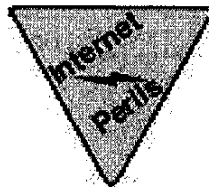
3



InternetPerils, Inc.
Mailstop 319
12407 N. Mopac Expwy Suite 100
Austin TX 78758-2429
512-272-8506
31 July 2003

Ms. Jennifer J. Johnson
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

From: John S. Quarterman <jsq@internetperils.com>
To: Federal Reserve <regs.comments@federalreserve.gov>
Cc: OCC <regs.comments@occ.treas.gov>
Cc: FDIC <comments@fdic.gov>
Cc: OTS <regs.comments@ots.treas.gov>
Cc: John S. Quarterman <jsq@internetperils.com>

Comments from InternetPerils on the U.S. Basel II Implementation

Federal Reserve Docket No. ?, 12 CFR Parts 208 and 225, Regulations H and Y
OCC Docket No. 03-XX, 12 CFR Part 3, RIN Number 1557-AB14
FDIC 12 CFR Part 325, RIN ?
OTS Docket No. ?, 12 CFR Part 567, RIN ?

Introduction

The Basel Committee on Banking Supervision (BSC) released a paper in April that asks for public comments by July 31, 2003 on the New Basel Capital Accord, or New Accord (Basel II).

The directives of Basel II sensibly set forth quidelines for operational risk, including Internet risk, without nominating metrics for establishing those risks. It is an exercise in standardless discretion that will not serve the International banking community well. In fact, it will delay the implementation of meaningful metrics that will accurately identify and assign operational risks attendant Internet usage.

Operational risks in a bank's context, for example, have to be quantified in correlation to the infrastructure that the bank engages when it joins a specific logical network topology. Further, the characterization of that topology and its inherent risks must be kept current since risks on the Internet are contemporaneous to conditions - which change from moment to moment, unlike any operational environment ever constructed. The Internet, to confront a maddening misnomer, is only a cloud to those who are ignorant of its nature or are willfully trying to obscure the fact that Internet performance can be mapped, measured and forecast like that of any number of operational environments.

This letter constitutes comments from InternetPerils on the U.S. implementation of Basel II as proposed in three documents prepared by the Federal Reserve staff for the Fed Board and other U.S. banking agencies: a summary document (ANPR) and one each on credit (A-IRB) and operational risk (AMA). The Fed documents also request comment by July 31, 2003.

One paragraph at the end of the ANPR specifically invites comments of the type we provide in this letter:

> "Commentators should specify whether certain capital and methodological standards would necessitate the acquisition or development of new compliance/information systems or the significant modification of existing compliance/information systems." p. 177.

The documents do not mention networks or the Internet specifically as sources of operational risk. Nonetheless, they mention applications such as e-banking that use the Internet, and they mention outsourcing, automation, natural disasters, terrorism, and vandalism. Outsourcing requires networks; automation requires automated monitoring; and the last three are examples of Internet perils. The Internet figures prominently in real-world applications of at least four of the seven

types of operational risk specified in the documents, especially those involving relations with trade counterparties or vendors. And the documents require on-going operational measurement, monitoring, alerting, and reporting. The documents would be much clearer and the Agencies' task of oversight would be much easier if they said that, rather than leaving it to the banks to decipher it.

The Internet is central in modern international banking; international banking needs to quantify (measure, test, verify, maintain, administer) Internet risk.

Comment

The documents spell out the implications for credit in great detail. Meanwhile, they make clear that operational risk is not yet completely understood. For example: "In the case of operational risk in particular, the Agencies recognize that measurement methodologies are still evolving and flexibility is needed." p. 23. While flexibility is needed, guidance would be clearer if it were more explicit about the types of operational risks entailed by use of the Internet, and by making the operational risk guidelines more parallel to the credit risk guidelines.

Among the list of seven operational risk categories in the AMA on p. 274 are these four:

iv.
: Clients, products, or business practices: an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.

v.
: Damage to physical assets: the loss or damage to physical assets from natural disaster or other events.

vi.
: Business disruption and system failures: disruption of business or system failures.

vii.
: Execution, delivery, and process management: failed transaction processing or process management, from relations with trade counterparties or vendors.

Each of these categories describes types of operational risk that can occur due to use of the Internet.

For example, iv would include picking the wrong ISP; v would include Hurricane Floyd or 9/11; vi would include DoS attacks and worms; and vii would include congestion, routing flaps, and other degradation of service between an institution and counterparties, as well as the ISPs conveying the service.

These extensive categories of risks entailed by use of the Internet emphasize the central role of the Internet in modern international banking.

The credit document says that banks wanting to support higher credit risks will require more economic capital. There should be similar verbiage for operational risk, i.e., banks that use riskier Internet connections should lay out more economic capital. Quantification of riskiness of Internet connections must be facilitated by on-going, independent third party measurement and analysis.

Yet the documents are very vague on how the measurements should be performed, translated into AMA parameters, maintained, and administered.

Page 17 provides useful A-IRB quantative risk drivers (inputs) that should be translatable directly into analogous AMA parameters:

1. probability of default (PD) over a given time horizon (typically 1 year), p. 38
2. loss given default (LGD) or proportion of the exposure that would be lost
3. exposure at default (EAD) or amount owed to the institution at loss
4. maturity (M) or remaining economic maturity of the exposure

PD
: requires ongoing comprehensive measurement of Internet topology for nonredundancy or overload, as well as of actual anomalies in accessibility or performance.

LGD
: can be derived from the measurements underlying PD by for example examination of which customers would be inaccessible if certain nonredundant nodes were to fail.

EAD
: for Internet operational risk could be based on total transactions passing over the Internet during intervals of specified lengths (minute, hour, day).

M
: may not have a translation into Internet operational risk.

Use of such operational risk parameters analagous to credit risk parameters would make operational risk quantifications more comparable to credit and market risk quantification, for computation of an overall risk metric.

Guidance for implementation and validation of operational risk quantification would also be clearer if phrased as parallel in

structure to that of credit risk. In particular, credit risk supervision requires four components. Operational risk supervision would be facilitated by a requirement for an analogous four components for Internet operational risk:

- a system that measures potential and actual Internet risks, assigns operational risk ratings, and validates their accuracy
- a quantification process that translates those ratings into AMA parameters
- a data maintenance system that supports the AMA system
- oversight and control mechanisms that ensure the system is functioning as intended and generating accurate ratings

The Internet is mostly external to international banking institutions, and global or even regional Internet measurement and monitoring is not a core business of banks.

The documents emphasize a need for independence of operational risk measurement and reporting:

> "An institution's operational risk framework would have to include an independent operational risk management function, line of business oversight, and independent testing and verification." p. 154; see also p. 155-156.

They mean independence of line management within a financial institution. They indicate another need, for consistency across institutions and geography:

> "An institution would have to appropriately use the advanced approaches across all material business lines, portfolios, and geographic regions." p. 23.

An independent external source of many such measurements would better address both needs.

Banks cannot run operational risk management; nor can other financial institutions; nor individual national banks. The financial industry and the Internet require an independent third-party institution.

Banks have until January 2007 to implement Basel II, but they have to publish implementation plans and get them approved well before then. Such plans, especially scenario analysis, could also benefit by independent third party assistance.

About InternetPerils

InternetPerils' mission is to provide intelligence about risks inside the Internet that cannot be estimated by an individual enterprise: the big picture of Internet perils and anomalies world-wide with fine resolution in time and space.

The aim of the Company is the provision of Internet peril intelligence as Intelligence Streams produced by on-going data collection, data fusion, deep analysis, and pattern recognition to reflect the constantly changing state of the Internet.

Any enterprise whose business depends upon the Internet to contact clients or to transfer files or other material of timely business value across the Internet needs the monitoring abilities of InternetPerils.

Industry and government need to know where the Peril Points in the Internet are; what the reliability of the connections is; how frequently connectivity fails, how risky connections are, and what the causes of slowdowns or failures are.

The founders of InternetPerils have decades of combined experience in the assessment, design, mapping, performance measurement, statistical analysis, monitoring and administration of computer networks and the increasingly complex network of networks that is the Internet. InternetPerils' brief is to use that experience to identify, taxonomize, and quantify ongoing risks on the Internet. InternetPerils stands ready to help bring actuarial science to the imperatives that BSC has drawn with such large, ambiguous strokes.