Compliance, corporate governance and the illusion of perfection

OCTOBER 2017

In the fifth of a series of regulatory columns by experts in Guernsey's legal sector, group partner Wayne Atkinson looks at the quest for perfection in relation to compliance and corporate governance in financial services and what regulators can reasonably expect.

Cars have bumpers for a reason and pencils have bits of rubber on the end for a reason too. As someone more eloquent than I once said: "to err is human." In the world of financial regulation however, regulators are increasingly seeing errors not as human failings but as evidence of corporate ones. The buck stops more and more with the board of directors. This line of reasoning, put simply, goes something like this.

"Mistake A happened because proper procedures were not in place to stop it and because nobody was overseeing things. This is, in itself, Mistake B and is far more serious than the isolated instance of Mistake A."

We shall think about how to combat such reasoning shortly but we must first admit that in some instances it is accurate to some degree. For example, if a school leaver with no anti-money-laundering training joins a firm and is put in a position in which his lack of training results in a failure to report an obviously suspicious transaction properly, then it is clearly more appropriate to blame the firm rather than the hapless employee.

At the opposite end of the spectrum, there is the rogue employee who has actively set out to deceive his employer and is deliberately circumventing operating controls that were put in place to help the firm comply with its regulatory obligations. Again, in that situation it is very easy to see where a regulator should place the blame.

What concerns me, as always, are those shades of grey that dwell between the two extremes. Increasingly it feels as though anything less than perfection is viewed as indicative (or at the very least potentially indicative) of not only an isolated failing but a broader procedural or 'governance' issue.

In this vein, regulatory regimes often require boards, directors and compliance teams to make subjective judgements when assessing AML risks or gauging the adequacy of protective measures and procedures in the case of cyber or data protection. A subjective judgement can look entirely reasonable the day before disaster strikes. The day afterwards, the same judgement can look rather different. It is exceptionally easy to conclude that a company did not have appropriate cyber security procedures the day after a huge "data breach." That does not, however, mean that such a conclusion is correct.

That said, it can be very beneficial to organise a compliance function in a way that can combat such an assumption. Such a structure not only helps to show the regulator that one's firm has good corporate and compliance governance; it also promotes those things.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

Courts are reluctant to substitute their own commercial views for those of directors. Moreover, they do not necessarily require directors to behave perfectly, or even to strive for "best practice," to avoid liability. The standard they require is that of a 'reasonable' director in the context of his particular company (see, for example, *Re D'Jan of London Ltd [1993] BCC 64; Madoff Securities International Limited (In Liquidation) v Raven and others* [2013] EWHC 3147 (Comm)).

In essence, the courts ask themselves not if a decision was a correct one but if it was one that a reasonable director could have made in the circumstances, with their attention focused firmly on the decision-making process rather than the end-result.

When questioning the boards of companies (and their compliance teams), regulators should perhaps more often ask "was this decision reasonable?" and "was this decision based on an appropriate decision-making process?" rather than simply "was this decision right or wrong?" These questions differ greatly from one another.

Allied to this issue is one of collective responsibility. Increasingly, in my experience, regulators judge the boards of financial firms (and find them wanting collectively) notwithstanding the possibility that this-or-that company may have delegated the responsibility for the area in which a specific failing exists to a specific director. By contrast, in the aforementioned case of *Madoff Securities International Limited (In Liquidation) v Raven and others*, the court made it clear that a director is entitled, in discharging his duty, to rely upon the judgment, information and advice of a fellow director whose integrity, skill and competence he has no reason to suspect.

One may argue, with some justification, that regulated companies are by definition subject to a higher standard than other companies and that in this context a different approach makes perfect sense. My response to such an argument is that in the absence of specific and suitably precise regulatory obligations, the regulator should not take a very different approach. It might prescribe different and perhaps more specific duties, but surely the objective application of its standards must ultimately be the same. Even though people often believe that regulations impose a higher standard than the common law, that standard must still be a minimum standard and cannot be set so high as to demand perfection. To do so would impose an impossible burden on the directors of regulated companies and would act as a massive disincentive to people who would otherwise be perfect candidates for directorships.

So how can a board avoid an allegation of poor oversight or corporate governance when and if an error occurs?

It is of course possible for procedures to break down in the face of unique or unusual scenarios. I would submit that it is often the response of the board and/or their delegates to such a breakdown rather than the existence of the breakdown in the first place which is indicative of good or bad governance. The first subject for discussion when an issue arises should be about the remediation of that issue. For a number of modern regulatory regimes, crisis planning or disaster planning is a required part of a firm's processes. It is essential for the firm to be able to respond quickly and appropriately. If it takes the time to install the necessary plans and resources to deal with potential crises before they happen, it will send the regulator a clear message about how seriously its board takes such problems.

Secondarily, to avoid any implication that an error has caught the board napping, its members can help themselves by approving a clear-cut process by which people oversee compliance procedures. Such a process can set out times for regular reviews and procedural updates, also doling out jobs to internal audit functions and making contingency arrangements to call

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

in external consultants to test things. If a board has delegated jobs to various experts in money-laundering control, data protection/management and cyber/IT, it should also run a feedback and oversight regime of some sort, with the experts talking to it. It may choose to rely on one of its number to do this, but it cannot simply dump responsibility for an issue onto one man's shoulders and wash its hands of it.

In essence, the best way for a firm to convince a regulator that its corporate governance in relation to its obligations to comply with regulations is appropriate is, as my maths teacher used to say, to show its working. If it has clear, written-down structures such as the ones described above and is able to provide minutes and board packs (i.e. board papers and other things that boards have to read to prepare for a meeting) at which the results of those processes are assessed and considered satisfactory, it will be able to prove that its board is paying attention to the right details.

Lastly, the existence of a robust and attentive compliance culture throughout a firm is essential. If the board demonstrates leadership on the subject of compliance by investing in and promoting a culture of good practice amongst staff - from top to bottom - this should lead to a largely unblemished regulatory history with demonstrable examples of 'best practice' whenever problems arise. A firm that is able to point to such a track record (as opposed to a more spotty history) will be able to show that any incident is an isolated one.

In conclusion, I think it is at best a questionable proposition to suggest that a financial firm's compliance failings are inextricably linked to poor corporate governance. In assessing the board's oversight of compliance issues, and the decisions it takes as a result, regulators should take the same approach as the courts and expect not perfection but reasonableness.

There is, in any case, much that directors can do to protect themselves against such an assumption and much that a compliance team can do to help them do it. Well-documented decision making and well-documented polices and procedures for updating and assessing the firm's compliance function are essential. It is far more difficult for a regulator to question a firm's commitment to its regulatory responsibilities if the board takes these steps and truly embraces its duty to lead culturally.

Remember: corporate governance is not a question of being perfect, but rather of striving to create an environment where perfection (or something close to it) is a possibility.

An original version of this article was first published by Compliance Matters, September 2017.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

COLLAS CRILL

For more information please contact:

Wayne Atkinson

Partner | Guernsey

t: +44 (0) 1481 734225 | **e:** wayne.atkinson@collascrill.com

Paul Wilkes

Consultant | Guernsey

t: +44 (0) 1481 734268 | **e:** paul.wilkes@collascrill.com

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.