

## Paper 157-2008

**Enterprise Risk Management Solutions**  
Austin Trippensee, SAS Institute Inc, Cary, NC**ABSTRACT**

This paper will discuss the challenges banks face integrating market, credit, and operational risk measures. This paper will cover the design of a data model for the front-end of your analytics, and will cover how a robustly designed repository for your output supports a robust business intelligence infrastructure. In the middle, users might want to configure proprietary measures. This paper will also address key issues around flexibility, auditability, and scalability.

**INTRODUCTION**

Today, banks are facing more regulatory requirements, more stringent rating agency oversight, and investor confidence issues. To meet these new challenges, many organizations are examining their policies, methodologies, and infrastructure (PMI). These three building blocks form the core of any enterprise risk-management environment (Crouhy, et al, 2005).

Policies represent the tolerance that an organization has for risk. The policies should be consistent with business strategy and should be communicated both internally and externally. The methodologies are the underlying mathematical models that are tied back into performance management. These models must be properly designed, implemented, and vetted. The infrastructure refers to having the appropriate people and operational processes (such as data, software, systems, etc.) in place to control and report on the risks (Crouhy, et al, 2005).

In the past 10 years, there have been countless books, journal articles, and other published works that describe a plethora of different ways an organization can calculate risk measures. These vary from a measure that looks only at one specific risk factor to more integrated measures; for example, economic capital.

Over the years, the market has endured the U.S. savings and loan crisis, the October 1987 market correction, the 1997 Asian financial crisis, and more recently the 2007 sub-prime mortgage crisis in the U.S. impacting the global banking community. Every one of these market events stresses the importance of having good risk measures and good risk management policies, methodologies, and infrastructure.

Of these three challenges, the bank is responsible for establishing its own policies and methodologies. These policies and methodologies will be influenced by the internal management organization as well as external factors, such as regulatory oversight and investor confidence.

The third challenge, infrastructure, is where the bank may benefit from external, third-party experience in terms of personnel, business processes, and information technology (IT). While many banks have internal IT departments, most will agree that technology is not part of a bank's core competencies. In this case, it may be best for the organization to leverage the knowledge, experience, and products from third parties who do have hardware and software development among their distinctive core competencies.

This paper will focus on the information technology infrastructure required to support good enterprise risk-management policies and methodologies.

**ENTERPRISE RISK MANAGEMENT IN THEORY**

Academics and financial engineers are quick to point out all of the "ideal" methodologies for creating enterprise risk measures. Journals and trade shows are full of different coherent measures that may be used to construct an enterprise risk measure. No matter if it is economic capital, risk-adjusted performance management, expected shortfall, or any other measure, at the core, these measures need to leverage a robust infrastructure to bring together risk factors from across the enterprise. These risk factors may include interest rates, credit ratings, or the probability of an IT failure. With all of the mergers, acquisitions, and consolidation witnessed in the banking industry, organizations are now facing very large, complex integration challenges.

According to COSO, the definition of Enterprise Risk Management (ERM) is, "A process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

There are two basic ways that a company can choose to manage risks: it can manage one risk at a time, or it can manage them on an integrated holistic basis. This latter approach is often referred to as enterprise risk management (Nocco and Stulz, 2006).

The goal of enterprise risk management is to measure risk and capital across a wide range of diverse business activities. This requires a methodology for aggregating risk types (market, credit, and operational) whose distributional shapes may vary considerably (Rosenberg and Schuermann, 2004).

The key measures used for looking at enterprise performance are economic capital and risk-adjusted performance measures. These measures aggregate the various risk components together into measures that can be readily used to measure risk at the enterprise level. Besides determining the appropriate methodology to measure, there are several infrastructure challenges an organization will face while implementing these measures. These challenges include:

1. having all the necessary data required for a given methodology
2. performing the calculations as defined in the methodology
3. delivering the information in an actionable timeframe
4. aggregating the information at all of the appropriate levels

**HAVING ALL THE NECESSARY DATA REQUIRED FOR A GIVEN METHODOLOGY** requires organizations to bring data together from front-office, back-office, and middle-office systems from across the entire enterprise. With many organizations operating globally around the clock, there are issues around timing and standardization to ensure that enterprise measures are meaningful. More advanced methodologies require a broader and larger array of data elements. The sheer volume of data alone can overwhelm most IT departments. To combat these large, complex data volumes, organizations need to focus on streamlining and supporting an efficient data infrastructure.

Minimizing redundancy and duplication is one way to ensure that the data volume does not become overwhelming. Additionally, organizations need to enable the various business units and operational groups to be more self-sufficient. Many organizations have bottlenecks because groups become interdependent upon data. Creating an environment where users can "help themselves" to data will free up IT resources.

Consistency is another big issue. Having one version of the truth requires having one common set of integrated data for everyone. It is not uncommon, in large organizations, to have two separate groups calculate the same measure and generate different results. Having one common data infrastructure ensures that everyone throughout the organization is using the same data.

**PERFORMING THE CALCULATIONS AS DEFINED IN THE METHODOLOGY** is basically ensuring that users get the right information. One of the largest risks an organization faces is "model risk." Model risk can be caused by either implementing a model incorrectly or using the right model but analyzing bad data. Either way, the user is at risk of the model not performing correctly and thus exposing the organization to model risk.

Organizations can leverage their internal distinctive competencies and knowledge about their customers and industries to create proprietary methodologies. These methodologies can yield models that improve the organization's risk measurement and therefore help to improve the risk management within the organization. The only way these models will be effective is if the organization has good data (inputs) available to support these models.

Today, the body of knowledge for integrating market and credit risks is well established. However, the enterprise, and therefore any enterprise-risk measure, also needs to include operational risks. Some may even go so far as to include reputation risks, business risks, and strategic risks.

Operational risk measurement is the topic of many recent regulatory discussions. These include both Basel II and Sarbanes-Oxley. Integrated risk measurement is moving beyond simple measures, like return on equity, to more advanced economic capital calculations.

The goal of integrated risk measurement is to measure risk and capital across a diverse range of activities including the traditional banking book, as well as securities and insurance. This requires an approach that integrates the various risks and underlying distributions (Rosenberg and Schuermann, 2004).

**DELIVERING THE INFORMATION IN AN ACTIONABLE TIMEFRAME** is key to enabling management, across the organization, to leverage their investments in risk management to actually affect the bottom line and shareholder value. If we look at the more advanced models, it could take organizations hours, weeks, or even months to bring together all the necessary data, perform the analysis, and report on the information. If risk measures are not delivered to management within a timeframe that enables them to act upon the information, then the measures become less about adding business information of value and more about historical accuracy. The latter may meet a regulatory requirement, but will not improve the risk awareness or risk behavior of the organization. In the end, the organization needs to define a methodology that can be implemented and lead to the creation of actionable risk measures.

**AGGREGATING THE INFORMATION AT THE APPROPRIATE LEVEL** will allow all levels of management to benefit. One of the goals of any enterprise risk management process is to create a risk-aware culture within the organization. Therefore, risk measures must be aggregated to levels that serve the many different levels and departments within an organization. For example, a branch manager in North Carolina would benefit if he could see how his portfolio risk contributes to the overall risk of the organization. This will allow the branch manager to begin to incorporate the impact that his decisions make on the overall risk appetite of the enterprise. The ability to aggregate or disaggregate risk measures will enable an organization to create a risk-aware culture.

As well, the ability to drill down into the measures will add a level of transparency to the calculation of enterprise risk. Whether it is measured as a Component VaR or some other risk contribution, managers need to be able to see how their decisions affect the enterprise risk measures. Regulators also want to be able to validate that organizations have a thorough understanding of the risks they choose to take versus those they may decide to mitigate.

### **ENTERPRISE RISK MANAGEMENT IN PRACTICE**

Nocco and Stulz (2006) probably summarized it best by saying, "While ERM may be conceptually straight forward, its implementation in practice is not." Banks today are the outcome of years of consolidation and reorganization of departments which separated risks into silos. While it may be common to have a trading group and a credit department, very few organizations have organized themselves to take full advantage of an ERM framework.

When banks merge or go through a significant reorganization (business change process), it not only brings together different policies and methodologies that must also be realigned, but it also brings together different infrastructures that need to be realigned. Banks are increasingly faced with integration and compatibility issues within their IT organization. Let us assume in a merger situation that banks can quickly agree upon new policies and methodologies; this leaves the largest burden on the infrastructure. The effort required to align the infrastructure can be daunting. IT departments must integrate various market and credit systems; various operational/management information front-, middle-, and back-office systems; and continue to support an ever-increasing regulatory reporting requirement.

In theory, it may be easy to prescribe the ideal scenario where policies and methodologies converge. In the end, organizations need to understand where they are today and plan how they get to where they want to be in the future. IT systems are a significant investment. Organizations spend millions of dollars to buy, implement, and support their current systems. Once a system meets internal and external approval, organizations will be reluctant to make changes.

However, change is an ever-present constant. In the past five years, banks have seen a dramatic increase in both regulatory and rating agency requirements. Organizations cannot rest on their past accomplishments but must continue to evolve, improve, and extend their competitive advantage(s). Therefore, it has never been more important for organizations to become more efficient, and this is attainable only by becoming more risk aware. The more accurately an organization can measure its risks, the more competitively it can compete in today's markets.

### **KEY CHALLENGES**

When setting up enterprise risk measures, banks are facing both internal and external challenges. Internally, banks have historically been designed into organizational structures that groups risks into silos. Banks have an investment

banking group, a retail group, and a corporate banking group. Now, to create enterprise risk measures, one will need to aggregate data from across these diverse internal organizations, processes, and IT systems.

Externally, banks have to meet new and ever-changing business, rating agency, and regulatory requirements. Banks must also be aware of, and cooperate with, external rating-agency requirements. The rating agencies will have an impact on the costs of funds the bank will require. The final consideration is investor confidence. Because investors will ultimately decide what the equity of a bank is worth, the bank must continually provide carefully managed transparency to investors in order to build this confidence. Investors will require the bank to demonstrate that its policies, methodologies, and infrastructure are consistent.

#### **KEY MEASURES**

Tradeshows, industry journals, and Web sites abound with suggestions on how to calculate risk measures. And, most would probably agree that some sort of measure that looks horizontally across the organization would be appropriate. Each bank must start from wherever they are today in terms of the infrastructure.

Even under the best circumstances, it can take three to five years to fully implement and integrate into an operational environment advanced risk practices. Furthermore, the cost of these systems is not insubstantial. The benefit is that once ERM is part of the risk culture and business units are identifying and managing risks on a day-to-day basis, the level of corporate oversight is often reduced (Gates, 2006).

There are several ways to calculate an enterprise risk measure. The first and most basic way would be to merely add all of the underlying risk measures together. Unfortunately, "Correlation is a minefield for the unwary." (Embrechts, et al, 1999). Some estimates suggest that an additive approach would overestimate risk by as much as 40% (Rosenberg and Schuermann, 2004).

To recognize the correlation between market, credit, and operational risks, one could use a copula approach. Using a correlation matrix, one could derive a normal copula that could be used to couple the marginal distributions for market, credit, and operational risk together. A more advanced approach would be for the user to use historical data or their own proprietary knowledge, along with a Student-t or Archimedean distribution, to define a copula. Both approaches use the statistical construct of a copula to join the underlying marginal distributions together. Depending upon how the copula is derived, this approach can be very efficient.

The benefit of the copula approach is that banks can use this approach to begin building enterprise-risk measures today. This process can continue while the underlying systems are integrated to support a more robust, single environment from which a true enterprise risk analysis can be conducted. In the end, everyone should strive to have one integrated environment in which all risk measures can be simulated together. This is the best way to measure true enterprise risk and account for all the underlying correlations and dependencies.

#### **COMMON CHALLENGES**

Regardless of whether one takes a more theoretical or practical approach, both methods will benefit by having extensive data integration capabilities. Users will benefit from being able to construct one common data model from which enterprise risk measures can be calculated. This will provide consistency and provide for one version of the data for everyone to leverage. As the data is updated, all the users will benefit.

This common data model will also help with all of the issues encountered when bringing data together from multiple sources. The key elements will include the frequency or periodicity of the data. Some data elements may change daily, while others may be updated weekly, monthly, quarterly, or even yearly. To support enterprise-wide calculations, the data needs to be uniform, or standardized. Users may also want to create a common set of business rules to manage missing data. In the end, the best analytical models are subject to the quality of the inputs. A good data model will ensure that only appropriate, consistent, and validated data are used in subsequent analysis. A good data model will also support archiving, partitioning, and auditability. The model should support the ability to trace any change made to the underlying data elements, and the needs of all the applications.

As noted previously, the only thing that is constant is change. IT systems can be very costly. Organizations should look for ways to leverage their investments in hardware and software. The recent increase in regulatory and ratings agency requirements only demonstrate the value of having a flexible and extensible solution. Organizations should build into the infrastructure design to not only consider the requirements of today but also consider yet-undefined future requirements.

Organizations should demand that vendors provide a solution that meets not only current requirements, but some assurance that when future regulatory, rating agency, or investor requirements arise the solution will be able to meet those requirements, too.

Future requirements could translate to increased performance or scalability. As risk measures are aggregated, the need for more robust and detailed analytics put a greater burden on hardware. For the past 40 years, Gordon Moore's predictions around hardware scalability have held true. Today, computers have more processing power, more memory, and more disk space. Solutions should leverage all of these hardware improvements. Organizations are starting to invest not only in SMP machines, but also in GRID infrastructures. The overall cost of computing is decreasing and, as a result, more and more organizations are able to leverage analytics that were previously believed to be impractical. New analytics will require IT systems to support multi-threading, parallel processing, and GRID technologies as ways to improve performance.

As the organization moves to a common infrastructure, it will facilitate the convergence of the analytics. The internal policies and methodologies will need to be supported by a common analytics platform. This common risk analytics platform will establish standards for how the fair value of each instrument is defined. Banks must determine the appropriate methodologies for calculating balance-sheet as well as off-balance-sheet instruments and positions. All of this will provide never-seen-before transparency into how risk is measured and reported throughout the enterprise. This will support the organization's policies to stimulate and support a risk-aware culture.

To meet advancing analytics, users should look beyond just calculating PD, LGD, and RWA. Most regulatory bodies are already talking about the need to create risk measures based on a type of economic capital calculation. As well, regulators are enabling more organizations to provide their own internal models to support regulatory capital calculations. In the future, banks will need to have analytical capabilities that can quickly evolve to meet changing regulatory requirements. Banks should demand vendors provide analytics that are not only transparent, but also extendible to meet future requirements.

Many banks have already begun to implement, or have already implemented, a common data model to support the underlying raw data or inputs. These input data models and data warehouses use industry best practices to improve efficiency, minimize duplication, and support a wide range of uses. However, as the bank creates risk measures, employees may quickly find that bringing risk information together to support enterprise-wide reporting is also very challenging. While a third-normal form may work well for organizing the inputs, this is not the best format for meeting the ever-increasing reporting challenges.

Some organizations may want to consider implementing a common risk-reporting repository. This repository would be designed purely to support the integration and reporting of enterprise risk measures. Whether it is simply supporting a common Web page for market, credit, and operational risk or if it is actually bringing together economic capital and risk-adjusted performance management, a common data model will support the enterprise infrastructure requirements. As well, a reporting repository can be used to support the partitioning and archiving of data.

The reporting repository should adhere to some of the more common data-modeling standards, including the use of valid to and valid from dates, mapping tables for integrating external sources, and hierarchies. The repository should support aggregated risk measures as well as decomposed measures at the entity, business unit, geography, or any other user-defined hierarchy.

Using a top-down approach, users may want to look at an aggregated risk measure and then drill down into the measure to identify where and how the risk may be attributed. This information can be used to help management identify areas of concern or reward groups that adhere to policies and methodologies and add value to the business. Because many risk measures may not be additive, reporting capabilities must be flexible and powerful enough to deliver the right information to the right people at the right time.

## **CONCLUSION**

All banks can benefit from having a robust infrastructure to support their evolving risk management requirements. This infrastructure should include a common integrated data model for supporting all of their (risk) applications. For example, a robust infrastructure serves to enable the deployment of an integrated set of risk methodologies for supporting both internal and external analytic requirements. A superior infrastructure serves to enable common risk-reporting repository to support ever-changing reporting needs. The infrastructure should be well designed and flexible enough to not only meet the risk management needs of today but also the needs of the future.

## REFERENCES

- "Enterprise Risk Management—Integrated Framework: Executive Summary." 2004. Committee of Sponsoring Organizations of the Treadway Commission. p. 2.
- Crouhy M, D. Galai, and R. Mark. 2005. *The Essentials of Risk Management*. New York: McGraw-Hill.
- Embrechts, Paul, Alexander McNeit, and Daniel Straumann. 1999. "Correlation: Pitfalls and Alternatives." Department Mathematik, ETH Zentrum, Zurich. March, p. 1.
- Gates, Stephen. 2006. "Incorporating Strategic Risk into Enterprise Risk Management." AIMS Conference Internationale de Management Strategique. Geneva.
- Nocco, Brian and René Stulz. 2006. "Enterprise Risk Management: Theory and Practice."
- Rosenberg, Joshua and Til Schuermann. 2004. "A General Approach to Integrated Risk Management with Skewed, Fat-Tailed Risks." Federal Reserve Bank of New York, Staff Report 185.

## ACKNOWLEDGMENTS

The author would like to acknowledge the contributions made by several colleagues:

Wei Chen  
Anthony Delorenzo  
Donald Erdman  
David Rogers  
Jack Yang

## CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Austin Trippensee  
SAS Institute Inc.  
100 SAS Campus Drive, R5103  
Cary, NC 27513  
(919) 531-2615  
Austin.Trippensee@sas.com  
[www.sas.com](http://www.sas.com)

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.  
Other brand and product names are trademarks of their respective companies.