

# RISK MANAGEMENT SYSTEMS: UNDERSTANDING THE NEED

Robert Levine

**A combination of regulatory and commercial pressures is driving organizations to spend more than ever on technology to manage risks. This article explains this trend and what such technology can do, and provides guidelines for meeting the challenges of a risk technology implementation.**

**S**PENDING ON RISK MANAGEMENT technology is significant and on the rise. The TowerGroup estimates that the total outlays on this technology will exceed \$40 billion in the next couple of years. Clearly, one of the main drivers of this spending is the evolving regulatory requirement for more advanced systems to better manage risks — especially the 2002 Sarbanes-Oxley Act and the modified Basle Capital Accord coming into effect in 2006.

However, the drive to implement such technology crosses industry sectors and is not just a result of regulation. All institutions making investment or trading decisions face pressures to better control credit and market risks by increasing data and systems integrity, and by performing more accurate calculations of risks and exposures. Yet even for those institutions in which credit and market risks are relatively straightforward, operational risks abound. The latter include the risks of IT system downtime, data security incidents affecting business operations, the chances of employee fraud, etc. Operational risk exposure has been a key element in recent business and news headlines dealing with corporate scandals and the threat of business disruption from terrorism or war.

This article discusses the various drivers for risk management solutions, outlines the technology issues that need to be considered in selecting a solution, and presents many of the

considerations and challenges that should be factored into a plan to implement such a solution.

## Definitions

Risk management is a collection of processes, people, and systems aligned for the purpose of measuring, managing, monitoring, and controlling risk exposures. We begin by defining some key risk terms:

**Risk.** In general, the likelihood of a negative outcome. In financial terms, the quantifiable likelihood of a loss or investment return being lower than expected.

**Exposure.** The amount of outstanding trades or transactions an organization has, usually stated in terms of a specific product type, counterparty, industry, or other grouping. Exposures can be stated in nominal terms (i.e., trade amounts) or risk-adjusted terms (trade amounts after applying risk adjustments).

**Excess/Violation.** Occurs when a limit or other risk restriction is breached. This can be caused by changes in market factors or is due to risk limits being intentionally ignored.

**Operational Risk.** The risk of negative consequences (including but not limited to financial losses) resulting from inadequate or failed

*ROBERT LEVINE has 15 years of experience in consulting and writing for the high-tech and financial industries. He can be contacted at robertlevine2000@yahoo.com.*

**V**aR does not present a full picture of the market risk of a portfolio because it does not consider potential losses in extreme cases. Therefore, it is required to perform event risk calculations as well.

internal processes, unauthorized or criminal activities (internal or external), business interruption, information system or security failure, human resource issues, or from external events. Operational risk does not include losses resulting from strategic, market or credit activities. Because it is embedded in processes, people, and systems, it is unlike market or credit risks, which are more transaction oriented.

Many operational risks are industry specific. Thus, a bank faces different operational risks in handling money than a healthcare organization that handles patient care. Finally, whereas market and credit risk systems often have good sources of data, operational risk is harder to quantify.

**Regulatory/Compliance Risk.** The risk that an organization is not in compliance with applicable law or regulation. As with operational risk, this risk category is industry specific.

**Human Resource Risks.** In general, these deal with any risks that result from willful mishandling of an organization's policies or procedures — and can include interpersonal conflict, such as harassment or discrimination resulting in lawsuit, or other policy violations.

**Market Risk.** Losses in market value of a portfolio due to changes in financial asset prices such as interest rates, foreign exchange rates, inflation rates and other economic factors, equity prices, and commodity prices.

**Value at Risk (VaR).** VaR is a measure of the loss in market value of a position/portfolio that is expected over a given holding period for a given statistical confidence interval.

VaR does not present a full picture of the market risk of a portfolio because it does not consider potential losses in extreme cases. Therefore, it is required to perform event risk calculations as well. *Event risk* is the risk of an adverse price change outside the confidence interval chosen for VaR calculation. Event risk is an evaluation of a portfolio against stress scenarios for one or more factors that determine the value of the portfolio.

**Credit Risk.** Exposure to loss relating to a change in the credit worthiness of a counterparty that may impact the counterparty's ability to fulfill its obligations under a contractual agreement. Changes in credit worthiness can be due to changes in the counterparty's credit rating or a default.

Credit risk is normally broken into the following subcategories:

- *Settlement risk:* exists during the period from trade execution to trade settlement.
- *Pre-settlement risk:* risk that a counterparty does not fulfill all its obligations under a contract, such as an interest rate swap, prior to actual settlement.
- *Issuer risk:* arises when one holds debt or equity securities, and is the risk that an issuer of a security will have some difficulties that will cause the value of the investment to decline.
- *Country risk:* arises from all the political, economic, and social uncertainties in a country that may cause borrowers, counterparties, or governmental authorities in that country to not honor their external credit obligation.

**Integrated Risk Management.** In general, the management of multiple risk categories in a unified fashion, with recognition that certain risks create or exacerbate other risks, and in other cases certain risks are simply correlated with each other.

## OVERVIEW OF REGULATORY AND INTERNAL CONTROL DRIVERS

The most significant regulatory driver for an enterprise-class risk system is the Basle II Capital Accord. The new Capital Accord (known as Basle II), from the Basle Committee on Banking Supervision of the Bank for International Settlements (BIS), introduces new, more sophisticated requirements for credit and operational risk management from the earlier Capital Accord. The market risk requirements from the prior Accord are still in place and are largely unchanged. This regulation affects banks in more than 100 countries.

The objectives of Basle II can be summarized as follows:

- Provide a risk management and supervisory framework that enhances risk sensitivity, competitiveness, and works with current market practices.
- Make financial institutions improve their risk management procedures.
- Align economic and regulatory capital. Capital is meant as a second line of defense to systems and controls.
- Increase the robustness and safety of the financial system, ensuring that there is as

**Y**our risk practices and technology should support validation by the auditors or regulators; risk processing and data flows should be transparent, accessible, and well-documented.

much, if not more, capital operating within it as a buffer for unexpected losses.

The Accord sets out three methods of varying sophistication for determining regulatory risk capital. This article does not describe these in great detail; instead, the reader is urged to consult the actual Accord, which is found at <http://www.bis.org/publ/bcbsca.htm>. It is important for a risk technology solution to support compliance with any of these methods.

Following recent corporate financial scandals, the U.S. Congress passed the Sarbanes-Oxley Act of 2002, which applies to all public companies in the United States. This act imposes new and strict guidelines around corporate governance and imposes heavy fines and even imprisonment for senior executives of firms not in compliance. In addition to introducing new requirements for executives to sign off on the financial statements of their companies, the act requires sound internal controls, including a robust risk management capability.

From an internal control perspective, auditors will likely require you to implement good practices for risk management, policies, and organizations (discussed later). Many of these practices can be found in Basle II. First, risk policy and control processes should reflect the actual risk and complexity of your organization. These processes should include all risks, products, geographies, etc. You must also show a documented, clear, and logical method for measuring and reporting risk for each of your product types. Finally, your risk practices and technology should support validation by the auditors or regulators; risk processing and data flows should be transparent, accessible, and well-documented.

#### OVERVIEW OF COMMERCIAL DRIVERS

Any firm — not just a bank — engaging in finance or investment activities will have a need for fast access to credit and market risk information. That includes, for example, a manufacturing firm that uses letter of credit financing and foreign exchange trading, an energy firm that trades energy or commodity derivatives, or an automobile company that finances leases and purchases of its cars. This is especially the case in “stress” situations, where sudden and significant market, credit, or operational events could materially increase the risk of default for one or more counterparties.

Further, identification of the true unified risk picture across organizational and system boundaries has a bottom-line impact. If a risk

manager can have an updated view of exposure to a certain counterparty, counterparty grouping, industry sector, product type, country, etc., then better investment and portfolio optimization decisions can be made. Also, the risk manager needs to understand which operational risks could arise or worsen as a result of new commercial ventures, mergers, acquisitions, etc.

Better use of modern risk measurement methodologies and technology can give your organization the ability to do more business under existing risk limits, if those limits were computed based upon a conservative estimation of risk. They also facilitate the ability to make better business decisions based upon a single picture of risk, and the ability to do deals quicker with a quicker risk limit check.

These drivers raise important requirements for data integrity and accuracy. By deploying an enterprise risk system integrated with the appropriate front office, middle office, and back office systems, you can reduce the risk of errors because manual data input, data rekeying, and data transformation are avoided.

#### OVERVIEW OF TECHNOLOGY REQUIREMENTS

##### Flexible Architecture, Data Model, Risk Measurement Capability

The first and most important technology requirement is *flexibility*. You may need the system to support enterprisewide product and risk coverage across various geographies — and handle tomorrow’s business, products, and risk indicators. Each of the traditional risk management cycle areas, including risk identification, prioritization, analysis, communication, and alleviation, should be supportable. The system must recognize both market-standard and proprietary pricing and risk models. The latter type of models can be computationally difficult because they can involve large amounts of data and intensive computation. The challenge with the former is converting qualitative operational risk into quantitative terms, which is necessary to calculate capital at risk and indeed to manage this risk.

An open, Internet standards-based data architecture (which means things such as XML support for translating content between systems) is essential. This should facilitate interfaces from various feeder systems that may be running on a host of legacy and open operating systems and network protocols; it should also support messaging middleware that makes this

**I**ndustry requirements can be quite dynamic, considering the impact of new regulations and legislation, new standards, and the ever-changing commercial and competitive landscape.

interface integration easier to build and maintain over time. The system must also support multiple branches and currencies.

Flexibility means a system design that can be easily modified to handle new regulatory requirements, new risk measurement techniques, and advanced risk management processes such as risk workflows. Such workflows could include the new product approval process, credit application process, approval handling and notification, negotiation of documentation and risk mitigation, limit assignments, risk monitoring, requests for one-time approval of transactions, and routing of excesses and violations to the appropriate risk officer for follow-up. For operational risk, such a workflow normally involves risk identification, risk assessment (impact and probability of the risk actualizing), and risk mitigation. An operational risk process known as control self-assessment uses the expertise of line staff and managers to assess their own operational risks. With this approach, individual departments test control procedures against an established template on a regular basis, and also following certain predefined risk events. They then rate their own level of compliance, develop action plans to address gaps, and monitor progress. Next, auditors test the validity of the self-assessment to ensure accuracy. Finally, key performance indicators act as a management control by quantifying and tracking the organization's risk-management performance.

The system should adapt easily to growth or reduction in product scope or volume due to business expansion, divestiture, mergers, or acquisitions. That means the data handling and storage capabilities in particular, but also the processing and analytics and computational capabilities.

It is important that the risk system support your specific organizational and industry requirements. The latter can be quite dynamic, considering the impact of new regulations and legislation, new standards, and the ever-changing commercial and competitive landscape.

#### **Data Handling**

When planning a data model, keep in mind that an enterprise risk management system typically requires five types of data that can be aggregated from multiple internal and external data sources.

**Transaction Data.** Information about each financial transaction or trade is vital for a thorough assessment of risk using modern techniques. Transaction data usually means the

instrument type, nominal amounts, rate or pricing information, key transaction dates, and information about any underlying securities, or option-related data if relevant.

**Valuation Information.** This data is normally used by trading systems to price a deal and to calculate profit and loss. A credit/market risk system will also need this information for exposure calculations. Valuation information typically includes rates; price and price history; market-to-market and present value of fixed or floating cash flows for a swap; volatilities; correlations; dividend rates; yield curves; etc.

**Static Data.** Static data is nontransaction-related data that normally does not change very frequently. This would include things such as customer or counterparty information, securities information, limit information, and other reference data. *Creditworthiness data* includes internal and external ratings, counterparty relationships, credit correlations, default probabilities, loss history, etc. *Risk mitigation data* involves static data that references legal agreements used to reduce credit risk. These include collateral agreements, payment netting arrangements, credit guarantees, and similar such measures.

Static data quality is key to the success of an enterprise risk system. First, the organization needs a common reference point for customer or counterparty identification and hierarchies, or risk will be incorrectly computed, assigned, and aggregated. Limit data must also be well designed and controlled, or improper assignment or sharing of limits will result. Other static data elements — particularly if they will affect risk calculations — must be accurate and updated.

**Loss Data.** This is information on actual internal losses suffered as a result of operational incidents, or credit or market events. Also, data on external losses must be collected and “sized” to be relevant for your organization to properly assess. For this scaling, it is common to use *size drivers* (for example, total assets, total staff size, etc.). Loss data typically includes the loss data and type, loss amount, loss recovery amount (if any), and affected business line.

**Operational Data.** This is the information used to assess operational risks. Such information can come from many sources, including human resources (turnover, absenteeism, performance reviews, etc.); a legal function (litigation, fines and warnings, employee complaints,

**T**he only way to effectively manage intra-day credit or market risk is if these risk exposures are updated on a real-time basis.

etc.); security (fraud, incidents, etc.); auditor (audit results); finance (finance and accounting indicators); middle office (transaction indicators); and line managers via self-assessments.

#### **Real-Time Infrastructure and Support**

Support for a global, real-time infrastructure is also important, especially for a trading-oriented environment. The only way to effectively manage intra-day credit or market risk is if these risk exposures are updated on a real-time basis. Support arrangements — not just for the credit and market risk system, but also for all of its interfaces — are essential.

While an operational risk system is not typically a real-time system, there are aspects of operational risk that must be managed on a real-time basis (such as information security). But the operational risk system itself will normally be fed the results of an information security management system on a batch basis only.

#### **Query and Reporting**

The enterprise risk system must provide a robust ad-hoc inquiry and reporting capability in addition to a suite of standard reports. This means custom sorting, selection, and calculation for risk managers across various geographical or organizational lines, or for individuals with different reporting needs. These reports include not just excesses or violations of market and credit limits, but also reports of deals and exposures; concentrations of risk by counterparty, geography, industry, etc., status of operational risk indicators; as well as risk exception reporting. The latter would include, for example, overdue credit reviews, credit files with missing information, counterparties with a significant history of excesses, trading in unapproved products or markets, rising operational risk indicators, etc. In addition to these internal reports, you may need to produce reports for regulatory purposes (e.g., capital allocation and charges, loss provisions, etc.).

Reporting increasingly means graphical as well as text and numeric output. For example, a risk manager may want a report of operational risks in pie chart or histogram format, or of VaR limit excesses in bar chart format. Export capabilities to industry-standard spreadsheets and databases are key as well.

#### **Anywhere Access**

Many organizations will want to be able to access risk information from anywhere. This

implies support for a “thin desktop” architecture, whereby end users do not need special software installations to use the credit system. For many organizations, the ideal scenario is that only a simple browser and network connectivity are required.

#### **Technical and Control Standards**

The performance and reliability of the risk management solution are key. Because credit and market risk information will often be checked prior to making a fast-moving deal, that information cannot be delayed. The result could be a transaction at a less favorable market price, or a transaction that goes forward without proper approvals, causing limit breaches.

Clearly, it is important that the risk solution chosen will support your organization’s technology standards. Security and privacy constitute a standard technology requirement that bears special mention. An organization’s credit data is among its more sensitive internal information. If trading counterparties found out what credit limits are actually placed around them (versus other counterparties), it could be potentially damaging to the business relationship. Methods and policies for measuring and computing risk exposures could also be extremely proprietary. Likewise, operational risk data — particularly about control weaknesses — is extremely sensitive because it can be exploited for malicious purposes. Finally, privacy legislation may place an additional regulatory compliance burden on the organization.

#### **Application Service Provider (ASP) Environment**

With an ASP solution you will likely want to contractually guarantee service levels as well as design in special security measures (such as encryption) if your ASP connection passes over the Internet or other public networks. The ASP should be subject to audit to validate its level of controls. It is important to consider multi-site disaster recovery provisions from your ASP vendor. Finally, you may want to investigate how difficult it would be to migrate from the ASP solution to an in-house solution if business needs change.

#### **RISK SYSTEM ARCHITECTURE**

A risk technology architecture is generally composed of real-time messaging middleware, a database or data warehouse, a risk or analytics engine, workflow support, and a reporting

***In making the buy-versus-build decision, it is critical to ask whether your organization is, in fact, so unique that it must build such a tool rather than buy and integrate one.***

engine. Real-time updating of limits and exposures is critical; further, many organizations are considering a real-time check of credit and market risk information prior to the actual transaction.

The risk system will allow users to check their risk limits and exposures, and perform inquiry and reporting on many selection, sorting, and consolidation criteria. Many advanced risk architectures allow dealers and traders to quickly query credit and VaR limits, and understand the impact of a possible deal upon their overall credit exposure, *before* doing a deal and without leaving their familiar dealing interface.

The risk systems should support both established risk measurement methodologies and more sophisticated techniques such as Monte Carlo exposure simulation, stress testing, scenario analysis, risk decomposition analytics, and risk modeling capabilities.

Data handling is also a key factor in designing a risk system. The solution must provide support not just for fast access to data for real-time limit checking and exposure or limit updates, but also must support the handling of historical data. For each type of data, you should understand how much history you need to maintain as well as its frequency (monthly, weekly, and daily).

The state-of-the-art for risk systems architecture is real-time, rules-based transaction reconciliation between your risk system and your back- or front-office feeder systems. This will immediately flag any interface failures or mapping errors that can cause your risk exposures to be inaccurate. This will also ensure that your risk data reconciles correctly with your back-office or finance data — which is helpful when complying with regulations such as Basle II.

## **IMPLEMENTATION CONSIDERATIONS AND CHALLENGES**

### **Buy or Build**

In making the buy-versus-build decision, it is critical to ask whether your organization is, in fact, so unique that it must build such a tool rather than buy and integrate one. Choosing the right path means first having a clear idea about your regulatory, commercial, and technology requirements. You should then perform a gap analysis between these requirements and the capabilities offered by commercially available packages.

### **Project Management and Planning**

Whether you decide to buy or build, good project management and a well-thought-out development and implementation methodology is key to successful implementation. The latter will need to include development and implementation standards, a written project plan with defined milestones, project status tracking mechanisms, clearly defined project deliverables and acceptance criteria, and a project team empowered to deliver results.

### **Risk Policy**

The rollout of an enterprise risk solution is an opportunity to clarify and strengthen risk policies, and to harmonize conflicting policies within your organization — but at any rate, you will need a risk policy on which to base system implementation and configuration decisions. Policy typically includes the following areas:

- How organizational “risk appetite” is determined and communicated
- Assignment of responsibilities for managing the various phases of the risk cycle
- How to measure risk for various product types, markets, clearing methods, etc.
- Which product types, market data sources, and operational processes are “approved,” and what the process is for new products, data sources, and operations
- How to assess risk, including a definition of “early warning” risk indicators that trigger follow-up action
- How to validate risk and pricing models
- How to control risk, for example, through limits, credit reviews, mandates for approved products or transactions, mitigation strategies such as unwinding a trading position, etc.
- How customer and counterparty risk is monitored on an ongoing basis
- How to detect breaches of risk policy
- How policy violations and operational incidents are handled
- Credit application format and requirements
- How to assign risk ratings to customers and counterparties
- How to judge risk management effectiveness
- How to raise risk awareness in the organization
- How special transactions are approved (or rejected)
- How and when risks are reported in the organization and externally (e.g., to regulators)

**N**o matter how flexible the risk system may be, your feeder systems might not be as cooperative.

### **Data Management**

Data is another key ingredient in risk management systems. Data mapping will be a key factor in the success of your credit risk system implementation. Project team members must include people with expert knowledge in risk and feeder systems data from internal and external sources, as well as members familiar with data modeling and mapping techniques.

Part of this expertise must include data warehouse management. Basle II, and good risk management practice, require the collection and archival of historical default probability, expected or actual loss, and other risk information for use in better calculating and predicting future risk. This includes external loss data, for perspective on industry trends and events, as well as internal information. While external loss data may be easier to obtain, without corresponding internal information, the external data does not necessarily tell you whether the risk associated with the loss is applicable to your business. Exactly how much data you need to keep is an organizational decision, but best practices often tend toward keeping ten years or more of historical data. As with any data warehouse, the quality of the data is a key success factor; thus, it is critical that individuals with subject matter expertise in the data areas, as well as in statistical modeling, be part of the implementation and maintenance efforts.

### **Data Quality**

No matter how flexible the risk system may be, your feeder systems might not be as cooperative. You will likely want your front-office trading systems to have the ability to display information from your risk systems (in real-time, preferably) in order to inform the trader of their risk limits, and of the impact of a proposed deal on outstanding risk exposures.

Data consistency and quality is a primary challenge, in light of the multiple trading, back-office, and risk systems you are likely to support. In addition to worrying about data accuracy and timeliness, you also need to collect meaningful historical risk observation data for risk modeling. Because these models can be limited by their reliance on high-frequency, low-impact events, they require a significant number of data observations. Finally, recognize

the need to make decisions regarding converting historical information from your legacy risk systems, which might include limit and exposure history, trends in credit excesses, etc.

### **Organizational Factors**

One challenge in implementing a successful risk management system occurs where there is a need for introducing openness into a closed corporate culture. Many employees are reluctant to report risks because this would appear to expose their own (or their department's) weaknesses. Also, consistent risk policies, risk treatment, and visible global limits will expose the activities of business units near and far to central risk monitoring. This could be perceived as a loss of local office independence, and even a threat to local jobs as it becomes easier to manage risks centrally. These perceptions must be recognized during a systems implementation.

### **System Limitations**

Another challenge that is shared with all enterprise systems is that, despite vendor claims to the contrary, no one system can do all things. Can one risk system properly value and account for the risk of each transaction in which an organization takes part? It is likely that some transactions will still need to be manually revalued using expert local knowledge. Make sure you understand the limitations of the system, and consider gaps in functionality and exception conditions in your project planning.

### **CONCLUSION**

Considering that integrated risk management is a very new idea, it is not surprising that many risk management systems still do not present a unified view of the different types of risk discussed in this article. Evolution in this area will be one of the more exciting possibilities for risk managers. Even as this capability evolves, risk systems can satisfy commercial, technological, and regulatory requirements when deployed correctly.

This article aimed to present why such a system capability is needed, and to explain typical system requirements and architectures. It then presented an implementation approach as well as typical challenges. ▲