CHECK UP TIME FOR OPERATIONAL RISK

by Steve Brown

Regulators want to be sure bankers have a good handle on operational risk. They are not referring to doctors and medical procedures in hospitals, but rather are focused on the risk of unexpected loss that a bank might experience as a result of inadequate information systems, operational problems, breaches in internal controls, fraud or other unforeseen catastrophes. That is a pretty broad categorization, but make no mistake regulators are serious about the precautions bankers are taking to address such operational risks. Areas of particular regulatory interest include pandemic preparedness and IT security. While the odds that a pandemic (an outbreak of an infectious disease that spreads across a large region) will occur may be considered small, regulators expect bankers to be prepared. The risk of avian flu has heightened focus on operational risk and regulators want to be sure bankers have considered actions appropriate for their particular situation in the event of an outbreak (as well as incorporating such actions into contingency strategies). While this may sound a bit far out for many bankers, rest assured regulators will be examining whether bankers have conducted a risk assessment that considers employee safety and business continuity, among other risks. In particular, bankers can address pandemic risk by establishing infection control procedures for the workplace, reinforcing inoculation, providing options for employees to work offsite while ill, increasing worker education, establishing contingency systems to support sustained worker absenteeism and working with outside vendors to ensure essential services are maintained. While a pandemic may never occur, bankers should nonetheless address the risk. In addition to pandemic preparedness, bankers will also need to review IT security as part of operational risk. With so many customers moving online, regulators want to be sure banks have added multi-factor authentication, limit access to sensitive customer information and ensure procedures are enhanced to protect the transfer of funds to unauthorized third parties. In short, banks will need to ensure they have the risk management controls necessary to authenticate the identity of customers accessing Internet-based financial services. While regulators do not endorse any specific technology, banks should conduct a risk assessment, increase customer awareness and implement risk mitigation strategies to ensure reliable authentication of customers. Operational risk is a broad category that goes well beyond pandemic and IT security risk preparation. While we have highlighted these (because the regulators have done so), bankers should also note there are many other activities as well. For instance, operational risk includes the possibility that newly integrated computer systems won't work after a merger or acquisition; back-up system capabilities; outsourcing arrangements; employment practices; misuse of customer information; damage to physical assets due to earthquake, fire or flood; data entry errors; collateral management; incomplete legal documentation; workplace safety; employee theft; and fraud, among others. To be sure, bankers should make the board aware of major operational risks and put in place processes to ensure it is identified, measured, monitored and controlled. As the old saying goes, an ounce of prevention is worth a pound of cure, so be sure to include operational risk within the bank's overall risk management processes.

BANK NEWS

M&A

United Community Banks ($6.5B, GA) will acquire the HC of First Bank of the South ($625mm, GA) for about $217mm, or 2.95x book.

M&A

Mortgage insurer MGIC Investment said it will buy long time competitor Radian Group for about $5B.

Bank Robberies

For 2006, robberies doubled in Dallas, while bank robbery rates in most other metro cities declined. In attempting to explain the difference, a new model is emerging that may help predict incidences. This model looks at a bank's number of branches, hours of operation; drug prices in the area, recent media reported successes capturing the bad guys and current crime statistics.

Robbery Deterrent

First Mutual ($1.1B, WA) is getting kudos from the FBI regarding their proactive policy, "Safecatch." The program encourages branch staff to make early contact with suspicious persons, offer to help and ask for ID. In addition, the program asks all employees to dial 911 at the first hint of suspicion. The program is credited with thwarting several attempts and operates on the notion that the sooner contact is made, the less the potential robber is "committed" to the crime. Since its introduction, the FBI has used First Mutual's program as a model for other banks.

Customers

A new study finds small business owners are some of the busiest people on the planet. Among the findings: 67% work on their days off, 67% work after-hours and at night; 50% work while driving; 33% can't remember their last vacation, 20% work 80 hours or more; 20% did work while eating dinner; 50% of those who took vacation said they worked during the vacation; and 20% said they read email while in the bathroom.