**Introduction**

Internal Audit (IA) teams can help their organizations improve their levels of effectiveness and efficiency by monitoring compliance with regulations, laws, policies, and procedures through reviews and analyses of the organization’s practices, services, and activities. However, IA faces a rapidly changing regulatory and business risk landscape with an internal audit strategy that is not always positioned to adjust and meet these changes. Existing audit approaches are focused on compliance and more reactive than proactive. IA is now being asked to incorporate dynamic risk planning into its approaches.

Today’s methods, tools, and expertise are positioned around point-in-time, static audit plans that inhibit transitioning into a risk-based approach. With decentralized documentation captured in multiple tools and systems that are difficult to integrate, there is often static reporting and limited coordination of objectives among risk, compliance, and audit groups. It becomes time consuming to report to the Audit Committee and senior management when information is dispersed throughout siloed systems that are out-of-date as soon as the Audit Report is completed.

These siloed audit systems often make it difficult to capture and distill integrated risk and control information into meaningful analysis. A lack of visibility into findings generated by other functions creates a difficult and time-consuming challenge for Internal Audit to track the status of findings and assure that risk mitigation efforts are occurring, and factor this into their audit planning.

In order to enhance Internal Audit’s value within the organization, they must take a coordinated, risk-based approach. Consolidating audit activities into one system that provides a consistent view along with other risk and compliance functions will:

- Improve communications with risk and compliance teams
- Enable IA to place more reliance on risk and control evaluation performed by other groups
- Reduce audit costs and external audit fees by creating efficiencies and improving documentation
- Allow auditors to focus on strategic work that helps grow the business
INTERNAL AUDIT CHALLENGES

Internal Audit teams cannot focus on helping the business evaluate new risks and opportunities because they are spending too much time evaluating past performance of controls. According to PwC’s 2013 State of the Internal Audit Profession Study, “Last year, many internal audit functions were struggling to maximize the impact of their contribution and were therefore in danger of losing relevance to other risk and compliance functions within the organization. Twelve months later, while we continue to see leading functions delivering at a high level, the majority of our survey respondents have made minimal progress.” Internal Audit’s time is focused on repetitive, compliance-driven audit testing and as a result, teams are not positioned to implement the more risk-based approach increasingly expected by regulators, governing bodies, and executives.

Let’s look at KPMG’s 2014 Global Audit Committee Survey. 80% of survey respondents said that internal audit’s role should extend beyond the adequacy of internal reporting and controls to include other key risks facing the business. Unfortunately, today’s internal audit teams lack visibility into other risk and compliance functions. This creates redundancy and gaps in the team’s coverage of key risks and underperforming controls, which can often lead to increased audit costs and an overwhelmed internal audit team.

Adding to this dilemma is a “documentation overload.” For example, on January 1, 2013, the cumulative paperwork burden of the U.S. was 10.22 billion hours, and it has continued to grow according to Sam Batkins, director of regulatory policy with the American Action Forum. Despite significant cuts to costs and paperwork burdens, net regulatory costs increased by $112 billion and the cumulative burden continues to climb.
THE IMPACT OF THE INTERNAL AUDIT STATUS QUO

Internal Audit has historically been the source of broad risk evaluation while other groups, such as credit and fraud, focus on specialized areas of risk. However, risk oversight functions have increased, adding to the robustness of risk information and creating confusion over coverage, scope, approaches, and priorities. Organizations today have varying approaches and levels of maturity, different toolsets, and sometimes competing priorities. A question from many IA groups is: what functions should IA perform versus what other oversight groups should do?

Furthermore, a static audit universe risk assessment often prohibits Internal Audit from adjusting their audit plan to react to new risks and business concerns. With decentralized documentation captured in multiple tools and systems that are difficult to integrate, there is often static reporting and limited coordination of objectives among risk, compliance, and audit groups. The lack of visibility into findings generated by other functions creates a difficult and time-consuming challenge for Internal Audit to track the status of findings and risk mitigation efforts. This can make it time consuming to report to the Audit Committee and senior management when information is dispersed and out-of-date.

TAKE INTERNAL AUDIT TO THE NEXT LEVEL

Organizations sometimes consider Internal Audit the last line of defense when it comes to compliance. When IA teams work in a silo and fail to communicate with the rest of the business, it increases the burden of compliance and raises the risk of overlooking important findings.

By incorporating a risk-based approach and collaborating with risk and compliance business partners, IA teams can integrate the appropriate view of risk when evaluating critical areas of the business. This also provides time to focus on strategic business initiatives that demonstrate value to the organization.

How can IA gain approval at the executive level?

The key to solving IA challenges often lies at the executive level. This year’s State of the Internal Audit Profession study by PWC finds that 68% of board members believe internal audit contributes significant value. Despite the clear value of the IA team, some organizations still use complex spreadsheets and outdated systems to manage their audit process. These tools fail to provide a comprehensive view of risk, making it difficult to complete audit engagements quickly and efficiently, leading to increased costs and lower quality of audits.

What if the IA team could rally its risk and compliance counterparts, and together tackle the most pressing risks and controls to the business?

Business, risk, compliance, and audit groups should be able to use one system to coordinate their work while maintaining the appropriate level of independence. This would enable IA groups to independently and objectively evaluate the quality and effectiveness of the controls they deem most critical, while leveraging the work of other risk and compliance counterparts. In addition, this would improve transparency and create a higher level of trust between the groups.
What if IA could partner with the organization’s risk and control teams and adjust their audit plans based on a dynamic view of operational risk?

Internal Audit must partner with its risk and compliance counterparts, sharing operational risk and control data that allows the group to adjust their audit plans based on the organization’s business priorities and latest assessment of operational risk.

What if Internal Audit could simplify and automate the audit process?

Organizations always strive for efficiency and cost-reduction methods. Internal Audit would benefit from one system where they could perform their entire audit process. This would eliminate the need for multiple systems, decrease inconsistencies in information, and reduce time and frustration.

THE RSA ARCHER AUDIT MANAGEMENT APPROACH

RSA Archer Audit Management puts organizations in control of the complete audit lifecycle, enabling improved governance of audit-related activities, while also providing integration with risk and control functions. The solution enables Internal Audit to use a consistent, risk-based audit approach to drive greater efficiency in the execution of the audit plan. Features include risk-based prioritization of the audit universe, resource scheduling and staffing, management of audit engagements, creation of audit reports, and tracking of findings and remediation plans. With RSA Archer Audit Management, organizations can transform the efficiency of the Internal Audit department, complete better-scoped audits more quickly, and decrease external audit fees.

Adjust audit plans and projects based on a dynamic view of risk

RSA Archer offers out-of-the-box best practices to partner with risk and compliance counterparts. These best practices allow IA teams to share operational risk and control data that enables them to align audit plans and prioritize their efforts based on the organization’s business priorities and latest assessment of operational risk.

Recognize interdependencies and analyze metrics

The RSA Archer Audit Management solution provides fluid risk identification, giving Internal Audit the ability to compare their view of risk to management by using comparative risk metrics at a macro (audit plan) or micro (audit engagement) level. Teams can easily integrate with third-party systems to enable analysis of critical data and metrics. Ultimately, Internal Audit can obtain transparency into the organization’s risk management program and capture real-time changes that may warrant adjustments to the audit plan.

Simplify and automate the audit process

Internal Audit can document issues and remediation plans or leverage those created by other risk and compliance management teams or other business functions. This allows the team to streamline the findings management process, focus on the most critical issues, and report what is most important to the management team and board of directors.
Facilitate interactions across the business

All business and audit issues can be catalogued within one central system to provide a holistic view of their significance and remediation status. The flexible RSA Archer platform allows organizations to tailor Internal Audit, risk, and compliance processes to their unique requirements without custom code or development resources. Audit programs are directly linked to key strategic objectives such as SOX compliance, risk management, and regulatory obligations.

Rally the risk and compliance counterparts and together tackle the most pressing issues and remediation efforts

All issues, whether they are raised by Internal Audit, other risk and compliance teams, or management, can be housed and catalogued within one central system to provide business workflow and a holistic view of their significance and remediation status by all business teams. This enables Internal Audit to better evaluate the current status, quality and effectiveness of the organization’s controls while summarizing and prioritizing critical results to the audit committee, as well as to risk and compliance counterparts. This establishes greater transparency and a higher level of trust throughout the organization.

ASSESS RISK AND MANAGE THE AUDIT PLAN

RSA Archer Audit Management enables IA groups to identify the universe of all auditable entities, perform Audit Universe Risk Assessments, and compare to management’s assessments of risk. Once the team has performed all necessary risk assessments, they can create and approve the Audit Plan, scope the entities that will be audited, schedule the audits, manage resources, report to the Audit Committee, communicate with management, and monitor the overall status of the audit plan on an ongoing basis.
PLAN AND EXECUTE AUDIT ENGAGEMENTS

After Internal Audit has determined the scope of the Audit Plan, they can perform audit testing, document findings, draft the audit report, create and manage work papers, and document and manage the lifecycle of work paper review notes all in an online or offline mode from the RSA Archer Audit Managements solution. Scoping an engagement means determining which areas will be audited. Management can define the scope of the engagement through the same relationships that exist for the audit entity such as business processes, policies, authoritative sources, or risks. This scoping will drive what testing the audit team will perform as part of any fieldwork activity.

The IA team can quickly identify weaknesses in how the business manages risk and provide recommendations to drive risk management consistency, control testing, and findings management across the organization. This collaboration enables IA to be actively involved in strategic initiatives throughout the organization.

RSA Archer supports a wide range of risk and compliance use cases. The Audit team can rely on the results of other related use cases, metrics, and results from functions across the business. Because this information is all stored within a single system, the IA team does not have to juggle multiple systems, data stored in emails or piles of paper, or documents spread throughout multiple facilities.
**SCHEDULE AND STAFF THE AUDIT TEAM**

With new comprehensive scheduling capabilities, IA teams can use RSA Archer Audit Management to determine the audit engagement’s scope, as well as schedule and staff resources for the audit. Internal Audit can track team member availability and schedules that include external resources, track staff credentials, schedule audit engagements and team resources, report on staffing and scheduling gaps, and monitor utilization.

**ACCESS CUSTOM DASHBOARDS**

What if IA could reduce the burden of external audits and regulatory scrutiny? With out-of-the-box workflow, user access roles, dashboards, and reports for external partners (e.g., external auditors), different groups can independently access the appropriate information, such as the audit plan, scoping decisions, and engagement documentation. This significantly reduces the amount of time that IA spends supporting and providing external groups documentation. This also increases the organization’s reliance on the work performed by Internal Audit.

The real-time dashboards of RSA Archer Audit Management help summarize critical information for key users including the audit committee, chief audit executive, management, Internal Audit managers and staff, and external auditors.
CONCLUSION

About half of the Internal Audit departments around the world are failing to deliver strategic leadership, coordinated assurance and other services that their stakeholders need. Internal Audit teams inefficiently use their resources due to having multiple tools and systems, with limited coordination of objectives among risk, compliance, and audit groups. The typical static Audit Universe Risk Assessment limits IA from easily adjusting the audit plan when new risks and business concerns arise. Furthermore, IA teams spend too much time assigning and managing their audit resources and coordinating with external audit.

RSA Archer Audit Management puts Internal Audit teams in control of the complete audit lifecycle. With this fully integrated solution, organizations can:

- Optimize the audit lifecycle by using one system that integrates and coordinates all relevant audit data.
- Document all issues and their associated remediation plans to ensure that management teams agree on the most critical issues and you report what is most important to the Board of Directors.
- Identify weaknesses in how your business manages risk, and recommend ways to drive consistency in risk management, control testing, and findings management across the organization. RSA Archer enables Internal Audit to be more actively involved in strategic initiatives throughout the business.