Reprinted from

OpRisk & Compliance

opriskandcompliance.com

Coming of age

$urendra Naidoo at Standard Bank of South Africa on the advantages of having a strong risk culture

$urendra Naidoo, risk management director and group head of operational risk at Standard Bank, believes the operational risk function can claim success when the firm's business managers are educated to the level where they manage op risk themselves. By David Benyon

Coming of age

STANDARD BANK'S USE OF CITICUS ONE

Standard Bank was an early adopter of Citicus ONE risk and compliance management software.

"Since 2000, we've used **Citicus ONE** to complete around 1,000 evaluations of our most critical information systems, and we are currently looking at extending our use of **Citicus ONE** to meet our AMA requirements".

$urendra Naidoo, January 11, 2010
e-mail: surendra.naidoo@standardbank.co.za

BIOGRAPHY

$urendra Naidoo is director, group risk management and group head of operational risk at Standard Bank of South Africa. Prior to joining Standard in November 2000 he was head of risk and internal audit at African Bank Investment Limited for a year. Prior to his entry into the financial sector he worked in the energy industry, at South African power company Eskom for 10 years. He started his tenure at Eskom in internal audit and diversified his career by serving stints as head corporate strategy (quality and productivity), chief financial planner, business financial manager and left after serving as the corporate finance executive (regulated business). He holds an MBA from University of the Witwatersrand and an accounting undergraduate degree from University of KwaZulu-Natal.

It is becoming clearer which banks have shown prudence throughout a decade of financial excesses, and those in South Africa seemed to have kept clear of the worst risks. The country has by many standards a developed economy, but suffers some of the infrastructure frailties common to its developing neighbours and, like the rest of the world, it has not been immune from the economic downturn. Standard Bank of South Africa, the country's largest bank, has remained fundamentally undamaged by the global crisis; affected only by its macroeconomic consequences. This success story can in part be credited to sound risk management.

"We have a strong risk culture in a country that does not have an excessive appetite for sexy and exotic products," says $urendra Naidoo, risk management director and group head of operational risk at Standard Bank. South African regulators have been cautious in their attitude to exotic instruments, limiting the appetite of the country's banks for structured products. Naidoo admits that while the downturn has had an inevitable effect on the bank's bottom line – and sent South Africa into recession – Standard Bank has been protected by the strength of its risk management principles.

"Standard Bank's approach to risk management is for strong governance, collective oversight, and comprehensive risk practices and risk reporting, at a more detailed and individual level," says Naidoo. "When you have a strong risk culture, it serves as an adjunct to management objectives. Because of that we were able to weather the storm well."

Standard Bank is the largest African-based global bank based on assets. Founded in 1862, it has headquarters in Johannesburg and a presence in 18 African countries. Outside of Africa it has operations in a further 20 jurisdictions, including a presence in New York and London, as well as Russia, China and Hong Kong. The bank's operations are also diverse. Since 2006 the group has owned retail bank BankBoston in Argentina; in 2007 it created Standard Ünlü in Turkey after taking a two-thirds stake in Turkish bank Dundas Ünlü Securities; and in May last year it took a 33% equity stake in Russian investment bank Troika. Standard Bank is divided into three main business units: a corporate and investment bank, a retail bank and an Africa-specific unit. Each of these faces of the firm has a business unit head of op risk.

Doing business in Africa presents its own challenges for operational risk. It means an op risk manager in the region could have a different order of priorities than their European or US counterparts. Resilience is one risk area of increased focus. "A major risk area for us is the business continuity of our operations to ensure uninterrupted supply," says Naidoo. "In some African jurisdictions it is necessary to have provisions for alternate sources of electricity. Hand in hand with that would be IT risks, such as ensuring change management at a country level is in step with rules and regulations."

"When you have a strong risk culture, it serves as an adjunct to management objectives. Because of that we were able to weather the storm well"

The breadth of the bank's operations – across dozens of diverse local legal and regulatory jurisdictions – also poses problems. Naidoo sums this up under information risk, another priority. "The bank's biggest asset is information. We are subjected to different regulations

across various geographies. If we store English client information in South Africa, or transactional data for a deal that was done in England, are these open to access under South African law? A firm might not have access to the data under English privacy law, but under South African law there might be leeway to get it. When you deal across the globe, these are the things you need to worry about. A major contributor to helping us understand and manage the risks associated with all information is that we have worked with our information risk management partner Citicus to identify and report on weak areas of information risk, and devise action plans to reduce it."

Naidoo heads overall group operational risk. He is responsible for developing the framework, methodology, policy and perform group-wide analysis, reporting directly to the chief risk officer, along with the group market and credit risk heads. He holds the tough responsibility of drafting the overall op risk framework and its supporting policies. This must be broad enough to apply to all aspects of the business, while allowing for a degree of customisation. He says management within the business plays an active role in maintaining the op risk framework, with the assistance of his peers, the business unit heads of operational risk.

"As an example, management takes responsibility for defining the RCSA; determining the action plans; engaging with each other to ensure the action plans are enacted by the required deadlines; and under the watchful eye of the business unit op risk people may either be prompted or where necessary matters found unsatisfactory are escalated to the appropriate forums – firstly in the management space and secondly in the risk space," he says.

This is not to say the operational risk manager is any less important. The role of the op risk function in the organisation, Naidoo says, is integral to business requirements. "Mitigating the risk is all about ensuring you design properly, with processes and frameworks that are fit for the purpose. The only way of doing that is by engaging operational risk management," he says.

When some op risk managers are asked to defend the 'value-added' they provide to their organisation, there can be an involuntary pause, in which they perhaps wish they possessed the quantitative data as evidence possessed by credit risk counterparts. Naidoo argues evidence of the value provided by a mature op risk function does not come from the op risk manager, but from the business managers who are educated to the level where they instinctively manage operational risk themselves, without the constant need for a nagging op risk manager shepherding them into place.

"Operational risk has been in play for some time," he says. "In the initial stages, the op risk practitioners were the initiators, catalysts and – chiefly – the nagging body, which pushed and pulled management into line. Now, with the mature op risk processes, wise management and robust framework that we have put into place, management has taken it upon themselves to ensure they manage operational risk; primarily to drive down losses associated with operational risk. Then on a secondary level, it is also to become far more competitive. Standard Bank enjoys an enviable cost and income ratio compared with our African peers. If management felt they were unable to contain operational risk, or ensure adequately designed systems and processes, the impact is a direct increase in the cost and income ratio. The value-added is seen in the uptake."

"We have reached a sufficient level of maturity, not just the op risk practitioners but management themselves have taken responsibility for operational risk"

Naidoo says Standard Bank's op risk management has reached an important moment in its maturity – the next step will be to move to an advanced measurement approach (AMA). "We have reached a sufficient level of maturity, not just the op risk practitioners but with management themselves having taken responsibility for operational risk," he says. "We know now we are ready to move to an AMA approach. The formal project plan is already engaged. We envisage the bank will be AMA-compliant by 2012."

The bank has a lengthy track record of managing operational risk. Standard Bank has treated op risk as an official discipline for almost a decade. For Basel II purposes, Standard Bank uses the standardised approach (TSA), official acceptance of which was confirmed by the regulator at the end of 2007.

Naidoo describes the bank's day-to-day approach to op risk management. "From a group perspective we flag issues and circulate the information to the business units, through my peers the business heads of operational risk," he says. "On a daily basis, our primary sources of information are the information management systems in place across the business. Management have brought in to their normal management reporting systems aspects relating to operational risk in their environment. Other than that, we look to the traditional operational risk tools – RCSAs, key risk indicator systems, and our incident management database – to provide specific operational risk data."

Internal op risk data collection through the incident management database is at the heart of these tools. The range of business undertaken by the bank necessitates some tweaks in how loss data is collected across the organisation. "Our primary data collection tool, called Orbit, was heavily customised to our own requirements," says Naidoo. "We've had the tool in place for eight years now for collecting data. In the retail space there is no floor or ceiling on incidents – all losses are recorded. In the investment banking space, we take the B2 recommended threshold of $5,000. That is our primary, internally focused information source that we use specifically for operational risk data. Then we would also look at the additional internal reports and management information systems. We also use external reports/sources of data as a source to monitor the ongoing op risk performance."

This is supplemented by the RCSA process, which has been entrenched within the organisation for as long as the bank has had a formalised operational risk approach. Naidoo says it is a mark of the bank's maturity, and the emphasis business places on it continues

to be crucial. "It is the basis upon which we start our initiative in terms of recognising the associated risks of a business unit and the mitigating controls," he says. "Over the years, the organisation has matured so that we have been fortuitous that management is now responsible for their RCSA; it truly is a self-assessment. The results are fed to the business unit operational risk managers, and they in turn would keep a detailed eye on the action plans generated as a result. The key risks are extracted and monitored more frequently, and the business as well as the head of op risk will watch these risks with greater scrutiny."

Not that the bank is introspective in its attitude to operational risk. The bank enjoys a good relationship with its primary regulator, the Banking Supervision Department of the South African Reserve Bank. There are two financial regulators in South Africa: the Banking Supervision Department covers the banking industry and the Financial Services Board (FSB) provides oversight for insurance, asset management and other financial products. Standard Bank's main core activity as a group is covered by the Banking Supervision Department. For TSA assessment, the regulator uses examples set by Canada's Office of the Superintendent of Financial Institutions, the Hong Kong Monetary Authority and to a limited extent the UK's Financial Services Authority (FSA). Naidoo cautions, however, that in an emerging economy such as South Africa it would not have been appropriate to adopt a 'light touch' regime similar to that adopted until recently by the FSA, but instead one tailored to match the complexities of an emerging market environment.

"There are definite benefits to be had from a singularly focused regulator," he says. "The regulator can provide clear focus and maintain objectivity. There is no duplication; no noise coming out of asset management or insurance versus banking requirements. However, for the group, there is a definite effort to ensure that whatever recommendations come out of the insurance industry or FSB get translated and communicated to the banking environment – and it works the other way around."

From a South African industry perspective Standard Bank enjoys op risk collaboration through the monthly meetings hosted by the South African Bankers' Association. South Africa's small banking community also lends itself to collaboration as well as focused oversight. "The fact we operate in a small country means our peer group is similar to the Australian or Canadian model," says Naidoo. "We have five large banks and then a multitude of smaller banks operating domestically."

The industry meetings are particularly focused on working to combat fraud and financial crime – endemic in Africa. The bank has also put fraud at the top of its internal priorities list. Naidoo admits that, like many banks, fraud – especially external fraud – causes more losses than any other form of operational risk. To this end, the bank has moved to create internal bodies specifically targeting fraud within its businesses. Naidoo says banks are commonly handicapped by a silo-based approach to addressing fraud, which Standard is keen to banish by gathering experts together and sharing information.

"It is top of our operational risk priorities," he says. "What we have done is form specific anti-fraud 'centres of excellence', particularly in the retail bank, where we find we suffer the most fraud losses. We have a collection of professionals who come in with product knowledge relating to debit cards, credit cards, leasing and home loans. We couple that with skilled anti-fraud experts and we have created an anti-fraud department in the retail space, which is allied to the retail op risk department. There is the group operational risk committee, which is the highest op risk oversight body within the bank, and we have created a subcommittee within that to look specifically at fraud, bringing people from the three parts of the business together to collaborate our efforts, to ensure we can reduce fraud, if not eliminate it altogether."