Mark W Olson: What are examiners looking for when they examine banks for compliance?

Remarks by Mr Mark W Olson, Member of the Board of Governors of the US Federal Reserve System, at the American Bankers Association's Regulatory Compliance Conference, Orlando, 12 June 2006.

* * *

Thank you for the invitation to speak today on an issue of great interest to many of us, that is, compliance-risk management and supervisory expectations. Over the last few years, legal and regulatory compliance breakdowns have attracted increased attention across the financial industry. Fortunately, most of you have responded to your evolving compliance risks by investing in effective compliance-risk management programs. However, now and then, headline-grabbing incidents of noncompliance continue to capture public attention, especially when they involve such sensitive areas as fair lending and the Bank Secrecy Act (BSA). Conferences such as this are valuable opportunities for you, as compliance experts, to share experiences and successful approaches to controlling compliance risk.

To assist you in your efforts to fine-tune your compliance-risk management programs, I'd like to give you a sense of what Federal Reserve examiners look for when they conduct examinations. I will also take a few minutes to address our more focused work in two particularly important areas of regulatory compliance: compliance with BSA requirements and Home Mortgage Disclosure Act (HMDA) data reporting requirements. Otherwise, I will not focus on examinations that look solely at the level of compliance with specific laws and regulations but will focus on how examiners assess the adequacy of a compliance-risk management program and its ability to manage the organization's compliance risk.

Compliance-risk management

Overall, a banking organization's compliance-risk management program should enable it to adequately identify, measure, monitor, and control the compliance risks involved in its various products and lines of business. These are fundamental principles not only for compliance-risk management, but also for sound management of credit, market, liquidity, and operational risk.

It's worth taking a moment to define *compliance risk*. It is the risk of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value that may arise when an organization fails to comply with laws, regulations, or standards or codes of conduct of self-regulatory organizations applicable to the business activities and functions of the banking organization.

While all banking organizations should have a program in place to effectively manage compliance risk, these programs can vary considerably, depending on the size, complexity, and geographic reach of the banking organization and the inherent risks of its activities. As with other types of risk, large multinational organizations will require more elaborate and formal compliance-risk management systems to address their broader and typically more complex range of financial activities and to provide senior managers and directors with the information they need to monitor and direct activities. Therefore, our supervisory expectations regarding an organization's risk-management program, and more specifically the scope of an examination, will vary according to the organization's size and complexity.

Assessing the adequacy of compliance-risk management programs

The Federal Reserve's supervisory approach in the area of compliance-risk management is consistent with our long-standing focus on the adequacy of banking organizations' overall management of risk. To this end, Federal Reserve examiners assess the quality of a banking organization's systems for identifying, measuring, and containing its risks. While historically there has been a greater emphasis on risk management in the areas of credit, market, operational, and liquidity risk, because of the growing complexity of banking operations and their regulatory frameworks the Federal Reserve is taking a greater interest in banking organizations' ability to manage their compliance risk.

Scoping the examination

Generally, a Federal Reserve examination team begins by defining the scope of the examination; this is when examiners determine the areas of focus and level of scrutiny. The scope of the examination will vary depending on the nature and circumstances of the banking organization. For example, as part of the scoping exercise, examiners will consider previous examination and audit findings to determine whether the organization has a satisfactory history of compliance or whether there have been previous concerns about its compliance-risk management program. The examination team will also review the organization's compliance-risk assessment. Depending on its quality, the risk assessment can also help direct the resources of the examination team. Altogether, the information gleaned from examination and audit findings and a current risk assessment will directly affect the scope of the examination, including the level and area of transaction testing required to assess the adequacy of the compliance-risk management program. At institutions with a less satisfactory record, a more extensive review will be necessary.

Federal Reserve examinations for compliance-risk management are not designed to be gotcha games in which examiners look for one-time breaches of specific regulations or laws. Rather, these examinations are designed to assess the adequacy of the structure and processes the institution uses for managing compliance risk. Examiners are expected to look for the bigger picture and to look at the effectiveness of the program (including policies and processes) for managing the organization's compliance risk. We want to understand whether you have the controls in place to manage the risk of *your* organization.

As with all areas of risk management, our expectations - and therefore the scope of many examinations in this area - are framed by an emphasis on;

- board and senior management oversight,
- policies and procedures,
- internal controls,
- monitoring and reporting, and
- training.

I'll give you a sense of some of the key components that examiners are likely to look for when assessing these fundamental areas.

Board and senior management oversight

A successful compliance-risk management program starts at the top of the organization. It is essential that the board of directors takes the lead by requiring a top-to-bottom compliance culture that is incorporated into the organization's day-to-day operations and is well communicated by senior management so that all staff members understand their compliance responsibilities and their roles in implementing the enterprise-wide program. Examiners will look to understand the board and senior management's roles in setting and communicating the compliance culture within the organization.

Examiners will also look to see that roles and responsibilities are clearly defined and communicated throughout the organization and that senior management and staff understand their compliance obligations. In order for the board and senior management to carry out their responsibilities, they need to understand the organization's *current* compliance risks. We have seen organizations that have experienced challenges as a result of a lack of clarity in this area as they grow and diversify.

Examiners will determine whether the organization has an effective risk assessment that accurately identifies its compliance risks and whether material risks are communicated to the board. Effective risk assessment measures the risk presented by clients, products and services, and geographic exposure within specific business lines or activities and aggregates these risks across the organization.

Risk assessment is critical not only to ensure that the board and senior management is well informed. It also serves as the foundation for risk-based policies, procedures, and internal controls. Examiners will look to understand the organization's risk-assessment process. For example, they will look to see the degree to which the business lines are involved, how frequently the risk assessment is updated, and how it incorporates new products, services, or legal entities.

Human and financial resources are, of course, critical to effective performance. Consequently, examiners will assess whether senior management ensures that the compliance program has sufficient financial resources and a sufficient number of qualified and well-trained staff to carry out its responsibilities effectively.

Policies and procedures

Policies and procedures essentially define and communicate the key goals and processes of an organization's compliance program. Examiners will look to see whether policies and procedures provide for adequate risk identification, assessment, measurement, and control.

As I mentioned a few moments ago, clearly communicated roles and responsibilities are a characteristic of an effective compliance program. Toward that end, examiners will also look to determine whether policies clearly delineate accountability and lines of authority across the organization's activities.

Examiners also expect to see a well-defined process for ensuring that when compliance risks or potential breaches are identified they are elevated to the appropriate level, in keeping with the risk to the organization. Procedures for doing so should be well-communicated to staff throughout the organization.

Overall, policies and procedures must be kept current, and, as with the risk assessment, examiners will look to see whether information gleaned from the compliance program operations is used to further tailor compliance policies, procedures, and controls to specifically address the inherent environment as it evolves.

Internal controls

Internal controls are a particularly crucial element of a compliance-risk management program. Examiners will verify whether the organization has established and implemented an effective system of internal controls, including appropriate reporting lines and separation of duties, as well as positive and negative incentives.

An essential part of the internal control framework is periodic testing to determine how well the framework is operating, so that any required remedial actions can be taken. The frequency of testing should be risk-based and should involve, as appropriate, sample transaction testing, the sample size being determined by volume and the degree of risk of the activity.

Examiners will carefully assess the scope and quality of the testing of the compliance program. Part of this assessment will include determining whether the testing was performed with appropriate independence. Examiners will also look to understand the specific delineations of responsibilities between the internal audit, compliance, and other independent functions or third parties. These delineations will vary by organization, but all roles should be clearly defined and communicated.

Examiners will also look at how well compliance-testing exceptions are reported to senior management and resolved by business-line management. They will assess methods for tracking exceptions until the exceptions are resolved; this assessment will include examining the organization's provisions for escalating unresolved exceptions to higher levels in the organization, including the board of directors.

Independence and separation of duties are also issues of importance beyond compliance testing. For example, in the case of large complex banking organizations that may have a corporate compliance function, examiners will be interested in understanding how the compliance function maintains its independence from the business lines it advises on compliance requirements and the implementation of required controls. In cases in which the compliance function has responsibility for monitoring and testing, examiners will assess whether procedures are established to ensure an adequate degree of independence and objectivity.

Monitoring and reporting

As I mentioned, the fundamental purpose of compliance-risk management programs is to identify, monitor, and manage compliance risk more effectively. Monitoring involves identifying and

communicating compliance concerns to the appropriate parties within the organization. Monitoring and reporting enable senior management and the board to effectively carry out their respective responsibilities. We have seen organizations silo critical compliance information rather than share it with all levels of the organization, which can handicap an organization's ability to identify systemic risks. As a result, examiners are interested in whether a compliance program is designed to monitor and report compliance concerns.

The level of sophistication of banking organizations' monitoring activities generally varies according to the size and complexity of the organization, and examiners' expectations will vary accordingly. For example, large complex banking organizations are typically supported by information systems that provide management with timely reports related to compliance with laws and regulations at the transaction level. Examiners will look to see whether these reports generally address monitoring and testing activities, actual or potential material compliance deficiencies or breaches, and new or changing compliance requirements. They will also assess whether reports are designed to ensure that information on compliance is communicated to the appropriate levels within the organization.

Training

Training on policies, procedures, and associated controls is a component of compliance-risk management that should not be overlooked. Examiners will determine whether the banking organization's training program ensures that compliance policies, procedures, and controls are well understood and appropriately communicated throughout the organization.

While the depth and breadth of training that an employee receives depends on that employee's role and responsibilities, examiners generally assess whether staff at all levels understand the organization's compliance culture, general compliance-risk issues, and high-level compliance policies and procedures.

Supervisory consistency and the Bank Secrecy Act

As banking organizations become more complex, consistency in the agencies' supervisory approach has become even more critical. The Federal Reserve views supervisory consistency as a means of enhancing supervision and reducing burden. This is particularly essential in the area of regulatory compliance, and specifically with regard to compliance with the Bank Secrecy Act and its regulations.

The Federal Reserve includes a review of BSA compliance within every full-scope safety-and-soundness examination. For larger banking organizations that are subject to continuous supervision, the Federal Reserve conducts a series of targeted BSA reviews over the course of the supervisory cycle. This, combined with off-site monitoring, allows the Federal Reserve to maintain a current understanding of BSA compliance within the organizations that are subject to its supervision. On-site examinations are essential to ensure that the BSA program is operating effectively.

Because of the complexity of banking organizations today, a number of institutions may be subject to the supervision of an increasing number of regulators. A consistent examination approach among regulators is critical in order to achieve a consolidated view of risk management within an organization, and also to reduce burden on banking organizations. Our work with the Federal Financial Institutions Examination Council to develop the *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, which was released last summer, marked an important step forward in our effort to ensure consistent supervision in the area of BSA compliance. Through the manual, the agencies have emphasized a banking organization's responsibility to establish and implement risk-based policies, procedures, and processes to comply with the BSA and safeguard its operations from money laundering and terrorist financing.

The agencies are currently updating the manual and plan to release the revised version this summer. I have been told that the revised manual will include not only updates reflecting changes in regulations and supervisory guidance over the course of the past year, but also, among other things, additional guidance on developing a BSA/AML risk assessment, which is the foundation of effective risk-based controls.

HMDA data and fair lending examinations

Examinations to evaluate a banking organization's adherence to fair lending laws and regulations are also a routine component of consumer compliance examinations conducted by the Federal Reserve. HMDA data play an important role in examinations of those banking organizations that are required to report the data. Examiners probe that data to understand how the bank is responding to credit needs and serving its community. The data are rich in many respects. They contain information about applicants' and borrowers' race or ethnicity, sex, income level, and property location. And, since 2004, the HMDA data have also included price information about certain loans with prices that exceed thresholds set by the Board.

The HMDA data help examiners better focus the fair lending examination. Particularly for banks with larger portfolios, the data, including any available pricing data, are incorporated into statistical management systems that analyze lending patterns and help direct the examination process to aspects of the bank's program that may warrant a closer look. Even in smaller banks where a statistical analysis cannot be performed, the HMDA data can be used to start the fair lending review. However, as we know, HMDA data have limitations. For example, the data do not include credit-risk factors such as credit scores and loan-to-value ratios. Because of these limitations, the examination process looks at additional information about a lender's practices, and about particular loans, before any conclusions are drawn. Examiners consider - together with HMDA data - information derived from consumer complaints, risks apparent from various business lines, and the adequacy of the institution's compliance-risk management program.

Since examiners will be looking at the data, it would be advisable for a bank to make a review of the data a component of a comprehensive fair lending compliance program and Community Reinvestment Act strategy. In fact, examiners will look carefully at analyses of HMDA data performed by a bank and talk with the bank to understand the reasons for any disparities in lending patterns. The bank is probably in the best position to understand what the HMDA data suggest about its ability to reach prospective borrowers. Consequently, its own assessment is useful to an examiner establishing the fair lending examination scope. Examiners want to know how banks have addressed any disparities and how the bank's analysis has led to any changes in controls that were made to ensure that policies are followed. I want to emphasize that, as with compliance-risk management programs, the breadth of a banking organization's program and system review should be commensurate with the size and complexity of its operations, the range of its products, and the demographics of its markets.

Beyond this review of HMDA data, examiners evaluate whether an organization's fair lending compliance framework makes it possible to identify, monitor, and effectively control risks. Examiners are looking for a clear articulation by the board of directors of the institution's lending strategy, including defined risk parameters and the execution of appropriate risk-measurement and risk-mitigation initiatives. Examiners will evaluate the extent to which management controls reflect the risk associated with the institution's lending strategy.

As with the broader area of compliance-risk management, examiners will look closely at how the compliance culture established at the top of the organization filters down into the everyday responsibilities of business-line managers and how those managers are held accountable for compliance.

Conclusion

Because of the growing complexity of banking organizations, the Federal Reserve is currently considering whether more-tailored guidance in the area of enterprise-wide compliance-risk management is warranted. In the coming months, we will continue to engage with you to better understand your successful approaches to identifying, monitoring, and managing risk across your organizations.

Thank you.