BCBS 239, Heightened Standards and Operational Risk

With regulators revising their thinking on the measurement of operational risk, it is time for the industry also to address this longstanding and still unresolved issue

Wednesday, May 11, 2016

By Peter J. Hughes and Allan D. Grody

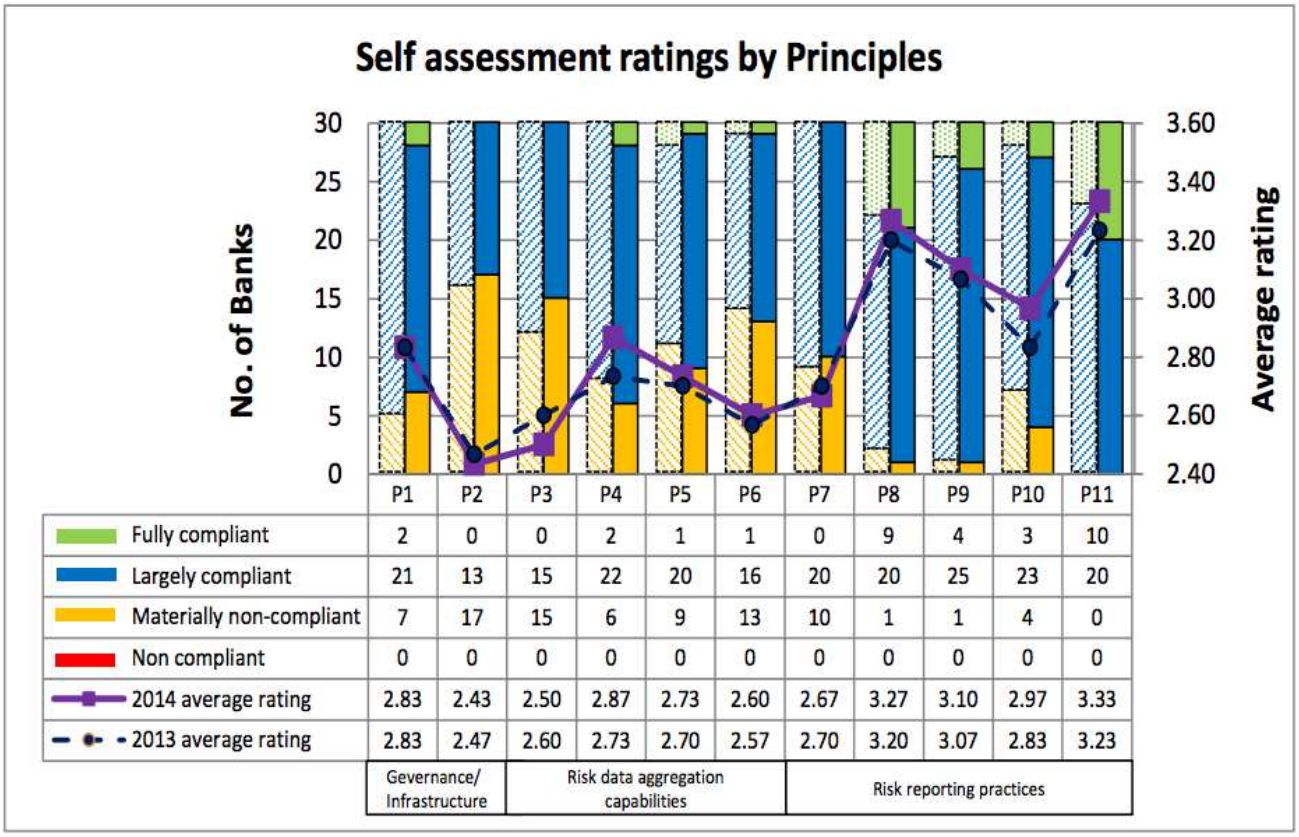
In a March 2016 GARP Risk Intelligence article, Risk Governance: Across the Three Lines, authors from KPMG commented on the U.S. Office of the Comptroller of the Currency's Heightened Standards for large financial institutions and delivered a call to action: "It's time for banks to deploy risk governance frameworks across three lines of defense."

A primary focus of OCC standards is the role of independent risk management, defined as ". . . any organizational unit within the bank that has responsibility for identifying, measuring, monitoring or controlling aggregate risks." The use of the term "aggregate" in this context could be viewed as provocative, given the financial industry's poor track record in this area.

Indeed, regulatory concern is such that in January 2013 the Basel Committee on Banking Supervision issued BCBS 239, "Principles for effective risk data aggregation and risk reporting," which included this observation: "Many banks lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately . . . Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices."

Deadlines Missed

The implementation of this mandate has met with some difficulty. In December 2015, the Basel Committee concluded in its BCBS 239 progress report that banks were falling short of full compliance by the due date of January 2016, and in some cases full compliance wasn't expected before 2018. An indication of the scale of the challenges facing the industry came via a white paper from SunGard, covered in a November 2014 GARP article The Bill for BCBS 239. SunGard estimated that aggregate industry-wide costs to achieve compliance would be $8 billion, with a warning that banks will be confronted by a "complex program of change."



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Fully compliant	2	0	0	2	1	1	0	9	4	3	10
Largely compliant	21	13	15	22	20	16	20	20	25	23	20
Materially non-compliant	7	17	15	6	9	13	10	1	1	4	0
Non compliant	0	0	0	0	0	0	0	0	0	0	0
2014 average rating	2.83	2.43	2.50	2.87	2.73	2.60	2.67	3.27	3.10	2.97	3.33
2013 average rating	2.83	2.47	2.60	2.73	2.70	2.57	2.70	3.20	3.07	2.83	3.23
	Gevernance/ Infrastructure		Risk data aggregation capabilities				Risk reporting practices				

At least one and as many as 17 banks rated themselves materially non-compliant on all but one of the 11 principles of BCBS 239, according to the Basel Committee's December 2015 progress report.

Banks are viewing BCBS 239, first and foremost, as a data quality challenge. This is understandable given banks' ongoing dependency on multiple data architectures and legacy IT infrastructures, which explains the very high cost of achieving the improvements now demanded through regulatory mandate. Reengineering inefficient data architectures that reside within out-of-date technology is expensive and takes time.

However, placing reengineering at the forefront of the BCBS 239 compliance program may cause banks to overlook one important fact: Risk data aggregation is applied to the outputs of risk measurement systems, not the data that are input to them. If banks solve their data quality issue in an architectural and technological sense, little will have been achieved relative to BCBS 239 if they do not also successfully define the common frameworks and metrics through which risk is measured and subsequently aggregated.

Failure of Operational Risk

It is perhaps worthwhile at this juncture to pause and consider the scale of operational risk that can be associated with "weak risk data aggregation capabilities and risk reporting practices."

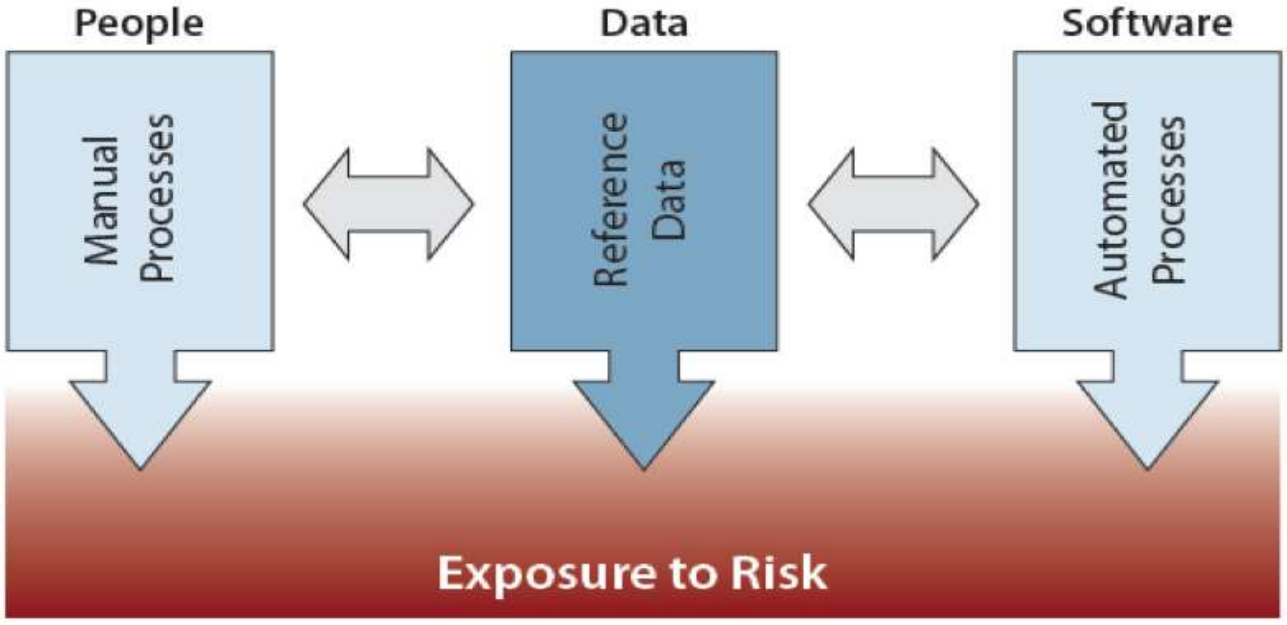
The Basel Committee's assertion in BCBS 239 of the magnitude of the problem at the time of the crisis was clear: "One of the most significant lessons learned from the

global financial crisis that began in 2007 was that banks' information technology and data architectures were inadequate to support the broad management of financial risks."

There can be no question that these inadequacies are attributable to the failure to manage operational risk, that being the failure of banks' internal processes, data and IT capabilities. There is also little question that these failures constituted a major causal factor in the many billions of dollars of losses suffered during the crisis, and many more billions of dollars that will need to be spent post-crisis to fix the problems.

Operational Risk in More Detail

Operational risk relates to the functioning of a bank's internal operating environment, comprised of the pillars shown in the accompanying diagram: manual processes (people) and automated processes (software) interacting with data. It is perhaps axiomatic to state that banks are wholly dependent on the proper and secure functioning of this dynamic. C-suite executives, general management, sales, operations, risk managers, model managers, data managers, finance, IT, audit . . . all use manual and automated processes to originate, capture, retrieve, enrich, analyze, control, validate and report data.



If the operating environment is faulty, then the data that is relied on when making decisions and reporting financial and risk positions will also be faulty.

It is not difficult to find evidence of faulty internal operating processes and data that either caused or failed to prevent massive, in some cases catastrophic, and unexpected losses in banks. The sub-prime fiasco, rogue traders and JPMorgan Chase's London Whale are all examples of banks' failure to identify, measure, monitor, control and accurately aggregate exposure to risk. In these cases, the first indication

CEOs received of the excessive build-up of risk in their respective firms was when they turned into losses.

In contrast to financial risks, there is no upside — only downside — to accepting an operational risk. Consequently, banks strive to create a risk-free internal operating environment whose benchmark can be defined as "100% straight-through processing (STP) in a totally secure and reliable IT environment with flawless data." The obvious concern here is that no bank can operate to that standard; it is arguably unachievable. So CEOs will want to know how distant their bank's operating environment is from that benchmark and what amount of exposure to operational risk exists as a consequence.


Allan D. Grody

Whereas bank boards and other stakeholders — governments, regulators, investors and customers — are informed through voluminous narratives included in audited financial statements on the status of risk management, they receive limited information on how much aggregate risk exists at the enterprise level. Critically, they receive no information whatsoever on aggregate operational risk simply because banks haven't yet figured out how to measure it.

The financial crisis demonstrated, and the Basel Committee asserted, that if a bank operates with high exposure to operational risk, there will be a corresponding negative impact on the ability to effectively manage and accurately report accepted financial risks. Expressed another way, banks' independent risk management units that are required to identify, measure, monitor or control aggregate risks cannot function in the manner intended until compliance with BCBS 239 has been achieved. Of necessity this should also apply to the aggregation of operational risks, given their materiality.

Measurement vs. Assessment

In the original 2003 version of the sound practices paper on the management and supervision of operational risk, the Basel Committee wrote:

"Reflecting the different nature of operational risk, for the purposes of this paper, management of operational risk is taken to mean the 'identification, assessment, monitoring and control/mitigation' of risk. This definition contrasts with the one used by the Committee in previous risk management papers of the 'identification, measurement, monitoring and control' of risk."

Note the reference to operational risk as being "different," and the transformation of the word "measurement" into "assessment." The inference is that exposure to operational risk can only be assessed — it can't be measured. This position from the global regulatory standards-setter effectively removed the obligation from banks to seek quantitative methods of managing this particular risk.

In the absence of a generally accepted method of explicitly measuring exposure to operational risk, banks have universally adopted assessment-based tools and

techniques such as Key Risk Indicators (KRIs) and Risk & Control Self-Assessments (RCSAs). The most common metric used by banks to report the existence and likely impact of operational risks is based on three colors — red, amber and green — the so-called RAG assessments.

Whereas assessment-based metrics provide a vital source of risk intelligence at the operating unit level, they are inherently subjective and not aggregable nor comparable along the vertical and horizontal dimensions of an enterprise. Expressed another way, colors can't be aggregated.

Basel II

In 2004 the Basel Committee published its second capital accord, Basel II, which included, for the first time, the requirement for banks to set aside protective capital for operational risks. In paragraph 665 it states: "a bank's internal measurement system (Advanced Measurement Approach — AMA) must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors (BEICFs)."


Peter J. Hughes

Noteworthy is the lack of reference to a bank's explicitly measured operational risk exposures, due to their unavailability, as an input to the internal risk measurement system. Some years later, in 2011, the Basel Committee issued supervisory guidelines on the AMA when it voiced concern at its limitations:

" . . . the range of practice continues to be broad, with a diversity of modeling approaches being adopted by AMA banks ... (this) clearly affects the AMA methodology of individual banks and, ultimately, the amount of capital resulting from the application of the AMA ... While flexibility allows modeling to reflect individual bank risk profiles, it also raises the possibility that banks with similar risk profiles could hold different levels of capital under the AMA if they rely on substantially different modeling approaches and assumptions."

These limitations ultimately led to a pronouncement by the Basel Committee in a March 2016 consultation paper to withdraw the AMA and thereby abandon any form of explicit risk measurement as a basis for determining regulatory capital adequacy. In its place, a Standardized Measurement Approach (SMA) has been proposed that "combines the Business Indicator (BI), a simple financial statement proxy of operational risk exposure, with bank-specific operational loss data."

You Can't Manage What You Don't Measure

Whereas it may be acceptable to decouple capital provisioning from an explicit risk measurement system, it is not acceptable to decouple risk management from risk measurement. We are all familiar with the truism "you can't manage what you don't measure." There would also seem to be little justification in excluding operational risk from BCBS 239, given that principle 4, Completeness, requires that "a bank should be able to capture and aggregate all material risk data across the banking group."

Similarly, OCC standards make repeated reference to a bank's risk profile, defined as "a point-in-time assessment of the bank's risks, aggregated within and across each relevant risk category." Arguments that operational risk should be excluded from these requirements on the grounds that its measurement is either too difficult or impossible will not be defensible over time.

The debate on how to measure exposure to operational risk is overdue. The authors of this article offer one possible starting point in "Risk Accounting" (see YouTube for an overview). Now contained in proof-of-concept software, which is the result of an industry and academia research collaboration supported by pilot operations at financial institutions, the risk accounting method and system are described in soon-to-be-published, peer-reviewed academic papers (Grody, A.D., Hughes, P.J. (2016), "Risk Accounting: The Risk Data Aggregation and Risk Reporting (BCBS 239) Foundation of Enterprise Risk Management (ERM) and Risk Governance," Journal of Risk Management in Financial Institutions [forthcoming]).

The fundamental premise in risk accounting is that operational risk, as a non-financial risk, can only be quantitatively expressed using a non-financial unit of measurement. Accordingly, risk accounting's standard unit of measurement is the Risk Unit or RU. Aggregated operational risk exposures are expressed in Rus. Over time, exposure in RUs can be correlated with actual losses to ultimately assign a monetary value to the RU.

If risk managers can accept the concept of a non-financial unit of measurement to quantify, benchmark and later value exposure to operational risk, then the design of more effective measurement-based operational risk management solutions becomes a lot more straightforward. Compliance with the aggregation requirements of BCBS 239 and OCC standards will be a natural outcome.

Returning to KPMG's article, it includes a number of recommendations under the heading "How to Begin Addressing the (OCC) Standards." We respectfully offer a further recommendation, missing from KPMG's list, which is to solve the longstanding issue of how to measure exposure to operational risk, one example of which is presented here as the Risk Unit.

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