BCBS 239: Is Spending $8 Billion on IT the Answer?

How is it possible that the introduction of a set of straightforward and perfectly sensible operating principles can throw an entire industry into confusion? A solution path through risk accounting.

Thursday, December 18, 2014, By Allan Grody and Peter Hughes

There is nothing outrageous or unrealistic about the 14 "Principles for Effective Risk Data Aggregation and Risk Reporting," as spelled out in the Basel Committee on Banking Supervision's 2013 document BCBS 239. It is plain common sense that risk reports should be validated, tied to a bank's official accounting books and records, derived from single authoritative sources and be available in a timely manner. And yet a November 2014 white paper from SunGard, as reported in "The Bill for BCBS 239," speaks of aggregate costs of $8 billion for the industry to achieve compliance and puts us on notice that we will be confronted by "a complex program of change."

Legacy Systems

Banks clearly have issues with legacy systems - a term applied to automated applications using out-of-date technology that is in need of replacement. Where they exist, legacy systems typically oblige banks to retain internal data repositories and structures that are similarly outdated.

This article is not intended to focus on the status of information technology and data architectures in banks, but we all understand from a myriad of regulatory reports and industry research that the issues associated with legacy systems are widespread. The result is that fragmented and fragile IT and data architectures do not readily or easily support risk data aggregation. The Basel Committee on Banking Supervision would appear to endorse this view. In the context of lessons learned from the financial crisis, it deemed bank IT and data architectures "inadequate to support the broad management of financial risks."

This condition is implicit in the SunGard paper: "The IT landscape of financial institutions is on the brink of fundamental change on a global scale . . . While a new IT

architecture is not a silver bullet per se, it should be seen as the crucial enabler of BCBS 239."

An earlier, equally illuminating report from the Celent research arm of Oliver Wyman, "Strategic Innovations in Risk Management - Compliance 1, Innovation 0," conveyed the same message but with a prescription for paradigm shifts in thinking. In Celent's view, the risk discipline is trapped by incremental thinking, overwhelmed by immediate compliance needs related to new regulations that appear almost daily, and dependent on IT departments to produce data from legacy systems that are not standardized and do not interoperate effectively. At the same time, financial firms are being asked to address the apparent new-paradigm thinking of their global regulators.

Celent estimates that global financial industry spending on risk and regulatory compliance will exceed $50 billion by 2015. The firm calls for real transformation guided by strategic principles underpinned by the right IT practices, not by unsustainable quick fixes. Celent cautions that this is not likely to happen merely with incremental approaches and upgrades in hardware and software infrastructure. There is significant risk that technology spending will focus primarily on near-term regulatory change and compliance, but what is required are innovative ways to bring new business ideas to life and enhance risk practices, operations, and IT infrastructure to avoid playing catch-up.

Celent describes an 'Innovation Framework for Risk Management," underpinned by an infrastructure-architectural realignment, with new in-memory database and complex event processing technologies enabling of Big Data analytics for the new risk regime.

The vision presents the challenge that innovation must lead to measurable changes: better ways to price risk, better metrics for risk-adjusted capital and incentive compensation, reduction in loss incidences, and even the holy grail of metricizing risk appetite and operational risk.

Allan D. Grody

Reconfiguring Architectures

A fundamental question arises: How will banks determine the IT and data architectures that are required to support the aggregation of risk data?

The answer can be found in the SunGard white paper's conclusion: "An IT architecture needs to follow both the business requirements and the data quality framework, which is backward-engineered from risk reporting data items . . . Adaptability, aggregation, drilldown, ad hoc, and timeliness, even in times of stress and crisis, define the technology solution."

It is not unreasonable for technologists to adopt this approach to determining the requirements of IT and data architectures - start with the outputs currently in use and backward-engineer them to identify the data elements and the respective sources that are used in their production. Once this information has been obtained, analyzed and understood, the design of the IT and data architectures that

will optimally support these data elements and their sources can be undertaken. If the resulting design is effective, data-aggregation paths can be defined and ad-hoc reports created to meet reporting requirements in a complete, accurate and timely manner.

But what if the reports currently in use are either not fit-for-purpose, or the methods used to produce them are flawed or lack consistency? In these circumstances, backward engineering as suggested by SunGard could result in banks' spending vast sums of money to produce outputs that do not, and possibly were never able to, satisfy the fundamental aims of risk reporting and risk management.

In contrast, the Celent report encourages developing "the ability to see not only a micro view of the trees, but also a macro view of the forest." Financial firms need to foster innovation for potentially disruptive effect in the industry as a whole as well as create innovative disruptions within and across their own business silos. "The technologies, levers, and paradigms explored in this paper offer a taste of things to come," Celent concludes. "A new world awaits, and institutions will need to find fresh ways of being. We indeed live in interesting times."

Current State of Risk Reporting

It would seem to make good sense that before banks embark on an $8 billion reconfiguration of IT and data architectures, they should first conclude whether their current risk reporting is fit-for-purpose. Regardless of what those internal evaluations may be, the BCBS appears to have reservations. In a July 2013 discussion paper, "The Regulatory Framework: Balancing Risk Sensitivity, Simplicity and Comparability" (BCBS 258), the international supervisors body observed that "risk is multi-faceted and far from straightforward to measure."

Expanding on that point later, it said, "Large internationally active banks are likely to employ a large number (possibly hundreds) of models to determine their consolidated capital requirements . . . These models are, in turn, based on a very large number of inputs, often parameters that are themselves estimated using complex quantitative techniques."

A senior central banker who is now the Bank of England's chief economist, Andy Haldane, was more direct in his assessment of risk reporting when he observed in an August 2012 presentation: "The quest for risk-sensitivity in the Basel framework . . . has spawned startling degrees of complexity and an over-reliance on probably unreliable models. The Tower of Basel is at risk of over-fitting - and over-balancing. It may be time to re-think its architecture."

A further example of not-fit-for-purpose risk reporting is the pre-crisis adoption value-at-risk (VaR) for the determination of market risk capital requirements. In its October 2013 second consultative document on "Fundamental Review of the Trading Book - a Revised Market Risk Framework," the Basel Committee stated that "a number of weaknesses have been identified with using VaR for determining regulatory capital requirements, including its inability to capture tail risk." In fact, the BCBS concluded that VaR actually "incentivized' banks to take on tail risk," precisely the opposite of the intended purpose of a capital adequacy regime to limit risk taking.

Unresolved Issues and Processes

Just considering this one perspective of risk reporting - regulatory capital adequacy - it is doubtful whether the backward-engineering approach suggested by SunGard is feasible, given the different modeling methods and techniques used; the multiplicity of aggregation paths and data sets used in quantitative modeling that do not necessarily tie to the books and records of the bank; the role that assumptions play in determining model outputs; and the flawed thinking behind some of the modeling techniques adopted.

It is certainly questionable whether a reconfiguration of IT and data architectures should be undertaken when the affected risk-reporting data items are being challenged and are yet to be resolved by banks and their regulators.

Banks' internal risk reporting tools and techniques also have issues relating to the fit-for-purpose test. In operational risk, for example, banks universally identify and assess their exposures through risk and control self-assessment (RCSA) and key risk indicators (KRIs). Both of these methods typically report possible risk exposures using a non-additive metric based on red, amber or green indicators, often referred to as RAG reports.

Aggregating non-additive risk data, let alone backward-engineering risk-reporting data items represented by colors, is simply not possible. What's more, VaR measures are also non-additive, forcing separate VaR calculations for multiple businesses to be combined through elaborate correlation assumptions, thus rendering the enterprise VaR numbers suspect.

The ultimate evidence that much of the risk reporting produced by banks may not be fit-for-purpose is the fact that the global financial crisis was caused by banks' failure to adequately identify and quantify accumulating exposures to risk. In these circumstances it is perhaps wrongheaded to believe that reconfiguring IT and data architectures will resolve the risk data aggregation and risk reporting issues that ultimately led to the crisis. Thus, Andy Haldane perhaps got it right when he concluded that "it may be time to rethink [the Basel] architecture".

Peter J. Hughes

An Accounting Perspective on BCBS 239

Principle 3 of BCBS 239 states that "controls surrounding risk data should be as robust as those applicable to accounting data." If BCBS sets accounting as a benchmark for risk data, then a determination should be made that accounting controls can be adapted for risk data.

Accounting involves the registration of all transactions, upon their approval, in accounting systems. Upon registration, each transaction is tagged with codes that are used to ensure that correct aggregation paths can be followed for financial reporting. From the codes, transactions can be aggregated to report profitability by, for example, business line, organizational unit, customer, product, location and legal entity. Transaction values are also captured which typically include historic, notional and fair (mark-to-market) values.

If different cuts of accounting data are taken to report, for example, product profitability, transaction values are used as population controls to ensure that the data used is complete and accurate. Almost by instinct, accountants embed control totals based on transaction values throughout their reporting processes to ensure the completeness and accuracy of reporting. As all financial reporting is derived from the single authoritative source of accounting data - the general ledger - it follows that all financial reporting can be reconciled back to that source.

Tags for Risk

Effectively adapting controls surrounding accounting data for risk data would require each transaction to be tagged with a new value - its exposure to risk - to complement the historic, notional and fair values already captured in accounting systems for financial reporting.

Such an approach would require, upon transaction registration, the application of a standardized calculation of exposure to risk by principal risk type, i.e. credit, market, liquidity, operational and interest rate. This in turn would require the design of standardized tables and templates that would translate risk factors into weightings used in the calculation of exposure to risk. Such risk factors would include the transaction's value, the associated product characteristics and the status of operating controls applied in the transaction's processing and risk management.

Through the integration of risk data and risk reporting with established accounting and general ledger control and reporting frameworks, BCBS 239 requirements would be addressed; risk data and risk reports would be validated, tied to the respective bank's official accounting books and records, derived from single authoritative sources and available in a timely manner. Further, reports typically produced for management reporting could be replicated for risk reporting using established aggregation paths for such aspects as business line, organizational unit, customer, product, location and legal entity.

The design of such a risk accounting framework as an extension of management accounting is an area of ongoing research and development that has been vetted through peer-reviewed academic papers, published working papers, articles in the trade and technical press, webinars offered by global professional bodies including GARP, and presentations at public conferences. This framework is now under development as industrial-strength software. (More information on Risk Accounting is available at www.financialintergroup.com.)

Conclusion

Banks, over time, will need to invest in upgrading their IT and data architectures where there are ongoing dependencies on legacy systems, but these are business investment decisions that should follow business priorities. The successful implementation of BCBS 239 is too critical to be dependent on prior reconfigurations of IT and data architectures that may take many years to achieve.

Banks and regulators must quickly resolve the downside risks associated with banks' present inability to completely and accurately, in timely and consistent fashion, report the risks they accept in the creation of shareholder value. Risk accounting can

potentially provide a viable solution at a fraction of the time and cost of reconfiguring entire IT and data infrastructures by adapting the control and reporting frameworks that already exist in accounting and general ledger systems.

Allan D. Grody, president of Financial InterGroup Holdings Ltd., is a former partner and founder of Coopers & Lybrand's (now PricewaterhouseCoopers') financial services consulting practice and former adjunct professor at NYU's Stern Business School, where he founded and taught its Risk Management Systems course. Peter J. Hughes is managing director of Financial InterGroup, a former banker with JPMorgan Chase and visiting research fellow at the Leeds University Business School.