

Operational Risk

Volume 3 Issue 2

March, 2002

At the centre of the financial enterprise

*Enterprise-wide operational risk solutions will increasingly be built on a foundation of process-based technology architectures and management disciplines aimed to reduce operational risk, not just measure it, argues **Reto Tuffli** of Centerprise Services*

THE FINANCIAL SERVICES industry now increasingly accepts that having a solid enterprise-wide foundation in process management and control is a prerequisite for all risk management, particularly operational risk management.

Consider the disciplines of industrial engineering, operations research and engineering risk research. These disciplines and their methodologies are used extensively in industries intolerant of process failures. Industrial engineers and their colleagues aim to bring together optimal combinations of people, information, systems and equipment to produce resilient and efficient organisations.

Examples of intolerant processes include aircraft maintenance, chemical and nuclear power plant maintenance, the application of

anaesthesia in medicine, offshore oil platforms, space missions and, perhaps the most classic example, national security-related command and control systems.

For whatever reason, these disciplines and tools have until recently received relatively little attention from financial services, particularly wholesale finance. Yet clearly the financial industry repeatedly proves susceptible

heavy regulation of the industry based on national policy goals intended to protect the public from the consequences of such failures.

The loss of nearly \$700 million reported in February by Allied Irish Banks as a result of alleged fraudulent trading by an employee is a case in point.

While many bankers may feel the risk-based Basle II bank capital adequacy accord and its

The financial industry repeatedly proves susceptible to dramatic institutional failures caused by breakdowns in internal controls, processes and risk management

to dramatic institutional failures caused by breakdowns in internal controls, processes and risk management. And it is susceptible, despite

op risk focus is just another piece of regulation meaning, therefore, more expenses, there's a move towards a more integrated, strategic view.

This view takes op risk into the realm of the chief operating officer, chief accounting officer, chief information officer and chief financial officer rather than making it just one of the responsibilities of the chief risk officer. More specifically, this approach brings op risk to the centre of the financial enterprise, rather than leaving it on the periphery.

I believe this mindset will in the longer term prove to be positive for the financial industry, in that gains will more than offset increased costs by making the sector more cost-efficient and resilient. Already regulators are serving as a catalyst in this shift in thinking.

What follows is a brief description of the key op-risk IT elements I see as necessary for achieving an integral, enterprise-wide op risk

Figure 1: The four op risk enterprise components



Source: Centerprise Services

framework that permeates an organisation's inner workings.

The goal and four-part solution

Within an organisation, op risk exists everywhere and in every process – from human resources to the front office, accounting, financial control and settlements – and warrants a strategic view and an enterprise-level perspective.

The enterprise's management system should interact with and allow effective orchestration of people, information, systems and processes not only to measure op risk but, more importantly, to provide a foundation for reducing operational risks while lowering costs. Such a solution takes op risk management well beyond the typically cited elements of risk assessment surveys, loss event databases and op risk capital calculations.

Op risk management should include four integrated components (see figure 1): data collection and monitoring; organisational management and accountability definition; business process management; and op risk measurement and reporting.

The top layer is strongly supported with several key underlying components, which are essential for reducing process-related risks, as we will see.

Data collection and monitoring

An enterprise-wide op risk solution must start with the proper tools to support data collection and aggregation. Typically, data from potentially hundreds of existing front-, middle-, and back-office systems is created and handled in a very decentralised manner.

Yet management of op risk must encompass the collection of data feeds as well as monitoring their readiness and completeness. Enterprise application integration (EAI) tools facilitate the monitoring of data feeds and support the data transformation required to gather data from various sources and bring it into consistent formats.

An enterprise op risk framework must also provide the tools for monitoring data feeds and their status – that is, for identifying inconsistencies, the types of data the feeds contain and the organisational entities that 'own' the data. Exception reporting for missing or incomplete feeds must also be

included in this framework, and business process management technology can be used for this purpose (see later).

Organisational management and accountability definition

The second foundation component for op risk management – organisational management and accountability definition – may sound obvious, but it's surprisingly lacking in most organisations.

At its core is a single, centralised repository and management tool that is used to define and maintain organisational and legal reporting structures as well as all employee roles and responsibilities. This repository includes the many detailed and critical sets of responsibilities, such as those of support staff with respect to front-office units, which aren't typically formalised or captured.

This tool should also support the complex, multi-dimensional reporting lines – such as 'matrix management' structures – often found in banking organisations that have intersecting managerial responsibilities. The firm's

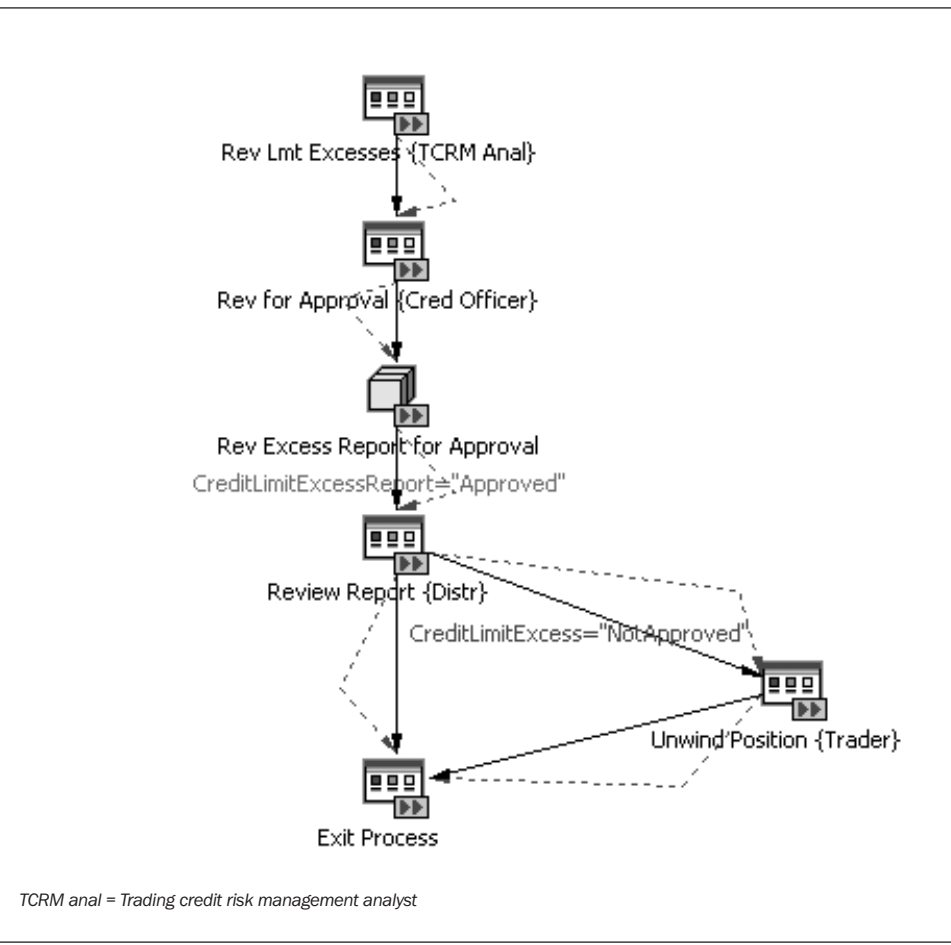
legal structure should also be integral to this framework.

Organisational management serves primarily as a foundation for the next two components. However, it also has numerous functions in itself. For example, the UK's principal financial watchdog, the Financial Services Authority (FSA), requires both organisational management and accountability definition.

Business process management

Situated atop the first two components, business process management (BPM), or workflow technology, provides for the automation of a business process, in whole or in part, with tasks passed from one participant to another for action, according to a set of defined business logic or rules. Workflows can also be used to document internal processes and should be cross-referenced with any relevant business policies.

Within capital market organisations, there are countless control-orientated processes where use of workflow technology would



eliminate, or significantly reduce, control gaps. These include review processes, an approval process, a request process or any process involving key action steps.

For example, any process that requires an approval during its execution should be automated and tracked using workflow – the process should start with the automatic generation of a report and end with the various individuals on the distribution list signing off, indicating that they have reviewed the given report.

Figure 2 is a workflow design diagram and illustrates how this technology can be applied to the daily process of reviewing credit limit excesses.

Workflow technology has several noteworthy features. It enables proactive, real-time monitoring of mission-critical processes with notification trigger rules and other alert features for identifying problems as they occur.

BPM's audit trail is another key element – it allows execution data to be automatically stored by the system and subsequently may be used as the source of risk exposure indicator metrics. For example, the system can collect data on where and how often within the organisation the risk reports were not being reviewed, or how often a credit approval process was delayed or forwarded to a senior person for a rushed decision.

At Centerprise, we view BPM technology as being at the heart of an engineered enterprise solution for reducing op risk. Its architecture allows firms to implement procedures and monitor compliance and results throughout the enterprise at each step of a process.

Many financial firms have well-documented policies and procedures, as do airlines on maintaining aircraft, but policy documents are not enough – which is why an effective op risk management solution must go beyond the statement of policy. It must actively manage, route and monitor each key process.

Operational risk management, analytics and control

Once the first three components are in place, firms can focus on the quantification and reporting aspects of op risk. This fourth component tends to be the traditional focus of

op risk practitioners. While important, it should be emphasised that this component on its own deals primarily with the measurement and analysis of op risk, rather than real-time management and control of it.

The four types of tools for measuring operational risk are: control self-assessments; a loss incident database; risk exposure indicator reporting; and analytics to calculate potential operational loss.

Control self-assessment reporting allows business units to survey their activities and highlight gaps in compliance in respect of internal policies and sound practices. Internal audit departments often use such survey results for audit planning purposes.

Typical reporting frameworks provide overall status reports of assessments and individual and composite ratings by any organisational unit. Less typical are control self-assessment programs that also maintain

Many financial firms have well documented policies and procedures, as do airlines on maintaining aircraft, but policy documents are not enough

links to organisational reporting lines, business processes and activities and policies.

A robust loss event database is necessary for gathering and identifying comprehensive op risk loss data. The database should be able to associate loss events with one or more causes and one or more effects, whether monetary or reputational. Mitigating factors – such as reconciliations or segregations of duties – may also be associated with events. Losses should be trackable by organisational unit, legal entity, op risk effect type or loss category, employee or country, and mappable from a firm's organisational structure to the standardised framework required by regulators. It is also desirable for the database to support multiple classification schemes for loss cause and effect categories so that loss data can be presented for internal, regulatory as well as industry consortium purposes .

Moreover, risk exposure indicator data should be retrievable from anywhere within the enterprise. This data could be related to operations or could pertain to other functions, such as risk management, accounting, systems manage-

ment or human resources, and the workflow audit trail relating to it may be an important source of an organisation's operational metrics. Op risk triggers should be assignable to virtually any risk exposure indicator – for example, employee turnover, trade volume or system downtime.

Analytics used to evaluate op risks are still evolving. A key challenge is data; there are very few observed, extremely large op risk losses. Hence, any methodology used to measure op risk must be able to extrapolate, via simulation, from the observed losses to larger 'tail' losses that are too rare to have been observed in the available history.

Any model used should also offer the ability to analyse certain subsets of the input data in a variety of ways. An example would be to assess how the loss distribution might change if arbitrary subsets of losses were excluded from the calculation. Such marginal risk contribu-

tion analyses can be used to allocate capital charges and/or resources for mitigating op risk to the areas with the highest return.

Flexible scaling of loss rates and amounts is also very useful when modelling op risk, as it allows an organisation to normalise loss data from various sources, such as industry consortium data or a firm's own loss data.

Taken together, these four components create a clear-cut framework for bringing the management of op risk into the centre of the financial enterprise. All four are necessary core elements to an enterprise systems strategy that can simultaneously achieve reduced cost structures and reduced process-related risk. ■

Reto Tuffli is chief executive and co-founder of Centerprise Services (www.centerprise.com), a technology software and services company offering enterprise management system solutions for the financial industry.

OpRiskCenter™ is one of 12 modules that comprise the firm's CenterSphere™ enterprise application suite for wholesale capital market firms.

Centerprise Services: Our Business Focus and Company Mission

Centerprise Services is a software and services provider of a modular yet integrated enterprise system built specifically for the financial services industry. Our software is complemented with services provided by both Centerprise and our partners to help financial firms implement our solution and manage the migration to an enterprise management paradigm.

Just as manufacturing companies have long used integrated ERP solutions to achieve operational efficiencies and control, Centerprise is focused on providing the same kind of integrated enterprise approach to the financial services space.

Our mission is to focus exclusively on helping management teams of financial services firms to implement their growing interest in a more comprehensive enterprise solution that serves to, simultaneously, reduce operating costs, and address risk and financial management, reporting and control issues, as well as outsourcing, co-sourcing and other e-business strategies.

With our CenterSphere™ application suite, we have designed an extremely cost competitive and control-oriented platform via tightly integrated functionality across the key management disciplines, including:

- financial reporting,
- risk management,
- portfolio management,
- human resources,
- customer relationship management,
- workflow,
- audit and compliance,
- system integration.

The result is a new paradigm for enterprise management, monitoring and control at a cost base not previously achievable.

Business Model

Centerprise supports two business models: the offering of traditional software licenses for our modular suite, CenterSphere, and outsourcing and co-sourcing solutions using CenterSphere within a variety of ASP configurations.

Our related implementation and migration support services are important aspects under both models. Centerprise and our partners, including IBM and key

consulting firms, provide project management, system integration and migration expertise to achieve your company's goals within a coordinated, well-conceived project management framework.

Market Focus

Our technology platform and functionality has been designed from the outset to support financial services organizations of any size, from the world's largest to firms as small as fifty people. Indeed, Centerprise is interacting with companies at both ends of the spectrum and those in the middle. Firms of any complexity or product range are good candidates for the Centerprise solution set. This would include the following types of companies or divisions:

- Investment banks
- Commercial banks
- Asset management firms
- Corporate treasury functions
- Private banks
- Insurance companies

CenterSphere is particularly well suited for capital markets organizations that have heterogeneous and expensive system infrastructures across trading, operations, credit and market risk management and financial reporting areas. This includes the largest of global firms seeking to tackle the cross-disciplinary and management complexity (multi-dimensional reporting) of their organizations; or firms struggling to comply with extensive regulatory requirements. CenterSphere is equally well suited for smaller firms with limited resources for risk management, control, and analytics that could benefit from a co-sourcing ASP model of these functions. All of these firms would benefit from a CenterSphere solution in terms of both cost savings and stronger operational controls.

Beyond pure capital markets firms, a CenterSphere solution would benefit a variety of institution types with similar challenges.

Examples would include an asset management division of a global insurance company, a capital markets function of an investment bank, a private banking subsidiary of a universal bank, a corporate treasury division of a Fortune 500 company, etc.