Focus on fundamentals

For too long, regulators have issued complex rules while seemingly oblivious to the fact that banks will struggle to comply, argues ***David Rowe****. A new initiative around effective risk data aggregation and reporting represents an overdue focus on the fundamentals*

The dire state of enterprise data represents the dark underbelly of the transformation in computer technology over the past 50 years. Computing migrated from enterprise mainframe devices in the 1960s to mini-computers in the 1970s, then PCs in the 1980s and beyond. This dramatically improved the agility of computer systems but, at the same time, computing power fragmented into thousands upon thousands of devices scattered across diverse geographic, organisational and technological areas. We are living with the consequences of this evolution and will continue to do so for decades to come.

In previous columns, I have addressed the adverse impact of fragmented and inconsistent data on the effectiveness of risk management (*Risk* April 2012, page 57, *www.risk.net/2161686*). For nearly three decades, regulation has become increasingly complex, while little time seems to have been spent asking whether banks are able to use the rules' associated metrics in a reliable way. The attitude seems to have been, 'Well, banks will just have to figure it out'. For better or worse, few banks have mustered the resources and sustained discipline needed to maintain comprehensive, accurate, timely and well-structured data at the enterprise level. Somewhat belatedly, regulators are starting to focus on the fundamentals of this problem.

In January, the Basel Committee on Banking Supervision published *Principles for effective risk data aggregation and risk reporting* (*Risk* July 2013, pages 48–50, *www.risk.net/2275806*).[1] This paper lays out enterprise data standards that it proposes be mandatory for all global systemically important banks and strongly suggests that they be imposed on domestic systemically important banks as identified by their national supervisors.

The 14 principles fall into four broad categories: governance, aggregation capabilities, reporting practices and supervisory review procedures. Perhaps the most significant initiative is to place responsibility for initial and continuing compliance with these requirements squarely on the shoulders of the board, acting through senior management. A significant part of this responsibility is the development of an IT architecture and infrastructure capable of meeting risk aggregation and reporting needs in both normal times and during periods of stress or crisis.

David Rowe is senior strategist for risk and regulation at Misys in London. Email: david.rowe@misys.com

While the report does not reference the concepts directly, this last requirement relates closely to 'risk velocity' and 'risk management clock-speed' as discussed previously in this column (*Risk* March 2010, page 79, *www.risk.net/1594873*).

Other principles deal with standard issues, including:

- Risk data aggregation capabilities:

(3) accuracy and integrity
(4) completeness
(5) timeliness
(6) adaptability

- Risk reporting practices:

(7) accuracy
(8) comprehensiveness
(9) clarity and usefulness
(10) frequency
(11) distribution to relevant decision-makers.

Much of this is motherhood and apple pie, but two items have major strategic implications, namely (5) and (6).

Timeliness requirements go to the heart of how data transmissions are structured. Traditional batch file processes are inevitably clumsy and slow. They were attractive when storage and communication costs loomed large, but these are far less important constraints today. An event-driven approach based on self-describing messages (typically in an XML format) supports migration to incremental updates in real time.[2] Such timeliness can never be achieved until batch updates are a thing of the past.

Adaptability focuses on the need for easy access to *ad hoc* analyses in a time of crisis. It is impossible to anticipate in advance what questions will need to be answered in the future, especially under the pressure of an unfolding crisis. Achieving the required degree of adaptability requires capturing massive amounts of detailed data down to the trade level. It also requires indexing these details along multiple vectors of interest – for example, country, industry, trade type, external legal entity and internal legal entity – and developing analytical tools to leverage these indexes to maximum advantage across risk types.

In effect, all these requirements should help make a bank's risk infrastructure better able to support management decisions. It is a sad commentary that bank executives need to be told to do this by regulators. ■

[1] *Basel Committee on Banking Supervision,* Principles for effective risk data aggregation and risk reporting, *Bank for International Settlements, January 2013*
[2] *For a rather too optimistic view of the prospective impact of XML, see* XML and the future of risk management *(*Risk *January 2000, page 89)*