Crowe

Smart decisions. Lasting value.℠

May 2020

Risk Assessments: Deep and Wide, or Shallow and Narrow?

An article by Paul R. Osborne, CPA, AMLP, CAMS-Audit

Regulatory expectations for financial services organizations constantly evolve. For example, some more complex organizations that have been taking a high-level approach toward their risk assessments lately have found themselves challenged by regulators to expand those assessments.

Not only does our low interest-rate environment threaten profitability for banks, but so does the lack of barriers to entry for competitors. It's not hard to understand why banks would prefer to stick with such high-level assessments. They might, however, need to dig deeper going forward to satisfy the regulatory agencies.

The current approach

To simplify the high-level approach, it helps to imagine the risk assessment as a spreadsheet. The left column lists an organization's regulatory obligations, such as Regulation B, the *Equal Credit Opportunity Act*, Regulation Z, the *Truth in Lending Act*, the *Real Estate Settlement Procedures Act of 1974*, Regulation DD, the *Truth in Savings Act of 1991*, and other consumer protection acts. The top row lists the organization's lines of business, such as consumer loans, mortgages, and commercial lending.

Many banks essentially rate each compliance regulation as low, moderate, or high risk for each line of business, based on assessments of inherent and residual risk. Inherent risks are the risks of doing business and possibly violating a section of a regulation. Inherent risks often can increase based on factors such as new lines of business or products, changes in business strategy, and external factors.

Once inherent risks are assessed, residual (or managed) risk levels are assessed based on an evaluation of the related controls (for example, policies, procedures, training, sample testing, monitoring programs, and audits) and their effectiveness. For example, if a line of business has high inherent risk related to Regulation B, automated and tested controls could help reduce the residual risk to a moderate or low level. Conversely, a lack of controls could drive a low inherent risk to a higher level of residual risk.

Once the spreadsheet is completed, the organization can use it as a road map for an internal audit plan that spells out the areas to be tested, sample sizes, and the frequency of testing. For example, areas with low residual risk might be tested every two to three years with relatively small samples. Areas with high residual risk require more frequent testing with larger samples.

This approach has appeared to satisfy regulators for some time now, but a trend has developed in the past 12 to 18 months that suggests the tide is turning. Regulators seem to be reconsidering the high-level approach, particularly for organizations with more than $10 billion in assets – in other words, those examined by the Consumer Financial Protection Bureau (CFPB). The concern is that these organizations have many more risks that might fly under the radar in a high-level risk assessment.

A more detailed risk assessment approach

Regulation B provides a useful tool for illustrating how this regulatory concern is manifesting. Rather than looking at it as a single obligation (12 C.F.R. Part 1002), certain agencies now are breaking the regulation down by section (for example, Section 1002.4, 1002.5, 1002.6) for examination purposes. The greater the possible consumer impact, the deeper the examination should be.

The scrutiny becomes even more detailed as the lines of business are differentiated by individual products and services. Instead of looking at the broad category of consumer loans, these agencies are examining unsecured loans, automobile loans, boat loans, home equity lines of credit, and so on. Mortgages are divided into, among others, 30-year fixed, 15-year fixed, one-year adjustable rate mortgage (ARM), three-year ARM, and so on. Also, branches in different geographic locations can be separated out. As the scrutiny becomes more granular, more and more rows and columns are added to the risk assessment "spreadsheet."

Implications for complex organizations

The expectation for a more detailed approach has widespread implications for complex organizations. Say the results of a high-level risk assessment determine an organization has robust controls for Regulation B compliance, producing a low residual risk. In that case, the internal auditor might test only 10, 15, or 20 adverse action notices for compliance.

If the audit plan is based on what regulators deem to be an inadequate risk assessment, though, examiners will not rely on the plan. They likely will instruct the organization's first and second lines of defense (the lines of business and the compliance department) to perform a deeper dive.

The more detailed risk assessment might find a certain loan officer in a remote branch who continues to process manual loan applications and then enter them into the loan underwriting system that automates notifications at the end of each week rather than the day of application. Such a manual process heightens the risk of delays in providing the requisite notifications, as notification and disclosure deadlines are triggered by certain regulations on the day of application.

In response, the auditor must fine-tune the testing. He or she might pull more notices for that specific loan officer, testing 35 notices, including 15 for manually processed applications. Or the auditor could determine it is advisable to pull every application taken by that loan officer for the past 45 days, then compare the dates the applications were completed with the dates the applications were entered into the system. And then, validate that disclosures were provided in a timely manner. This small step can help to make sure regulatory requirements have been met.

Higher costs

The bad news is that costs of risk assessment could increase. However, those costs could be offset by areas of lower risk that have been rotated based on the expanded risk assessment. This means that areas identified as lower risk are often not tested as frequently as those categorized as higher risk. Costs therefore should level off after the first round of expanded testing, when the auditor need only update the testing.

Of course, the risk assessment itself is not the only potential source of higher costs. For example, an organization currently offering only fixed rate mortgage loans may want to expand its mortgage offerings to include an adjusted rate option. In this case, it will need to provide additional disclosures based on interest-rate adjustments. To comply, it must for instance, develop the processes and personnel to reduce the risk of 1) failing to identify the proper index applied to adjust rates, or 2) failing to accurately compute the new payment amount.

Time to reconsider the risk assessment

To be clear, the more detailed approach to risk assessment has not yet been mandated for financial services organizations. However, recent examination experiences indicate that some regulators are suggesting it.

Rather than taking a wait-and-see approach, organizations would be wise to evaluate the merits of a deeper and wider risk assessment that leads to more focused testing by internal audit. Especially as organizations become more complex, high-level risk assessments might not tell the true story, and relying on them could prolong and complicate regulatory examinations.

Learn more

Paul Osborne
Partner
+1 317 706 2601
paul.osborne@crowe.com

This article was originally published in the May/June 2020 issue of ABA Bank Compliance magazine.