



Taking a Risk-Based Approach to Compliance


By Kevin K. Watson

Taking a proactive risk-based approach to compliance demonstrates wise, cost-effective bank management. However, considering all potential compliance events is a monumental task. This column will explain how to zero in on compliance risk by developing a compliance risk assessment.

In most cases when a risk based approach is required, we like to trot out our trusty spreadsheet software and create a model to help us. A scaled down sample compliance risk assessment is included here in Exhibit 1 for your reference. Feel free to tinker with the model until it looks and feels the way you want it to.

Exhibit 1 Compliance Risk Assessment

Regulatory Risk	Activity Levels	Likelihood of Risk Event	Impact of Risk Event	Risk Rating	Action Items
ALLL	1.5% Delinquency/ 55% LTD	High	High	9-High	1. Semi-annual loan reviews 2. ALLL Methodology Validation
Regulation O-Insider Loans	No insider loans allowed by policy	Low	High	6-Med	Periodic policy training for lending staff
BSA	30 MSBs, 100 wire transfers per day	High	High	9-High	1. Hire qualified, dedicated BSA officer 2. Robust annual independent testing



Generally our approach is to begin on the left with a column containing the risk categories. In the case of compliance that would be all of the regulations applicable to your institution, such as Regulation A, B, C and so on. Besides the alphabet regulations, you should include the various federal Acts such as BSA, CRA as well as applicable state laws. For example, the California Financial Code has its own requirements for insider activities, information security, and predatory lending. You might also include some regulatory hotspots like ALLL

and CRE Concentration. Don't forget the Federal Trade Commission's Unfair or Deceptive Practices.

The next step is to rank the importance of these compliance categories. To do this, you need some information. We suggest you capture some of this in a column you can call Notes, Activity Levels, Risk Drivers or some such name. For each regulation, include information that would impact the risk, such as number of transactions, management or staff changes, previous examination or audit criticisms, regulatory hot spot trends, new regulatory guidelines, or other pertinent information that would help you to quantify the risk.

In order to rank your various compliance categories, you will need a rating system. We like to use at least a three point system of low, medium or high. The best practice is to consider both the likelihood that a risk event occurs as well as the impact if it actually does occur. Even if the likelihood that you will have a compliance error is great, if the impact is small, few people care and the category should be assigned a low risk rating. Our preferred approach is to assess the impact and likelihood as low, medium, or high for each category. Then you can convert from a Risk Score Matrix (Exhibit 2) to an overall score. 7s, 8s, and 9s are considered high risk, while 1s, 2s, and 3s are considered low. Of course, a 9 is riskier than an 8.

Exhibit 2

		Risk Score Matrix		
Impact	High	6	8	9
	Medium	3	5	7
	Low	1	2	4
		Low	Medium	High
		Likelihood		

Now that you have assigned a risk rating to each compliance category, you can sort to determine those categories with the highest risk and then plan your compliance strategy and budget accordingly. Another helpful technique is to add a column describing the mitigating controls, action items, or other risk management activities that you will implement in order to bring the high inherent risk down to an acceptable level of residual (remaining) risk. In many instances, you can never achieve a zero risk. Also, some times the cost to mitigate a risk is simply too high and you need to make the decision to either accept a higher residual risk or totally discontinue offering that particular product or service.

You can make good use out of your compliance risk assessment by reviewing it at management compliance meetings as well as certain board meetings, especially the Audit Committee. Also, most certainly show it to your auditors and examiners. We realize the compliance risk assessment involves a large degree of subjectivity. None-the-less, it allows you to clearly tell a high risk from a low risk, it costs little to maintain, and may it save you some compliance embarrassments as well as some risk management dollars.

Kevin K. Watson is CEO of AuditOne, LLC (www.audit-one.com), a California-based independent internal audit firm specializing in banks and their service providers throughout the United States . Watson has 22 years of experience in the banking and auditing industries. He can be reached in AuditOne's Southern California office at 562-802-3581 or kevin.watson@audit-one.com.