Regulatory Compliance Management ("RCM")

Graham Segger, FCPA, FCA

There is a new string of letters in the grand lexicon of regulatory inspired acronyms. As of May 2015 Regulatory Compliance Management ("RCM") as articulated in the November 2014 OSFI Revised Guideline E-13 officially replaces Legislative Compliance Management ("LCM") as the umbrella expression for the set of key controls through which a Federally Registered Financial Institution ("FRFI") manages regulatory compliance risk. The LCM framework was first introduced ten years ago. The new Guideline incorporates over 20 relatively minor edits and updates from the draft Guideline issued in April, 2014. OSFI has provided on their website a useful cross-reference table in the letter accompanying the Guideline summarizing the comments received on the Draft and how those observations have been addressed or incorporated into the final Guideline.

This Guideline is very timely as at least twice in the last year I have heard senior managers of insurance companies comment that they see the management of regulatory risks as one of their top risks. The Guideline helps articulate expectations and also provides a framework for managing and mitigating such risks. For this purpose, regulatory compliance risk includes potential non-conformance with laws, rules, regulations and prescribed practices ("regulatory requirements") in any jurisdiction in which an FRFI operates. Interestingly, this does not include compliance with ethical standards, a much more subjective field.

The structures, processes and other key control elements which make up the framework are documented in the Guideline. OSFI has emphasized on numerous occasions that they do not view the RCM framework to be a significant expansion of current requirements and procedures, but rather a better articulation of what is expected, aligned with other more recent pronouncements. It is a risk-based approach and, in theory, provides flexibility for the framework to be scaled to the size and complexity of the FRFI. In their Impact Analysis Statement OSFI lists the objectives of the revised Guideline E-13 as:

- Outline OSFI's supervisory expectations with respect to FRFIs' control frameworks for mitigating regulatory risk, which contribute to their safety and soundness;
- Promote industry best practices in regulatory compliance risk management;
- Be consistent with OSFI's Supervisory Framework (2010) and Corporate Governance Guideline (2013);
- Be more consistent with international risk management standards.

Before examining the elements of the framework it is important to understand the three lines of defence model which underpins it. These lines are, according to OSFI, a useful way of considering the adequacy of risk management responsibilities and capabilities:

- first line - operational management
- second line - a compliance function
- third line - Internal Audit or other independent review function

The nine elements of the framework articulated in the Guideline are:

(i) Role of the Chief Compliance Officer ("CCO")

The CCO, who has a direct reporting line to the Board of Directors, has responsibility for assessing the controls in place and concluding, based on testing, on their adequacy for achieving regulatory compliance.

(ii) Procedures for identifying, risk assessing, communicating, effectively managing and mitigating regulatory compliance risk and maintaining knowledge of applicable regulatory requirements

These procedures should be risk-based so more resources are applied to higher risk areas, and updated as underlying business situations change.

(iii) Day-to-day compliance procedures

These procedures should be tailored to and built into business processes and include periodic testing and evaluation.

(iv) Independent monitoring and testing procedures

This element of the framework consists of both the second and third lines of defence mentioned above. The CCO is responsible for monitoring the adequacy of, adherence to and effectiveness of day-to-day operational compliance procedures and reporting consistently across the entire enterprise, using a risk-based approach. The third line of defence is an independent review of both the operational and monitoring processes.

(v) Internal reporting

This element discusses reporting procedures and compliance reports which are expected of an FRFI. OSFI gives the following examples of content that reports should cover: results of enterprise-wide compliance oversight, material RCM framework weaknesses, instances of material non-compliance, material exposures to regulatory risk (and their potential direct or indirect impact on the FRFI), related remedial action plans, information about significant legislative and regulatory developments, industry compliance issues, emerging trends and regulatory risks. Both the CCO and the Independent reviewer (likely Internal Audit) must report to the Board.

(vi) Role of Internal Audit or other independent review function

The activities carried out by the CCO and operations with respect to regulatory risk should be subject to periodic review by Internal Audit or other independent review function.

(vii) Adequate documentation

The roles and responsibilities of those involved in the management of regulatory risk, the control framework and the results of testing must be well documented and reported.

(viii) Role of Senior Management

This section emphasizes that senior management must be involved in the implementation of the RCM framework and assure that it is appropriately designed and maintained.

(ix) Role of the Board

The regulator expects that the Board will have ultimate responsibility for effective enterprise-wide regulatory compliance management. The Board must therefore be aware of material exposures, RCM policies, reports and mitigation plans and have a view on the overall effectiveness of compliance oversight.

Whether or not this Guideline expands requirements or simply documents current requirements may be a matter for some speculation and perhaps debate. Many I have spoken to are concerned that this Guideline does expand the burden for demonstrating compliance. I suspect most FRFIs will have some work to do to ensure all of these elements are incorporated into their processes. Branches in particular may have to carefully consider how this Guideline can be incorporated into their unique governance and management structures. May 1, 2015 is looming and companies, their Boards and CCOs will be well advised to carefully benchmark their regulatory compliance management against the revised Guideline.