing has brought us, among other large-loss events: the NASA Challenger shuttle disaster; infant deaths at the Bristol Royal Infirmary; the BP Deepwater Horizon and Texas City incidents; and many banks’ mortgage selling pre-2008.

• Nelson’s eye: This game is named after the famous one-eyed English admiral, who chose to ignore a command signal to retreat by placing his telescope to his blind eye and remarking to his deputy “I see no signal”. There are several variants – simply look away, misdirect others’ attention, report on some other irrelevant factor, or just deny the existence of a challenge – but the aim of the game remains the same: to ignore anything which contradicts the player’s intended course of action.

• Reframing: If the reported results don’t fit expectations, run a new series of tests until the numbers improve. Alternatively, re-base your system of measurement; re-define your key risk indicators; or otherwise “move the goalposts”. A variant of this is to engage in target-chasing, relying on narrowly-defined numerical measures of performance (such as headline sales figures) and deliberately ignoring behavioral factors (such as levels of customer complaint).
Games with systems
(including regulatory-political regimes)

• Agreeing that inspections are pre-notified: A genuine inspection entails an unannounced visit by auditors. Then there’s the other, performative kind of visit: the carefully prepared inspection where a personal call from the regulator to a senior manager warns the regulatee in advance to expect a visit – so that the subsequent visit goes smoothly, with materials and disclosures carefully prepared. The attraction of a pre-notified inspection for regulatees is obvious: time to hide any awkward issues. Less immediately obvious, but no more ethical, is their attraction for the resource-stretched regulatory case officer. It’s a whole lot easier to inspect and report a compliant business than to have to go through the messy and labor-intensive effort of investigating a breach. Inspectors are busy people whose resources are limited, who have performance targets of their own to meet and political masters to keep happy. Enough said?

• Blink (a.k.a. Who Blinks First): Recent research has revealed the corporate-level version of this old game from the children’s playground (where it’s played as dare, or stare or chicken). As in the playground, the winner is the player who moves the least in the face of a challenge or threat. This may mean simply not blinking, or more riskily, staying in the path of an oncoming train; or facing down a regulator’s request for disclosure. Where the game takes place at a corporate level, there have to be some preconditions in the structures of commerce and government. The commercial player has to be confident that it can outlast and out-fund any challenge presented by a government, whose electoral mandate may reasonably be expected to expire at some point. The commercial player thus enters the game knowing that it has two major advantages over the regulator: economic power and longevity. Knowing this, it can call the regulator’s bluff. At its most brutal, this game produces a challenge from a practitioner to an inspector: “You have no expertise or experience here”; or even as a straight block: “Or else what?” (In one variant of the game played by corrupt governments, a regulatory agent seize the advantage by publishing a rulebook whose practical enforcement is deliberately kept unclear, so that arbitrary fines on regulatees offer a ready source of cash.)
• Constructing ignorance: This game is played by regulatees, regulators and politicians. A new risk control measure is introduced, often in a flurry of headlines about “clamping down”. But the intervention is designed to include “deniable spaces” or “firebreaks” which exempt the originator from blame in the event that the control fails.

• Fake Academy (a.k.a. Capture or Super-Capture): In this game the regulated industry either directly owns or effectively controls the resources responsible for certifying its own good behavior. One classic study of this game found a regulator’s “safety college” simply selling compliance certificates to visiting regulatees. The game is usually played more subtly than this, trading off vested interests and smoke signals, but the results can be just as harmful to the public good.

CONCLUSION
As seen above, research into games of compliance continues to uncover alarming lessons about what happens when democracy and commercial interests fall out of balance. When public agencies appear unable to keep control, the hazard is that commercial firms may become not so much “too big to fail”, as “too big to care”.

With regulators on both sides of the Atlantic now promising to recalibrate what they mean by “acceptable” forms of contracting and starting to push back against previously “normal” activities such as proprietary trading, many other peripheral risk-taking activities may now come to be caught in the regulator’s conduct spotlight. For providers who used to expect to outwit or outmaneuver the regulator, or avoid discussing concerns by playing a “Game of No Game”, times have changed.

New understanding is required and providers must become willing to look beyond their own organizations for proof that their own behavior is acceptable. What techniques they will need to use to achieve this outside-in view, in order to keep a conduct regulator satisfied, the next paper in this series will reveal. Meanwhile, take heart: if you have ever witnessed a regulator’s case officer being outmaneuvered by creative compliance and this made you uncomfortable, you have taken at least a first step on the road to developing an understanding of good conduct. The fact that you have paused to consider “how it feels to do the right thing” is a strong pre-indicator that you already have the capacity to look to develop a positive risk culture and organizational behaviors which support this.
Endnotes

1 Such as HM Government’s ‘Resilience UK’ and other Emergency Planning initiatives.

2 While still, of course, trying to reduce the impact and likelihood of hazards.

3 From among a huge research field on factors of “career determinism” between public-sector and private-sector service (including neurological factors), a recent example: Van Ryzin, G: The Curious Case of the Post-9-11 Boost in Government Job Satisfaction, American Review of Public Administration, January 2014

4 Though in fact, apocryphal: News reports are no guarantee that an event actually happened

5 In some research fields these activities are referred to as performative behaviors, and field of social pathology overall as performativity

6 We welcome your examples of other cases, either topical or historic; please email favorite examples to info@DrRMiles.com

7 This logic of “everyone’s doing it” is called by academics social proof, or if you’re really into the field, informational social influence. In a nutshell: “The more other people are doing something, the more I should do it”. Though it’s dangerous, we all do this at some time or another. It leads to, among other things: market bubbles; mis-selling scandals; sitcom “canned laughter”; and all kinds of political bandwagons, such as witch-hunting.

8 This social-science word essentially means “saying you’re doing something, as a substitute for actually doing it”. As in: “I’m just taking out the trash”, when you know it’s actually still in the kitchen.

9 A.k.a. the Fight Club game: where everybody knows that a game is being played, but if you talk about it, you get ejected from the game (and forfeit any winnings). First explored by psychiatrist R D Laing in Knots (1970).

References


2 Miles R.: From Compliance to Coping, Centre for Risk Management, King’s College London 2012; also Miles R. in Operational Risk: New Frontiers Explored, Risk Books, 2012

3 McGoey, L. On the Will to Ignorance in Bureaucracy, Economy and Society 36/2, 2007

4 Bloor M., Datta R. and others Unicorn Among the Cedars, Social and Legal Studies 15/4, December 2006
THOMSON REUTERS ACCELUS™

The Thomson Reuters Governance, Risk & Compliance (GRC) business delivers a comprehensive set of solutions designed to empower audit, risk and compliance professionals, business leaders, and the Boards they serve to reliably achieve business objectives, address uncertainty, and act with integrity.

Thomson Reuters Accelus connects business transactions, strategy and operations to the ever-changing regulatory environment, enabling firms to manage business risk. A comprehensive platform supported by a range of applications and trusted regulatory and risk intelligence data, Accelus brings together market-leading solutions for governance, risk and compliance management, global regulatory intelligence, financial crime, anti-bribery and corruption, enhanced due diligence, training and e-learning, and board of director and disclosure services.

Thomson Reuters has been named as a category leader in the Chartis RiskTech Quadrant™ For Operational Risk Management Systems, category leader in the Chartis RiskTech Quadrant™ for Enterprise Governance, Risk and Compliance Systems and has been positioned by Gartner, Inc. in its Leaders Quadrant of the “Enterprise Governance, Risk and Compliance Platforms Magic Quadrant.” Thomson Reuters was also named as Operational Risk Software Provider of the Year Award in the Operational Risk and Regulation Awards 2013.

For more information, visit accelus.thomsonreuters.com