Five ways to manage operational risk in an even riskier world

By Craig Herbert, General Manager, Financial Services Sector, IBM Australia and New Zealand

September 2001 has come and gone, and for all intents and purposes so has the way the global financial services community looks at operational risk.

Senior managers are reviewing with critical urgency the framework of their business processes, looking for exposures they might have brushed aside in August. What was impossible in the past is possible now, and banks, insurance companies and investment firms across the globe are rethinking their definitions of risk, process control and recovery.

A little history

Operational risk came to the top of the ledger in the early 1990s, when a series of operational catastrophes - the most notorious involving the collapse of Barings Bank - affected a number of financial institutions. In the decade that followed, headlines about banking failures splashed across newspaper front pages more than 40 times, the latest banners appearing in the last few months, following the failure of online services provided by several Australian banks.

In releasing the new Basel Accord, the Bank for International Settlements has made it clear that operational risk is now a critical issue for financial institutions, which have until 2004 to allocate capital targeted specifically at cutting exposure to operational risks. If anything, the events of September 11 have tightened the focus of financial services companies on the urgency of coming into compliance.

The big challenge in addressing operational risk is to quantify extremes. Even the most sophisticated intelligence mechanisms, for example, were unable to predict the stunning ferocity of the damage imposed on New York's Financial District. The fact is, conventional statistics don't work well with extremes. The challenge is being addressed, though, in IBM Research labs, where work proceeds in chaos theory and alternative statistical systems.

The risk management top five

In readdressing their IT operational risk positions in a post-September world, financial services companies need to ask some serious questions about their capacity to do five things:

- To control
- To detect
- To optimise
- To solidify
- To recover.
Control refers to an enterprise's ability to control information crucial to its continued operation. Data and knowledge have become the key assets of banks, insurance companies and investment firms, and the way they use it - their data management strategy - increasingly determines their success.

Ensuring a high level of data quality requires a sophisticated solution that includes process and workflow management, as well as organisational design and technology - the actual hardware, middleware and software controlling a system.

Part of that control also entails the creation of a history of losses, which is necessary to bring financial institutions into compliance with the Basel regulations. A quantitative assessment of operational risk can only be performed using an accurate and complete history of direct and indirect losses. Internal and external data sources have to be combined to determine the risk from high-impact, low-frequency events such as the World Trade Centre tragedy.

**Looking for trouble**
The New York disaster also highlighted the importance of being able to detect suspicious and criminal activity – such as money laundering and illegal transactions - within a financial service company's business processes. The key is operational software utilising Artificial Intelligence and neural-network technology to recognise changes in behaviour and customer-use profiles.

The quality of a bank or insurance company's risk evaluation depends on the capacity of its back-office operation to optimise decision management. The real challenge is to build an overall framework that integrates workflow, human resources and administrative data into the decision-making process - a holistic approach that will optimise management's ability to monitor risk.

Solidifying a financial institution's IT infrastructure means making it more resilient to physical and digital risk. Increasingly, that requires the creation of an environment in which a server diagnoses and fixes itself, while configuring and managing its own environment. IBM's eLiza initiative, for example, revolves around the development of an autonomous system in which servers automatically configure themselves when new hardware is added, ‘heal’ themselves on the fly without any disruption of service, and marshal system resources on demand to handle any task.

An eLiza server environment also offers features that protect it from unauthorised access anywhere in the network, and to predict and avoid failures - assets of particular value when it comes to managing operational risk. The foundation for eLiza is available today on all IBM eServers.

**Calling for back-up**
Lastly, a financial institution's ability to recover from system hits - a catastrophe, equipment failures, viruses, theft and accounting-mix-ups - is
dependent on a whole range of factors, from strict adherence to process and operational procedures, the robustness of its hardware and operating system, to the extensiveness of its back-up operations.

And it goes without saying that the effectiveness of the entire enterprise information package is relative to its alignment with the business' communication network.

Many financial services companies, opting to do what they do best, are turning to outside experts like IBM for operational risk advice and service. The reason: IBM has built a significant number of bank systems, and has made financial services enterprise support one of its core competencies. It's also one of the few companies with global experience offering a complete set of risk-management skill and solution components.

Wherever a financial services company may turn for its operational risk management, one thing is obvious: it can't turn back. September has come and gone. But the risk remains.