

A low-angle, black and white photograph of several tall skyscrapers reaching towards a bright, cloudy sky. The perspective creates a sense of height and scale. A semi-transparent white horizontal band is positioned across the middle of the image, serving as a background for the text.

WHITE PAPER

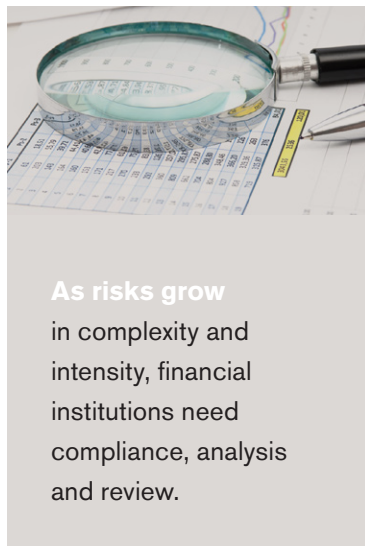
Developing a Compliance Risk Assessment Framework

EXCHANGE PLACE



Succeed. Transform. Compute. Perform.

Developing a Compliance Risk Assessment Framework



EXECUTIVE SUMMARY

As compliance risk continues to be a focal point for regulators, compliance officers in banks and other financial institutions are encouraged to take steps to ensure that compliance risk is adequately managed.

GUIDELINES AND STANDARDS

Best practices for compliance management ensure that compliance risk is adequately managed. On a periodic basis, management should identify and assess the primary compliance risk issues applicable to all business activities including the related control mechanisms utilized to identify, measure, monitor and control the relevant risks. Regulatory and standard setting bodies such as the Board of Governors of the Federal Reserve System and the Basel Committee continue to issue guidelines and standards regarding compliance functions in banks. Specifically, the Board of Governors of the Federal Reserve System has adopted the requirement of the Basel Committee paper entitled “Compliance and the compliance function in banks”¹ with respect to bank compliance standards by issuing a Supervisory Letter, SR 08-8/ CA 08-112 in October 2008².

DEFINITION OF COMPLIANCE RISK

Compliance risk is defined as: The risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations (SRO's) applicable to the banking organization (applicable rules and standards).

COMPLIANCE RISK ASSESSMENT FRAMEWORK

The key object of a Compliance Risk Assessment Framework is to effectively assess the legal and reputational risk exposure of an institution's business activities, not only in terms of adhering to

¹ [Basel Committee on Bank Supervision, Compliance and the compliance function in banks, April 2005](#)

² [Board of Governors of the Federal Reserve System, SR Letters 2008, SR 08-8 / CA 08-11](#)

applicable laws and regulations, but also to relevant internal firm policies and standards of conduct. A compliance risk assessment should include the following three key components:

Regulatory Matrix - Includes an inventory of federal and/or state laws, regulations, rules, standards and other guidelines to be used in determining the applicability of each to relevant business units and/or activities. Additionally, the matrix will reflect (at a summary level) the results of each risk review, including inherent risk, control factor assessment(s), residual risk and any recommended corrective action.

Compliance Risk Analysis – Provides a detailed analysis of the level of compliance risk inherent for each applicable law or regulation, including the effectiveness of the compliance risk control methods used to measure, monitor and control all identified risk(s). The risk analysis will result in a calculated level of residual risk and will contain recommended corrective action(s) to reduce unacceptable residual risk to an acceptable level.

Compliance Reviews – Provide for an assessment of overall compliance with respect to applicable laws, regulations, rules, standards, guidelines and/or firm policies and relevant control environment used to identify, measure, monitor and control compliance risk.

CONCLUSION

The Compliance Risk Assessment Framework provides the methodology for assessment of compliance risk and the assignment of risk ratings that best describe the level of compliance risk with respect to applicable laws, regulations, rules, standards or guidelines. Thus, a financial institution's compliance risk management program should be documented in the form of compliance policies and procedures and compliance risk management standards. The processes for managing compliance risk should be formalized in a compliance program that establishes a framework for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risks across the organization, and for providing compliance training throughout the organization.