INTERNAL AUDIT GRC SERIES: CHALLENGES AND SOLUTIONS TO ALIGNMENT

Internal Audit (IA) is one of many organizational groups whose mission is to assess risks, evaluate controls, raise issues and improve processes. Other oversight functions with similar charters include Enterprise Risk Management, Security and Compliance. With some common objectives and not-so-common approaches, there is value in aligning methodologies, resources and results. However, since IA needs to maintain a certain level of independence, how does IA strike this balance? This white paper discusses the dilemma as well as practical ways alignment can occur while maintaining independence.

CONTENTS

RSA PERSPECTIVE

THE NEED FOR INDEPENDENCE

Internal auditors have an essential need for independence. In fact, it is a requirement for the profession. The Institute of Internal Auditors (IIA) Code of Ethics states: “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.” One of the IIA Code’s principles on objectivity states: “Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.” This independence begins at the highest levels in the chief audit executive’s reporting relationship to the organization’s board of directors and filters down to all levels below.

The profession revolves around this concept of independence, which is further influenced by such factors as having to work closely with regulators or external auditors, who must exercise even more independence from client management. This independence is relevant as internal audit (IA) groups strive to gain the confidence of their external auditors in order to strengthen the relationship, encouraging external audit to rely more and more on the work of IA.

Another factor driving independence is events, such as the corporate scandals of the early 2000’s and resulting regulations such as the Sarbanes-Oxley Act of 2002, and the need for IA to maintain its credibility as separate from company management. However, another result of this and other increased regulation is that internal control oversight requirements have increased and the number of oversight functions has multiplied. This is occurring across industries such as financial services, and primarily among publicly traded companies. Increasingly, oversight is occurring in less-regulated sectors as well.

In this new world, IA is no longer the only oversight function in an organization. IA's need for independence has conflicted with the need to coordinate, or at least communicate, with other oversight groups to ensure some level of synchronization. Two primary oversight areas of most concern to IA are the management of risks and monitoring of controls. Examples of groups monitoring and testing controls, in addition to IA, include internal control and compliance organizations. In addition to these internal control groups is the expansion of risk management functions, including enterprise risk management (ERM) and operations risk management (ORM).

IA was historically the source of broad risk evaluation while other risk groups, such as credit and fraud, focused on their specialized areas of risk. However, similar to control oversight, risk oversight functions have also increased, adding to the robustness of risk information and to the confusion over coverage, scope, approaches and priorities. This has not been an easy transition, with separate organizations, varying approaches and levels of maturity, different toolsets and sometimes competing priorities.

A question in the minds of many IA groups is what functions should IA perform versus what other oversight groups should do? Gartner also raises this dilemma in their September 13, 2013 research report entitled, “How to Differentiate and Align the Roles of Security and Internal Audit.” Gartner reported that there is confusion regarding the potential overlap between the roles of information security and IA, which leads to conflict and dysfunctional information risk management.

BEING A STRATEGIC PARTNER

Alongside the need for independence is a competing priority for IA to be a "partner" with management. As directed by IIA standards, IA reports to the Board of Directors and senior management. To contrast the Code of Ethics quoted earlier: "Internal auditing is an independent, objective assurance and consulting activity…." The challenge for IA groups is how to strike the right balance between independence and partnership.

The formalization of governance, risk and compliance (GRC) as an operating framework has begun to force the discussion around how IA and other oversight functions can work together toward common goals, and has increased the opportunities for IA to partner with management.

One example is the RSA Archer GRC Reference Architecture [Figure 1] which represents the alignment of organizational elements and processes under the GRC framework. The framework strives to organize the functional and topical elements of GRC with some tangible end results. By aligning approaches, programs, resources and efforts of interrelated GRC processes, this can result in improvements in visibility, efficiency, accountability and collaboration, which are needed to optimize business outcomes. (See whitepaper on the RSA Archer GRC Architecture for more information.)

Alignment of these varied GRC functions, processes, approaches, methodologies, goals, objectives, programs and resources takes many forms. This could include adopting similar risk assessment approaches and methodologies or combining control testing. Alignment is an important activity as its benefits include better resource utilization, improved coverage of risks and controls and other synergies. An important step in alignment includes identifying and assessing the differences and challenges between the aligning functions. As these groups have introduced themselves, compared their goals, approaches, resources and structures, this has highlighted redundancies and gaps.

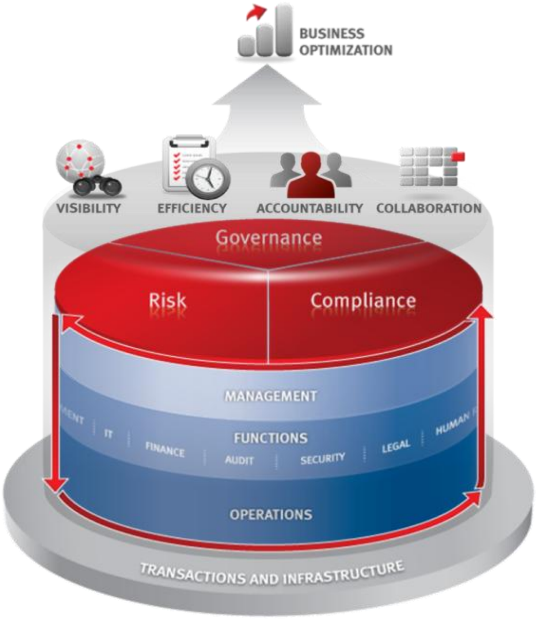

Figure 1: RSA Archer GRC Reference Architecture

THE GROWING PAINS

The Tuckman Model of Group Development [Figure 2] illustrates that it takes time, effort and pain to align and be productive as a combined function, or team. The alignment process evolves from simply bringing similar groups, functions or processes together (forming); to determining the best approach moving forward (storming); to aligning, and ultimately performing efficiently (norming and performing).

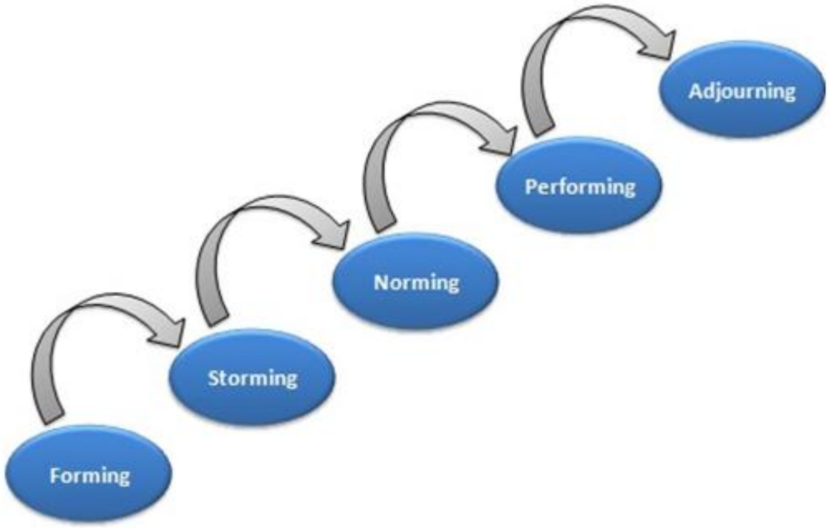

Figure 2: The Tuckman Model of Group Development

The RSA Archer GRC Architecture discusses benefits of a GRC approach and categorizes them into four areas – Visibility, Efficiency, Accountability and Collaboration. Before resulting in benefits, these attributes start out as growing pains during the alignment process.

- Emerging Visibility – GRC groups begin to identify other oversight functions performing similar activities, yet with different and sometimes competing priorities. Initial reactions are to protect the empire instead of aligning with these groups. It is new to everyone and further complicating matters, political, geographic or financial (e.g., funding) factors stand in the way of alignment.
- Inefficiency – With increased visibility into these multiple oversight groups comes the realization that duplication exists. This equates to inefficiency due to duplicate resources, processes and misaligned objectives. In some cases, these groups may be working against each other, however unintentionally. As these factors come to light, the redundancies and inefficiencies become exposed.
- Lacking Accountability – Closely following the visibility of these separate GRC functions is an analysis of their objectives. Looking at the whole often results in the disclosure of gaps or areas no one group is focused on. This could be certain risk categories, control exposures, geographies or process areas. The question then becomes which group needs to address these gaps.
- Lack of Collaboration – The question quickly becomes "why aren't these groups working together?" and "how much time, resources and money have we been wasting doing the same things?" This lack of collaboration also exposes more gaps and lacking accountability.

The question for IA is how closely to align their approaches, thresholds and decision criteria with others. A simple example is that IA conducts an annual audit universe risk assessment (AURA) by identifying potential auditable entities, assessing their criticality via the AURA, and determining for which entities to perform audit engagements. Other groups, such as ERM, also perform risk assessments which drive activities such as risk evaluation, gap identification and remediation plans. It stands to reason that IA and ERM should align at least some level of their assessment approaches in order for risks to be evaluated under the same lens, and for the two groups to leverage each other's results. Other intersections exist where IA could leverage other groups' work and vice versa. Automated tools can help in this process as approaches can be applied more consistently, and results along with supporting documentation are more visible and accessible. Multiple groups can access and leverage the information and alignment is better achieved.

Another factor in this dilemma is the use of tools and how to align them across these groups. If a common technology solution is used, IA must weigh the benefits of sharing information against limiting access to such areas as privileged and confidential audit projects.

THE RIGHT BALANCE

The "right balance" is a relative term that depends on the organization and the industry, and its place on the maturity spectrum, regulatory issues, management priorities, and many other factors. IA must continue to strike a balance between independence and partnership. In their decision process, IA needs to realize that business requirements and resulting risks are becoming more complicated and far-reaching, and the organization needs IA's perspective and recommendations. To accomplish this in addition to its audit plan of scheduled audits, it is imperative that IA coordinates with other existing and emerging risk and control groups, to the point that IA seeks these functions out, evaluates their objectives, and determines how they should coordinate with them.

As the Internal Audit and GRC Integration Model [Figure 3] represents, there are emerging topics that IA should also factor into discussions, and some of these may be better addressed by other oversight or specialist groups. Communication with regulators and external auditors will provide additional guidance to IA as to areas they feel could be aligned or maintained separately.

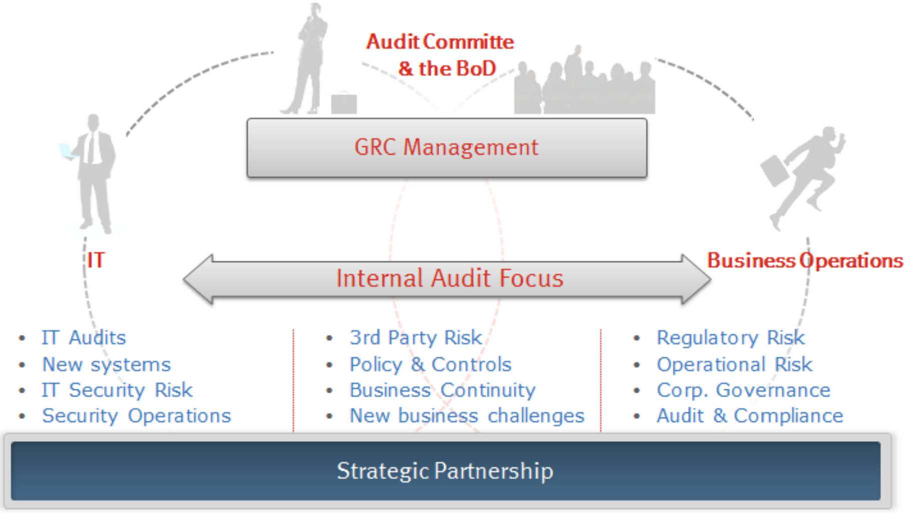

Figure 3: Internal Audit and GRC Integration Model

One way IA has attempted to accomplish this balance of independence and partnership is by differentiating the types of audits, reviews and projects that they perform. For example, a regularly scheduled audit as required by their AURA or by regulatory requirements may be categorized as an "independent" audit engagement. This risk-based or regulatory audit typically concludes with an audit rating, formal audit report and findings. Conversely, management requesting IA to participate in the review of a special topic might be categorized as consulting activity. A management request or consulting engagement may also conclude with a report, but without a rating and with less formal recommendations. IA also often allocates a portion of their available resource hours for management requests.

More requests for IA's time and expertise are occurring as management recognizes the strategic perspective and background of its internal auditors and relies more on assistance for certain topics. For example, IA is frequently asked to work with management on such projects as mergers and acquisitions, third party reviews and product launches.

PRINCIPLES IN PRACTICE

A global financial services company dealt with this dilemma in a proactive and creative way. An Internal Control (IC) function was tasked with evaluating controls in its charge card business unit. The IC group's review procedures were very detailed and because of their focus in that one business area, they had developed the level of knowledge and expertise that made them very familiar with the control and operating activities of the business unit. This credit card unit often was included in IA's AURA and resulting audit plans due to the risk and criticality of the area.

IA made the decision that instead of performing full audits in the area, they would work closely with the IC group and rely on its control evaluation and testing work. IA would select a sample of audits performed during the year and review the work of the IC group and in some cases, recreate some of the testing activity if necessary. If discrepancies existed, IA and the IC group would resolve them. Finally, IA would reference this arrangement in its audit report and reporting to management and the audit committee.

CONCLUSION

IA and enterprise GRC programs should look to remove as many boundaries between them as possible. However, IA must decide where boundaries should exist to enable them to maintain an appropriate level of independence. As the organization proceeds down the path of alignment and moves ahead on the spectrum of group development, the growing pains of alignment will turn into realizable benefits, such as:

- Visibility – Disparate groups begin to understand each other's activities and priorities better. Higher value opportunities for alignment present themselves.
- Efficiency – Typical GRC topics better managed, and process inefficiencies come to light that are better addressed by process improvement activities.
- Accountability – Alignment results in efficiency and finding areas that were previously falling through the cracks. This enables the organization to assign accountability at all levels, from risks to processes to findings.
- Collaboration – The old proverb "many hands make light work" comes into play here as opportunities to better divide and conquer emerge. Approaches such as risk assessment methodologies can be improved due to a balanced perspective from ERM, IA, legal and others.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, **CONTACT** your local representative or authorized reseller—or visit us at www.EMC.com/rsa

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice