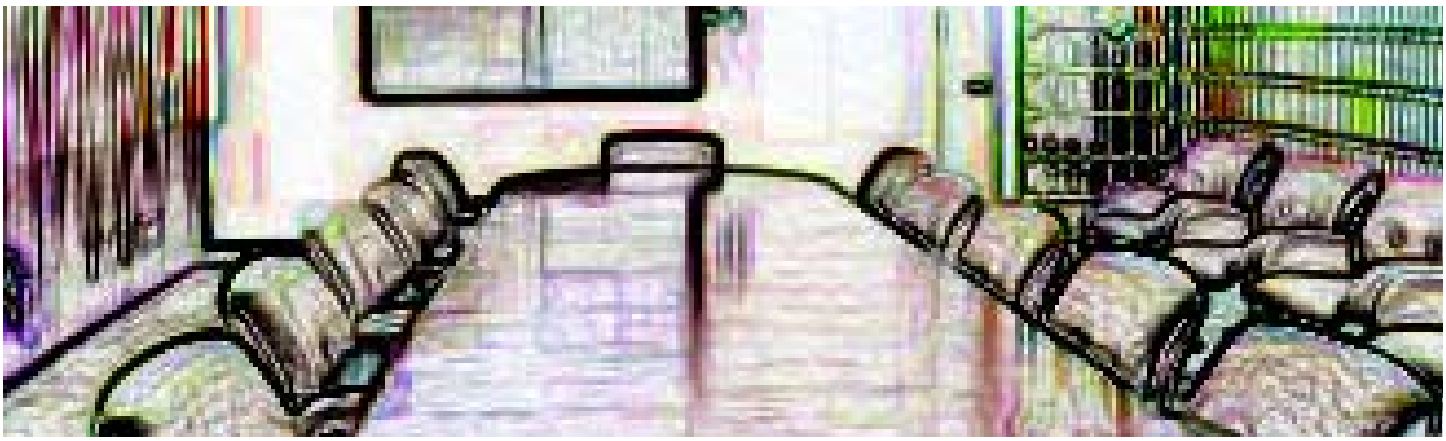
MAYER BROWN ROWE & MAW

A version of this article appeared in the June 10, 2003 issue of *American Banker*

Operational Risk, Internal Controls, and Management Responsibility after the Sarbanes-Oxley Act of 2002

Brian W. Smith and Gregory S. Feder



In response to events over the past two years (e.g., 9/11 and the corporate scandals involving Enron and othe rs), the political and regulatory landscape in which financial institutions operate has changed. Wall Street, Congress, and regulatory bodies are placing unprecedented emphasis on internal controls and accountability. Corporate governance, business resumption, and risk management have become watchwords in boardrooms and on the front page. Failure to comply with recently issued regulations and guidance will impact a financial institution's ratings and will result in adverse regulatory action. It is incumbent that the directors and management of every institution—not just publicly traded organizations—undertake an analysis of their internal controls and institute appropriate policies and procedures in light of the size, complexity, risk profile, and resources of the institution.

Several recent enforcement actions demonstrate this emphasis on management accountability and internal control. A recent written agreement between Fifth Third Bancorp on the one hand and the Federal Reserve Bank of Cleveland and the Ohio Division of Financial Institutions on the other required Fifth Third to take steps to improve its management oversight, risk management, and internal audit functions in order to avoid future problems of the kind that required Fifth Third to take an $82 million pretax charge in the third quarter of 2002 to account for reconciliation errors in its treasury department. Other recent formal actions have focused on the role of internal controls in information technology and anti-money laundering. While these enforcement actions provide insight into those areas the regulators consider important, they fail to provide a roadmap for other institutions to follow.

Recently, the federal banking regulators released two publications that purport to provide guidance to financial institutions seeking to comply with Sarbanes-Oxley. Aside from clarifying those obligations that banks already have (under Section 36 of the FDI Act or Regulation O, for example), however, the banking agencies provided little in the way of specific new instruction for financial institutions seeking a "safe harbor" that will provide insulation from the criticism of examiners viewing an institution's decisions in hindsight. In the same way, several other recent issuances set forth the supervisory expectation that directors and management will develop policies and procedures concerning internal controls, information technology, and operational risk, but provide little in the way of how to satisfy such expectations. Examples include:

- the OCC's revised Handbook on Internal and External Audits;
- the Interagency Statement on the Internal Audit Function and Its Outsourcing issued by the federal banking agencies;
- FFIEC's revised Information Technology Examination Handbook;
- the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System issued by the Federal Reserve, Comptroller of the Currency, and Securities Exchange Commission; and
- the Operational Risk Guidelines issued by the Basel Committee on Banking Supervision.

So, what are directors and management to do?

There is no one-size-fits-all approach to compliance with Sarbanes-Oxley, its implementing regulations, and the other guidance mentioned above. It is clear, however, that the lens of corporate governance and accountability pervasive in society at large will be turned on any action taken by financial institutions. Thus, at least until industry "best practices" develop over time, the process that an institution's directors and management follow is perhaps more important in the first instance than the decisions made via that process. The following factors should be present, whether an institution is developing a disaster recovery/business continuity plan, developing trust department reconciliation processes, determining capital reserves for operational risk, or outsourcing back-office functions:

- The board of directors, perhaps acting through its (independent) audit committee, must act closely with management and the employees responsible for day-to-day operations—it is important that that the personnel who truly understand the daily operations of the institution be given some responsibility for policymaking, but ultimate responsibility and accountability must lie with the directors.
- It is important that institution personnel understand that the analysis and development process is for the betterment of the institution, and that "lip service" not be paid to compliance efforts—directors and senior management are responsible for instilling in the institution's employees a culture of high ethical standards and accountability, what SEC Chairman Donaldson has called the institution's "moral DNA."
- Areas of operations and operational functionality must be identified and prioritized, risks assessed, and justification provided for the determinations made—think about "what could go wrong" at each step of every process and plan accordingly.
- Policies and procedures developed must be objectively reasonable for the size, complexity, risk, and resources of the institution.
- Deliberations and decisions must be well-documented—in many cases, a record of such decisions should be in the minutes of the audit committee.
- Once policies and procedures are established, they must be subject to periodic testing and review—the process must be ongoing (including training), rather than a one-time fix.

While this list is clearly not exhaustive, the overwhelming theme of Sarbanes-Oxley and other recent regulatory guidance underscores the importance of internal controls and accountability in the operation of financial institutions, as well as in other industries. The directors and management of financial institutions and their support organizations must play an increased role and be subject to increased accountability in the areas of operational risk and internal controls described above.

Mr. Smith, former Chief Counsel to the Office of the Comptroller of the Currency, is a Partner and head of the Financial Institution Regulatory Practice Group, where Mr. Feder is an Associate.