The GRC Audit Quandary

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

by Jason Mefford

A "quandary" is an interesting word meaning: a state of perplexity or uncertainty over what to do in a difficult situation. Several internal auditors have told me they are in a quandary when auditing GRC capabilities. They often find it difficult to determine whether GRC capabilities are designed effectively. They find it difficult to know who should provide this assurance—internal auditors or another assurance function.

How can we know if a capability is designed effectively when as auditors we may not be experts in the detailed activities of GRC capabilities? Who should provide the assurance?

The OCEG GRC Capability Model states: "Assurance should focus on the ability of the capability to meet its objectives while being consistent with the decision-making criteria for acceptable residual levels of reward, risk, and compliance."

This means we must take a risk-based audit approach, focusing on the key objectives of the organization, and the areas we audit, instead of just focusing on internal controls. It is true that we need to test the internal controls, but should limit our testing to just those controls that help our organizations meet their objectives.

Mefford

The mission of the assurance function, in the context of the OCEG GRC Capability Model, is providing assurance that the GRC capabilities are well designed and operating effectively. This is a simple concept, but perplexing part that seems to be the assurance of design.

It is easy to develop audit tests to determine if a capability is operating as designed, but more difficult to confirm the designed actions and controls are reflective of objectives and supportive of strategies to meet those objectives. Without objective criteria on which to base their audits, auditors are often left to use what they identify as best practices, which can be easily disputed by management as being suitable criteria.

This is where the OCEG GRC Capability Model, and companion materials, is so valuable. Suitable criteria, for the design and assurance of GRC capabilities, have already been established. Auditors no longer need to use best practices as suitable criteria. The OCEG GRC Capability Model provides a roadmap, both for those designing GRC capabilities and those who need to provide assurance on them.

Independent, objective assurance personnel, using professional standards with experience in the subject matter, provide the highest level of assurance. How does an auditor gain or prove experience in the subject matter of GRC capabilities?

> The mission of the assurance function, in the context of the OCEG GRC Capability Model, is providing assurance that the GRC capabilities are well designed and operating effectively.

One way is by having a GRC Professional and GRC Audit certification. These certifications help both those managing the capabilities, and those auditing them. These certifications prove experience and knowledge in establishing, designing, and auditing GRC capabilities in accordance with an internationally recognized, and publicly vetted GRC framework. It also means we know how to audit using internal and external audit standards to audit GRC activities.

This leaves us with the last quandary: who should provide the assurance on GRC capabilities?

Internal auditors are independent and objective, making them a logical choice. They are well suited to perform this assurance because they also utilize professional standard when performing audits. But internal auditors are not the only group that can provide assurance on GRC capabilities. Other assurance personnel in organizations, often these "second line of defense functions," who are objective of the area being audited, can also provide the assurance.

IIA Standard 2050 states: "The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts." The auditing of GRC capabilities is one of the areas where internal audit should coordinate with other assurance professionals within the organization.

A complaint I often hear from other assurance functions is internal audit re-performing work they have already performed. Instead of auditing the second line of defense functions to determine their effectiveness, many internal auditors disregard the work already performed by these groups and jump right to auditing the same detailed controls already tested by the second line of defense function.

This sounds like duplication to me. One way we can improve auditing GRC capabilities is better coordination with the other assurance functions.

As we use criteria already established in the OCEG GRC Capability Model for determining design effectiveness, and coordinate better with other assurance functions performing work on GRC capabilities, we can resolve the quandary in which many organizations find themselves. By doing so we will also provide more value to our boards, and other stakeholders, that our GRC capabilities are designed and operating effectively. ■

Jason Mefford is the president of Mefford Associates, a fellow and director of training for OCEG, and the managing director of GRC Certify.

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.

GRC Illustrated

Review GRC Capabilities for Principled Performance

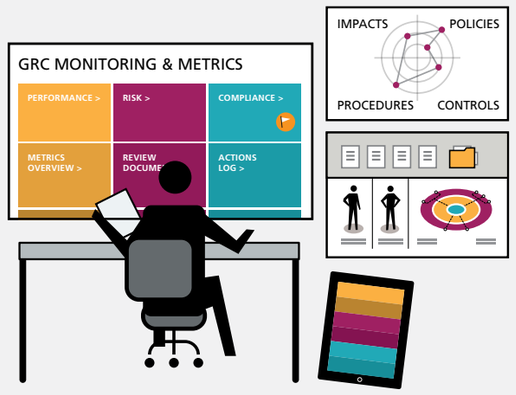
To achieve Principled Performance, an organization must monitor and conduct assurance activities for established GRC actions and controls to ensure they are utilized and are functioning properly to meet objectives. Changes to the external and internal context may demand changes in the GRC capabilities design or reconsideration of strategies and even objectives.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM The Institute of Internal Auditors, acl transforming audit and risk

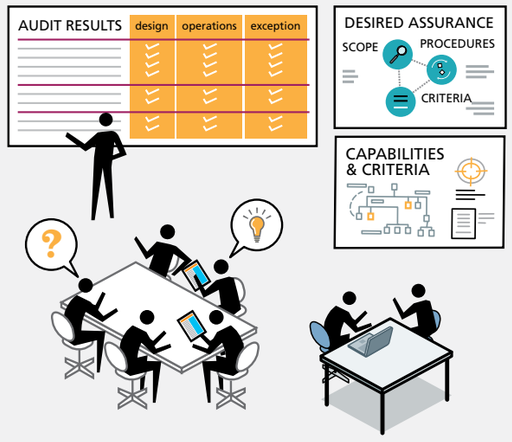
Monitor
Defined Actions and Controls

Every organization should monitor and evaluate the performance of GRC processes, technologies and organizational structures to ensure they operate as intended to mitigate risks and achieve stated objectives. How each organization mixes and layers the various types of monitoring actions and controls that allow it to perform this critical checking activity will depend on its identified opportunities, threats, and requirements and how each ranks in importance to the organization.



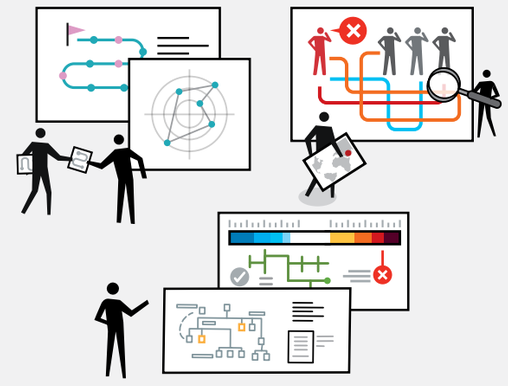
Assure
Governing Authorities and Management

The level of assurance may vary at different times and for different purposes, but capabilities must be assessed to confirm that they are effective, efficient and responsive to change. Independent assurance personnel with experience in the subject matter and use of professional standards provide the highest level of assurance.



Improve
GRC Capabilities

Management can identify opportunities for improving GRC capabilities by reviewing information from monitoring results and assurance reports. When operational effectiveness is poor, or context changes are significant, the organization must redesign and define acceptable actions and controls consistent with the established decision-making criteria to meet organizational objectives. Continual systemic improvement is the hallmark of a mature and high performing capability.



Analyze
Throughout

Information and findings gathered during the monitoring and assurance processes should be consolidated, analyzed and prioritized for actioning. A mature and continuous analytics process should be designed to provide full hindsight into the level of performance of each GRC capability, supply the necessary insight to determine the root causes of weaknesses for remediation, and enable sufficient foresight to respond to emerging opportunities or threats, including a reconsideration of organizational objectives and strategies.

KEY STEPS

1. Execute a schedule for periodic re-evaluation of each capability design in light of objectives, opportunities, threats, requirements, and changes to the business context.
2. Identify information that you will use to support evaluation of how the capability operates.
3. Perform monitoring activities to support the evaluation of the operation of the capability, including continuous monitoring for defined key aspects that are best evaluated on continuous basis.
4. Evaluate the results of monitoring activities to identify weaknesses and opportunities for systemic improvements.

KEY STEPS

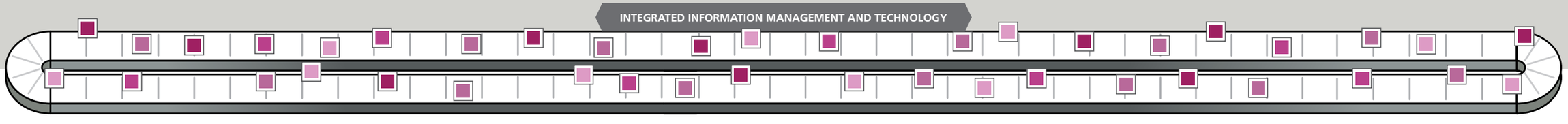
1. Determine scope, procedures, and criteria required to provide desired level of assurance to relevant stakeholders.
2. Use a risk-based approach and focus on the ability of the capability to meet its objectives while being consistent with the decision-making criteria for acceptable residual levels of reward, risk, and compliance.
3. Perform procedures, evaluate results against criteria, make relevant recommendations, and report results and conclusions.
4. Perform follow up procedures to ensure that relevant recommendations were adequately implemented and re-evaluate previous conclusions and level of assurance achieved.

KEY STEPS

1. Review information from monitoring and assurance to identify opportunities for improvements to GRC capabilities.
2. Develop and act on a prioritized plan for implementing improvements to the capabilities, including change management activities to ensure people are aware and accepting of changes.
3. Allow for implementation of new innovations and technology as they become available.
4. Incorporate feedback loops and post assessment (lessons learned, root-cause analysis, etc.) activities into organizational processes to ensure that areas of needed improvements are identified and addressed.

KEY STEPS

1. Determine the format, content and sources of information required to analyze the enterprise wide performance of critical GRC capabilities.
2. Using advanced analytics techniques, consolidate information and findings across the enterprise to obtain the required level of GRC intelligence.
3. Evaluate impact of identified patterns and trends on your understanding of the business context, the degree of alignment of GRC activities, and the level of performance of your actions and controls.
4. Consider the top down and bottom up changes required to improve your organization's principled performance and achieve optimal alignment of organizational objectives, strategies and supporting GRC capabilities.



[AN **OCEG ROUNDTABLE**]

Reviewing the Design and Operation of GRC

SWITZER: I think most people would agree that every organization should have some independent evaluation of the performance of its GRC processes, technologies, and organizational structures to ensure they are well designed to address identified risks and requirements. But there isn't any one-size-fits-all approach and there is less agreement about how to do this and who should take the lead. So let's begin by asking, what is the role of internal audit in assessing appropriateness of the design for risk and compliance management actions and controls and providing assurance about that design?

PELLETIER: While management is clearly responsible and accountable for GRC processes, an independent and objective internal audit department is uniquely positioned to provide valuable insights and assurance over these processes. The enterprise-wide scope of the internal audit department aligns well with the breadth of GRC processes, positioning internal audit to identify gaps and/or redundancies in the design of GRC processes from one department to the next and to facilitate important conversations across departments ensuring the gaps are communicated to and understood by the right decision makers. Given the complexity of GRC processes, it is critical that the internal audit function collaborate closely with those in both the first and second lines of defense.

CERNAUTAN: Internal audit should be the 'orchestra conductors,' facilitating a cross-functional, collaborative approach to reach desired levels of assurance. Collaboration is vital due to required domain expertise and the time-sensitivity of assessments. Audit teams don't always have sufficient domain knowledge in operations but they understand compliance risk management. Therefore, they need to collaborate with a number of specialists to address identified risks and requirements. Just as the conductor does not play every instrument in the orchestra, but brings it all together nonetheless. However, because internal audit represents the third line of defense, the timing of their assessments may be too late. Therefore, the first and second lines should take front-end responsibility for constantly re-evaluating the design of actions and controls to form an uninterrupted chain of defense.

SWITZER: It's equally important to monitor and evaluate the operation of the GRC capabilities. They can be well designed but that doesn't mean much if they aren't actually operating as designed. How do you decide which operations should be periodically reviewed vs continuous monitoring, and then how do you determine the depth of independent vs self-review by the management team in charge of each capability?

CERNAUTAN: Processes can be well designed but, if they are not operating as intended, they are not useful. Determining the nature, timing, and extent of monitoring activities is important and should be risk-driven. For example, review of routine processes such as p-card policy compliance lends itself well to continuous monitoring. Non-routine processes, such as merger and acquisition strategy, require more judgment and skill to administer and should be carefully monitored. The depth of the evaluations should be based on the risk and impact of each capability and the degree of independence required. For example, the more significant the risk score, the greater the degree of independence required to ensure there is no conflict of interest and collusion by management to manipulate results and vice-versa.

PELLETIER: Even the best designed processes fail when they are not executed properly. Once your organization is comfortable with the design of its GRC processes it's critical to follow up to ensure those processes are being carried out according to plan. It's not possible to test every control and, even for the controls selected for testing, it's not possible to test each one in great detail. That's where a risk-based approach becomes critical. Taking a risk-based approach begins with an understanding of the organization's risk appetite, the amount and type of risk that an organization is willing to take in order to meet its strategic objectives. The risk appetite, combined with the likelihood and impact of each risk, leads to a logical prioritization of the risks. This prioritization is critical in determining the depth of review for each capability, with higher risk areas requiring more detailed, independent review and lower risk areas being eligible for self-review.

SWITZER: It's also clear that modern technologies offer the opportunity for both continuous and periodic monitoring of key controls, metrics, and reports that can be used on a daily basis but also for audits of the design and operation of the GRC capabilities. What are some examples of the ways we can use analytics to ensure continued effective design and operation of the GRC capabilities?

CERNAUTAN: The potential for analytics is limited only by our imagination. For example, we recently designed an analytic at ACL to predict the areas of highest risk of bribery and corruption within organizations using the relationships between sales by region and the country corruption perception index. The problem is not with use case ideas for analytics. The issue is that they are frequently performed at the lower levels of the organization without strategic oversight and direction. Consequently, organizations frequently implement partial analytics capabilities rendering them ineffective. Gartner tells us that analytics should address four main capabilities: describe the matter, diagnose the problem, predict the outcome, and prescribe a course of action. Any use cases that are strategically aligned and address these capabilities will be more effective.

PELLETIER: In order for analytics to be effective, they must be considered early in the design process. Too often, analytics are not discussed until processes have been implemented and they become limited by the data and information that happens to be available. By moving the development of analytics earlier in the process, the data and information required to produce them can be included as part of the design of GRC capabilities. In this way, key performance indicators or key risk indicators can be developed up front to ensure they align with organizational objectives, the data necessary to produce the analytics will be readily available, and the production and reporting of analytics will be streamlined.

SWITZER: Obviously, there isn't much value in identifying things that need to be improved or changed, if we don't take action. What are the steps that we need to take to ensure feedback from monitoring and review activity is considered and acted upon?

PELLETIER: One thing that is consistent across most organizations is that people are busy and often have more than enough work to do. For corrective action to be taken, it must be considered important by those that need to take action. Corrective actions must be clearly communicated and should link to risks and, ultimately, objectives of the organization within the context of the risk appetite of management and the board.

CERNAUTAN: Organizations invest substantial resources in monitoring and reviewing activities of GRC capabilities to produce meaningful recommendations. However, driving change from ongoing reviews is challenging. There is often a process gap between identifying opportunities for improvement and taking corrective action. Most review activities culminate with the presentation of findings, exceptions, and visualizations of continuous monitoring results. This is where the process typically loses momentum. Implementations of many recommendations fail because they are simply not acted upon. To ensure that feedback is communicated to stakeholders and recommendations are implemented, we need to fix the process gap between reporting insights and taking action. Implementing technology to trigger automated mandatory workflows based on monitoring results can help eliminate that gap.

SWITZER: In many organizations, enhancing the role of internal audit as an adviser at the start of risk and compliance capability design is really a new idea. I think that using resources like the "GRC Fundamentals" and "GRC Audit" on-demand courses for your internal audit teams is a good starting point, but what additional advice do you have about ways to increase communication and understanding across and between the internal audit, risk, and compliance teams?

CERNAUTAN: To increase collaboration between GRC teams within an organization we must start with the integration of GRC activities by design. At the strategic level, this means defining the roles and responsibilities of the individual GRC teams in organizational risk and compliance management, including the role of IA in advising the first and second lines of defense on capability design. At the tactical level, a few key process improvements can be made to maximize the effectiveness of the collaboration. First, aligning the risk and compliance management methodologies between teams will help achieve consistency in managing GRC capabilities across the enterprise. Second, the methodology for the design of GRC capabilities should include a requirement to 'bake in' risk and compliance management controls into business processes. Third, using a common tool for managing integrated GRC activities across the organization is critical in achieving full transparency and visibility.

PELLETIER: Another key to increasing communication and understanding across and between organizational functions is to go back to basics. First, ensure everyone is using the same terminology and is interpreting that terminology in the same way. It is common for audit, risk, and compliance teams to develop their own language, especially when it comes to the use of acronyms. Starting with a common foundation reduces opportunities for miscommunication and misperception. Second, use meetings effectively. Not only can meetings be huge time wasters if not managed correctly, they can damage an individual's credibility in the long term if people feel that there was no value in attending. Go back to basics by sharing an agenda in advance, setting expectations for attendees on what should be accomplished at the meeting, and ensuring that an action plan is developed that includes those responsible. Finally, knowing your audience and what works for them is important. When it comes to increasing communication and understanding, one size does not fit all. ■

ROUNDTABLE PARTICIPANTS

MODERATOR
Carole Switzer
Co-Founder & President,
OCEG

Sergiu Cernautan
Director, GRC Strategy,
ACL

Jim Pelletier
Vice President, Professional Solutions,
The Institute of Internal Auditors

[GRC ILLUSTRATED]