

Collaboration delivers better risk management: Reduce the risk of enterprise risk management implementation

John Cant, MPI Europe

Portfolio diversification – reducing overall risk sensitivity by taking positions in a range of instruments rather than one – is a well-known investment risk management technique. This paper looks at how some of the same principles can be applied by combining a mix of business and consulting skills with products from application and technology providers to better implement enterprise risk management (ERM). In particular, it concentrates on techniques that avoid some of the underlying technology and infrastructure issues (that scored as highly important obstacles in a recent SAS ERM survey), so the end users can focus on the business aspects of an ERM implementation.

Context – the need for ERM

Enterprise risk management is the process by which a company's management and staff manage the broad spectrum of risks (market, credit and operational) across the whole enterprise within their defined risk appetites, to deliver their strategic objectives. Implementing ERM in financial sector firms is complex and involves changes in analysis, technology and culture. Amongst the key challenges is collecting and analysing data for the range of risks from a wide range of sources across the organisation.

The pressures to adopt ERM have come from both internal and external sources, as illustrated in the diagram. External influences include regulations



such as Basel II, which require banks to address market, credit and operational risk together under one regulation. Other factors such as the Enron crisis have heightened requirements to fully understand credit exposures across your entire firm. The internal demands include the need to manage the risk of complex instruments that straddle traditional product and geographic boundaries, growing use of algorithmic trading – circumventing traditional manual processes and controls – and the increased demands from investors for transparency and better cross-asset reporting.

So risk, compliance and IT functions are facing the paradox of increased demands from the business for enterprise systems to deal with dynamic and complex data, but at the same time keep the implementation costs and risks under control. This is confirmed by a recent prediction by Gartner that “Through 2008, 60 percent of financial services CEOs will still be asking why it costs so much to implement enterprise systems yet still lack adequate management information.” So what is the answer to this paradox?

The collaborative approach

The full answer starts with the important steps of proper definition of the business requirements and selection of the correct application software. Once this is complete, we can start the physical implementation – the area of interest for this paper. Our assertion is that successful ERM implementation has to be provided by a mix of powerful application software with deep domain and infrastructure knowledge. However, simply having multiple vendors and applications involved in an implementation is not new. The difference in what we are proposing is an improved split, and coordination of implementation tasks into business, application and infrastructure layers can allow partners to concentrate on their key strengths with minimal disruption to others. By partnering, each firm can deliver best-of-breed components for ERM solutions to financial sector firms and beyond.

So much for the theory, let's look at how and why this works in practice. We will consider each of these areas below.

- Cost of ownership
- The importance of data and storage
- Reducing ERM's operational risk

Cost of Ownership

Whether you are a hedge fund or the largest global universal bank, you need to select an ERM application and IT platform to suit your needs. This is not without its potential pitfalls as some, apparently cheaper, solutions can often cost more due to higher integration costs, customisation, maintenance and upgrade problems, and difficulty in dealing with the high volumes, performance demands and availability requirements of ERM.

Performance

Performance within a budget has been a perpetual issue in risk architectures, e.g., for compute-intensive activities such as Monte Carlo simulations. With different manufacturers such as Sun, HP and Intel supplying a range of high-performance architectures for ERM applications such as SAS, these need to be considered carefully alongside the specific business requirements and budget constraints. The answers may not be obvious – I can recall several discussions with senior risk managers to convince them that simply buying the fastest new chip did not automatically guarantee good performance. To reduce the risk of poor performance, it is worth undertaking activities such as setting up a “proof of concept” for a client's new risk architecture or undertaking performance benchmarking with representative data. During these, application vendors and technology infrastructure staff can help by tuning their respective architecture layers.

Achieving good run-time performance needs a balance between compute and data performance. When manipulating large volumes of risk data, performance can be addressed in three main steps: firstly, from a business requirements perspective – identifying and using the right data – or in other words addressing the business layer; then secondly, handling data correctly in the chosen application; and thirdly, have the storage infrastructure set up correctly. As an example, we will look specifically at the third category.

A high-performance compute server requires a high-performance file and data storage configuration to feed it data at the speed required for the most demanding data intensive application tasks. With complex metadata being handled in the application, the infrastructure layer can concentrate on delivering rapid access to data. Also, it is important to understand that the need to read, and potentially write, data across multiple systems requires proper planning and integration to avoid the significant performance overhead of typical shared file systems without the need to alter the application layer.

The importance of data and storage

One of the key principles that ERM application providers such as SAS bring is that an understanding of the importance of data and data management is key to your business and to risk management in particular. Correctly implemented ERM software combined with a well-designed infrastructure layer allows the storage and analysis of data on the firmwide, often global, scale required by ERM today. Some examples are presented below.

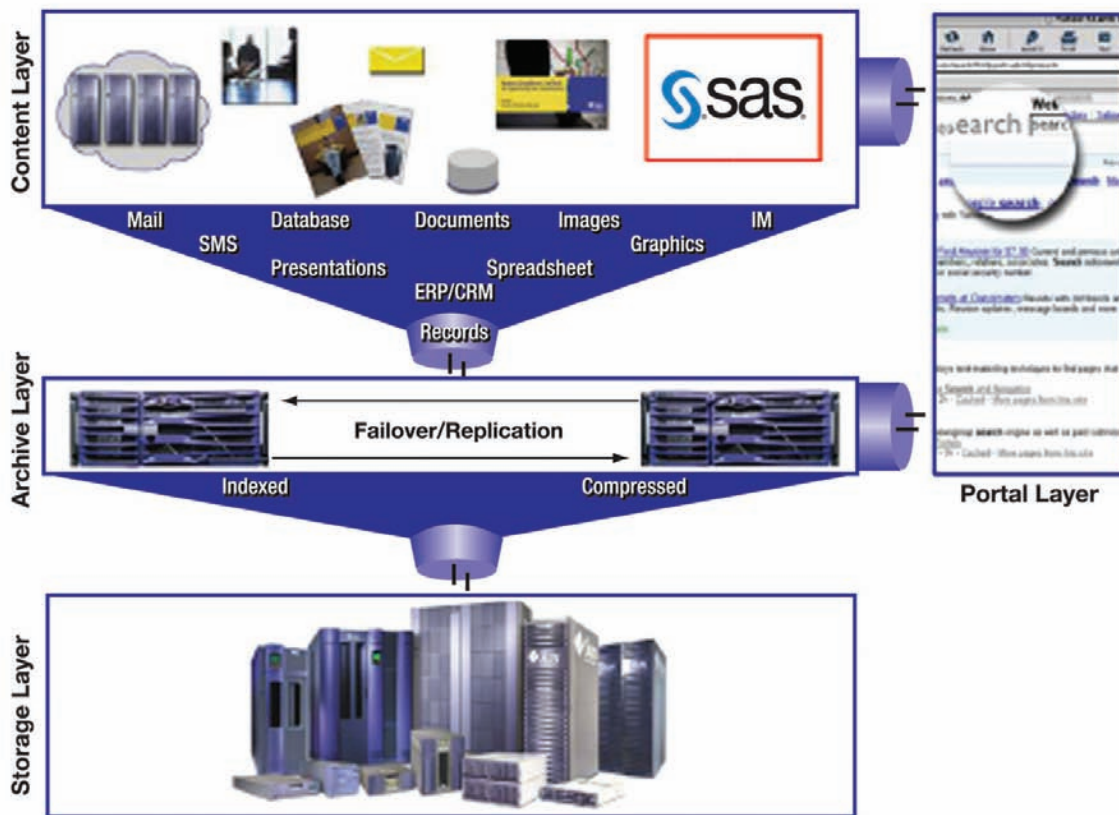
Intelligent storage Not all risk data is equal. Some data may be accessed on a regular intraday basis, whilst other data may only be accessed occasionally but needs to be retained online e.g., for regulatory searches or enquiries. By optimising the movement of data between storage types using an intelligent policy-based approach in the infrastructure layer, the ERM application does not need to manage the exact placement of its data on the financial firm's storage estate. Vendors estimate that they can deliver cost savings of up to 50 per cent compared with disk-only systems.

Information lifecycle management

An information lifecycle management approach, where data can be maintained within the storage layer from creation to archiving, can be used to efficiently support the complex data retention and legal discovery requirements that pervade trading, settlement and risk management. These requirements look only set to increase; take, for example, the new retention periods for trade-related data set by MiFID. There can be significant efficiency gains by implementing this in the storage infrastructure rather than in each application.

Reducing ERM's operational risk

Even risk systems are subject to operational risk, and prudent organisations need to manage this risk. In recent research completed for Sun Microsystems, over 86 per cent of financial institutions identified reducing the operational risk inherent in their IT infrastructures as being either important or very important to them (Source: Future Directions – Financial Technology 2006). With Basel II, this strong internal desire to better understand and manage IT operational risk becomes a regulatory necessity. The following takes just a few examples to show how the proper design and use of technology can materially augment an ERM application suite.



Incremental backup ERM applications are expected to hold a large amount of input, time series, historic and calculated data. For these types of application, traditional backup techniques are insufficient. For example, they may require copying of an entire large file simply because a small amount of recent active data has changed. Instead a continuous and dynamic archiving mechanism—independent of the specific database structure—is required, so the risk management application can be continuously available as there is no need for the traditional “backup window” when an archiving process had to have exclusive access to the system.

BCP/DR capabilities Sensible disaster recovery and business continuity arrangements need to be put in place for risk management systems. Due to the bankwide nature of ERM systems and their multiple information feeds, these arrangements can be overly complex if

the architecture is not planned appropriately. Fitting business continuity arrangements onto an ERM implementation retrospectively is likely to be expensive and highly inefficient. Working with clients at an early stage to design, implement and maintain their specific resilience and recovery procedures, and build much of this functionality into the infrastructure layer, can prevent many of these issues. The types of areas to consider include managed services, clustering, data vaulting, replication and testing. These cover the three main areas of network availability, application service availability and data availability.

Conclusion

This paper has touched on several key ways that engaging the right partners in the right way is a potent combination in Enterprise risk management. Financial institutions can create an integrated platform by engaging leading software vendors and providers of technology

infrastructure, facilitated by domain consultants, in a way that plays to each vendor’s strengths. This supports the holistic, integrated view of risk across the enterprise based on a robust, efficient, extensible and cost-effective risk intelligence and data management platform that is a solid foundation for future challenges in enterprise risk management.

John Cant
 is the Managing Director of MPI Europe, a consultancy specialising in helping financial sector clients deliver business benefit through IT and risk programmes. With 20 years of experience in finance, John has worked in a variety of roles from banker to software product manager to KPMG Consulting Partner, giving him an in-depth understanding from a broad range of aspects as to how to deliver successful projects.