It has been my experience that risk monitoring activities undertaken by compliance, internal audit or risk departments – (collectively referred to as "risk departments"), and the individuals undertaking such activities, are not usually given sufficient weight or authority to ensure that risks are being properly mitigated. This may result from a false perception that no business value is obtained from risk monitoring reports. Why is this so?

There are a number of asset management companies that have adequate risk system, and business controls. They also have risk systems that produce Key Risk Indicators and other risk information. However, the compliance jigsaw is missing several pieces. One is the linkage between risk information and risk monitoring – its absence can result in over-monitoring at best, and under-monitoring of critical risks at worst. Also often missing are quality monitoring resources.

Purpose of Compliance Monitoring Procedures

The purpose of a structured approach to compliance monitoring is to ensure that the standard of monitoring is consistent across in all areas of the business and that all risk areas are covered. Regulators expect risk monitoring to be undertaken using a risk-based approach. However, this begs the question of whether compliance departments actually understand the business processes and therefore what the risks are. A full understanding of the business process is essential to gain the support of line management and to be able to carry out appropriate risk reviews.

The results of risk monitoring activities are generally provided to line management in an initial report, with an agreed final report provided to line and senior management. All reports should be in a consistent format. The report must be accurate, and be seen to add value rather than a document for the purpose of individual criticism. Appropriate buy-in is needed from all areas of the business to ensure that compliance monitoring is viewed as a tool that assists day to day operations.

Risk-Based Monitoring Approach

The Risk department must establish a risk-based monitoring methodology and there are many ways to achieve this objective. However, I believe the risk-based methodology should include an understanding of:

- Generic risks across the asset management industry (or a specific sector of it)
- Specific risks to the entity's business activities
- Business processes that involve higher levels of risk within the business entity
- Risks within each business process

The Risk department must document the risks at each of the above levels to determine the specific business functions that will be included in the annual strategic monitoring plan, and whether that plan should include a detailed review, a desktop review[1] or no monitoring at all. In addition, if risk indicators received during the year highlight either a downward trend in controls or upward trend in risk, then that business function should be subjected to a tactical monitoring review.[2]

Business processes that contain higher levels of risk

[1] Discussing a completed internal control questionnaire with the line manager completes a desktop review. This is only appropriate provided that the control environment has previously been subjected to a detailed review and the control environment was considered to be satisfactory.

[2] Tactical monitoring is undertaken when KPI/KRI trends indicate that the initial assessment of the control environment may have changed. The business process becomes subject to an immediate detailed review to identify why such trends have occurred and what remedial action is required.

Each business process contains elements of operational risk that can be classified under regulatory, legal, operational, people, financial or reputation. The objective of a risk-based monitoring approach is to identify those business processes that contain a higher level of operational risk so that sufficient monitoring resources can be applied to those business processes. The objective of the monitoring activity is to recommend improvements to business processes and to either strengthen the control environment or mitigate the risk altogether if required.

In order to identify those business processes that contain a higher level of risk, historical data is needed to indicate the effectiveness of the existing control environment, i.e. whether a business process has a high level of residual risk. Historical data should be considered as indicative of the residual risk in each process going forward. All of the business processes must be identified and recorded, (eg in a Business Process Matrix-type document) and should be discussed widely to ensure all business processes are captured.

Likelihood

A risk assessment scale should be determined to rate the probable, albeit in some cases subjective, likelihood of an event occurring such as an error, a breach of a regulatory requirement, receipt of a complaint or a cost. The indicative risk indicators are derived from historical operational information and likelihood risk scale must be determined for historical errors, breaches and complaints, as these are **the barometer of operational efficiency.**

Previous monitoring activity should also be used as an indicator of residual risk within business processes. This historical data is divided into two parts: when the last review was undertaken, and the results of that review. Rates must be created and applied to such information.

However, not all historical indicators should be considered as carrying the same level of importance. To ensure that each indicator is appropriately factored, a weighting should be applied to probability of an event occurring. This will provide an additional refinement to the risk indicator.

Impact

A risk assessment scale is also used to rate the impact of historical events on the business. Impacts on the business can be measured in terms of the cost of errors and breaches, regulatory sanctions, impact on the business operations, and reputation in the public eye.

However, as noted above, not all historical indicators should carry the same level of importance. Again, a weighting percentage should be applied to all the probable impact indicators. This weighting should be applied in accordance with the company's risk appetite.

Management Input to Risk Assessment

After the risk department's initial calculation of the weighted likelihood and impact risk indicators, it is appropriate to discuss this review with line management. Discussion with line management should yield additional information which may impact the initial risk assessment. Systems may need enhancing or replacing, outsourcing business functions, new products and/or human resource issues may also need to be considered. Senior management input is also required on both likelihood and impact based on their business intuition using the same scale applied by the risk department.

The combination of historical data, line and senior management input and weighting percentages provides a weighted likelihood and impact indicator to determine the business processes that should be subjected to a detailed review during the forthcoming year.

Each business process should then be plotted on to a Risk Prioritisation Matrix (some refer to this as a Risk Heat Map using red, amber and green as levels of severity) to identify the business processes that will be subjected to a detailed review. The Risk Prioritisation Matrix should be colour co-ordinated to reflect the severity of the risk perceived in each business process, and those processes deemed to be in the red section of the matrix will be subjected to detailed reviews. Those noted in amber may be subjected to a desktop review, and those in the green section will not be subject to any formal review process. However, if risk indicators identify a change in risk perception during the year, a tactical review will be undertaken forthwith.

Risks within each business process

The next task is to identify the risks within the business processes that should be subjected to independent monitoring. These risks should be recorded in a Business Review Planning Memorandum and should be discussed with line management as part of the review planning process. The risks identified can again be classified as structural, regulatory, operational, people and financial.

Business Review Planning Process

A Business Review Planning Process is essential to yield an effective and efficient review and to ensure that monitoring procedures add value and are seen to add value to the business..

Planning should include face-to-face meetings with line management to explain the objective of the review, noting that if any critical matters do arise they will be informed forthwith. As noted above, it is also important to explain that the report is not a personal criticism, and that the review and the resulting report should be viewed as a tool to improve the control environment that will benefit both line management and the company's reputation.

The planning memorandum should include a short paragraph explaining the background, scope, nature, resources and the approach to be adopted. However, the added value of the planning memorandum is the inclusion of a Risk Appendix, noting all identified risks within the process and including a Risk Prioritisation Matrix (ie all risks plotted as to likelihood and impact) that provides a graphical overview of the risk profile of the business process to be reviewed.

The next stage of the planning process is to prepare an Internal Control Questionnaire ("ICQ")[3] and a Substantive Monitoring Programme ("SMP").[4] The ICQ must include questions on all risk issues within the business process. The SMP must include all regulatory requirements to be checked during the transaction processing review. Used appropriately, the ICQ and the SMP will provide line management with a holistic view of the risks within business processes.

The Report

The initial report will be provided to line management in draft form to avoid misunderstanding. The report should be clearly identified as a draft subject to discussion with line management and should not be provided to the final distribution list until all matters have been agreed as valid findings. In the event that a finding cannot be agreed between compliance and line management, this point should be escalated for senior management to agree upon an outcome. In the absence of such agreement, this point should be escalated to the CEO for final resolution.

[3] An ICQ is a series of questions covering structure, regulatory, operational, people and financial issues on the controls that a reasonable business would be expected to have in place.

[4] An SMP is a transaction-based walkthrough of the system to ensure that it processes a transaction accurately and that all controls are effective.

The final report should include an executive summary. CEOs do not have time to read a longwinded report on minutiae – that is a responsibility for line management. However, CEOs do need to know about important issues. The final report should include the added-value Risk Appendix and Risk Prioritisation Matrix described above.

Conclusion

There is value to be added by an effective risk management process and by having efficient risk monitoring resources. A risk monitoring process, if well thought-out and executed, will help line management operate their business processes with added efficiency.

For further information please contact:

Fiona Nangle: *Director:* + 353 (0)87 328 5255 *fnangle@fmconsult.ie*