Let's Change the Way We Talk About Controls

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 Carole Switzer

If you have any familiarity at all with internal control concepts, you probably have an understanding of the traditional designations of preventive, detective, and corrective controls that relate to discouraging, finding, or correcting errors and irregularities. In the modern business world, I submit that this approach to internal control is simply not enough, and both the names for these groups of controls and the definitions of them must evolve.

Today, organizations are seeking Principled Performance—defined as reliably achieving objectives while addressing uncertainty and acting with integrity—and they want to address both downside threats and the upside offered by identifying and grasping opportunities. Nowhere is this clearer than in the context of the controls we establish for governance, risk management, and compliance (GRC) capabilities.

The OCEG GRC Capability Model notes:

> *"To achieve Principled Performance, the organization must proactively encourage conduct and events that support its objectives and prevent anything that threatens meeting those objectives. It also must be able to detect ongoing progress toward objectives and determine if undesirable conduct, conditions and events have occurred, or appear likely to occur. Finally, the organization must respond appropriately to desirable and undesirable conduct, conditions and events."*

With the growing availability of technologies that allow for fast and user-friendly analytics, the way we structure controls can offer so much more than detection of errors. We can use an integrated and layered system of various control types, including process, human capital, technology and physical controls, based on risk assessments and analyses to increase an organization's confidence in its actions.

In some frameworks and professions, the concept of control is narrow; in effect it is the "check" on actions management has put in place. For example, someone with such a view of control would say that a company policy or training program is not a control, but the review of metrics that shows whether the policy or training has been distributed according to plan would be a control. In other frameworks and professions, the policy and training would also be considered controls, because they are designed to ensure the desired conduct.

I don't really care which view you take of the vocabulary, and to argue it is probably a waste of time. OCEG addresses this divide by referring to "management actions and controls" together. Whatever terminology you apply, the outcome needs to be the same. We need to classify management actions and controls under headings that reflect the ways they are used to help the organization achieve Principled Performance.

I propose that the modern categories for controls are those set out in the OCEG GRC Capability Model – **Proactive**, **Detective,** and **Responsive**.

» **Proactive management actions and controls** include prevention but go beyond it. Proactive management actions and controls should be used to encourage desirable conditions and events and prevent those which are undesirable.

» **Detective management actions and controls** determine progress toward objectives and identify the actual or potential occurrence of desirable and undesirable conduct, conditions, and events.

» **Responsive management actions and controls** do more than correct errors. They help us to recover from undesirable conduct, events, and conditions; fix identified weaknesses; execute necessary discipline; recognize and reinforce desirable conduct and deter future undesired conduct or conditions. They support our ability to grasp opportunities.

What do we do differently if we think about management actions and controls in this way? First, we examine the objectives set by leadership, whether at the entity level or for a particular program or project, and establish actions and controls not only to address whatever might prevent achievement but also for what might enhance the likelihood of meeting those goals. Our entire control framework starts from that holistic perspective. Second, we build a control structure based on the understanding that each action or control can serve more than one purpose. This leads us to establish a layered range of controls to avoid a single point of failure for high risk areas, while neither under-control nor over-control anything based on a risk assessment. Third, we recognize that we can, and must, be both proactive and responsive at the same time. Technology available to us today, and the resulting analytics and reports, allows us to be constantly reevaluating and rebalancing the full range of actions and controls. When we take such an integrated approach to the internal control environment, we are well positioned to achieve Principled Performance. ■

Today, organizations are seeking Principled Performance—defined as reliably achieving objectives while addressing uncertainty and acting with integrity.

Carole Switzer is the co-founder and president of OCEG, a non-profit think tank that develops standards and guidance to help organizations achieve Principled Performance—the reliable achievement of objectives while addressing uncertainty and acting with integrity. www.oceg.org.

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

Perform GRC Actions and Controls for Principled Performance

All organizations must address threats, opportunities and requirements by encouraging desired conduct and conditions and preventing what is undesired. Establish a mix of proactive, detective and responsive actions and controls, supported by strong analytics based on strategic objectives, risk appetite and capacity, and risk decision-making guidance established by leadership.

DEVELOPED BY OCEG®

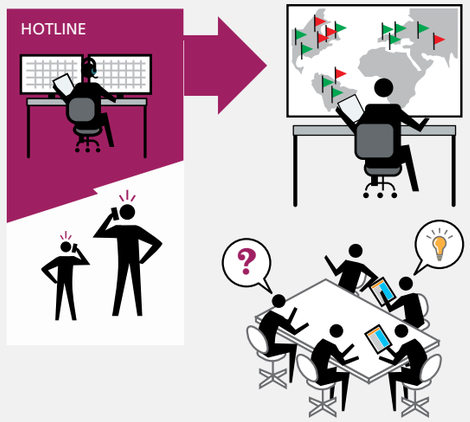
WITH CONTRIBUTIONS FROM MetricStream convercent™

Proactive
Actions and Controls

Being proactive means taking action and establishing controls to prevent undesired conduct conditions and encourage or identify what is desired. This requires having policies, training, communication, incentives and strong analysis to manage conditions in performance, risk and compliance.

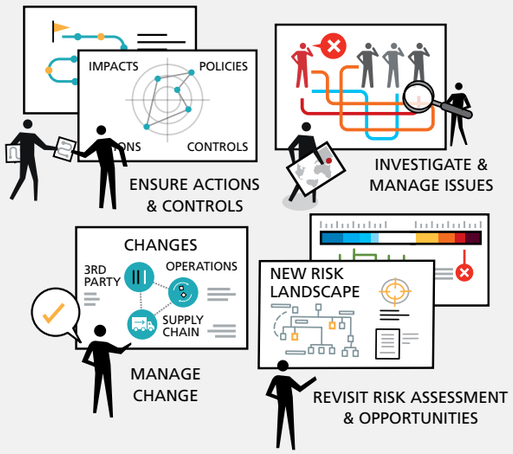
Detective
Actions and Controls

Finding out about desirable and undesirable conduct or conditions in a timely fashion is as important as proactively driving what you want. Discovering opportunities for risk taking, as well as identifying downside risk, is critical to achieving superior performance. Systems, both digital and human, that detect both internal and external anomalies are critical to success.



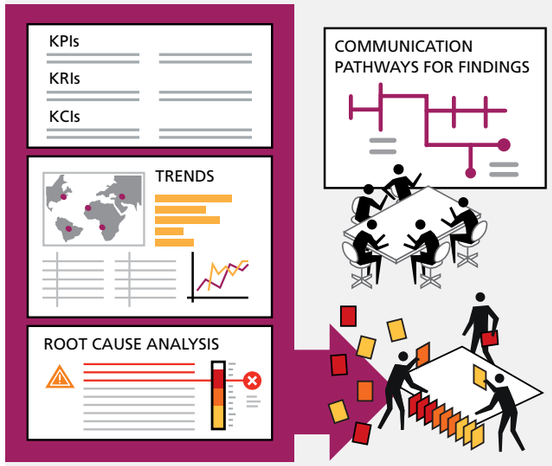
Responsive
Actions and Controls

Action must be taken on analyses of information received from proactive and detective controls. Sometimes this is process driven; other times automated technology responses (such as access control change) are established. Ensure processes and controls are established to investigate and manage incidents, launch consideration of opportunities or risk reassessment, and manage change.



Analytics
Throughout

Analytics tied to performance indicators unleash the power of unstructured and structured information. Use analytics to prioritize and analyze trends, identify root causes of problems, predict behaviors and conditions, and gain insight for risk-based decisions. Leverage analytics to see potential impacts and become more agile in meeting performance objectives.



KEY STEPS

1. Define and establish policies and policy management structure, including processes for exceptions, and define role-based procedures to follow
2. Design and deliver appropriate training and education opportunities through multiple channels and modes of delivery, using different methodologies and risk based curriculum
3. Communicate about risk decision-making guidance and expectations in a determined flow through multiple channels
4. Monitor key indicators and ongoing operational information to ensure issues are resolved and processes and controls are adjusted as necessary to align with risk profiles and remediation plans

KEY STEPS

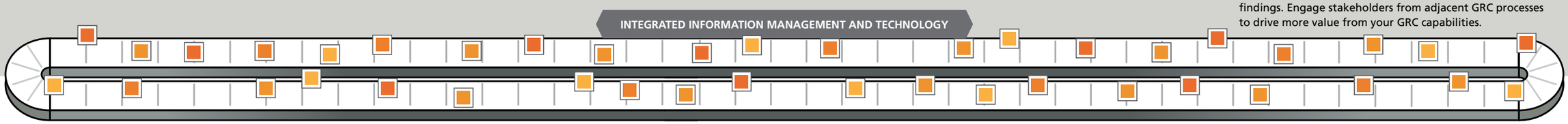
1. Define and establish pathways for individuals to push reports of concerns or information about threats, undesirable conduct or incidents, and passing along information about opportunities.
2. Use multiple channels to pull both internal and external information to support early detection of threats, improper conduct or conditions, and possible opportunities.
3. Use available technology systems for detecting variances, anomalies, breaches, inappropriate controls, and early warnings about possible violations of policies/procedures or control avoidance.
4. Evaluate information, forward opportunities and issues for resolution, and adjust controls as necessary.

KEY STEPS

1. Define and implement pathways for triage of identified issues, concerns and opportunities, using established procedures and supportive technology, in some cases enabling automated resolution of issues.
2. Establish investigation and issue resolution procedures, identifying key personnel and tools to be used in conducting processes and maintaining an audit trail of resolution of each issue.
3. Ensure timely reporting to internal and external stakeholders when required or appropriate.
4. Evaluate information received throughout resolution processes and use to adjust established actions and controls as necessary.

KEY STEPS

1. Establish Key Indicators for Performance, Risk and Compliance tied to strategic objectives and appetites; develop processes for collecting data and analyzing results.
2. Design information architecture to support the analytics framework, using reliable internal and external datasets to provide contextually relevant insights that leadership can act upon.
3. Continually evolve the analytic framework as it begins to yield richer information on trends, emerging threats, vulnerabilities and opportunities, predicted conditions and root cause analysis across a broader and more granular array of domains and topics.
4. Collaborate with the board, senior management and business operators to ensure two way communication and action on findings. Engage stakeholders from adjacent GRC processes to drive more value from your GRC capabilities.



[AN **OCEG ROUNDTABLE**]

Performing GRC Actions and Controls

Switzer: In the PERFORM component of the OCEG GRC Capability Model, we're looking at what types of actions and controls are essential in any organization to help it meet objectives, manage risk and ensure compliance. In general, when we talk about controls we refer to them as proactive, detective, or responsive in nature. What do we mean by proactive controls and what are some key examples?

Delmar: Organizations today are dealing with a great deal of change—the rise of the global, extended, digital enterprise, regulatory conflict at the global/local level, evolving workforces, emerging technologies and disruptive competitors. With this comes new risk to manage in the face of heightened standards and more demanding performance objectives. Successful organizations take a proactive stance in everything they do, while keeping a hand firmly on the operational rudder. Proactive controls actually exist at every level—strategic, tactical, and operational.

An example of a proactive control for strategic business objectives is defining risk appetite and guardrails that can then be translated into what is acceptable and what is not in operations. An example of a tactical control is building a human capital plan to ensure we build an agile and resilient organization, where the right employees are attracted and retained. Examples of proactive operational controls include establishing operational limits, preapprovals, and access rights to prevent negative outcomes, and address issues in a highly responsive way, as they arise. It's all about motivating and inspiring desired conduct.

We are seeing more thoughtful consideration given to how to drive proactive controls into the day-to-day operating fabric of the organization —like driving a policy into specific procedures, which are then translated into performance driven authorities in actual job descriptions or SLAs with third parties—all designed to make the process highly responsive and agile.

Quinlan: Though they're preventative in nature, it'd be a mistake to think that proactive controls are "set it and forget it" activities—though admittedly updating policies and refreshing course content can be some of the more arduous components of the compliance team's function. It's important to take input and key findings from monitoring processes and priorities set throughout your objectives, strategies, and operations and apply them to your controls. This continuous feedback loop also fosters continuous improvement of controls by better aligning them to ever-evolving requirements and expectations and ensures that you're staying within your established risk capacity.

Switzer: When we look at detective controls, we're talking about how you find out about conditions and behavior, both good and bad. How are forward thinking companies managing this process today, when there is so much information moving so fast in the organization?

Quinlan: We've entered an age where a compliance function that relies solely on a "push" strategy won't cut it—it's simply not enough. There's a synergy that needs to be achieved in the push and pull of information between the compliance team and a company's employees, and forward-thinking companies are being far more thoughtful and intentional about the channels they provide their employees. Beyond giving employees a choice of channels, companies increasingly focus on accessibility, ease of use and user experience in these channels.

This is important: If your employees know how to get the information to you, and you make it easy for them to do so, in an environment that makes them feel comfortable and secure, it stands to reason that they'll be more likely to give you more and better information to work with.

Now you have the information in your hands, and you've got to do something with it. Your risk profile and appetite can help prioritize and route the information appropriately so that the issue at hand can be addressed by the right people in the appropriate timeframe. Once that's done, look beyond the one-and-done triage. Use the data you've collected to create or fine tune controls that are targeted at the drivers of those incidents, conduct or threats—behavioral or environmental.

Delmar: Increasingly these channels are reaching beyond the traditional into social media and online communities where conversations are actually happening and behaviors may be crossing the line. We are seeing the emergence of technologies that support correlation and anomaly detection—actually 'sensing' when behaviors go outside the guiderails—and reign them in with blocking controls that respond in "machine-time" or automated escalation to the right people who can respond in "human-time."

Switzer: Clearly, there is also the need for responsive controls, which may be in the nature of investigations and at other times automated responses are appropriate. From a process and technology perspective, how do you ensure the information developed from operation of proactive and detective controls is considered and responses take place?

Quinlan: The data from your controls has to be integrated. Bottom line. The manual aggregation of siloed data is a huge hindrance to the productivity, efficacy, and value of many compliance teams. It's also a risk in and of itself because the more disconnected your controls and their data are, the more likely it is that something will be overlooked. If all of that valuable data is in one place, you're not only less likely to miss the outliers that need to be addressed, but you're more able to identify and address important trends within your organization and you're able to filter, slice and prioritize it as needed; by your risk areas, for example. Taking a more federated approach to controls also allows the compliance team to ensure the occurrence and consistency of responses.

Delmar: What we are seeing now is attention paid to a kind of "right-sizing" of responsive controls across critical processes. What we know is that if controls are heavily layered in one part of the process, the ability to respond in an agile way downstream is often severely hampered. To get to the root cause it's sometimes necessary to get up a few levels and get stakeholders looking at the entire end-to-end process—which could take you out of the boundaries of the organization, into third parties or technology service providers, into communities and social media. A hang-up or disconnect through the operational "weave" can cause real response problems for organizations, with real bottom-line impacts. This is particularly evident in supplier chain failures, business disruptions and cyber-breaches, for example. We live in an increasingly dynamic, automated, and complex world that is driving us continuously to seek greater flexibility and effectiveness in our control fabric.

Switzer: This leads us to talk about analytics—an essential element to consider and establish for all types of controls. What can be done today that couldn't be done, or even dreamed about five years ago?

Delmar: The use of analytics in measuring performance has been around for centuries—it's human nature to set goals and mark progress, whether it's the yield on crops, conquering new lands, or exploring space. The game-changer in the last five years has been greater ease of use of analytics that comes with automation—we can truly get a near-real time picture of outcomes against key performance, risk, and control indicators now by slicing and dicing big data—both structured and unstructured data.

Remember—a metric is simply arithmetic—whereas an analytic is something that yields insight on which you can make decisions and act. Decision makers are no longer looking in the rear view window—but looking forward to where they want to drive performance to meet goals.

So we are seeing more emphasis on questions like"What's happening now? What could happen? What can we reasonably predict? What's working or not working? What are our options? What's our opportunity?" Today's successful organizations are thinking very deeply about how to leverage an agile analytics framework to yield real-time indicators as they drive performance in their operations, and more importantly, out into their larger eco-systems of suppliers, third parties, customers, and employees on which their success depends.

Quinlan: When you look in the C-suite of a company, compliance is a relatively new function when you compare it to finance, HR, and the like, and I think the quality of performance metrics and expectations have been a reflection of that newness. Boards and executives haven't quite been sure what to expect compliance reports to look like, so what they've gotten over the past decade or so have been very metric-based: number of calls to the hotline, training completion rates, etc.

But those don't give you insight into what's really going on within your company, they don't help you answer some of those important questions that Yo mentioned and they certainly aren't on par with the performance analysis and insight the rest of the team is bringing to the table. The compliance executives that have been able to establish and advance a more productive conversation around compliance within their organizations are the ones that have focused on establishing and producing detailed analyses across their controls. ■

ROUNDTABLE PARTICIPANTS

Moderator
Carole Switzer
Co-Founder & President,
OCEG

Yo Delmar
Vice President, GRC Solutions
Customer Engagement Programs,
MetricStream

Patrick Quinlan
CEO,
Convercent

[GRC ILLUSTRATED]