Making sense of the GRC landscape

+

Interview: Toshihide Iguchi
Sharing scenarios: Disclosure of confidential information
How to build a reputational risk model
Data classification: Business disruption through hoaxes

www.riskuniverse.com

The Risk Universe

Cyber Defence

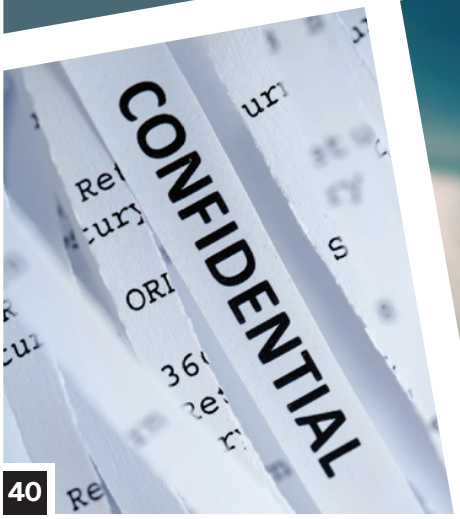
New cooperative initiatives to counter cyber threats

ISSUE 30
June 2014

ISSUE 30

June 2014

CONTENTS



40

36

04 **EDITOR'S LETTER**
Fines, sanctions and more fines – anything else to worry about? Unfortunately yes, the virtual, digital, cyber world.....

05 **NEWS**
More sanctions and fines, concerns around systemic risk and cyber crime, a new regulator and forthcoming changes in regulations, a damning report on the quality of external audits, while the IOR makes awards.

16 **OPINION**
Columnist Annie Searle takes a look at insider threats and why, in her opinion, human behaviour is perhaps the most significant threat to the firm.

18 **INTERVIEW Toshihide Iguchi**
The Risk Universe interviews former Daiwa Bank rogue trader Toshihide Iguchi on his views on what happened at Daiwa and some of the parallels with today's issues in the industry.

22 **BOOK REVIEW**
My Billion Dollar Education – In the Mind of a Rogue Trader
Toshihide Iguchi shares the inside details of how he concealed what became a $1.1bn loss for 12 years.

24 **SPOTLIGHT**
Cyber Defence
Mike Finlay attends the public launch of the Bank of England's CBEST cyber vulnerability testing framework and takes a look at initiatives around cyber intelligence sharing.

13

DON'T MISS OUT ON RECEIVING THE NEXT ISSUE OF *THE RISK UNIVERSE*

SUBSCRIBE HERE

28 **HOW TO**
Create a basic economic capital model for reputational risk
Alfredo Roisenzvit outlines an economic capital model under trial in Latin America.

32 **MAKING SENSE OF THE GRC LANDSCAPE**
David Houlihan outlines the different ways in which current GRC vendor offerings should be considered.

36 **SHARING SCENARIOS**
Significant business disruption through hoaxes
This month's scenario looks at the potential business disruption impact caused by hoaxes and threats. Find out the results of last month's scenario benchmarking exercise on inappropriate gifts, contributions or bribery for business ends.

39 **DEAR CEO**
Every month, an anonymous senior executive of a financial services firm writes a letter to his CEO detailing some of the issues and concerns he has always wanted to raise or share.

40 **RISK CLASSIFICATIONS**
Intentional Disclosure of Confidential Corporate Information
Mike Finlay takes a look at the deliberate disclosure of confidential inside information for reasons other than identity theft or insider trading.

43 **CLASSIFIED**
Information on upcoming industry events and ***The Risk Universe*** monthly comic.

HOW TO...

Create a basic economic capital

While the Basel II definition of operational risk explicitly excludes reputational consequence (or, as some people refer to it "reputational risk"), most regulatory jurisdictions then add it back in under Pillar 2 capital requirements. But how can we do this? *The Risk Universe* takes a look at one approach being trialed in Latin America.

THE AUTHOR

ALFREDO B. ROISENZVIT
Executive Director, Risk*Business* Latin America, Professor of Banking Regulation and ERM/Operational Risk at the Masters Program of the Universidad de San Andrés, Buenos Aires, Argentina

In its "Enhancements to the Basel II framework", published in July 2009, the Basel Committee introduced reputational risk as one of the Pillar II risks to be managed by regulated institutions, specifically to be taken into account in their Internal Capital Adequacy Assessment Process (ICAAP) reports. The Committee defines reputational risk as "the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding". The Committee also establishes that "A bank should identify potential sources of reputational risk to which it is exposed. These include the bank's business lines, liabilities, affiliated operations, off-balance sheet vehicles and the markets in which it operates. The risks that arise should be incorporated into the bank's risk management processes and appropriately addressed in its ICAAP and liquidity contingency plans".

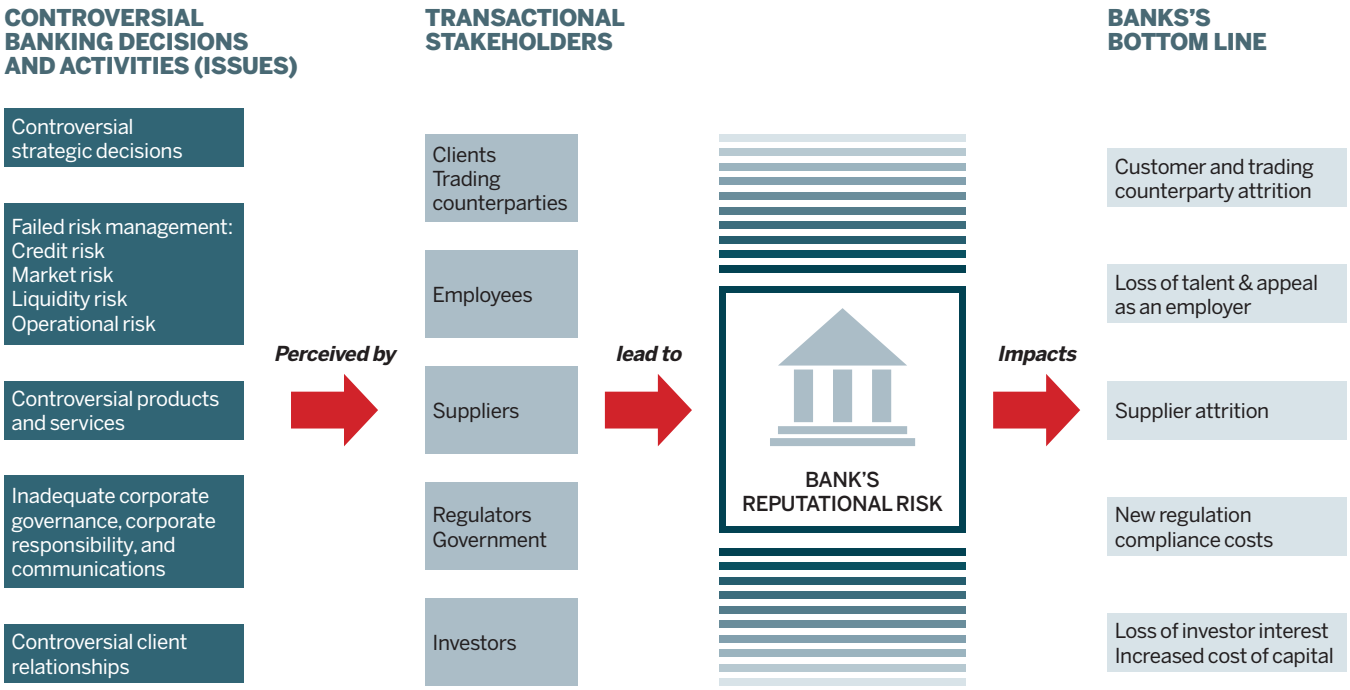
Based on these standards and instructions, many regulators in countries with diverse stages of development in terms of Basel II/III implementation, have issued regulations that take them rather literally. In this light, many banks have encountered the need to develop not only a specific framework for the management of reputational risk, but also to come up with a definition and allocation of economic capital and include them in both the quantitative and qualitative sections of their ICAAP reports. These requirements are intrinsically different for banks with different degrees of complexity in their operations, size, target markets and regional or continental span. In essence, it can be interpreted that the broader idea of reputational risk and implicit support as defined by the Basel Committee, are related to the more complex operations of bigger banks, that are very active in the interbank or securitisation markets, as substantiated by the Committee in the cited introductory document. However, for smaller and simpler banks, their take on reputational risk may differ substantially, yet local regulations typically make no difference in treatment. So smaller and simpler banks are faced with the difficulty of the need to define a reputational risk model that allows for its management and for the determination and allocation of economic capital for reputational risk.

Many firms in the Latin American region fall into the described universe and frequently seek tools to assist them to comply with regulation while, at the same time, improving their risk management process. Against this background, one can define a reputational risk model, with the mandate to keep it a simple one, that is easy to calculate and measure and which is applicable to the simpler operations of smaller banks.

FUNDAMENTALS

Since the definition of reputational risk is even broader than that of operational risk, it is beneficial to adopt an appropriate broad approach, intending to cover the main defined drivers for reputational risk. To that order, the joint work of GARP and ECOFACT in terms of the identification of drivers and effects form a useful starting point, providing this graphic summary of drivers and effects for reputational risk:

model for reputational risk



Source: ECOFACT/garp

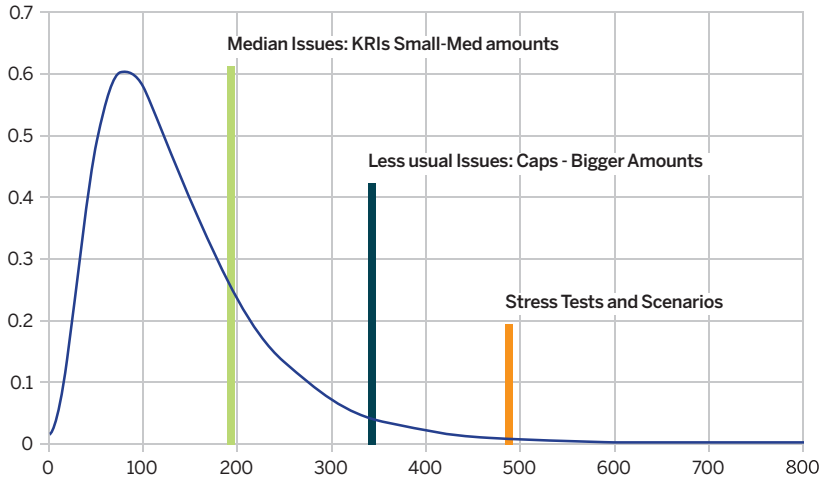
The logic behind the basic model is to analyze, process and stylize data supporting the identified risk drivers, then convert it into Key Risk Indicators, which are then translated into weighted inputs for the model's calculations.

METHODOLOGY

Based on the described fundamentals, we can identify three main sources of information related to reputational risk drivers that are present in virtually any firm, regardless of complexity and size:

Data Source	Drivers covered
1 **OPERATIONAL RISK ISSUES** A) Events/Losses recorded in the internal database of the firm that have reputational causes, relationships or consequences B) Events/Losses from external databases	● Failed Risk Management ● Inadequate corporate behaviour ● Controversial Products and Services ● Controversial Client Relationships
2 **COMPLIANCE ISSUES** A) Cases from the customer relationship databases (customer complaints, call centres) B) Internal audit and compliance findings C) Regulatory breaches and fines	● Inadequate corporate behaviour ● Controversial Products and Services ● Controversial Client Relationships
3 **SOCIAL MEDIA ISSUES** A) News mentions (i.e. Google keyword searches) B) Social media reports (negative mentions, response times)	● Failed Risk Management ● Inadequate corporate behaviour ● Controversial Products and Services ● Controversial Client Relationships ● Inadequate Communications

Reputational risk



Theoretical example of the applied Methodology

We have defined three subsequent methodological treatments for data, based on their relative importance with regards to the risk drivers and its manifestation. We chose to graph these in a distribution curve for graphical explanation, as well as to keep the model aligned with the symbology of the other risks managed in all banks, presented in accordance with the magnitude of its impact (above right).

The quantifiable issues that are gathered as information to feed the model are therefore qualified based on frequency and severity:

- Those which fall below the defined confidence interval are measured as KRIs, then stylized into the model as weighted multipliers based on their evolution (volumes), acceleration (pace of change), or threshold perforation count (limits).
- Those that have a big severity are taken as an impact measure, then are translated into the model as maximums, benchmarks, or direct charges.
- The results of different scenario analyses and stress tests are also taken into account for results and for calibration methodologies.

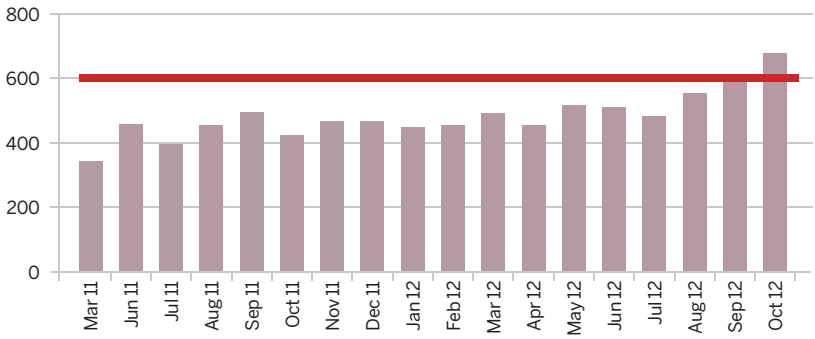
Once the model has been calibrated and the weights, thresholds and all variables have been set, it will yield a calculation of economic capital for reputational risk, based on the explained drivers and derived from a series of weighted percentages of charges based on a fixed benchmark, usually the total regulatory capital charge, but which can be adapted to each case in order to better capture the risk proxies of each institution. Other possible fixed benchmarks are Gross Income as used for the Basic Indicator Approach (BIA), operating volumes, maximum losses, etc.

In order to better illustrate how the model works, let us examine a fictional case and use it as the basis for calculation:

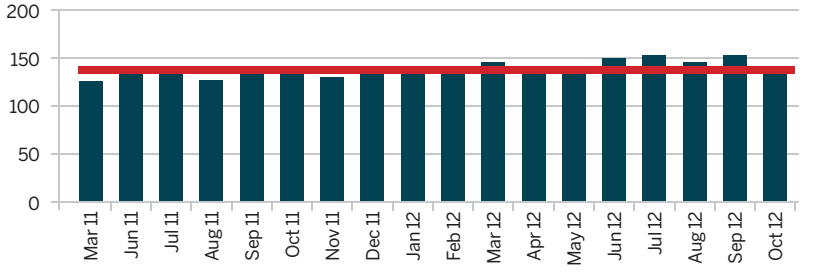
A **Drivers**: basic info: internal data (Operational Risk events that have reputational linkage).
Type: KRIs. Translation: threshold hit.
Rationale: If the KRI hits the threshold in the measurement period of last 12 months, then it triggers the weighted charge. Each firm defines how many KRIs they monitor and their individual thresholds.
As the KRIs perforate the threshold, they trigger the weighted multiplier. This process is repeated for each defined KRI of the model, in each of the driver categories described in the model methodology

B **Drivers**: Compliance: Regulatory fines publically announced.
Type: Events. Translation: maximum.
Rationale: As events are identified and deemed to qualify according to the model´s methodology (previous page), they must be factored into the model as a maximum hit.
However, since these are already taken into account in Operational Risk Capital, a multiplier is also defined.

ATM Fund Unavailability



Twitter Negative Mentions



For each type described, the data is factored in as per the defined methodology:

Drivers	Type	Threshold Hit	Multiplier	Base Benchmark	Base Amount	$ Charge	Weight	Model Outcome
Driver 1	KRI 1	✔	0.12	Total Gross Losses	$ 347,800	$ 41,736	5.00%	$ 2,087
OR Data	KRI 2		0.12	Total Gross Losses	$ 347,800	$ 41,736	5.00%	
	KRI 3	✔	0.12	Total Gross Losses	$ 347,800	$ 41,736	5.00%	$ 2,087
	KRI 4	✔	0.12	Total Gross Losses	$ 347,800	$ 41,736	5.00%	$ 2,087
	KRI 5		0.12	Total Gross Losses	$ 347,800	$ 41,736	5.00%	
	KRI 6	✔	0.12	Total Gross Losses	$ 347,800	$ 41,736	5.00%	$ 2,087
Driver 2	KRI 1		0.02	Volume Operations	$ 3,685,600	$ 73,712	2.50%	
Compliance	KRI 2	✔	0.02	Volume Operations	$ 3,685,600	$ 73,712	2.50%	$ 1,843
	KRI 3		0.02	Volume Operations	$ 3,685,600	$ 73,712	2.50%	
	KRI 4		0.02	Volume Operations	$ 3,685,600	$ 73,712	2.50%	
Driver 3	KRI 1		0.07	Gross Income	$ 975,000	$ 68,250	10.00%	
Social Media	KRI 2	✔	0.07	Gross Income	$ 975,000	$ 68,250	10.00%	$ 6,825
	KRI 3	✔	0.07	Gross Income	$ 975,000	$ 68,250	10.00%	$ 6,825
	KRI 4	✔	0.07	Gross Income	$ 975,000	$ 68,250	10.00%	$ 6,825
	KRI 5		0.07	Gross Income	$ 975,000	$ 68,250		
Driver 1	Event 1	✔	0.18	Event Loss	$ 1,300,000	$ 234,000	5.00%	$ 11,700
	Event 2	✔	0.18	Event Loss	$ 1,100,000	$ 198,000	5.00%	$ 9,900
	Event 3	✔	0.18	Event Loss	$ 1,450,000	$ 261,000	5.00%	$ 13,050
Driver 2	Event 1	✔	0.18	Event Loss	$ 1,200,000	$ 216,000	5.00%	$ 10,800

Data is analysed 12 months back

Total charge	$ 76,115	% of Gross Income	6.34%

The results must be calibrated through defined benchmarks in order to adjust the weights and multipliers accordingly. One such calibrator is a comparison with the BIA's alpha or 15% of Gross Income. In this example, the capital charge would be 6.34% of Gross Income. Other useful calibrators are a percentage of total capital charge, percentage of Pillar II capital charge, etc.

SPECIFIC APPLICATION

Despite this being a very recent development, the approach is currently being implemented under trial conditions across a range of large, medium, small and niche organisations, based in Argentina. Argentina was selected as the base for the trial and development stage of this model, because it has a very specific regulation with regards to Pillar II capital. This regulation requires all banks to hold Pillar II specific capital requirements for reputational risk and to include the qualitative management and the quantitative measures in the ICAAP report, which must be submitted to the regulators annually, as part of their evaluations for capital adequacy in general. In essence, the regulations are very straightforward in terms of requirements, which generates great demand for models, especially in smaller firms.

In essence, the regulations are very straightforward in terms of requirements, which generates great demand for models, especially in smaller firms

Development and implementation varies between the pilot cases, as they have different levels of access and ability to stylize the different types of information the model requires. Preliminary results look very promising, and all of them have used the already defined instances of the model to comply with the 2014 version of the Argentine ICAAP requirement due last April 30th. TRU