



Giving Your Control Environment Strong Foundations

By Jeremy Taylor, AuditOne LLC

Managing a consistently profitable operation requires – for banks more than for most other types of businesses – the successful management of risk. Why banks in particular? Because few businesses willingly take on risk the way banks do. Credit risk most obviously, but it doesn't stop there. While other types of businesses have risks to watch for, mainly to avoid, for bankers, it's "in the very air they breathe." Forgetting risk management may boost your earnings this year...but watch out down the road.

In our internal audit experience with close to 200 client institutions, many patterns and themes suggest themselves as recurring differentiators of (risk-adjusted) performance over time. One of the strongest relates to the culture of risk management as embodied in an institution's practices in four key areas:

Policies: These define what can be done, as well as what must be done. Clearly, applicable banking regulations need to be reflected and respected in policy. It also implies sound business practice, especially when it comes to managing risks. Policy documents should be subject to at least annual board review and approval. They should be carefully reviewed not just for content but also for typos, grammar, formatting, etc., then converted to PDF once finalized. Ensure all employees have ready and timely access (e.g., via bank intranet) to the latest version. Any exceptions to policy need to be reported to the next board meeting. Remember that these are official statements as to how the bank does business; they need to be treated with due sanctity.

Limits: Formulating limits is (or should be) part of policy writing – but an important enough part to pull out here as a separate topic. Limits capture the bank's risk appetite. You know you may be willing to take on a little more or a little less risk, but putting in limits forces you to think in terms of how much. It also signals willingness and ability to put in place systems to measure and report the amount of risk, so as to monitor limit compliance. Having an appropriate selection of limits (not too many, not too few) may require getting feedback from outside (accountants, auditors, consultants). Finally, attention should be paid to ensuring that board reporting presents a clear summary statement of all applicable policy limits and the bank's latest-period compliance with them. Don't have limits if you're not going to report them.

Procedures: Policies are there to guide management in what to do; procedures lay out how to do it. When things get done in a certain way, they evolve into accepted "procedures." What's important is documenting them. This ensures that different individuals (perhaps in different groups/departments) working together are all fully aware of their respective roles and responsibilities. It provides continuity if someone's away and training for someone new. It enforces accountability by having formal, written expectations for individual performance for evaluation purposes. If you're going to restructure, re-engineer or otherwise improve processes, you need to start with a full understanding of how things currently are done. Finally, written procedures give auditors and examiners a tool for assessing whether things are in fact being done correctly. Written procedures should be reviewed and updated at least annually, with higher-level (maybe even board) review and sign-off. Out of our four key areas, this one may be the most pronounced differentiator; it's understandably not a priority at smaller, newer institutions, but we're often encouraging management to recognize and address the

valuable discipline of preparing, updating and adhering to written procedures.

Certifications: We view this, done properly, as a fourth cornerstone. It's what allows management and the Board the comfort that things aren't sliding between auditor/examiner visits. No, it's not an audit, only an internal review and sign-off. It doesn't have the depth of sampling and other rigors of a formal audit. (But make sure the integrity of the certifications process gets reviewed as part of internal audit scope.) It should be comprehensive in terms of verifying that call-backs, reconciliations, tests/reviews and other control functions are being done as policy and/or procedures documents require, across a broad range of operational activities. For certain items, like teller cash counts, the element of surprise is important; have those reviewed on a different date each month. Make sure (as auditors/examiners will look for) that certifications are completed and signed off within a reasonable period after month-end.

Doing these basics correctly is of course no guarantee against surprises. But we strongly commend the discipline provided by a) carefully-written (though not overly-detailed or overly-prescriptive) policy documents, backed up by b) written procedures that are both detailed and prescriptive, further supported by c) limits that make sense to those bound by them and that are scrupulously monitored and board-reported, all complemented by d) monthly certifications which are given board attention and management follow-up. Get these four right and you'll sleep at night with the comfort of knowing that the internal control environment at least has some strong foundations.

[<back to April 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.