



Managing Compliance Risk

By Jeremy Taylor, AuditOne LLC

The scrutiny that credit and funding risks are receiving in the current economic and financial environment is not surprising. These are, after all, life-and-death issues. Perhaps more surprising is the attention also being given to compliance matters, where generally an institution's survival would not seem to be at stake. But mess up on compliance these days and you may start to wonder.

Community banks are more vulnerable for several reasons. Most importantly, due to the lack of specialization and the constraints on segregation of duties that are innate to a small institution; more on this below. Second is the fact that the regulatory spotlight is now falling on consumer and residential lending where many community banks have low but non-zero exposure. When resources are tight, these are the exposures more likely to escape management attention. For these and other reasons, compliance costs are often cited these days as a driver of ongoing banking consolidation.

Directors cannot be expected to demonstrate detailed familiarity with all of the myriad banking regulations that apply to their institution. What is expected is that they ensure an appropriate control environment and supporting infrastructure for the management and monitoring of compliance risk. What should you look for as the key components of an effective compliance management program and the controls embedded within it?

A policy document for each regulation representing material exposure (in terms of accounts, transactions or loans);

Written procedures outlining all of the documenting, monitoring, reporting, and other activities required to ensure compliance with each, and who/how/when/etc. they need to be done;

Hiring an experienced compliance manager (be wary of "learning on the job" in today's regulatory environment) and keeping them current via regular training and by access to supporting resources such as databases, subscriptions, consultants, as appropriate;

- An effective, comprehensive training program, including directors' training, for BSA and for other compliance areas;
- Consumer complaint response procedures;
- A board Compliance Committee;
- Risk assessment, annually updated, to rate the inherent risk to the bank across all applicable regulations (more on this below), which then feeds into staffing, budgeting, audit needs, and other resource allocation decisions;

- Regular management and board reporting sufficient to apprise them of compliance trends, exception issues, changes in compliance risk exposure, etc.;
- Independent internal audit;
- A disciplined process of corrective action on all examination criticisms and audit findings.

On the audit side, again the challenges may be greater for smaller institutions where the compliance and audit functions often overlap. At the board level, an "Audit and Compliance Committee" is commonplace. At the management level, clearly a compliance manager will not be auditing their own work, but their responsibilities will often include periodic monitoring of compliance activities and coordinating with outside auditors. Attention needs to be paid to ensure that audit integrity is not compromised by the exigencies of a streamlined organizational structure.

Much of this ultimately comes back to assessing the risks – of one regulation versus another, but also of compliance relative to other areas. A compliance risk assessment involves addressing the inherent risk to the institution (i.e., based on the type, volume, changes, complexity, etc. of the business being done and how it is done, before taking account of internal controls in place) posed by each of the regulations applying to the institution. This reflects the likelihood of a "loss event," together with the dollar impact such an event would have. These considerations are trickier to identify and quantify for compliance risk than for credit, interest rate and various other risk types. If we think of a loss event being a regulatory violation, then likelihood is a function of examiners' emphasis, the bank's regulatory history and status, and whether or not there is activity in a particular area. Impact is even more subjective: it could be a civil money penalty (e.g., flood violations), but more likely it falls into the category of reputation loss, which could mean lost business but also increased costs from examiner scrutiny.

The fact that compliance risk is hard to assess does not mean you should forget about it. Go with simple (e.g., 4- or 5-point) ratings scales. Get input from different sources to seek consensus on those ratings. Revisit them at least annually to test against shifts in regulatory emphasis, bank strategy, etc. And tie the results in directly to the way in which compliance risk is managed, monitored, audited and reported.

[<back to October 2011 Directors Digest>](#)

Jeremy D. Taylor is president of AuditOne LLC (www.audit-one.com), and CEO of Insight Risk Consulting. He can be reached in AuditOne's Southern California office at 562-802-3581 or at jeremy.taylor@audit-one.com.