PERSPECTIVES

ROLE OF RISK CULTURE IN EFFECTIVE IMPLEMENTATION OF RISK GOVERNANCE

BY **RUCHI AGARWAL AND SANJAY KALLAPUR**
> ISB

Poor risk culture is a major reason for many financial institutions' failure. It often manifests in top management not walking the talk – the vision and mission statements are on paper only and do not hold in practice. The recent incident at Wells Fargo provides several insights into the financial industry's risk culture and its association with poor leadership, improper incentives, weak controls and unethical employee behaviour.

While the importance of culture is well recognised, boards have a tendency to take it as a given rather than something they can create and influence. Risk culture is all about behaviours by organisational actors that translate into organisational norms, values and practices. The UK Financial Conduct Authority (FCA) has highlighted that culture is not optional; it exists everywhere, whether we like it or not. Companies and their boards need to think about what the right culture is, and how to achieve it.

Risk culture in financial organisations has received the attention of financial regulators and professional bodies worldwide. The International Institute of Finance (IIF), the Financial Stability Board (FSB), the Institute of Risk Management (IRM) and very recently the Australian Prudential Regulation Authority (APRA) have emphasised that organisations are responsible for their risk culture. The split of the UK regulator, Financial Service Authority (FSA), into the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) in 2013 was a stepping stone in this

direction. The FCA's primary role was to develop and inculcate good risk culture in UK financial institutions. Companies have repeatedly found that merely establishing structures and policies for risk governance is insufficient until these are aligned with culture and good practices.

This raises a question for practitioners: how to develop a good risk culture? To understand this, we studied several organisations in India and the UK and found three types of risk culture, described below.

Compliance-based risk culture – do what you are being told

Financial institutions operate in a strict regulatory environment. Following the 2007-08 crisis, regulations became more stringent worldwide. In some companies, regulation rules risk governance and sets the bar. Their primary interest is in meeting the regulatory standards in form rather than substance. This leads to a compliance-based risk culture, with a tick-box approach. These companies often find that by the time they make changes in the system to accommodate changed regulations, newer regulations are introduced.

Defensive risk culture – do what pleases the management and protects you if something backfires

In many organisations, truthfulness in risk reporting is not encouraged, and senior executives

have been fired for revealing problems in the system. Employees wonder why they should put in the effort to manage risk effectively when they are asked only to report it at the end of the year. The actual quality of risk management does not matter; rather, top management wants to hear good news in the short term by prioritising profits over professional ethics. Defensive attitudes and behaviours are inculcated: "If something goes wrong, somebody else made the decision, not me." Fear of action and litigation has led to defensive behaviour being ingrained in a defensive risk culture. Over-reporting of risk is one such behaviour: the reporting employee is protected because he or she reported it, never mind that the higher-ups to whom it is reported do not have the time or the understanding to process everything that has been reported. But higher-ups are also protected because decisions are made by committees, so either nobody is responsible or everybody is responsible for any mishap.

> **"Tick-box or quick-fix approaches backfire and limit the usefulness of risk management efforts."**

Cognitive risk culture – understand your risks, roles and responsibility and report adequate risk to management

In contrast to compliance-based risk culture and defensive risk culture, a few companies worked on understanding the root cause of poor risk culture. The board of a British insurance company began with the three lines of defence model of risk governance (frontline employees being the first line, CRO's office the second line and internal audit the third). The company found that the root cause lies in poor risk reporting: the control self assessment (CSA) method fails to engage employees and promotes a defensive attitude. Another challenge it identified was that risk reporting was considered to be a year-end activity rather than a regular activity. The company understood that it is not possible to improve risk culture until everyone in the organisation understands the risks, and their roles and responsibilities in the three lines of defence model of risk governance. The company created new rules and introduced several tools to improve risk culture. Some frontline employees were trained to become risk champions who bridged the gap

between the first line and the second line. Risk apps were developed to update senior executives and the board regularly, while roles and responsibilities of every employee were mapped using a management awareness of risk (MAR) index.

Conclusion

Cognitive risk culture in the organisation supports good practices in risk governance and thereby promotes the sustainability of the organisation in the long term. It must be encouraged, and organisations must approach risk management efforts by understanding them holistically from a system perspective. Tick-box or quick-fix approaches backfire and limit the usefulness of risk management efforts. R&C

Ruchi Agarwal
Senior Researcher
Indian School of Business (ISB)
T: +91 981 098 6496
E: ruchiagarwal1982@gmail.com

Sanjay Kallapur
Professor of Accounting and Deputy Dean
Indian School of Business (ISB)
T: +91 40 2318 7138
E: sanjay_kallapur@isb.edu