Operational Risk & Technology

Survey Reveals Greatest Risks, Best Practices

By Eric Holmquist and Charles Taylor

Whether they are smaller than $500 million or greater than $100 billion, all financial institutions have technology-related operational risks. RMA's December 2004 survey of 105 institutions identified concerns across the board over Internet security and vendor risk, as well as the need to focus more on external operational risks than those inside the institution. Following are highlights of the survey.

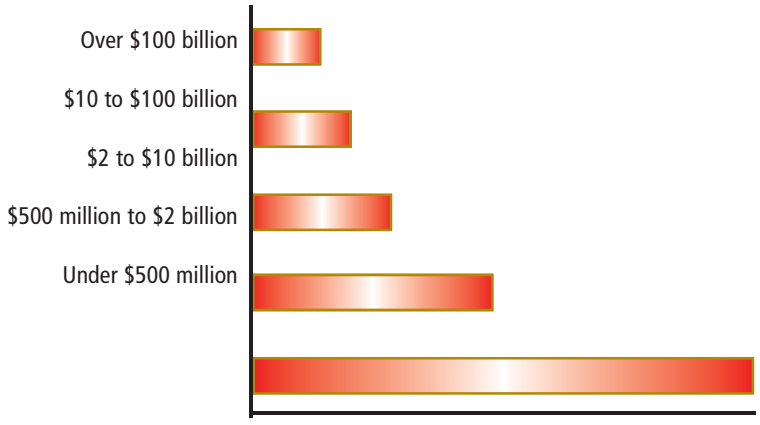
Greatest Risks

Unauthorized access from both insiders and outsiders, together with attacks on bank systems and identity theft, rank high on the list of technology risks banks face. Over a third of respondents scored these four risks a "1" or a "2" on a five-point scale. Large institutions appeared more concerned about unauthorized access, while small institutions worried more about attacks and identity theft.

Banks were perhaps most divergent in their views about the failure of IT planning to align investment with business priorities. While only seven banks reported this risk, three—all of which exceeded $100 billion—gave it top priority. The fact that failure to align those priorities attracted very little concern from smaller institutions suggests, not surprisingly, that it is a risk that rises sharply with technological complexity.

Generally, external risks ranked high and internal risks low. This result might have been

RMA Operational Risk and Technology Management Survey: 105 Respondents



 Eric Holmquist is chair of the RMA Operational Risk Management for IT Committee; he is a vice president and director of Operational Risk at Advanta Bank Corp. Charles Taylor is director of Operational Risk at RMA. *RMA thanks all survey respondents for their participation and the members of the RMA Operational Risk Management for IT Committee who helped with the design and assessment of the survey.*

reversed if respondents had been surveyed about *residual* rather than *inherent* risks or about *new* as opposed to *well-known* risks. RMA's Operational Risk for IT Committee, believing that industry attention should be focused on high residual risk points and emerging risk points, plans to explore this area further.

Technology Risk Management

The great majority of banks have technology risk management programs, and the programs share many similarities.

- 90% (94 respondents) have a program or plan to have one.
- Most integrate the program to some degree into a larger operational risk management program.
- Boards and senior managements understand and support the technology component.
- 87% (91 respondents) either have or plan to appoint an information security officer.

Differences in practice begin to emerge in due diligence over IT vendors—how incidence response teams and disaster recovery are organized. Banks under $500 million in size tend to give responsibility for disaster recovery to IT staff members or consultants, whereas larger institutions tend to give this job to non-IT staff.

Surprisingly, IT departments don't report much on losses to a central operational risk group, even in large banks. Less than 10% make any attempt to estimate the size of losses, and fewer than 33% do any causal analysis. These percentages are fairly true for banks of all sizes. Since loss-event databases are common these days among large banks, there appears to be room for improvement in assessing the financial impact of IT events.

SURPRISINGLY, IT DEPARTMENTS DON'T REPORT MUCH ON LOSSES TO A CENTRAL OPERATIONAL RISK GROUP, EVEN IN LARGE BANKS.

Technology Risk Assessment

Technology risk assessments presented to institutions' boards are fairly similar. For example, over 90% do (or are planning to do) penetration or vulnerability studies of some kind. But there are differences as well:

- Only 36 of the 94 (38%) who responded to this question said their boards gave guidance to their institutions on establishing an appetite for operational risks in IT.
- Methodologies for calibrating the assessments vary widely.
- Practices for assessing operational risks in advance of significant change vary widely as well, whether considering new products and services, new processes, new IT, or acquisitions.

Disturbingly, nearly 25% of institutions don't have the skills set to implement controls in response to risk assessments.

Technology Strategy

Less than a third of all banks look at technology risks methodically during strategic planning, and less than half have strategic technology plans that address technology risk. This may help explain why business expectations are not always met by IT departments, and represents another potential *area* for improvement.

Compliance

About half of the respondents report a heavy focus on technology risk management in recent safety and soundness exams, and about half report limited attention paid to the subject. This may well reflect the gradual introduction of a technology focus among bank examiners. If the past is a guide, it seems there is a significant chance of such a focus in future exams.

Coming Soon...

RMA's committee plans a series of follow-up 60-second surveys to gain a better understanding of such issues as which residual risks are most important to banks. The committee also plans to sponsor round tables focused on specific technology topics related to practice differences, seeking avenues for convergence in the near future. ❐

Contact Eric Holmquist by e-mail at eholmquist@advanta.com. *Contact Charles Taylor by e-mail at* ctaylor@rmahq.org.