Lessons From Winnie the Pooh on Risk Assessments

Using an integrated GRC approach to risk assessments and risk-based audit planning

This illustration is part of the OCEG GRC Illustrated Series. You can download it and earlier installments at www.oceg.org/illustrations or from "GRC Illustrated" in the toolbar "News" pull-down menu under "Topics" at www.complianceweek.com

By Jason Mefford

I have spent almost twenty years as an auditor; externally, internally, or training auditors. When discussing the subject of risk assessments and annual audit plan development, I am reminded often of a quote from Winnie the Pooh.

"Here is Edward Bear, coming downstairs now, bump, bump, bump, on the back of his head, behind Christopher Robin. It is, as far as he knows, the only way of coming downstairs, but sometimes he feels that there really is another way, if only he could stop bumping for a moment and think of it."—*A. A. Milne*.

Mefford

How much of the time do we feel we are hitting our heads when doing risk assessments and annual audit plans, realizing there is a better way, but not knowing how to change? We do the same things over, and over again, just like Winnie the Pooh coming down the stairs.

Internal auditors need to use a risk assessment to develop their annual audit plan. The Institute of Internal Auditors (IIA) standard 2010.A1 states "The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually."

I am, however, still amazed at how many of those in various internal audit activities believe the standard means they must be the one who performs the risk assessment. In fact, I have observed one of my clients where at least six different risk assessments are performed by different functions throughout the organization. This is not only confusing to everyone, but also a big waste of time and resources. If your organization already has a competent risk-management function, consider using the risk assessment prepared by that group as the basis for your audit plan.

In order to have a truly integrated GRC capability it is necessary for internal auditors to work with other GRC professionals in their organization. They must align their annual audit plan with the organization's objectives, strategies, and initiatives of the other GRC professionals. They must collaborate, coordinate, and align their audit activities with other GRC professionals to increase visibility, improve efficiency, accountability and collaboration.

Another common mistake is developing audit plans based on business units, processes, or internal controls instead of plans focusing on the organization's objectives. I see many auditors creating very similar audit plans year after year.

"The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals," notes the IIA's Standard 2010 – Planning report. Auditors should identify the key actions and controls used by management to reduce the threats (and corresponding risks) to meeting organizational objectives. This is completely in line with the concept of Principled Performance and an integrated GRC approach. Auditors need to take this approach instead of doing the same things over and over again in a Winnie the Pooh fashion.

There are nuances to an integrated GRC capability that will require auditors to plan and perform audits with more input and coordination of others in the organization. Auditors can no longer "go it alone" in their assurance efforts. For this reason, it is beneficial for auditors to get an understanding of GRC concepts by becoming certified as GRC Professionals and understanding the nuances and tools available in auditing GRC activities by becoming certified as a GRC auditor.

As Albert Einstein is famous for saying "Insanity is doing the same thing over and over again and expecting different results." It's time to stop the insanity.

Deepen relationships with other GRC professionals in your organization. Start using the organizational risk assessment as the basis for developing your annual audit plan. Stop relying on a rotational audit approach that focuses on business units, processes, and internal controls. Start developing a plan that truly considers organizational objectives and is integrated with your GRC capability. This is the only way we can stop the insanity and avoid bumping our heads over and over again. ■

Jason Mefford is the President of Mefford Associates and an internationally acclaimed trainer and business coach. He is also the Managing Director of GRC Certify and serves as an OCEG Fellow. Mefford Associates provides business training and coaching to organizations in the areas of ethics, corporate governance, risk management, compliance and internal audit. www.meffordassociates.com

Compliance Week and the Open Compliance and Ethics Group have teamed up to provide readers with this regular illustrated series on governance, risk, and compliance programs. For information on this series and a downloadable version of this illustration, please go to www.complianceweek.com, and select "GRC Illustrated" from the "Topics" pull-down menu on our toolbar.

Maturing Audit Plans and Processes

Historically, the relationship between audit, risk, and compliance capabilities has been shallow—if it existed at all. Less mature audit approaches have addressed regulatory compliance but have failed to use risk management and performance metrics information to scope and efficiently perform audits that are targeted to the entity's real issues. Today, technology enables a more mature approach to audit, using compliance and risk capabilities to improve and define audit plans and processes that bring true strategic advantage.

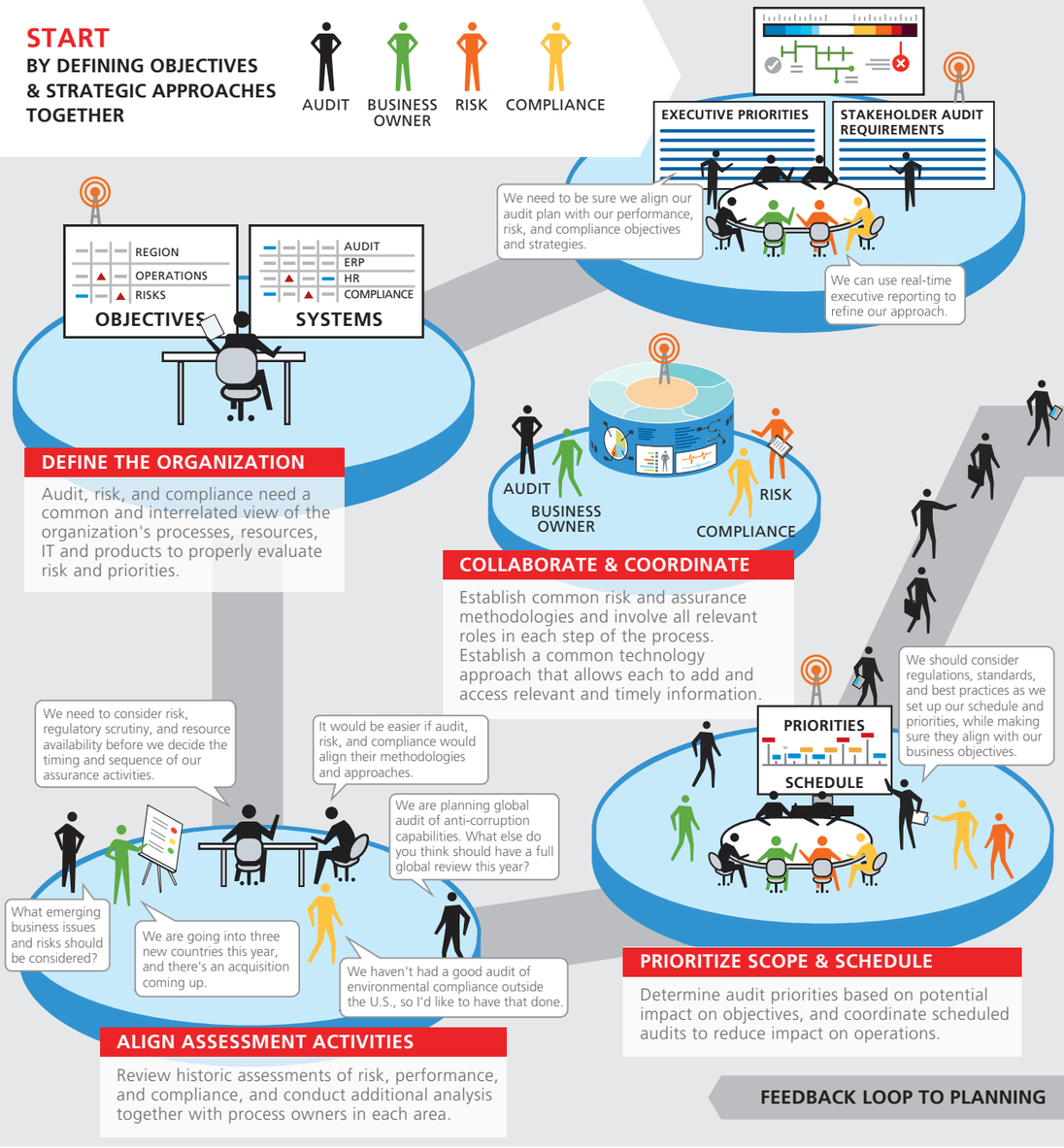
DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM RSA® The Security Division of EMC

1. PLAN
Align audit objectives with the organization's strategic and operating objectives.

START
BY DEFINING OBJECTIVES & STRATEGIC APPROACHES TOGETHER

AUDIT · BUSINESS OWNER · RISK · COMPLIANCE



DEFINE THE ORGANIZATION
Audit, risk, and compliance need a common and interrelated view of the organization's processes, resources, IT and products to properly evaluate risk and priorities.

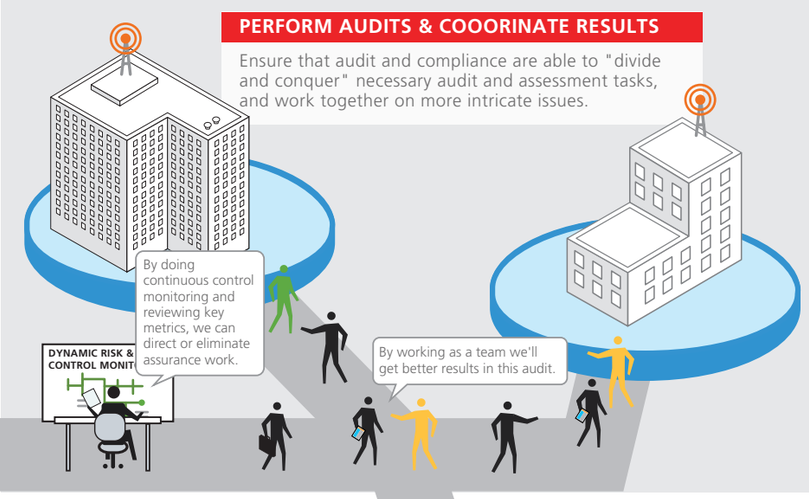
COLLABORATE & COORDINATE
Establish common risk and assurance methodologies and involve all relevant roles in each step of the process. Establish a common technology approach that allows each to add and access relevant and timely information.

ALIGN ASSESSMENT ACTIVITIES
Review historic assessments of risk, performance, and compliance, and conduct additional analysis together with process owners in each area.

PRIORITIZE SCOPE & SCHEDULE
Determine audit priorities based on potential impact on objectives, and coordinate scheduled audits to reduce impact on operations.

2. DO
Coordinate dynamic risk evaluation, continuous control monitoring, and assurance work across audit, risk, and compliance to drive updated and efficient coverage of the risk universe.

PERFORM AUDITS & COOORINATE RESULTS
Ensure that audit and compliance are able to "divide and conquer" necessary audit and assessment tasks, and work together on more intricate issues.

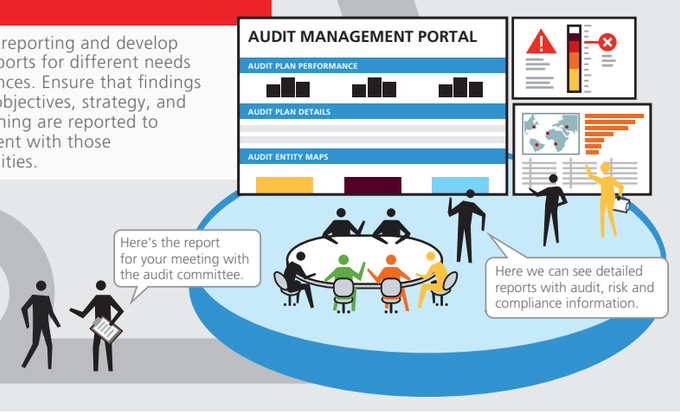


3. CHECK
Manage audit results, issues, and remediation plans through one coordinated approach to drive the best prioritization, resource utilization, follow up, and reporting to executive management.

ANALYZE & ACT ON FINDINGS
Establish combined view of findings in the system automatically with different views for different users and for monitoring.

MONITOR PROGRESS
Monitor action on findings and recommendations.

REPORT
Automate reporting and develop custom reports for different needs and audiences. Ensure that findings affecting objectives, strategy, and audit planning are reported to management with those responsibilities.



FEEDBACK LOOP TO PLANNING

ALIGNING ASSURANCE ACTIVITIES

Removing boundaries between audit and other assurance groups can lead to many benefits:

VISIBILITY
Understanding each other's activities and priorities leads to higher value opportunities for alignment.

EFFICIENCY
Inefficiencies come to light that are addressed by process improvement and standardization.

ACCOUNTABILITY
Areas that were previously falling through the cracks are identified; enabling 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 as opportunities to better divide and conquer emerge.

COMMON MISTAKES

- Establishing a purely rotational approach for every area of audit
- Equally distributing available resources without prioritizing
- Failing to consider scheduling burdens or to create a unified audit plan
- Designing an audit that does not tie to specific objectives and related risks
- Auditing what you know, not what is important based on risk assessments
- Limiting audits based on available resources rather than asking for more

SEPTEMBER 2014 WWW.COMPLIANCEWEEK.COM » 888.519.9200

[AN **OCEG ROUNDTABLE**]

Building a Risk-Based Audit Plan

Switzer: The role of internal audit, especially in large, geographically diverse organizations has become more complex. What are the greatest challenges in developing a meaningful entity-wide audit plan today?

Saint: Risk coverage is among the greatest challenges. Properly creating the audit plan based on an assessment of entity-wide risks and strategic objectives requires a balancing act. We have to balance the cost of audit with the risks of not auditing a risk topic, process, or location. We make that determination in consultation with the audit committee and the management team, gaining alignment with our stakeholders on where we draw the line. Resources are perennially at the top of the internal audit department's constraints—as they are with every business unit in a company. And we in internal audit have to continually assure we have management's buyin to the scope of our work, especially when it's outside the narrow boundaries of financial controls. So to risk coverage, I would add "gaining and maintaining trust and credibility in the audit process and the internal audit department" as ongoing challenges.

Potter: Audit planning is arguably the most important step in the internal audit process because it involves evaluating the organization's risk profile to drive a year's worth of audit activities. Internal audit has undergone seismic changes over the last few years, including a myriad of emerging risk issues still coming that many internal audit groups are not prepared to deal with. The global nature of most organizations introduces intricacies internal audit groups can't address either geographically or topically, raising the question of do we have the right resources to achieve the audit plan? As far as the audit plan itself goes, most internal audit groups need better measurement on whether the plan is covering enough of the company's risk profile, raising another challenge of whether internal audit understands the organization's risk profile well enough, and was the audit plan based on the right evaluation of risk, especially if multiple groups (internal audit, risk management, etc.) evaluating risk might have different methodologies and approaches.

Bayer: To achieve true enterprise-wide assurance coverage, internal audit departments must become better collaborators and contributors. By that I mean that they have to be more open for working with and relying on other oversight functions of the company such as compliance, law, financial risk, and even HR. They should be champions of this collaboration due to their stature and power within the company. In most organizations, internal audit departments have more mature processes and methodologies along with required self-quality assessments. These best practices could be leveraged companywide which will also increase the ability of relying on other risk assessments and audits being performed. It will also achieve greater efficiency with limited resources to focus on "real risk" and areas of "unknown risks" that are most often times the ones that our audit committee and boards are most concerned with.

Switzer: How do you go about defining and prioritizing the auditable entities in your organization?

Potter: The challenge is really getting to an organized and consistent view of the auditable entity universe. For example, does the organization have one common view of how such elements as business units, divisions, business processes, IT infrastructure, and regulatory topics all relate together? Do internal audit, risk, and compliance groups use this same reference architecture to define entities? There can be such a myriad of organizational units, topics, locations, and other entity designations that the question become: Did we cover the universe completely and in a way that lends itself to executing the right audit work? Different slices of the universe (e.g., defining an entity by combining a business process with its applications, or regulatory topics) may escalate or dilute its risk score in the audit universe risk assessment to the point that we inappropriately rank that entity. It not only takes an understanding of the audit entities individually, but how they fit together into the operating fabric of the organization to appropriately rate and rank them. Another key factor is in the risk assessment methodology. Many times internal audit and operational risk groups (ORM) will have separate methodologies, thresholds, and drivers. It's best to align these where possible. It's important to at least understand how each other is evaluating risk, especially if internal audit relies on more dynamic risk information coming from ORM.

Bayer: The best practices of defining the audit universe that I've experienced involve looking through at least four different lens thus creating varied methods of defining coverage and risk. Strategic risk coverage is best aligned with focusing audit work on the key performance indicators and also strategic goals and the initiatives to reach those goals. Financial risk coverage is best aligned with focusing audit work on a percentage of account balances and disclosures. Compliance risk coverage is best focusing on new or key laws and regulations, contract requirements and aligning work to determine design and effectiveness of the controls in place to meet those requirements, or the metrics in place to monitor them. Operational risk coverage is usually the hardest to ensure adequate coverage and aligns to key processes and sub-processes within the company and their impact to the organization meeting its strategic goals.

Saint: We start with a risk assessment, beginning with business units because this is how the organization has designed accountability. We decompose business units into the processes and sub-processes they own and execute. We evaluate how sub-processes align to achievement of strategic objectives: How do they affect the company's value drivers? Next, we map financial statement lines to the sub-processes to help prioritize from that lens. Finally, for each sub-process we consider specific risks that could hinder achievement of strategic objectives, as well as fraud risks, significant accounting estimates, benchmarking/hot topics, and ERM risks. We created an "intensity rating" that measures how often a process/sub-process was mentioned in our stakeholder interviews as a risk to the company. And we also considered how cross-functional a process is so that the element of complexity—a risk accelerator—could help determine audit plan priorities. This year's plan development process was quite intense, but I think we did a good job of creating a baseline so that future risk assessments are more efficient.

Switzer: What information can you use from risk and compliance functions to define and prioritize audit plans?

Saint: The most recent enterprise risk-management risks are a key input to the risk assessment that drives the audit plan. Similarly with compliance risks.

Bayer: At one organization, we developed and changed a risk assessment methodology involving five categories of risk that all oversight groups utilized in rating and prioritizing not only their planning but also found gaps during our assessments. But just as in planning coverage, prioritization must be multi-dimensional and collaborative. Also, many internal audit departments are expected to cover the entire audit universe in a certain period of time. Therefore, the priorities cannot always be the most obvious risk areas but also have to include some areas to capture unknown risks.

Potter: Internal audit has a wealth of information available from ORM and compliance organizations they can use to supplement or adjust their own audit plans. For example, internal audit can gain an understanding of how ORM assesses risk, what risks they have identified, and what their risk mitigation priorities are and why. Internal audit can also understand what their compliance group's "universe" consists of and why. internal audit can review the results of their work, findings, and remediation plans and reduce their own testing based on the level of reliance internal audit can place on their work, or rely on existing remediation plans to address risks.

Switzer: How can you reduce the audit burden on business operations?

Potter: This really comes down to internal audit, risk, and compliance groups coordinating their audit plans and work, synchronizing on findings before they're assigned to the business, and ensuring that duplicate remediation plans are not assigned. Internal audit can also reduce their testing where appropriate by reviewing, placing reliance on and incorporating more business unit control self-assessments, as well as incorporating more continuous control monitoring metrics to supplement or reduce audit procedures.

Bayer: The burden to business operations can be greatly improved by (1) ensuring that their process clearly outlines what is required of them (key laws, controls, reporting); (2) ensuring that those control procedures are embedded into what they do and not just performed because audit makes them—evaluate them as the best procedure to meet the risk; (3) guiding them to self-monitor and (4) ask once and answer many. This involves relying on metrics, self-assessments, and other assessments instead of one department asking them this week and then another group asking them the same questions and for evidence the next week.

Saint: If you begin the audit planning process by asking the leaders of the company how and where they view risk, you begin to get buy-in and acknowledgement of the importance of internal audit's role in assuring the company's attainment of strategic objectives. That's critical because then the perception of "audit as burden" changes somewhat to "audit as value driver." We also take into account the rhythm of the business, and schedule our work accordingly. We ask the business units under audit how and how often they want to be communicated with. We also try to self-serve as much as we can if we're granted access to data and repositories of information. When and where we can, we collaborate with the business so that internal audit is a part of their body of work, rather than a separate project to deal with. We continuously evaluate our audit process so that we identify areas where we can improve. All this is done in consideration of doing everything possible to allow the business to run while still doing the job we've been hired to do. ■

ROUNDTABLE PARTICIPANTS

Moderator
Carole Switzer
President,
OCEG

Melissa Bayer,
GRC Expert

Patrick Potter,
GRC Strategist
at RSA, The Security
Division of EMC

Carolyn Saint,
Vice President,
Internal Audit,
7-Eleven

[GRC ILLUSTRATED]