

Sometimes, a 'rogue trader' could actually profit banks

Paul Aldrich and Peter Metzger propose a new acid test to help manage risks



Paul Aldrich & Peter Metzger
CTPartners

If there is one quote that Oswald Gruebel, former chief executive of UBS, won't live down it is this: "Risk is our business." He told Bloomberg in November last year: "I can assure you, as long as I'm here, as long as my colleagues are here, we do know about risks."

UBS management couldn't have known of the risk when they hired Kweku Adoboli in 2006. And never mind that Gruebel imposed new risk

controls and sent traders instructions not to lose money after joining as chief executive in 2009. Unfortunately, the timing of the revelations that Adoboli allegedly lost US\$2.3 billion in unauthorised trading couldn't have been worse for UBS which lost over US\$50 billion during the global financial crisis. It also provoked questions regarding the banking sector as a whole, coming in the midst of a crisis in confidence in Greece and other European nations.

However, a couple of things are worth remembering. First, classic investment banking is an advisory business that in itself does not involve financial risk but which may lead to certain banks underwriting risks. For instance, investment banks such as Goldman Sachs underwrite some capital market transactions but advisory firms such as Rothschild and Lazard do not.

Second, given the volume of legitimate trading undertaken globally, losses incurred by individual are clearly exceptions.

At a macro level, regulators are seeking to ensure banks are secure and in future will not need to be rescued by taxpayers. To be fair, all organisations, not just banks, face risks in undertaking their activities: one just needs to recall the collapse of Enron or the DP Deepwater Horizon oil spill disaster. But, unlike many sectors, banks can suffer significant losses from the actions of one individual or a relatively small part of their operations.

To mitigate such risks, banks already have a new business and new product committees, middle and back-office processing and analysis, risk management functions and both external and internal audits. Fraud and billion-dollar losses need not happen if risks are properly understood, robust processes are established and individuals are made to work strictly within set processes and risk limits.

While 'rogue' bankers working in 'casino' banks make great headlines, they do not reflect the daily realities. The problem is that most banks often don't think and plan like rogue traders. The complexity of modern banking makes day-to-day risk management beyond the ability of management.

Many enterprises are attempting to converge information security, risk management and compliance into a single entity that is responsible not only to the chief executive, but also the board. Some are taking the progressive view that risk management executives should have a direct line to the board for certain matters. Indeed, the role of the chief information security officer has evolved from one of information-technology security administration to high-level risk management.

Additionally, it has been reported that some banks and clearing houses are employing "ethical hackers" to attach their payments and other systems.

One could also ask, therefore, whether banks should consider employing "ethical rogue traders" to attack their own trading systems. Of course, banks would need to decide critical factors such as the objectives and terms of engagement; and whether they should use independent consultants or their own staff; and who they would be accountable to.

Maybe it's time for banks like UBS to consider testing their own systems by giving "ethical rogue traders" a seat in the dealing room. That could just be the acid test that trading systems in banks need.