REPRINT

R&C risk & compliance

FOUR TIPS FOR ENSURING THAT COMPLIANCE AND RISK MANAGEMENT PROGRAMMES WORK EFFECTIVELY

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2017 ISSUE

DIAZ REUS
ATTORNEYS & SOLICITORS

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

PERSPECTIVES

FOUR TIPS FOR ENSURING THAT COMPLIANCE AND RISK MANAGEMENT PROGRAMMES WORK EFFECTIVELY

BY **RICHARD N. WIEDIS**
> DIAZ, REUS & TARG

Companies with strict internal controls, even when operating within a highly regulated industry, are not immune to dramatic and costly compliance or risk management failures. All too often, despite having the foundations of a successful compliance programme in place, companies experience dramatic failures resulting in criminal penalties, civil fines, job losses, congressional hearings and mass destruction of shareholder value. This is an unfortunate reality that is underscored by the recurrence of catastrophes that come in the form of a 'black swan.'

Evidencing the broad reach of these failures, the passage of the Sarbanes-Oxley Act of 2002 (SOX) was a direct response to a series of compliance-related events that drastically decreased the public's confidence in securities markets. SOX requires publicly traded companies to establish and maintain an adequate internal control structure and procedure and to assess their effectiveness for financial reporting.

Unfortunately, companies sometimes fail to realise that these blocks are only a starting point and that not all solutions come in the form of a specific prescription.

In cases when risk management and compliance fail, many similarities exist. These similarities can be found in failures ranging from AIG's accounting scandal and subsequent liquidity crisis, to the compliance issues that gained public notoriety in 2016, such as GlaxoSmithKline's (GSK) violations of the Foreign Corrupt Practices Act (FCPA) and the highly publicised revelations at Wells Fargo. There are four key lessons to be learned through these disasters which, if implemented, will ensure that risk management and compliance frameworks are better equipped to avoid or minimise damage, while preventing a black swan type event.

Compliance and risk management heads must have enough gravitas within their organisation to make a difference

A successful organisation must have a robust corporate governance structure which also has teeth. Ideally, the chief compliance officer or risk management head will be an executive officer and will be included in important decision-making. They should also have direct access to the board of directors or at least to the audit committee. Additionally, having a lawyer in this role is a huge advantage.

The spectacular financial collapse at AIG in 2008 came as a surprise to many, but not to everyone.

> **"The passage of the Sarbanes-Oxley Act of 2002 (SOX) was a direct response to a series of compliance-related events that drastically decreased the public's confidence in securities markets."**

One of the lesser known elements of the story is that internal auditors and compliance experts raised alarms about the rapidly declining value in the credit-default swaps (CDS) that AIG had sold to protect buyers against the default risk on the buyers' other investments. As the collapse started, the AIG compliance and risk management team learned that the CDS buyers had already asked the company to make billions of dollars of payments on their failing investments. By many accounts, however, the head of the AIG financial products unit, Joseph Cassano, was so powerful that he was able to silence the concerns of one internal auditor and exclude him from important meetings during which CDS were

valued. The internal auditor, who had expressed concerns, told Congress that Mr Cassano had "deliberately excluded" him from meetings where the escalating risks were discussed; as a result, he eventually resigned.

In the case of AIG, although corporate governance and risk management processes were in place, the champions of the processes did not have enough power or gravitas within the organisation to make their concerns known to the ultimate decision-makers. The results were disastrous. If the compliance team had direct access to AIG's C-suite and board, those executives could have acted to stem the rapidly escalating risk, prior to the tremendous destruction of shareholder value that prompted the company's downfall.

Companies can minimise institutional and financial damage by acting swiftly and aggressively to address problems while they are small and before the problems grow into black swans

Another element, almost always present in risk management disasters, is the presence of someone in the organisation who knows about the problem before it becomes material. However, the issue becomes increasingly serious when the organisation does not act swiftly or aggressively to address it while it still can be contained.

The recent scandal at Wells Fargo, much like the AIG case, also demonstrates this principle. On 8 September 2016, Wells Fargo announced that it was paying $185m in fines to city and federal regulators over allegations that it, among other improper activities, opened customer deposit accounts

and transferred funds without customers' consent. The bank will pay another $5m in what it called "customer remediation." In addition, a Form 10-Q filed with the SEC on 3 November 2016 estimated that the bank's litigation exposure from the scandal could reach an additional $1.7bn. Then, there is also the resignation of the company's chief executive John Stumpf, which came shortly after his testimony before the United States' Congress.

Issues at Wells Fargo, including pressuring customers to buy services they did not need or want, opening credit card accounts without customers' permission, forging customer signatures on paperwork and opening ghost accounts, were publicly reported by the press as early as 2013 when an article published by the LA Times summarised information from 28 former and seven current employees. Company leadership had been aware of these issues for many years, as the same practices resulted in a lawsuit in Nevada four years before accounts were published and seven years before the problem became public knowledge.

Ongoing investigations by federal and state authorities will determine precisely what occurred at Wells Fargo over the six-year period between 2009 and 2015. What is beyond dispute, however, is that the bank's risk management and compliance functions did not move swiftly or aggressively enough to terminate the bank's fraudulent sales practices. A properly operating compliance or risk management team would have identified the cause of the issue in 2009, reported the problem to the C-suite and the board, fired the wrongdoers and revised the bank's policies and procedures to stamp out the fraudulent practices. Had Wells Fargo's risk management and compliance regime been operating properly, this scandal would never have reached Congress, caused the loss of the bank's chief executive and the immense losses likely could have been contained.

The compliance team must include a rapid-response, agile and aggressive internal investigation team empowered to carry out the ethical tone at the top

When problems do surface, organisations must be ready, at a moment's notice, to investigate the cause of the issue. To be ready, they need to have sufficient resources in place before a compliance problem

surfaces. Further, having an investigation team may not even be enough, unless the team is composed of ethically oriented compliance professionals, with sufficient experience, knowledge of the law and a mandate from senior management to do the right thing. Those elements were absent in another recent risk management disaster – the foreign bribery scandal at GSK.

In September, GSK agreed to pay $20m to settle SEC charges that between 2010 and 2013 the drug maker's Chinese subsidiary, and a China based joint venture, violated the FCPA by providing inappropriate gifts to foreign officials and falsely recorded them as legitimate expenses. According to a report in the Wall Street Journal, the bribes took the form of gifts, improper travel and entertainment with no or little educational purpose, shopping trips and cash, among others. In addition, in 2014, a Chinese court found the company guilty of bribery and penalised GSK $491.5m in the same matter, which was touted at the time by Chinese state media as the largest-ever corporate fine in China.

Another report in the New York Times argued that the situation was caused by "missed clues, poor communication and a wilful avoidance of the facts," and that for more than a year the drug maker brushed aside repeated warnings from a whistleblower about systemic fraud and corruption in its China operations. "The company's internal controls were not robust enough to prevent the fraud, or even to find it." The Times' reporter concluded that "Glaxo just wanted to make its problems go away. It offered bribes to regulators. It retaliated against the suspected whistleblower." It hired external investigators to dig into the woman's background, family and government ties as a way to discredit her.

It is evident that what happened here was that the compliance team used the wrong methodology to address the issue. Furthermore, the tone at the top of the company and the compliance department was not focused on gathering sufficient facts to evaluate the severity of the issue. The fact that the company resorted to hiring external investigators likely diluted the company's ability to control the investigation as effectively as if the proper compliance resources had been in place and were appropriately utilised.

Strong relationships and sound communication between employees and compliance leadership are essential

No compliance or risk management regime can achieve complete effectiveness unless its leaders are widely known to, and are trusted by the organisation's workforce. If salespeople, managers, finance staff and HR personnel know and trust the compliance and risk management staff, they are far more likely to reach out to them about a problem or potential problem. In fact, in many cases staff will want to report issues they see because they want to feel they are doing the right thing.

Further, although a company may have an ethics or whistleblower hotline, these devices are of little value unless the workforce uses them, and they are effectively manned by the compliance team. Wells Fargo's new chief executive Timothy Sloan said during a town-hall meeting in November 2016 that the bank found "some instances" where reports by employees of bad behaviour to its ethics line were not handled appropriately. This is evidence that the bank's compliance and risk management team suffered from the weaknesses described above, and that information relayed through the bank's ethics line likely did not reach senior management as it should have.

Having a compliance regime, including an ethics hotline, is not enough. The compliance team must get out of the office, travel to foreign offices, meet with management and employees and establish relationships. Then, and only then, will the elements of the compliance regime work properly.

Conclusion

As the above cases demonstrate, risk management failures occurred, in part, because the compliance and risk management teams did not have enough power in their organisations or direct lines of communication to the board or the C-suite to cause effective remedial action. Also, the compliance issue was known within the organisation before it became material, but the company failed to swiftly and aggressively contain the issue before significant damage occurred. The organisation did not have a team in place that successfully addressed the threatening compliance issues. Finally, employees who identified the problems were not able to effectively sound the alarm so the issues would receive effective attention from executive management and the board of directors.

SEC regulations passed in the wake of the financial crisis require all issuers of publicly traded securities to report in proxies about their board's role in the oversight of risk management. SEC Item 407(h) of Regulation S-K requires a board of directors to define and report to shareholders about how they will oversee the risk management function. While the above-described compliance and risk management techniques are not easy or inexpensive, directors would be wise to thoroughly review their company's compliance and risk management regimes to ensure that the right characteristics are in place. Directors who fail to perform such a review may be sitting on top of compliance and risk management programmes that are in danger of not operating effectively, or preventing black swan events that can dramatically harm their companies and their shareholders. R&C

Richard N. Wiedis
Partner
Diaz, Reus & Targ
T: +1 (202) 684 2334
E: rwiedis@diazreus.com