THOMSON REUTERS ACCELUS™

FUNDAMENTALS OF GRC: THE CONNECTED ROLES OF INTERNAL AUDIT AND COMPLIANCE

WHITEPAPER

THOMSON REUTERS

CONTENTS

INTRODUCTION 3

THE ROLE OF INTERNAL AUDIT 3

THE ROLE OF COMPLIANCE 4

CONNECTION POINT: THE BOARD OF DIRECTORS 5

CONNECTION POINT: SETTING THE TONE AT THE TOP 6

CONNECTION POINT: RISK MANAGEMENT 6

CONNECTION POINT: MONITORING AND TRACKING 7

SHOULD COMPLIANCE AND INTERNAL AUDIT BE A COMBINED FUNCTION 8

OPTIMIZING THE COLLOBORATION BETWEEN INTERNAL AUDIT AND COMPLIANCE 8

ABOUT THOMSON REUTERS GRC 10

INTRODUCTION

The advent of new and pending regulations as a result of Dodd-Frank, the UK Bribery Act, and FCPA enforcement has heightened the need for connected governance, risk and compliance well beyond the internal audit and compliance departments. Executives, corporate boards, risk management and business line managers are all under increased oversight and scrutiny by regulators, shareholders and external auditors. As a result, internal audit and compliance professionals are faced with ever increasing information requests, new compliance requirements, and are under constant pressure to do more with less.

The traditional approach to governance, risk and compliance relies on working in silos and using separate point solutions to address each assurance group's requirements. This creates a fragmented approach that leads to inefficiencies, added costs and an inability to maintain compliance initiatives and make informed and accurate decisions.

Governance, risk, and compliance activities are by nature interconnected and rely on common sets of information, methodology, processes and technology. By establishing a common, integrated discipline around regulations, policies, risks, controls, and issues, leading organizations have demonstrated that they can better leverage information, gain operating efficiencies, and provide greater transparency into legal, regulatory, operational, and overall business risks.

This leads to a natural question. In this new world of connected GRC, what is the role of internal audit compared to compliance? Where do these roles remain separate and where do they share responsibilities? How can these professionals work together to drive business value?

This whitepaper will establish the hallmarks of a good corporate governance program, outline the primary roles of internal audit and compliance and share ideas on where these two important professions intersect and can leverage one another in a connected GRC environment.

THE ROLE OF INTERNAL AUDIT

The scope and role of internal audit is directly tied to the board audit committee. Publicly traded companies are required by most major exchanges to have a board audit committee. Charged with oversight of the organization's audit and control functions, the audit committee responsibility includes the oversight of the processes and structures implemented by the board and monitoring the activities of the organization toward the achievement of its objectives.

In addition to exchange requirements, audit committee responsibilities are also highlighted in legislated rules including those listed in section 301 of the Sarbanes-Oxley Act which states amongst other things that:

- "The audit committee must be directly responsible for the appointment, compensation, retention and oversight of the work of any registered public accounting firm engaged for the purpose of preparing or issuing an audit report or performing other audit, review or attest services for the issuer, and the registered public accounting firm must report directly to the audit committee.
- The audit committee must establish procedures for the receipt, retention and treatment of complaints regarding accounting, internal accounting controls or auditing matters, including procedures for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.
- The audit committee must have the authority to engage independent counsel and other advisors, as it determines necessary to carry out its duties."

As with all governance initiatives, the audit committee is accountable for the administration of these activities, not the actual work. Internal audit has a direct reporting line into the audit committee and they are tasked with execution on the audit committee's objectives.

Fundamental to the role of internal audit is independence and objectivity. Internal audit provides management and the audit committee with assurance as to the design and operation of the governance, risk management and control processes in their organizations, which requires an unbiased view. However, it is important to note that the role of internal audit is not simply to conduct audits. Internal audit exists to provide:

ASSURANCE. This includes an objective examination of evidence intended to provide confidence as well as providing accurate and current information to the stakeholders about the efficiency and effectiveness of its policies and operations, and the status of its compliance with the statutory obligations.

ASSESSMENT AND RECOMMENDATIONS. Internal audit adds value by assessing and making recommendations on the effectiveness of the mechanisms that are in place to ensure that the organization achieves its objectives and by performing this duty in a way that demonstrates informed, accountable decision-making with regard to ethics, compliance, risk, economy and efficiency.

OVERSIGHT. Internal audit contributes to the basis by which decision-makers achieve oversight and control of their organizations, apply sound risk management, target their attention to areas in need of improvement and demonstrate accountability. Accordingly, internal audit takes a disciplined, evidence-based approach to determining whether or not assurance can be provided that key systems and processes are appropriately designed and are functioning as intended.

ADVISORY SERVICES. As an adjunct to the assurance role, and within their sphere of expertise, internal auditors will also provide advisory services to their organizations. In this respect, internal auditors are also expected to offer solution-oriented recommendations

THE ROLE OF COMPLIANCE

Compliance is typically described as the process of adhering to obligations derived from laws, regulations, industry and organizational standards, contractual commitments, corporate commitments (e.g., social responsibility statements, corporate filings), values, ethics, and corporate policies and procedures. Similar to internal audit, the compliance function plays a critical role in providing information to the board and other roles across the organization that contribute to good corporate governance.

The existence of the compliance function is strongly suggested by regulatory bodies and enforcement organizations such as the United States Department of Justice, The Basel Committee on Banking Supervision, and the UK Financial Services Authority. Regardless of the industry, the role of compliance is becoming increasingly important as government and industry regulation expands and enforcement becomes more rigorous. Central to the role of compliance is the management of compliance risk; the risk of legal of regulatory sanctions, material financial loss, or loss to reputation.

While the role of the compliance professional varies by industry and the types of regulations that must be addressed, there is a common set of duties that is required of most compliance professionals. These can be broken down into four major categories: tracking and assessing regulations, developing and implementing policies, providing education and guidance, and monitoring, auditing, and documenting.

IDENTIFY, TRACK AND ASSESS REGULATIONS. Compliance officers are responsible for understanding what regulations are in force or emerging, and how they apply to the company and its operations.

DEVELOP AND IMPLEMENT POLICIES. Organizations needs to decide what specific measures are required for compliance and implement them throughout the organization. Implementation methods may include codes of conduct, new procedures and controls, and training and communication. A policy is a document that establishes rules for expected behavior of individuals, processes, and/or relationships. Policies are typically high level and strategic, they set the tone, context or intent and are relatively short by nature. Procedures are documents that provide an established or official way of complying with a policy.

EDUCATE AND ADVISE. The compliance function is responsible for establishing written guidance to staff on the appropriate implementation of compliance laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

MONITOR, AUDIT AND DOCUMENT. The compliance officer needs to make sure that policies and procedures are being followed and that compliance efforts are being clearly documented. In this monitoring and enforcement role, disciplinary actions must be sufficient to send a clear message that failure to comply with policies will be met with adverse consequences.

CONNECTION POINT: THE BOARD OF DIRECTORS

Although the roles of internal audit and compliance have diverse job functions and requirements, these two professions find themselves connected throughout the GRC lifecycle. A strong connection point between internal audit and compliance is the relationship with the board audit committee. Both audit and compliance take direction from the board and in simple terms, both functions serve a similar master.

As stated earlier, the function of internal audit in most every case has a direct reporting line to the board's audit committee. In many organizations, the chief audit executive reports to the head of the audit committee as well as a senior member of the leadership team. The work product of the internal audit team is a set of documents that are assembled as the board audit report and a set of documents that comprise the enterprise assessment of risk of the organization.

Government regulations and many industry regulatory organizations have pushed companies to have independent chief compliance officers (CCOs) who report to the CEO. However, the prevailing wisdom is that the compliance function should be organized according to a company's specific situation and that a compliance-oriented culture is as important as a specific structural solution.

What is not in dispute is that compliance oversight is an increasing burden for boards. While some boards are creating separate compliance committees, for many organizations the responsibility for compliance at the board level falls to the audit committee or one of their subcommittees. Audit committees hear frequently from the compliance officer, and they are interested in how they might engage more deeply on compliance issues.

Both the internal audit and compliance functions have accountability for assessing and reporting specific risks of the organizations and the independence required for board reporting relationship. With this connected reporting relationship, it is critical that compliance and audit leverage a common language of risk and control and provide transparency in their reporting to provide the most cohesive and coordinated information flow to management and the board.

CONNECTION POINT: SETTING THE TONE AT THE TOP

Extending from the common relationship with the board is the fact that internal audit and compliance play a critical role in the establishment of the culture of control and compliance within the organization. The compliance culture encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an organization's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

These high level internal objectives are often referred to as the tone at the top. The right tone at the top involves a system of organizational integrity where the business organization has a set of guiding values that are understood, and support ethically sound behavior by all employees. These ethical values are the responsibility of all employees, not just the internal auditors or compliance official's.

Best practice standards and controls suggest that the tone and culture set by management has a trickle-down effect on employees. If top managers uphold ethics and integrity so will employees. But if upper management appears unconcerned with ethics and focuses solely on the bottom line, employees will be more prone to commit fraud and feel that ethical conduct isn't a priority. In short, employees will follow the examples of their bosses.

The board's role is to promote a top-to-bottom compliance culture that is well-communicated and incorporated into the organization's day-to-day operations by senior management. A strong compliance culture is evidenced by the extent to which employees work together both to raise concerns about compliance risks and to design and establish effective controls. The presence of an independent internal audit function and the recognition that this group will continuously monitor and assess compliance with the standards outlined by the board plays a critical role in establishing the culture and tone.

Compliance is a primary steward of the tone at the top as they create a corporate code of conduct and the supporting policies that provide a framework for establishing an effective compliance environment. Corporate codes of conduct are policy statements that define ethical standards for behavior. This should include statements that prohibit certain kinds of conduct, broad statements on values and objectives, and messages on how a company does business. The compliance team is accountable for the creation, communication, education, and sign off of the corporate code of conduct.

Through the coordinated efforts of establishing and communicating a corporate code of conduct and putting in to place the appropriate policies, controls, assessments, and audits of these assurance elements, internal audit and compliance teams jointly deliver on the management of the compliance culture.

CONNECTION POINT: RISK MANAGEMENT

Risk management, assessment and communication are part of a process cycle for both internal audit and compliance. Risk management refers to the design and implementation of actions and remedies to address risks through a consideration of potential treatments and the selection of the most appropriate course of action. Both internal audit and compliance play a fundamental role in the risk management activities of an organization.

A primary role carried out by both professions is that of performing risk assessments. Risk assessment is a key analytical tool to identify and assess the extent of a likely hazard and to estimate the probability and consequences of negative outcomes for humans, property or the environment. Risk assessments are typically conducted on regulations, policies, processes, strategies, and other attributes of organization.

For internal audit, risk assessment is an activity that is a requirement that is outlined by the professional practices framework of the Institute of Internal Auditors. According to these professional standards, internal audit must evaluate the effectiveness and contribute to the improvement of risk management processes in the firm. This includes evaluating risk exposures relating to the organization's governance, operations, and information systems. With this professional charter, internal audit in many organizations is the primary owner for conducting the enterprise assessment of risk and the owner of the risk management function.

Risk drives the agenda of many compliance departments as well. While the focus of internal audit is on all types of risk across the enterprise, the compliance function focuses on regulatory and compliance risk. With a significant inflow of regulatory requirements, compliance departments typically employ a discipline of risk assessment to manage the prioritization of compliance activities. These risk assessments dictate where the compliance department spends its limited resources, allocates staff, and conducts day-to-day operations.

In addition to using risk assessments for prioritization, compliance professionals also manage compliance risk. Compliance risk can be defined as the risk of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value that arises when a organization fails to comply with laws, regulations, or the standards or codes of conduct of self-regulatory organizations applicable to the organization's business activities and functions

Because there is some potential overlap in risk assessment activities, coordination of planning efforts between audit and compliance typically improves the risk assessment results thereby benefiting both functions as well the organization. Also critical to the connected activity of risk management is the use of a common language of risk and methodology for assessment and reporting between these two professional functions.

CONNECTION POINT: MONITORING AND TRACKING

Although both internal audit and compliance are evolving beyond that of corporate policing, both functions play a critical and complimentary role in monitoring the internal processes, controls, risks, and policies of and organization. Fundamental to the role of internal audit is the responsibility for auditing and monitoring.

Auditing can be characterized as process of obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria. In comparison, monitoring is more of a point in time activity to determine whether internal controls over processes, risks, and policies is operating effectively and reports are reliably and accurately prepared. For both of these activities, internal audit is involved in determining the areas to focus on (audit plan) and the criteria in which to raise issues (risk tolerance) related to the occurrence of fraud, embezzlement, theft, operational performance, and recommend controls to prevent or detect such occurrences.

If the result of an internal audit activity is the breach of a compliance issue, in many cases the internal audit team will turn over the issue to the compliance team for further investigation. Compliance has the expertise to deal with legal and regulatory violations and is prepared to handle matters to minimize legal risk. As it relates to monitoring, the compliance function typically takes a more narrow scope. In many organizations, compliance is accountable for establishing feedback mechanisms for employees to confidentially report compliance violations. These hotlines or other reporting systems serve as the means for compliance to monitor reported issues and conduct investigations on those items reported.

Central to both of these processes is the requirement for transparency in reported issues and corresponding follow up remediation plans. Centralized issue tracking provides the capability to track outstanding issues and action plan recommendations from internal audit, compliance and business process owners. By leveraging a common system and process, audit and compliance teams are empowered to be in lock step on the material issues facing the organization and track the steps for follow up and correction.

SHOULD COMPLIANCE AND INTERNAL AUDIT BE A COMBINED FUNCTION

Although there are many overlaps in job responsibilities, there is a strong argument to be made that compliance and internal audit remain separate functions. The fundamental argument for separate functions centers on the concept of independence. This concept suggests that in order to maximize the effectiveness of both assurance functions, they should not be placed in a position where there is a possible conflict of interest between their core responsibilities and any other responsibilities they may have.

Independence can be achieved by each function having formal status within the organization, a designated leader and executive in charge, and clarity from the board on duties and reporting requirements. As part of this independence, the compliance department, similar to all other parts of the organization, is subject to oversight and review by internal audit

Regardless of how your organization structures these important governance functions, corporate compliance and internal audit are most effective when they work in a collaborative manner, one that includes joint planning and coordination of risk assessment efforts to review for overlapping areas, coordinated reporting to management and the board on significant issues, and shared involvement in key compliance related committees, task forces and other working groups. Understanding the similarities and differences as summarized in this whitepaper should help to ensure such collaboration is deliberate and effective.

OPTIMIZING THE COLLOBORATION BETWEEN INTERNAL AUDIT AND COMPLIANCE

Although internal audit and compliance are separate functions, it is clear that they share many common connections points. To ensure an effective coordination of activities between these two functions, it is optimal that these assurance groups leverage a common language of risk and control, common methodologies, and leverage a common technology solution.

A comprehensive assessment of risks and controls requires the use of standard risk and control taxonomy. Effective collaboration requires that risks and controls be classified and reported against standard models on which the internal audit and compliance groups agree. The benefits of utilizing a common language for risks and controls are far reaching and include:

- Improved reporting throughout the organization
- Consistent coverage where all risks are considered
- Improved business performance – risks explain performance gaps
- Better, risk-based decision making
- Less external oversight and audits where controls are standardized

A common methodology for compliance and internal audit leads to an agreement about what information must be gathered and how it will be gathered. This includes defining the risk types that will be assessed and the risk thresholds that will drive the depth and quality of the review. An effective compliance program will define the thresholds beyond which risks would require mitigation or additional management, what controls require testing, and rules governing the creation of issues for reporting and resolution.

Finally, organizations on the leading edge of managing compliance depend on comprehensive information technology that relies on data from multiple assurance groups including risk management, internal audit, policy management, and compliance.

When a company uses different technology solutions from different vendors to manage internal audit and compliance efforts, it runs the risk of inconsistencies and inefficiencies that may lead to unnecessary high costs. Multiple systems with multiple deployments cause conflicting versions of the truth. A standardized solution resolves these problems and establishes a single version of the truth for the entire enterprise.

Standardized technology also provides greater efficiency, improves collaboration, and reduces the time and resource costs associated with compliance processes. Investment in technology enables organizations to break down the walls between internal audit and compliance groups and provides expanded value as organizations deploy the software across the enterprise. By unifying the many business process owners, a comprehensive software solution can eliminate information silos, redundant data entry and improve information transparency and communication.

ABOUT THOMSON REUTERS GRC

Thomson Reuters Governance, Risk and Compliance (GRC) business unit provides comprehensive solutions that connect our customers' business to the ever-changing regulatory environment. GRC serves audit, compliance, finance, legal, and risk professionals in financial services, law firms, insurance, and other industries impacted by regulatory change.

The Thomson Reuters Accelus™ suite of products provides powerful tools and information that enable proactive insights, dynamic connections, and informed choices that drive overall business performance. Accelus is the combination of the market-leading solutions provided by the heritage businesses of Complinet, IntegraScreen, Northland Solutions, Oden, Paisley, West's Capitol Watch, Westlaw Business, Westlaw Compliance Advisor and World-Check.

Learn More
Email: enterprisegrc@thomsonreuters.com
Visit: accelus.thomsonreuters.com