How risky is your risk information?

Received (in revised form): 21st July, 2008

Robert M. Mark*

is the Chief Executive Officer of Black Diamond Risk Enterprises, which provides corporate governance, risk management consulting and transaction services. He serves on several boards. In 1998, he was awarded the Financial Risk Manager of the Year by the Global Association of Risk Professionals. He is on the board and is the Vice Chairman of The Professional Risk Managers' International Association. Prior to his current position, he was the Senior Executive Vice President and Chief Risk Officer, as well as Corporate Treasurer, at the Canadian Imperial Bank of Commerce. Prior to this, he was the partner in charge of the financial risk management consulting practice at Coopers & Lybrand. He earned his PhD, with a dissertation in options pricing, from New York University's Graduate School of Engineering and Science, graduating first in his class. Subsequently, he received an Advanced Professional Certificate in Accounting from NYU's Stern Graduate School of Business. He is also a graduate of the Harvard Business School Advanced Management Program.

Dilip Krishna

is head of Teradata's enterprise risk management and capital markets practice in North America. He and his team have consulted on enterprise risk management and Basel II initiatives with several US financial corporations. He has had 15 years of experience in technology and business consulting in the financial industry and brings significant experience in the successful management of large-scale projects. He has written numerous articles about risk data architecture and implementations and has also spoken on the topic in diverse settings. He holds Chartered Financial Analyst (CFA) and Financial Risk Manager (FRM) designations, as well as engineering degrees from the Ohio State University and the Indian Institute of Technology.

*Black Diamond Risk Enterprises, 3478 Buskirk Avenue, 1007 Pleasant Hill, CA 94523, USA
Tel: +1 925 212 7348; fax: +1 925 299 6859; E-mail: bobmark@blackdiamondrisk.com

Abstract A well-designed approach to managing risk information is a critical component of a superior risk management programme. A high-quality risk information management programme continues to be a blind spot and elude even the largest of financial institutions (FIs). For example, risk management at many large FIs has proved ineffective in organising their risk information to model the risk of complex structured products. This paper shows how inferior information quality adversely affects risk management. It then discusses ways to assess the quality of risk information in financial institutions as well as showing how to address this problem in a cost-efficient manner.

Keywords: *data integrity, information risk, modelling, model risk, risk information, risk information management, superior risk management, structured products*

INTRODUCTION

Recent market events have uncovered monumental risk information challenges at financial institutions. Financial institutions have written down more than US$319bn related to mortgage losses and write-downs.[1] The CEOs of some of the world's largest financial institutions have lost their jobs (including Charles Prince of Citi, Stan O'Neal of Merrill Lynch and Marcel Ospel of UBS) — clearly senior management in these firms did not have a clear idea of the valuation of very

large parts of their portfolios. These dramatic risk events come on the back of what had been perceived as the best of times for risk managers. For example, financial institutions have spent significant resources in this past decade on risk management programmes.

In the wake of the credit crisis, unanswered questions include:

- How did outsized losses materialise so suddenly, even though the housing market had been an area of concern for several prior months?
- Why did some of the largest financial institutions with acknowledged competency in risk management fall prey to these problems in such a public way?
- How is it possible that companies could not estimate their write-downs correctly, leading some to make massive financial restatements just weeks after disclosing already outsized write-downs?
- Why did rating agencies rapidly downgrade their credit rating assessment as opposed to a continuous series of downgrades as a function of the declining credit quality?
- Why did the regulatory community as well as the legislative and executive branch of government fail to act in a timely manner to forestall the subprime crises?
- Why did large institutions experience massive losses in businesses outside their core franchise? (For example, as at March 2008, UBS had taken US$18.4bn of losses against 2007 in its fixed-income business — fixed-income had hitherto brought in less than one-quarter of the company's revenues. Meanwhile, in the fourth quarter, Bank of America took a US$3bn write-down in its investment banking unit, which contributes only one-fifth of the bank's revenue.)

Many companies reporting these issues had challenges with processing and distributing critical risk information to key management stakeholders in a timely manner. One example of this can be found in the 'Shareholder Report on UBS's Write-Downs'.[2] This report contains numerous references to the lack of information for risk management. For instance, page 32 of this report suggests that a cause of loss in the FX/CCT Trading Portfolio was due to 'Lack of granular data'.[2] The document is peppered with oblique references to information unavailability — page 31 assigns blame for losses in the AMPS portfolio to the 'incomplete capture of risk attributes'.[2] Numerous other commentators have made similar observations.[3–5]

In contrast, as quoted from the Senior Supervisors Group report on recent market turbulences, 'Firms that avoided such problems demonstrated a comprehensive approach to viewing firm-wide exposures and risk, sharing quantitative and qualitative information more effectively across the firm and engaging in more effective dialogue across the management team'.[6] Superior risk management can be benchmarked in terms of the qualities of a firm's risk policies, methodologies and infrastructure.[7] Risk information management is a key component of the risk infrastructure.

Information risk is a major blind spot in risk management that every firm in the financial markets is grappling with. Risk management has come a long way towards implementing superior risk methodologies and adopting sophisticated risk policies. The problem of improving the quality of risk information management must be

urgently addressed, especially as the industry continues to innovate and expand. On a hopeful note, upgrading a firm's risk information capabilities is 'low-hanging fruit'. This paper will discuss ways to improve risk information management.

THE IMPLICATIONS OF RISK INFORMATION

Information is integral to risk management. For example, historical data are essential to building a good model. Risk management policies are toothless unless information is readily available to those charged with their implementation. Further, the need to disclose information has a significant impact on policies themselves. This section will study the impact of information by looking at aspects of risk management such as model risk, transparency and risk monitoring.

Model risk and triangulation

Quantitative models have become a cornerstone of financial risk management. Models have been used for valuing complex derivatives as well as to calculate the market and credit risk of these derivatives. Models have also been used to measure and mitigate operational risk such as credit card fraud, apprehending terrorist financiers and so on. Models are at best stylised representations of real-world behaviour. The dangers of model risk have been increasingly recognised. Many sources of model risk exist including model misspecification, model misapplication and incorrect implementation.[8,9]

The lack of data can significantly increase model misspecification risk. Model development is an iterative process and is based on a mathematical hypothesis to describe economic reality. Historical data are often segregated into two sets — the training set and the control set. The former is used to create and fine-tune the model while the latter is used to prove that the model works using sample data. Models must be periodically back-tested to ensure that their predictions are in line with actual experience. A well-known example comes from the implementation of the 1998 Basel Accord for market risk. The market risk regulatory rule states that a firm's value-at-risk (VaR) models must be continuously tested on a daily basis against actual outcomes. If the actual trading losses exceed the predicted VaR measure beyond the 1 per cent loss tolerance level (for more details, see Crouhy *et al.*[7,10]) then the regulator can raise the minimum required capital level. It is self-evident that a lack of quality historical data will adversely affect this process and can potentially lead to a poorly-specified model.

In the case of mortgage-backed securities, modelling complexity is exacerbated by the intricate linkage between many parties. Originators make retail loans which are packaged by intermediaries (such as government sponsored entities like Fannie Mae as well as commercial and investment banks) into a series of complex securities including mortgage-backed securities and collateralised debt obligations. Investors take on exposure by direct or indirect means, the latter via synthetic derivatives such as credit default swaps. Monoline bond insurers (such as MBIA) also take on a significant contingent exposure in this process.

These securities have significant levels of complexity and risk including:

- credit and prepayment risks embedded in the mortgage structure;
- market and liquidity risks of the mortgage-backed securities;
- operational risks such as model risks, legal risks, fraud risks and so on.

Several methods for valuing these securities exist. Each has strengths and weaknesses:

- Analytical models often make simplifying assumptions, execute quickly and may be based on little underlying information. For example, Moody's binomial expansion technique calculates a diversification score for the portfolio and replaces the actual portfolio with a much simpler hypothetical portfolio of homogeneous, uncorrelated securities. Such models have generally functioned poorly in abnormal markets.
- The main inputs in the Monte Carlo simulation approach are asset-level probabilities of default and pair-wise asset correlations, which are turned into an estimate of the entire collateral pool's loss distribution. Monte Carlo approaches can potentially produce accurate loss distribution estimates, but are computationally resource-intensive.
- Collateralised debt obligation indices such as the Dow Jones iTraxx, created in 2004, have experienced a great degree of popularity in recent years. Their illiquidity and the often unrepresentative nature of the products they serve to represent have reduced their value.
- Stress testing evaluates the potential impact on portfolio values of unlikely but plausible events. Bottom-up stress testing includes subjecting individual units within the portfolio to stress factors such as loan, borrower and collateral risk characteristics. Stress testing offers valuable insight.
- Rating agencies are considered to have expertise in credit rating. They are generally regarded as unbiased evaluators. Their ability to predict credit deterioration of structured securities has come under sharp attack.

There is no perfect solution as each of these techniques for valuing securities on a standalone basis has drawbacks. It is therefore important to benchmark (or triangulate) the predictions of one model against others. Triangulation uses several methods in combination with one another to guard against over-reliance on any one model. The construction and assumptions of each model can be refined by comparing each model result with the others. Triangulation is also subject to information risk (although this can be mitigated, as discussed later):

- Were the models run on the same underlying set of data?
- Can adjustments be made for model inconsistencies?
- Can the models be audited and back-tested?

Successful triangulation depends on each model using the appropriate set of underlying data. Only if the data are of sufficiently high quality and consistency can a quantitative analyst be confident that the inconsistency in results between models can be attributed to their theoretical underpinnings and not the data used to build them.

Transparency

The importance of making risk transparent has been raised to new levels. A couple of recent examples serve to illustrate. On 27th February, 2008, Bear

Stearns was trading at US$87.50. By 17th March, its funding liquidity had dried up to such a point that it agreed to be sold at a fire-sale price to JP Morgan Chase for US$2 a share (subsequently revised to US$10). The deterioration in Bear Stearns' condition was precipitated by clients of the firm who did not have a clear understanding of Bear's funding liquidity and its ability to honour its obligations. This lack of transparency in turn caused the proverbial run on the bank, with catastrophic results. The lack of transparency regarding Bear's financial position rapidly brought the bank to its knees and caught the street, regulators and perhaps even Bear's senior management utterly by surprise. The Bear Stearns case brought back memories of the Long-Term Capital Management collapse in 1998, which also followed a dramatic drying up of liquidity.[11]

One of Bear Stearns' rivals dealt with the same crisis in a very different way. Senior executives of Lehman Brothers (including its chief executive and chief financial officer) orchestrated a well-executed plan to rapidly bring transparency to its funding liquidity when it found its liquidity position being questioned. As recounted in the *Wall Street Journal*,[12] they quickly prepared two pages of 'talking points' to detail the firm's financial position and compare this with its competitors. Their data were fed to hundreds of managers to assuage client concerns, ultimately saving the firm from Bear Stearns' fate.

Transparency is at its heart an informational issue. As the above two examples illustrate, the ability to ensure timely access and dissemination of information has become an important dimension of superior risk management. To quote Joseph Mason's testimony to the US Senate Committee on the Judiciary, 'The market today is struggling to sort out information. Investors will not join back in until information about values and holdings is improved'.[13]

Risk monitoring

A key function of risk management is to monitor a firm's risks frequently as the risk profile can change dramatically via changes in the portfolio or market environment. Monitoring frequency is a function of the firm's portfolio of businesses. A multinational financial institution engaged in large trading operations will need a much more timely monitoring system than a regional bank.

Timeliness is not the only challenge in risk monitoring. Access to risk information must also be carefully controlled. For example, Barings could have known well in advance about unauthorised cross-trading in the bank's 'error account', where Leeson concealed his unauthorised trades and exposed the bank to significant market risk. Unfortunately, his unauthorised access to both the front and back office enabled him to circumvent standard procedures and book trades at fictitious prices.

ASSESSING INFORMATION QUALITY: HOW DOES *MY* ORGANISATION STACK UP?

Information interacts with risk management policies, methodologies and infrastructure in subtle ways. It is imperative that information risk be addressed in a structured, methodical way just like any other operational risk. Each organisation should tailor its information management environment

to its needs rather than designing requirements to a 'gold standard'.

Consider the contrasting views of a particular business function such as risk-based pricing between a large investment bank and a regional property and casualty (P&C) insurance company. It is critical for the investment bank to price all risks into each transaction in a timely manner. The potential loss from systematic risk mispricing can easily justify a timely risk information management system. In contrast, the P&C insurance company, with regulatory constraints on pricing, needs risk information perhaps only monthly.

The particular aspects of overall information quality to be assessed will also depend on the company's unique situation. Near-term regulatory compliance imperatives (eg an anti-money laundering initiative) may focus on issues like data correctness. The ability to satisfy regulatory scrutiny needs to be harmonised with business-driven imperatives.

The term 'information quality' has different connotations and needs further clarification. Table 1 provides information on the essential components of information quality.

Table 1 can be used to assess the quality of information within any particular risk management function. A regulator or a rating agency might want to benchmark information quality across

Table 1: Components of data quality

Integration	Adequately capture relevant data relationships; for example, does information about insurer-wrapped tranches link to information about the insurer itself, including current ratings information etc?
Integrity	Data integrity is essential; for example, do risk exposure roll-ups reconcile with financial statements?
Completeness	Capture all exposures across the organisation (eg bespoke deals that are held *ad hoc* on trader's spreadsheets).
Accessibility	Users should have easy access to current and historical data and be able to reuse data in any form they require within limits set by security and other requirements.*
Flexibility	Users should be able to analyse data across any dimension they choose.† Flexibility includes being able to filter or summarise information in any dimension, at will. This is critical in a 'test-and-learn environment' used to value complex structured products. For example, summarising data by credit rating and geography may lead to an insight that further drill-down by weighted-average maturity would be useful. The ability to rapidly access successive layers of information is crucial to effective analysis.
Extensibility	It is often necessary to include new types of data in valuing complex instruments. Extensibility refers to the ability to bring these data into the environment along with all relevant linkages and the appropriate level of data quality.
Timeliness	How soon is data (deal information, market data, revaluations etc) available after the occurrence of the relevant business event? For example, real-time stock information is worth many hundreds or thousands of dollars per month, while information that is 15 minutes delayed is available for free on websites like Yahoo and Google.‡
Auditability	Data are easily traceable from reports back to their source. It is hard to have confidence in information that has been tampered with maliciously or inadvertently.

*A good example of this issue can be found in the UBS Write-Down Report: 'Neither risk management nor the control functions had readily accessible data upon which to perform fundamental analysis of the securities in the portfolio, for example vintage, 1st or 2nd lien or FICO score'.[2]
†The report by the Senior Supervisors Group exemplifies this problem by pointing to the few best-practice firms that escaped most of the market turmoil: 'They could quickly vary assumptions regarding characteristics such as asset correlations in risk measures and could customize forward-looking scenario analyses to incorporate management's best sense of changing market conditions'.[6]
‡The UBS Write-Down Report points to this problem as well: 'BUC explained that such delays have occurred for a number of reasons, including data issues and priorities changing in light of market developments'.[2]

various organisations. A financial institution can use it to benchmark progress in information quality initiatives and to set targets for improvement.

Figure 1 provides an illustrative example of a risk information maturity assessment. Each component of information quality has been measured along a maturity grade from inadequate to competitive edge. The current state is shown by the squares, while the desired state is shown by the circles.

A detailed discussion on assessing the quality of information is beyond the scope of the present paper (the interested reader is referred to Mark and Krishna[14]). Instead, a brief description will be given to give the reader a flavour. The risk management function first needs to be deconstructed into relevant functional components. For example, this will include analysing functions responsible for setting business strategies, deciding on risk tolerance, approving authorities, providing disclosure, designing risk measures and stress tests as well as providing valuation/vetting services and publishing performance measures. Three sets of evaluations are then performed:

- Senior risk officers prioritise the relative importance of individual functions. For example, a financial institution under regulatory scrutiny would score disclosure high relative to performance measurement, whereas one that is aggressive about new products will focus more on valuation/vetting.
- Risk executives prioritise the importance of information characteristics for each function. For example, risk measurement executives can be expected to score timeliness as a high priority.
- The organisation's raw ability to satisfy the policy and methodology dimensions with information is scored.

These inputs can be transformed into a form shown in Figure 2 via a series of analytical manipulations previously described by Mark and Krishna.[14] This chart combines all variables such as

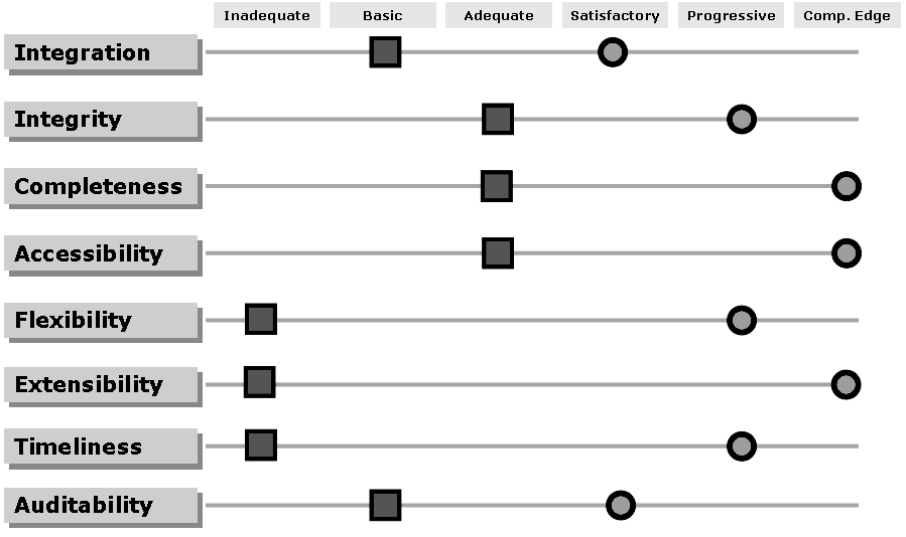

Figure 1: Assessing and setting goals for information quality

organisational goals, cost-benefit considerations and an assessment of the current quality of information into a 0–100 per cent scale, where achieving 100 per cent is the organisation's goal. Some of the scores in Figure 2 seem very low. Nevertheless, experience shows that these scores are representative of much of the industry.

SOLVING INFORMATION QUALITY

The information quality assessment can identify symptoms. For example, Figure 2 suggests challenges in integration and extensibility, but improvements to information quality cannot be solved in isolation. Rather, they must harmonise the often-conflicting goals of risk management, business and technology executives. The key to applying technology effectively is to translate business expressions of information quality into actionable infrastructure counterparts. There are two aspects to data management infrastructure:

- the people, processes and technology needed to implement and operate a risk information environment;
- an appropriate implementation methodology suited to large, potentially multinational financial institutions.

People, processes and technology

Risk information is sourced from and distributed to all parts of the organisation. Organisations need holistic risk information management environments (rather than an isolated 'system') that effectively link data producers and consumers. There are usually many alternatives to resolving data issues. For example, source data quality problems can be fixed in the risk information repository or by improving the relevant business processes. Therefore, a risk information management environment needs to consider business processes as well as technology. This environment will include the components shown in Figure 3 and described in Table 2.

Each component can be directly addressed. For example, the metadata issue can be solved by putting in place procedures to keep metadata updated,

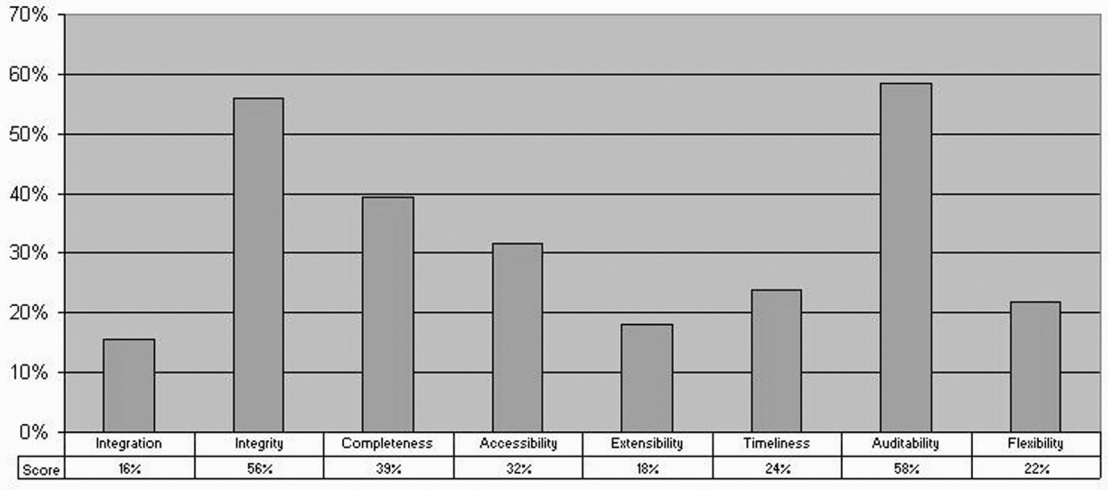

Figure 2: Assessment of information quality by component

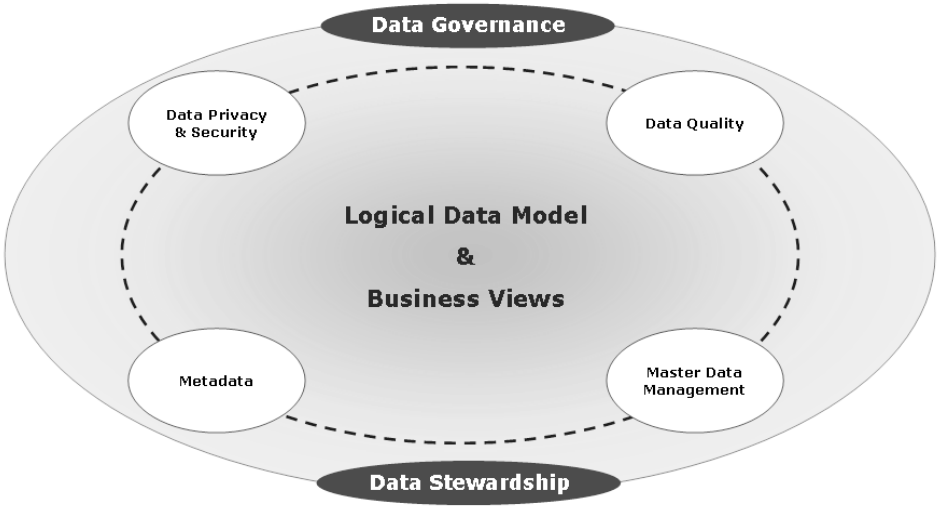

Figure 3: Enterprise data management framework

Table 2: Components of a data management framework

Data governance	Ensures senior management oversight and support
Data stewardship	Encompasses data management processes
Metadata	Helps define data semantics; for example, 'facility' can be interpreted differently in the trading room and the loan book
Data quality	Ensures accuracy and completeness; for example, ensuring that trade-date is always on or before settlement date
Reference or master data	Relatively static data such as customer information, product masters and organisational hierarchies; as aggregations typically use reference data, poor quality reference data can cause large inaccuracies
Data privacy and security	Important from business and regulatory perspectives (eg Gramm-Leach-Bliley Act in the USA and EU Data Protection Initiative) Significant regulatory, reputation and operational risk can arise; for example, TJ Maxx disclosed in 2007 that hackers made away with 45 million customer records, exposing the company to significant financial, reputation and legal risk*
Logical data model	Enterprise-wide blueprint for data

*Gaudin, S. (2007) 'TJ Maxx breach costs hit $17 million', *InformationWeek*, 17th May, available at: www.informationweek.com/news/security/showArticle.jhtml?articleID=199601551 (accessed date 3rd August, 2008).

building technology interfaces between various systems to load metadata and implementing a commercially available software package to allow business and technology users to use the metadata.

The logical data model

Data need to be appropriately structured to ensure that high-quality information can be generated. An enterprise-wide blueprint for data, technically referred to as a logical data model (LDM), serves to resolve data element and relationship ambiguities. A simplified illustrative LDM example is shown in Figure 4. All organisations should strive to create one (but only one) data model standard and attempt to make this as complete as possible.

An LDM is a high-level diagram of data in an organisation done to engineering precision. When building a house, one often begins with a sketch showing the various rooms. This initial

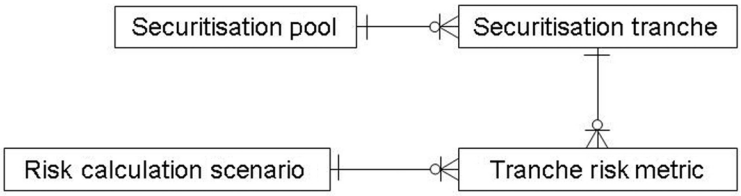

Figure 4: Simplified logical data model for securitisation

drawing does not include detailed construction-specific information such as the type of materials needed, but does include details such as room dimensions, plumbing details and electrical details. This first sketch can be thought of as the LDM.[15] In essence, the LDM illustrates the relationships between various aspects of data within an organisation.

Using the simplified example shown in Figure 4, the following relationships, for example, can be immediately deduced:

- each securitisation pool has zero, one or more tranches, but each tranche has one and only one pool;
- each calculation scenario can generate zero, one or more risk metrics; however, each metric must be tied to one and only one scenario;
- pools are connected to scenarios only via the tranche and its associated risk metric;
- a tranche can have many versions of risk metrics depending on the scenario run.

Specifying this level of detail is important. An analyst can now command his database to 'give me tranche 1234567 along with its pool ID and all of its risk metrics', confident that he will not inadvertently miss any other pools that the tranche may be related to.

Figure 5 shows the complete LDM for a particular organisation's structured product data. Many more objects and their interrelationships are now shown.

Ad hoc questions can easily be answered using an LDM. For example, tranche risk metrics (see A in Figure 5) can be linked to tranches (B) to yield an analysis of the most risky tranches; the connection to pool (C) and party (E) can also indicate what pool and counterparties were involved). If the object of the exercise is to understand the risks measured by a particular scenario then it is also possible to filter by scenario (D).

This LDM structure (cast in the so-called 'normalised form'[16]) can serve to answer almost any kind of question about the data. An LDM is an invaluable tool in enabling risk analysts to posit views about risks in their portfolios, and then efficiently and quickly to verify the accuracy of their views. In a well-managed risk information environment, analysts can use the LDM to perform analyses confidently.

Effective implementation: Mitigating information risk

Most organisations do not have the luxury of a 'green field' implementation of a risk information management environment. Rather, the challenge is to improve an existing environment towards a standard of excellence in the face of inevitable constraints. A number of risk management and business initiatives will already be underway. Priorities therefore need to be set for each information management initiative.

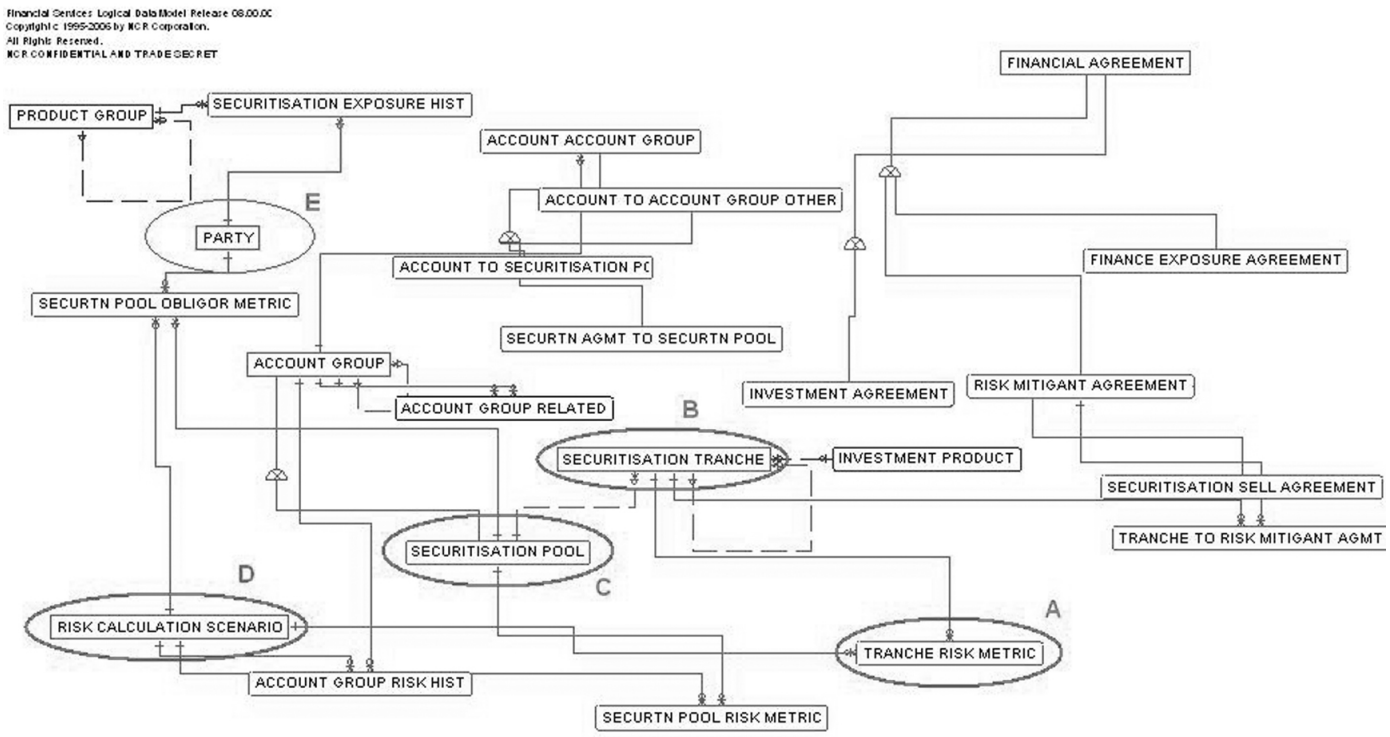

Figure 5: A logical data model for securitisation (partial view only)

Finally, cost constraints will inevitably be present.

Some proven success factors are given below:

- The organisation must see some early benefits which in turn will ensure a growing base of advocates as well as provide programme managers with success stories to use in selling the idea to potential new participants.
- It is best to win some easy victories with 'low-hanging fruit' early in the programme. The momentum gained will allow more difficult problems to be addressed.
- It is better to implement the programme in small increments that produce repeated successes.
- It is important to ensure that business requirements are properly captured.
- 'Analysis-paralysis' must be avoided at all costs. This is especially true because most requirements change over time, so it is hard to get them right the first time.

A methodology for progressively implementing a risk information management environment is described below. The four steps are:

1. Assess the current data environment.
2. Design a future-state data environment (based on well-thought-out requirements), and identify gaps between current and future state.
3. Develop a future-state implementation roadmap.
4. Implement the roadmap in incremental steps that generate value at each stage.

The current state of the data environment should be assessed in two

ways. First, the infrastructure (ie the people, processes and technology) itself should be assessed across several dimensions including data infrastructure technology (such as tools used to ingest, host and deliver data to users). Secondly, the risk information management organisation must also be assessed, including funding and prioritisation of new requirements and provision of user access capability. This assessment will identify any obvious shortcomings in the environment.

A gap assessment that is benchmarked against requirements must be created (as described earlier) as a guide to creating the future-state risk-information architecture as it is unnecessarily expensive to fully address each shortcoming. Several architecture frameworks are available, including the Open Group Architecture Framework,[17] which attempts to tie business processes to the information, applications and infrastructure. The result is an end-state consisting of four architectural layers: business, functional, information and infrastructure. Each describes a facet of the end-state while remaining consistent with the overall vision.

Business architecture describes processes relevant to generating risk information. These include front-office processes such as trading, underwriting or credit card operations. The business architecture will detail these changes as these processes often need modification to resolve risk information inconsistency. The functional architecture describes the technology applications that are to be used in business architecture processes (along with their information interconnections) which in turn are used to design for information exchange (the so-called information architecture). Infrastructure support for information is detailed in the infrastructure architecture.

An implementation roadmap can then be developed. This should consider organisational realities (such as business priorities) as well as information architecture gaps and should consider the success criteria discussed earlier (iterative steps, measurable business value at each stage etc). A plan that takes advantage of data reuse (eg transaction data as a common factor in credit, market and liquidity risk modelling) will also have a better chance of success.

CONCLUSION

Risk management has come a long way in the last two decades, especially in financial institutions. Huge strides have been made in methodologies to measure risk as well as in risk policies and corporate governance. Yet information risk continues to be a persistent thorn in efforts to improve risk management's ability to enhance its relevance to business management. The pace of financial innovation, rapid globalisation and the 'always-on' nature of today's markets have given risk infrastructure a punishing burden. No longer is information risk a bothersome but irrelevant issue; in fact, it is the Achilles heel of risk management. Financial institutions should recognise this nascent but potent threat to their organisations and purposefully execute a plan to build an effective information environment for risk analysis and management.

On a positive note, solutions are increasingly available. Advances in enterprise integration technology and organisational change management have come together to offer effective solutions. It is hoped that the present

paper provides food for thought and advances readers' efforts in executing a plan for a better risk information environment.

References

1 Onaran, Y. (2008) 'Banks raise $231 billion capital as credit losses surge', Bloomberg, 30th April, avalable at: http://www.bloomberg.com/apps/news?pid=20670001&refer=&sid=a7bIjIq1YbQw (accessesd 3rd August, 2008).

2 UBS AG (2008) 'Shareholder Report on UBS's Write-Downs', 18th April, available at: http://bigpicture.typepad.com/comments/files/080418ShareholderReport.pdf (accessed 3rd August, 2008).

3 Mason, J. R. and Rosner, J. (2007) 'Where did the risk go? How misapplied bond ratings cause mortgage backed securities and collateralized debt obligation market disruptions', 14th May, available at: http://ssrn.com/abstrat=1027475 (accesssed 3rd August, 2008).

4 Bies, S. S. (2003) 'Managing Business Risks', Speech before the Oregon Bankers Association, Independent Community Banks of Oregon and Idaho Bankers Association, Sunriver, OR, 16th June.

5 FitchRatings (2005) 'A comparative empirical study of asset correlations', FitchRatings Structured Finance, Quantitative Financial Research Special Reports, 14th July, available at: http://www.fitchratings.com/dtp/pdf3–05/gcom0714.pdf (accessed 3rd August, 2008).

6 Senior Supervisors Group (2008) 'Observations of risk management practices during the recent market turbulence', 6th March, available at: http://www.newyorkfed.org/newsevents/news/banking/2008/SSG_Risk_Mgt_doc_final.pdf (accessed 3rd August, 2008).

7 Crouhy, M., Galai, D. and Mark, R. (2005) 'The Essentials of Risk Management', McGraw-Hill.

8 Aragonés, J. R., Blanco, C. and Dowd, K. (2005) 'Keeping all eyes on model risk', *Futures and Options World*, September, pp. 57–60.

9 Rebonato, R. (2002) 'Theory and practice of model risk management', in Field, P. (ed.) 'Modern Risk Management: A History', RiskWaters Group, London, pp. 223–248.

10 Crouhy, M., Galai, D. and Mark, R. (2000) 'Risk Management', McGraw-Hill.

11 Perold, A. F. (1999) 'Long-Term Capital Management case study', Case No. 200–007, Harvard Business School.

12 Craig, S. (2008) 'Lehman finds itself in center of a storm', *Wall Street Journal*, 18th March, p. A1.

13 Mason, J. R. (2007) 'The looming foreclosure crisis: How to help families save their homes', testimony to the United States Senate Committee on the Judiciary.

14 Mark, R. and Krishna, D. (2007) 'Evaluating enterprise risk information management', White Paper, Teradata Corporation, available at: http://www.teradata.com/t/page/173909/index.html (accessed 3rd August, 2008).

15 Srikant, S. (2006) 'Logical data modeling: A key to successful enterprise data warehouse implementations', *DM Review Magazine*, September, available at: http://www.dmreview.com/issues/20060901/1062071-1.html (accessed 3rd August, 2008).

16 Hoberman, S. (2005) 'Data modeling made simple: A practical guide for business & information technology professionals', Technics Publications, LLC, 17th October.

17 The Open Group Architecture Framework (2006) 'Welcome to TOGAF', available at: http://www.opengroup.org/togaf/ (accessed 3rd August, 2008).