



April 24, 2020

Certified Financial Planner Board of Standards, Inc.
1425 K Street NW #800
Washington, DC 20005

SUBJECT: Comment Letter from FPA Board of Directors on CFP Board’s Proposed Procedural Rules

Dear CFP Board Board of Directors,

The Financial Planning Association® (FPA®), the country’s largest voluntary membership association for CERTIFIED FINANCIAL PLANNER™ professionals and those who support financial planners and the financial planning process, is pleased to provide the following comment letter to the Certified Financial Planner Board of Standards, Inc. (CFP Board) in response to the availability of the *Proposed Procedural Rules* [“Proposed Rules”] on March 24, 2020.

FPA was formed in 2000 through the merger of the International Association of Financial Planners (IAFP) and the Institute of Certified Financial Planners (ICFP). Since that time, FPA has been committed to providing a professional home for those practitioners who strive to adhere to the high standards evidenced by the CFP marks. As the largest professional membership association for CFP® professionals, FPA is profoundly interested in seeing the marks be recognized by the public as an indication that a CFP® professional is committed to the highest standards of competency and ethical behavior.

In accordance with FPA’s Primary Aim, which is “*to elevate the profession that transforms lives through the power of financial planning,*” this comment letter serves to support FPA’s role in elevating the profession and being the voice and advocate for CFP® professionals.

FPA and CFP Board, through their work within the Financial Planning Coalition, are working to build the financial planning profession. The standards and processes that CFP Board maintains, as the standard-setting body, are critical and the continued review is essential. For that reason, FPA applauds CFP Board for consolidating the Disciplinary Rules and Procedures and the Appeals Rules and Procedures into its *Proposed Procedural Rules*. We agree with CFP Board that one set of rules will be easier for CFP® professionals and the public to understand. We acknowledge that enforcement of the new *Code and Standards* will begin on June 30, 2020 (as FPA advocated for on behalf of our CFP® professional members) and that the *proposed Procedural Rules* will take effect on that same date.

FPA believes these *Proposed Procedural Rules* must be viewed in connection with the findings contained in the report of the Independent Task Force on Enforcement [“Task Force”]. CFP Board gave the Task Force the following charge:

The Independent Task Force on Enforcement will examine CFP Board’s current enforcement program. The blue-ribbon group will make actionable recommendations to the Board of Directors about potential changes that will allow the organization to enforce its ethics and conduct standards in a manner that best fulfills its mission to benefit the public. [Report, Page 1]

The Task Force found that the root causes of weaknesses in CFP Board’s enforcement program were grounded in its governance structure, strategic planning and the enterprise risk management processes:

While the Task Force finds that there were significant failures in the execution of the CFP Board’s enforcement program and attendant communications to the public, we find that the primary cause for the failings that prompted the creation of the Task Force are systemic, longstanding, governance-level weaknesses, and that the problems discussed in this Report cannot be adequately addressed without commensurate governance reforms. [Report, Page 3]

In its [comment letter](#) dated January 21, 2020, FPA praised the Task Force for drafting a highly readable set of twelve robust recommendations. FPA commented that the recommendations are grounded in the best practices of Governance, Risk Management, and Compliance principles. FPA attached as Exhibit A to that comment letter “The Building Blocks of GRC: Visualizing an Effective Capability,” which is also attached to this letter.

FPA again encourages CFP Board to embed internal and external reviews and assessments of its enforcement program into its governance protocols, and again urges CFP Board to increase the role and authority of public members, as recommended by the Task Force. [Recommendation 1, Page 9]

With respect to the *Proposed Procedural Rules*, FPA expresses five concerns.

- 1. Standard of Proof:** In the pursuit of truth and justice, the ability of those accused to effectively defend themselves is a critical component in the adjudication process. While there are varying standards that can be applied within a hearing, the weighing of such evidence is subjective at best. Given the stakes, FPA feels the standard of proof applied to hearings conducted by CFP Board should be as strong as reasonably possible. CFP Board proposes to use the very lowest standard of proof—the mere preponderance of the evidence standard—in *Proposed Procedural Rule* Article 12.1. Such use could mean a guilty verdict where the proof is 50.1% favoring guilt and 49.9% favoring a not guilty verdict. FPA recommends that the “clear and convincing evidence standard” be used. “Clear and Convincing” is the standard required in Article 14.2 when a CFP® professional seeks reinstatement, so this proposed change would bring consistency to the process and set a precedent that will bring our profession in-line with the standards applied in other bona fide professions. Using the “Clear and Convincing” standard would also be in alignment with the standards and processes of other adjudicating bodies within our own profession, including FINRA.
- 2. Witnesses:** As stated above, the ability of the respondent to put forth an active and viable defense is critical in any reasonable adjudication process. The perceived ability for anyone to accuse or incriminate a CFP® professional should, at a minimum, require that accuser to face the accused, as well as the ability of counsel for the accused to ask reasonable questions of the accuser to get to the ultimate truth. FPA recognizes that CFP Board does not have the power to subpoena witnesses; however, FPA urges CFP Board to revise the *Proposed Procedural Rules* so that a rebuttable

presumption arises that a complainant is not to be believed whenever such complainant is unwilling to testify on the record and be subject to cross examination.

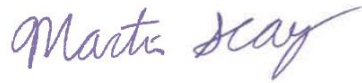
- 3. Procedural Rules:** FPA is concerned about the rules of the proposed process. For example, in Article 1.d.4., an oral examination does not have to follow federal or state evidentiary or procedural rules. Further, in Article 10.6, the Hearing Panel is not bound by federal or state evidentiary or procedural rules and has the power to exclude evidence. As suggested above, the rules of evidence used in these hearings is of utmost importance to the accused and accuser alike. FPA believes that accuracy and thoroughness is more important than the speed at which these hearings can be conducted. The potential exclusion of evidence is of particular concern, rendering the final result(s) as potentially suspect. Proposed Rule 17.2 requires Respondent's counsel be an active member in good standing of the bar. FPA suggests an amendment to require that CFP Board counsel and Respondent's counsel decide which federal or state evidentiary and procedural rules will be used so as to protect the rights of the Respondent. This would allow flexibility in the process, providing each respondent the ability to fully defend themselves and receive a fair and impartial hearing.
- 4. Peer-Review Process:** The first paragraph of the Preamble states, "*CFP Board enforces its standards through a peer-review process set forth in these Procedural Rules that is credible to the public and fair to those whose conduct CFP Board is evaluating.*" Given the influence of staff and the governance concerns outlined at the outset of this comment letter, FPA believes that the process is not procedurally peer-review. Both optically and practically, the continued advancement of financial planning as a bona fide profession depends on both high standards and an independent adjudication process. Under the current structure, the potential for significant influence from CFP Board and staff creates problems. As a result, FPA suggests CFP Board revise the *Proposed Procedural Rules* so as to protect the independence of the Counsel and those who serve on hearing panels, whether practitioners or public members, from potential inappropriate influence from CFP Board and staff. Specifically, we suggest codified separation between said parties, and assurance that CFP Board counsel is not involved in the rendering of any related decisions.
- 5. Qualifications and Training:** FPA understands the heavy obligation to discover truth and deliver justice that is placed on members of the hearing panel. It is understood that the Disciplinary and Ethics Committee (DEC) consists of both permanent members and volunteers that may participate in a limited number of hearings. FPA requests that CFP Board develop/enhance, and make public, the qualifications and requirements of those who serve on the DEC. This may include proposed terms and the rules governing and protecting the independence of those chosen to serve in this important role. It is also understood that CFP Board has a current training and continuing education program for all hearing panel members and an additional training protocol for those asked to serve as chair. In the interest of transparency, FPA recommends that the training program details be made public. The FINRA Arbitrator training program appears to be an appropriate model and example.

Conclusion

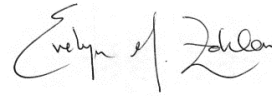
FPA's relationship with CFP Board is incredibly important and we share a goal of creating a viable, active profession that is recognized for the important role it plays in the lives of those CFP® professionals serve. We once again applaud CFP Board for carefully reviewing their standards, procedures and processes and considering opportunities to strengthen the marks and protect them from scrutiny. As the principal membership association for CFP® professionals, FPA is willing to further engage in discussions on this

important matter and stands ready to help our members understand the *Proposed Procedural Rules* once finalized.

Respectfully Submitted on Behalf of the 2020 FPA Board of Directors,



Martin C. Seay, Ph.D., CFP®
2020 FPA President



Evelyn M. Zohlen, CFP®
2020 FPA Chair



Skip Schweiss, AIF®
2020 FPA President-elect



Lauren M. Schadle, CAE
Executive Director/CEO



THE BUILDING BLOCKS OF GRC:

Visualizing an
Effective Capability





OCEG IS A GLOBAL, NONPROFIT THINK TANK AND COMMUNITY. WE INVENTED GRC.

We inform, empower and help advance more than 50,000 members on governance, risk management, and compliance (GRC). Independent of specific professions, we provide content, best practices, education, and certifications to drive leadership and business strategy through the application of the OCEG GRC Capability Model™ and Principled Performance®. An OCEG differentiator, Principled Performance enables the reliable achievement of objectives while addressing uncertainty and acting with integrity. Our members include c-suite, executive, management, and other professionals from small and midsize businesses, international corporations, nonprofits, and government agencies.

Founded in 2002, OCEG is headquartered in Phoenix, Arizona.
For more information visit <http://www.oceg.org>

Thank you to the OCEG GRC Solution Council members and others who participated in the development of this series:



INSIDE THIS BOOK

Introduction	2
Illustration: Pathway to Principled Performance	3
PART 1: LEARN	
Roundtable: How to Keep Business Plans on Track	4
Illustration: Learn Your Business Context for Principled Performance	5
Column: Learning Lessons for Principled Performance	6
PART 2: ALIGN	
Column: Aligning the Organization for Principled Performance	6
Roundtable Discussion: Align the Business for Principled Performance	7
Illustration: What do We Need to Align for Principled Performance	8
PART 3: PERFORM	
Roundtable Discussion: Performing GRC Actions and Controls	9
Illustration: Perform GRC Actions and Controls for Principled Performance	10
Column: Let's Change the Way we Talk About Controls	11
PART 4: REVIEW	
Column: The GRC Audit Quandary	11
Roundtable Discussion: Reviewing the Design and Operation of GRC	12
Illustration: Review GRC Capabilities for Principled Performance	13

PRINCIPLED PERFORMANCE

Aligning the Building Blocks of Success

Today's business climate is more complex and more challenging than ever before. Even small businesses, non-profits, and government agencies face issues that historically affected only the largest international corporations.

Internal and external stakeholders demand not only high performance, but also transparency into business operations. Contemporary risks and requirements are numerous, ever-changing, and fast to impact the organization. And, if that were not enough, the costs of addressing risks and requirements are spinning out of control. In short, the status quo for many organizations is neither sustainable nor acceptable. For some, their very lives are at risk.

So how do we address this growing web of issues? By adopting a vision of Principled Performance — a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty and acting with integrity.

Think for a minute about your organization in the same way you might view a living organism. It can be healthy; it can get sick; and, with the right support, it can recover from illness and return to a healthy state. It can be marginally functional, or it can be strong, agile, and resilient.

Then think about what is necessary for life in the organism or for the organization. In the organism, it starts with amino acids — commonly referred to as the building blocks of life. Protein is 100% amino acids... and protein regulates nearly every biochemical reaction in the body. Our neurotransmitters,

hormones and muscles are made of the 21 amino acids that support life. And RNA and DNA require amino acids, so they are necessary for our genes to function properly. All of these systems need to operate in an integrated and harmonized way, and they can be enhanced and have greater success with good nutrition, effective exercise and a non-toxic environment.

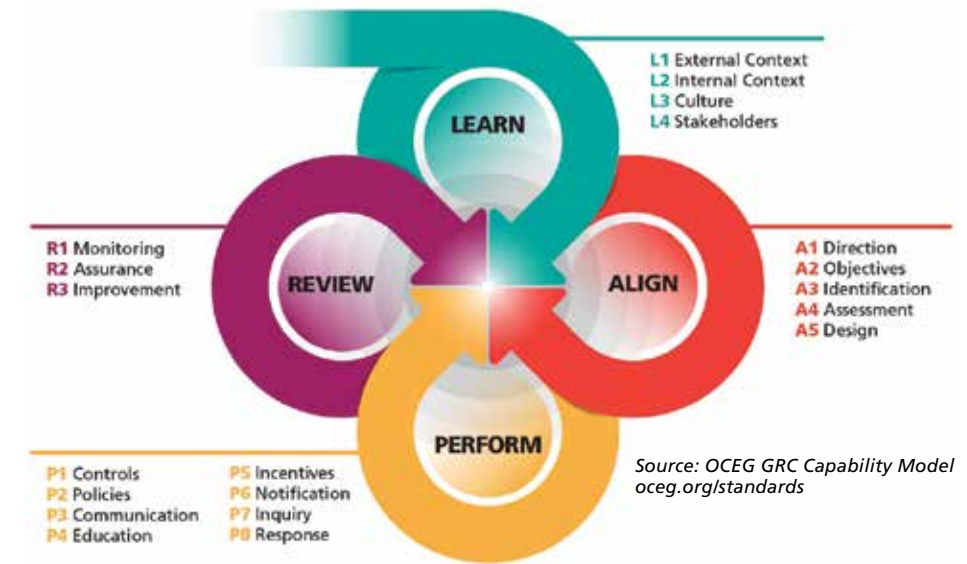
For the organization, it's not so different. For it to live and succeed there are many functions that must operate together; from core business units such as governance, finance, production, and sales to adjunct areas like performance management, risk management, internal control, compliance, and audit. And they all must use the same data, but in different ways, just as functions of the body all use the same 21 amino acids in different combinations. And yet, despite the need to integrate and harmonize in support of the health and success of organizations, many manage these activities in disparate departments with little if any cross-functional communication. Even worse, in others, these activities are not really managed at all; they are literally untouched by modern business process improvement techniques.

Principled Performance, the healthy and vigorous state of being that ensures life and enables success for an organization, can only be achieved by integrating and orchestrating information and functions that, in many organizations, are fragmented and siloed, and supporting them with strong communication, effective technology, and development of the desired ethical culture.

It's not enough to aggressively move toward established objectives without consideration of the boundaries of laws, social mores, and uncertainties that arise with regard to potential risks and rewards. Nor can the management of risk, compliance, and ethical conduct be separated from the objective-seeking activity, any more than an organism's muscles function independent of its neurotransmitters or hormonal system.

The successful attainment of Principled Performance requires a holistic view that addresses the governance, management, and assurance of performance, risk, and compliance; each with consideration of the other. Just as amino acids are the building blocks of life, so too are the people, processes, and technologies in every organization. And in the way that amino acids underlie critical functions of the living organism that must operate together in harmony, with seamless communication, so too must these building blocks of the organization. Only then will it not only survive, but do so in a state of Principled Performance.

In the pages that follow, we offer a series of articles and infographics from OCEG's GRC Illustrated Series that walk you through the core components of OCEG's GRC Capability Model and guide you on the pathway to Principled Performance. We hope you find them useful and we welcome your comments.

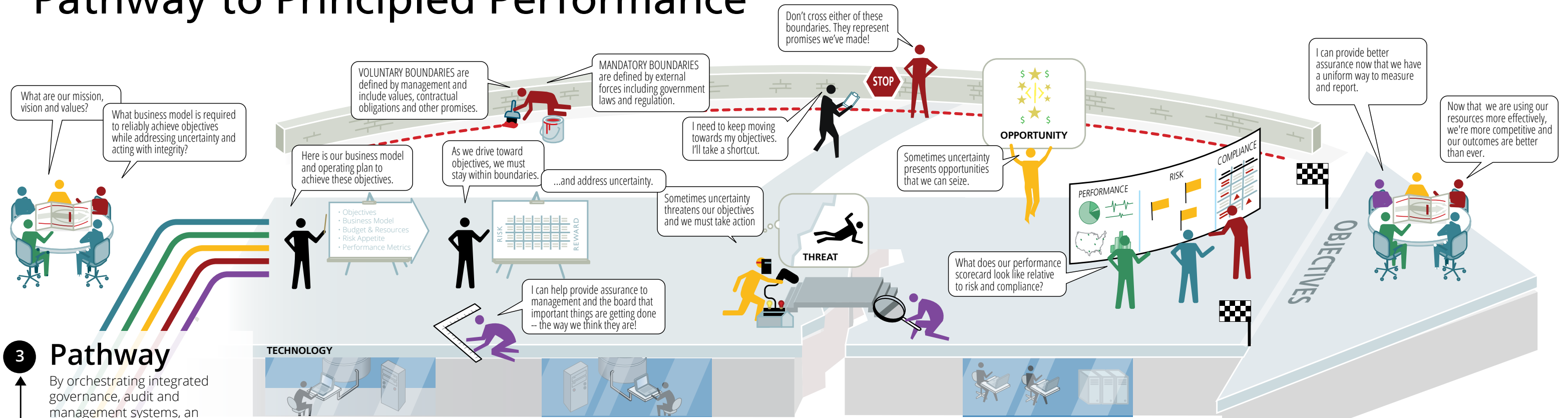


Scott Mitchell
OCEG Co-Founder and Chair



Carole Switzer
OCEG Co-Founder and President

Pathway to Principled Performance



3 Pathway

By orchestrating integrated governance, audit and management systems, an organization can reliably achieve objectives, while addressing uncertainty and acting with integrity.

2 Systems

Core governance, audit and management systems are the backbone of an organization. They leverage common capabilities for multiple purposes.

1 Capabilities

Think of capabilities as "tools" to use for many different purposes. Develop capabilities that can be leveraged by all of your governance, management and audit systems. This way, when you improve the capability, all systems benefit.



LEVERAGE COMMON CAPABILITIES



LEVERAGE COMMON CAPABILITIES



LEVERAGE COMMON CAPABILITIES

LEARN



Learn about the organizational context, culture and key stakeholders to inform objectives, strategy and actions.

ALIGN



Align strategy with objectives, and actions with strategy, by using an effective decision-making approach that addresses values, opportunities, threats, and requirements.

PERFORM



Perform actions that promote and reward things that are desirable, prevent and remediate things that are undesirable, and detect when something happens as soon as possible.

REVIEW



Review the design and operating effectiveness of the strategy and actions, as well as the ongoing appropriateness of objectives to improve the organization.

Learning How to Keep Business Plans on Track

SWITZER: Too often you don't learn about changes and continue down a planned path that isn't right anymore. How are companies dealing with this challenge?

Rost: No matter how confident a management team may be in a given growth strategy, current operation, or process for regulatory compliance, the future is not foreseeable. The problem is that companies do not have the processes and systems in place to deal with this constant state of change. To solve this problem, organizations should consider connecting their GRC initiatives to broader business performance objectives and building a risk discipline and set of processes that will engage the first line of defense at the operations level. They also should maintain a set of risk policies and tolerances to ensure that all are working from the same set of assumptions and are utilizing systems and tools that provide a collaborative and flexible set of capabilities.

MCDONALD: In the early days of GRC, there was a big desire for a single technological platform to manage all the GRC related activities within an organization. This was in part a technology consolidation initiative, but also a move toward unifying methodologies and data attributes for controlling a broad spectrum of risks. The industry is filled with success stories but also with projects that were doomed by the seeming audacity of their goals relative to the insufficient levels of collaboration among stakeholder groups, or by the desire to automate too much. Some functions, like compliance, need the flexibility to change their methodology to suit fast-changing requirements, so over-automation can be a problem. We've learned from these early years that GRC initiatives need to more fully anticipate and accommodate the need for change as regulatory and other stakeholder demands shift at a fast pace.

DICKINSON: It's the challenge we all face when demand for responsiveness meets big data—it gets complex quickly. Today bad news travels fast and exacts damage quickly. Is your external-facing infrastructure capable of monitoring every relevant action and event that affects your business and are you able to respond speedily and appropriately? It comes down to data, systems, and processes—and good connectivity between all three. Many companies have tried to address the challenge by forcibly adapting existing internal GRC systems never designed or built to monitor the complexity of the outside world—even less so at speed. Today, many are coming to realize that to properly deal with the challenge they need best-of-breed outside-the-firewall solutions that can be federated with their internal GRC infrastructure.

SWITZER: Can you give us some examples of what you need to keep an eye on typically, both inside and outside the organization, and what the flow of the information you gain might be?

MCDONALD: Well, one might say "the targets are moving." Many GRC objectives revolve around the mandates of regulators. As those standards and rules

evolve, the GRC focus might have to pivot to mitigate the risk of regulatory infractions and demonstrate that regulatory risks are well-managed. This means that companies need to watch the ever-changing regulatory landscape, including changes to rules, news, analysis, enforcement actions, etc. For most organizations investing significant amounts on GRC programs, the stance of the regulators can be the most important factor shaping the objectives of the initiative; so clearly as much intelligence as possible about the regulatory environment is necessary for a successful GRC program.

DICKINSON: The key thing to remember is that the world is dynamic—things are always changing. When changes occur, you need to know quickly. One of the biggest things to keep an eye on is an unfavorable change in status of a third party—you must know asap if a party you're connected with has suddenly breached internal standards. Information flow from external compliance data sources should be electronically connected in real time to your third-party monitoring platform and it, in turn, should be monitoring 100 percent of your third parties—whether one thousand, ten thousand, or a hundred thousand. It's now possible and feasible to monitor them all.

ROST: Lately, many organizations have invested in addressing areas of external change such as third-party relationships and regulatory issues. But it's just as important to keep your eye on internal changes through continuous assessment of risk policy, risk tolerance, and key risk indicators; control testing and assessment results; and reporting on assurance activities, including internal audit, control management, and compliance. Effective information flow for these internal activities is best achieved by effectively capturing the data and the narrative from the first line of defense process owners and linking that information together in dashboards and management reports for review by management and assurance professionals.

SWITZER: Often, data breaches, bribery, and other reputation risks are caused by third parties. What must we learn about so we can adjust controls or strategies when necessary?

DICKINSON: You need to manage all your third-party relationships during their lifecycle, from the pre-contractual selection process to operational to post-contractual. You also need to monitor them across three core dimensions: risk, performance, and compliance. Monitoring needs to be comprehensive—whether its bribery, corruption, information security, data privacy, corporate and social responsibility, environmental standards, or conflict minerals, to name a few—there should be no infrastructural limit to the number or type of monitoring programs you can operate. You also need a single unified view of all your third parties—be they suppliers, vendors, resellers, distributors, agents, or affiliates, you can't settle for pre-selected subsets that you believe represent the only risk worth monitoring. Then there's the added dimension of multiple contractual relationships with a single third

party, each with different risks, exposures, performance expectations, and compliance rules.

MCDONALD: We spoke earlier of factors that upset the best-laid GRC plans. Another challenge is the interdependence of businesses these days, and the difficult to see risks embedded within suppliers, partners, and counterparties of all sorts. It surely isn't easy to monitor one's own risks, controls, and compliance mandates but is far more difficult—and necessary—to be informed about the practices and risks of third parties. To deal with this, many of our customers are continually monitoring their third parties; which means not just updating risk assessments and questionnaires but ongoing screening and adverse media and sanctions checking, and assessing the affiliations of individuals and entities with other known high-risk parties. While our financial services customers are greatly concerned with financial fraud risk, our corporate customers are screening for slavery and human trafficking, and against sanctions lists. Workflow platforms make this automation possible but there remains the need to source screening data, as well as the enhanced due diligence that customers buy when screening data shows questionable results.

ROST: Two areas that we see our customers focused on with regard to third-party management are surveys and policy certification. Requiring third parties to complete periodic surveys provides a mechanism for that third party to disclose changes to business operations and associated risks and also enables the organization to assess risk across a group of third parties. Effectively communicating relevant policies to third parties and receiving some form of auditable certification that those third parties have read and understood those policies provides a discipline for policy communication and a control for minimizing risk.

SWITZER: Keeping track of everything isn't possible, we know that. How do you best go about setting priorities, allocating resources, deciding on layering of approaches, and ensuring reports get to the right places at the right times

ROST: Having a fact-based understanding of the most critical business objectives, processes, and uncertainties is crucial for getting in front of this issue. It requires a well-executed program of assessing risk and connecting that information to business objectives and performance

metrics. To best execute and optimize this collaborative and document-centric requirement, organizations need flexible and dynamic processes and tools that support the linking of risk, controls, and documentation to planning, management reporting, and board level information. You need to deeply engage process owners and people on the front line in this process and effectively capture their information and assessments. Making quick and informed decisions and keeping the information fresh will all be dependent on how effectively you can engage those on the front line.

DICKINSON: It's important to recognize technology is rapidly improving what we can track cost effectively—our view of the world is getting more accurate and costing less. While you can't track everything, many organizations are not tracking everything they feasibly could be. There's an opportunity cost between accuracy of risk, thoroughness of response, and cost of both. If you're not tracking events at the highest level feasible, your compliance program is running suboptimally—it will always force you into more severe trade-offs than necessary. Make sure uncertainties you're choosing to pay less attention to are not ones you could be monitoring for want of better technology deployment; Software as a Service, or SaaS, is the only delivery mechanism sufficiently responsive.

MCDONALD: We see this as the real job of the GRC professional—and one which all solutions should be supporting. For companies with little or no GRC infrastructure or supporting tools, it can be shocking how much time someone with a law degree or GRC sensibilities can spend just gathering data into spreadsheets or creating periodic reports when they were hired for their experience and judgment. This applies no less to advisory services partners who are engaged for their GRC perspective but too many times deployed to help with simple data aggregation or software implementations. The point of GRC systems, or any vendor-provided controls, regulatory intelligence, etc., should be to empower the GRC professional to make informed decisions, not to spend their time maintaining the systems or locked in never-ending implementations. The right kinds of tools and, more importantly, the right kind of risk data should make ongoing prioritization easier, though nothing will replace the good judgment of the professionals.

ROUNDTABLE PARTICIPANTS



MODERATOR
Carole Switzer
Co-Founder & President,
OCEG



Greg Dickinson
CEO,
Hiperos



Steve McDonald
Head of Market
Development Risk Americas,
Thomson Reuters



Mike Rost
Vice President,
Vertical Solution Strategy,
Workiva

Learn Your Business Context for Principled Performance

You can't set and maintain meaningful objectives and strategies without learning about key influencing factors in your external and internal business contexts. These can affect your ability to perform, reduce uncertainty and act with integrity so constant monitoring and analysis of influencing factors is critical. Start by considering current objectives and strategies as you design what you need to learn.

DEVELOPED BY



WITH CONTRIBUTIONS FROM



Understand the External Business Context

External factors influence how you establish and maintain appropriate objectives, detailed strategies and resilient capabilities. Monitor and analyze changes to create actionable information.



Evaluate the Internal Business Context

How you "do business" has a key influence on setting or changing objectives, strategies or capabilities. Learn about business plans and operations and develop a clear understanding of how organizational culture and risk decision-making guidance from leadership are driving actions.



Define the Points of Impact & Relationships

Changes in each factor may have different impacts and potential for cumulative or cascading effect. Be sure to map each factor to areas of management or business operations they might affect so that you can provide timely information to the right people.



Establish the Priorities & Process

Prioritizing items to be monitored will ensure continued flow of information about significant changes to and from management. Adjust priorities and processes as new information arises or changes occur in objectives, strategies or operations.



KEY STEPS

1. Map all external information, third party relationships, and corporate objectives and strategies into a baseline view of the business environment.
2. Establish monitoring priorities based on analysis of the potential impacts of changes in each external factor on current objectives and strategies.
3. Define pathways and triggers for feedback loops and workflows to respond to and escalate identified issues or changes that present critical or time sensitive threats or opportunities.
4. Continuously monitor the identified priorities and track the external environment for changes that may alter priorities.
5. Respond to information about changes promptly and fine tune monitoring and future responses based on lessons learned.

KEY STEPS

1. Develop a full view of business operations, including third party operations, and identify how each contributes to meeting objectives.
2. Define and track activities and controls that affect ability to meet strategic and operating plans.
3. Monitor tone and behavior modeled by leadership and how their examples are followed.
4. Learn in advance about possible changes in objectives, strategies or operations.
5. Determine how capabilities address risk and compliance to support performance.

KEY STEPS

1. Conduct impact assessment on policies, procedures, controls and training.
2. Determine potential impact on operations, third party relationships, supply chain and business continuity.
3. Evaluate likely cumulative or enhanced impact from multiple changes.
4. Understand appropriate response to each impact and ensure organization is ready and able to execute.
5. Assess organizational resiliency and risk capacity.

KEY STEPS

1. Develop multiple channels ensuring high impact changes will be identified quickly and elevated for consideration.
2. Ensure all operational relationships and risks, including third parties, are fully mapped when setting priorities.
3. Establish pathways to report on potential, planned and actual changes including cumulative impacts.
4. Change monitoring for any revised objectives, strategies, risk assessments, operations or defined actions and controls.
5. Ensure reports are provided on any impacts requiring reconsideration of tactics, strategies or objectives.

INTEGRATED INFORMATION MANAGEMENT AND TECHNOLOGY



Learning Lessons for Principled Performance

BY CAROLE SWITZER

Imagine your company has an objective for global expansion and you've established a strategy that requires the use of many third parties to build products, develop sales contracts, and make deliveries. Your products contain some parts that are obtained from yet more third parties and the production of some result in toxic waste streams. Your products are sold to a variety of customers including government agencies, and the deliveries will cross many borders.

So, you put in place a due diligence process for signing up all those third parties, you rely on them to identify the disposal requirements for each waste stream and the export/import rules that will apply, and you put some training, policies, and controls in place to prevent bribery or corruption with regard to the government sales process. All seems good.

Time goes by, and you merge with another company that also has third parties doing similar work, and you expand into even more countries. Sales are up and still all is good, or so it seems.

But then, you hit a few bumps in the road.

Unbeknownst to you, several of your third parties have been acquired and are now owned by a group of individuals who are, shall we say, less than savory in their known business practices, and some bribery charges arise. It turns out that environmental regulations have tightened up in a few of the countries where your third parties operate (or where they have moved production without your knowledge). That has made their costs (and yours) sky rocket where they have complied, and enforcement has caused shut downs where they haven't.

Now, one of the key parts in your best selling product is only available from two suppliers, and they are both located in an area of extreme geopolitical upheaval that puts their operations at risk, but you don't really get that until civil war breaks out and supplies are disrupted. It comes to light that your finance team has started taking risks beyond the level at which leadership is comfortable and the culture in that group is driving the behavior. One of your key third parties has been substituting counterfeit parts, but you don't know that either until a major customer suffers a significant product failure as a result. To top it off, leadership is contemplating yet another merger and to prepare is planning some extreme reductions in workforce.

If you had known about any of these changes as (or better yet before) they occurred, what might be different? You might have added layers of controls to ensure products were built as required. You could have lined up alternative third parties or helped them to gain

new parts suppliers. You could have evaluated whether the newly acquired third-party relationships that came from the last merger (or from the next one) support or detract from your strategy and operational approaches. You would have made sure that risk appetite and tolerances were not only communicated, but followed.

Your risk assessments and GRC capabilities to manage performance, risk, and compliance that relied on those assessments would all have been reconsidered and many changed. You might have changed some of your objectives or the strategies that support them. In any case, you would have been agile and able to respond quickly to the changes; picking your shots instead of being behind the proverbial eight ball.

Many of us have faced some version of this scenario, in which we don't have information that we need to know in time to use the knowledge to our advantage. And yet, if we are going to achieve principled performance, and be able to set and meet objectives while addressing uncertainty and acting with integrity, we must establish a way to learn necessary information about changes and how they might affect our performance. We need to know what is changing in the external business environment, be it through regulatory intelligence, third-party oversight, or monitoring of geopolitical, environmental, and other areas of risk. We need, just as much, to have a handle on internal culture, risk taking, and ethical conduct, and we must be on top of planned and actual changes to business operations and strategies. We must know where the impacts will hit us if various changes come to pass and consider the cumulative effects as well.

We have to be ready to change our controls, tactics, strategies, and even objectives if need be, to achieve principled performance. That is why the concept of "Learn" is the first component in OCEG's GRC Capability Model. If we don't stay on top of our game by observing change, analyzing what it means for us and responding appropriately, everything else we do—from risk assessments to action on strategic and operational plans to compliance efforts—will be stagnant and just plain wrong before we know it.

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.

Aligning the Organization for Principled Performance

BY CAROLE SWITZER

We all know that keeping a car's wheels in alignment is essential. Misalignment causes a lot of problems, from loss of steering control to reduction in the safety and durability of the tires. In the same way, alignment failures in the GRC capabilities of an organization can knock us off the pathway to principled performance, cause us to swerve beyond the boundaries of acceptable operations, use up resources unwisely, and put the organization at risk.

But what does alignment really mean? And what needs to be aligned? Is alignment in the GRC context just about keeping risk management, compliance, and technology in line with each other, or is there more?

Alignment is defined by Merriam-Webster, as the "proper positioning or state of adjustment of parts ... in relation to each other." And the term "proper" is defined as "of the required type; suitable or appropriate."

Going back to the car, anyone determining the proper alignment for its wheels must consider how the car will be operated and the impact that forces such as speed, tire pressure, road or off-road conditions, and load weight will have. There isn't one setting that is right for every vehicle in every situation; proper alignment depends on conditions in which the car will be used and staying in alignment requires continual attention to changes brought about by those forces and conditions. Alignment is not just about the relationship of the wheels to each other, it also is about the relationship of the objectives you have for use of the car and the relationship of the conditions that will exist with that use so that the vehicle will operate at its optimum state.

The same is true for alignment in an organization. It is not enough to ensure, for example, that risk management activities are aligned throughout the organization to use the same techniques and reporting styles, or to align all parts of GRC technology into a unified architecture; although both of these are important aspects of alignment in high-performing GRC capabilities. It is also essential to ensure that the GRC capabilities stay aligned to the objectives of the organization and that those objectives are aligned to the business environment and realities of available resources. This demands a principled performance approach, to ensure the reliable achievement of objectives while addressing uncertainty and acting with integrity. We have to always ask ourselves:

» How do we ensure strategies for addressing opportunities, threats, and requirements align to the internal and external business context, organizational culture and decision-making criteria set by leadership?

» How can we know if compliance actions and controls align to both mandated and voluntary requirements?

» How will we align our resources with a strategy that optimizes the use of our people, processes, information, and technology to keep the organization agile, resilient, and lean?

» How should we establish performance, risk and compliance indicators (KPIs, KRIs, and KCIs) that align to established outcome objectives and decision-making criteria?

It must begin with leaders at all levels articulating the goal of principled performance and demonstrating the pathway to its achievement in word and deed. We must incorporate the goals of managing uncertainty and acting with integrity into stated objectives and decision making, and define risk appetites, tolerances, and capacities before confirming objectives and strategic plans. Then, leadership must provide decision-making criteria and guidance to ensure management actions and controls support the objectives while managing uncertainty

Alignment continues with ongoing evaluation of the factors that may affect the ability to achieve objectives, making adjustments as necessary. We must regularly assess current and planned approach to address threats, opportunities, and requirements, taking into consideration the possible need to revise objectives or strategic direction. Changes in each factor may have different impacts and potential for cumulative or cascading effect, so we must be sure to map each factor to areas of management or business operations they might affect and provide timely information to the right people.

And today, just as the mechanical operation of your car is supported by multiple integrated onboard computers, the need for alignment of the business calls for the use of modern technology that provides a repository for all relevant information and reporting capabilities for a variety of needs. Having consistent and reliable information, metrics, and triggers for review of established management actions and controls is essential to establishing alignment and keeping the organization agile, resilient and responsive to change.

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.

Align the Business for Principled Performance

SWITZER: Any organization's success depends on the coordination of many moving parts and attention to many details that are constantly in flux. The goal of principled performance—the reliable achievement of objectives while addressing uncertainty and acting with integrity—depends on having strategies and tactical plans that ensure many parts of the organization work together off of the same information. Why do you think the concept of alignment is useful as we discuss this need?

LIN: Alignment is one of the key building blocks your company needs in order for your GRC program to be successful. Alignment ensures that all components of your GRC ecosystem are focused on the same goals and are coordinated toward the same effort. It's almost easier to talk about what happens when alignment is missing. If audit and risk are working toward specific targets, but the ethical culture of the organization is not aligned with those same targets, can the company truly achieve its goals?

A program that is out of alignment will never fully achieve company objectives, or protect the company as fully as it should. Alignment ensures that all parts of the enterprise are working toward those objectives and that the people, processes, and technology are coordinated to make that happen.

CALDWELL: In the end all of us GRC professionals have the same mission. Whether we are in audit, risk management, compliance, legal, or security, it is our mission to protect, preserve, and perform—the three Ps.

Achieving the three Ps, though, becomes much more difficult if we are not all coordinating our activities. We don't all have to be pulling the same direction at the same time, but we do need to understand each other, follow the same first principles, agree on the policies, and use the same language to describe key performance indicators, key risk indicators, and key control indicators. So having a common understanding of objectives, the risks to those objectives, and the rules and policies that we have to follow in getting to those objectives is fundamental to a high-performance enterprise. Not that a GRC solution is the sole answer to that, it is simply not possible to maintain that common understanding over time without a common system of record for sharing information.

SWITZER: So, do you set objectives and then align strategies and tactics for management of risk and compliance to those objectives? Or do you consider the business context—both internal and external—to see what the objectives should be? Do you start somewhere and go step by step or is it all going on at the same time?

CALDWELL: Achieving alignment to business strategy and objectives through GRC requires both top-down and bottom-up approaches. Most organizations begin with a bottom-up approach; that is, they have as a goal gaining more productivity in their GRC activities whether that is

audit, risk management, cyber-security, or compliance. They are overwhelmed with managing their program through spreadsheets, home grown applications, and niched solutions. That means getting a particular program on a scalable application that doesn't require a lot of manual effort to support the management and reporting within their silo. That's when many GRC leaders realize that truly to be effective they need a common view of which risks are most significant and which rules have the greatest impact on the business. The only way to know that is to focus on the common goals and objectives of the business, and to do that you have to understand the business strategy, the objectives of the strategy, the risks to those objectives, and regulations and related rules and policy.

So, it is okay to start from the bottom up—you must relieve your immediate pain, but the sooner you also incorporate the top down approach, the sooner you will be able to prioritize the GRC program's priorities in a way that also delivers the right risk and compliance information to decision makers that help them to drive the business forward to achieve its objectives.

LIN: Realistically, when you're looking at the business context, you're always going to have higher risk areas that demand prioritization. There are regulatory and legislative demands that vary by industry that need to be considered. It's helpful to start with a compliance risk assessment, because that allows you to analyze the risks that are the most critical in your business context in the larger context of the external business and regulatory landscape. Once you've assessed your risks, you can map your current program against those risks and set objectives that align with both the business objectives at large and your largest risks.

Technology can be tremendously useful in this regard, because it allows you to manager that entire process in one place and document it as you go. An integrated GRC solution also allows you to access and report on data from all aspects of your program, so you can spend less time gathering data and more optimizing your program to achieve better results.

SWITZER: Clearly, you can't manage or plan for every threat, opportunity, or new requirement that might arise with the same level of attention and resources. So how do you go about assessing and prioritizing what should be addressed at what level as you perform, control, and measure outcomes of your performance, risk, and compliance management?

LIN: This ties back into the compliance risk assessment I mentioned earlier. Without a clear picture of the risks that are most relevant to your organization, your industry and the regulations you're subject to, it's really difficult to begin to prioritize and pull a plan together. Once you have that assessment in place, you can take an inventory of the resources you have available to address them, such as

manpower, processes already in place, and technological systems you have to support you. After that, it's a matter of assigning resources (or building the business case for further resources) to each threat depending on the size and urgency of the threat, your risk tolerance and the overall goals of the business. It's equally important to have a monitoring process so that you're not caught unaware by a shift in the regulatory landscape. This is where having a trusted, knowledgeable business partner, such as your GRC solutions vendor, becomes a critical extension to the resources you have.

CALDWELL: You can only prioritize by having that common view of the business objectives. However, we have to keep in mind that there are activities within each silo that have to be done no matter what. Saying that the requirements for privacy compliance, for instance, are not directly related to the launch of a new product may be true, but one data breach and you may lose customer confidence and sales of that product might slow because of the damage to your reputation.

SWITZER: Assuming your leadership has set objectives that align to the realities of the business context and available resources and that take into account the organization's risk culture, how do you go about the next step of establishing detailed strategies and tactics to support those objectives? And how do you make sure that the activities and controls you establish stay in alignment with each other and with those objectives as changes take place that affect the correctness of your decisions? How do you even make sure you know those changes are taking place?

CALDWELL: Over the years, I've observed that most executives are very familiar with the business strategy and objectives, and they believe they know the risks. In reality they don't know all the risks and the rules that impact those objectives. That information is typically two or three levels down. However, the managers and employees and those levels often have an insufficient understanding of the strategy and objectives. Effective GRC programs ensure that the relevant information on risks and controls for managing those risks and adherence to regulations is surfaced to the executive and board level. However, the corporate directors and executives do not manage those risks and controls on

a daily basis, so knowledge of risks and controls at senior levels is insufficient. What we have to do as GRC leaders is to ensure that our programs also communicate the business strategy and objectives to those people who are managing risks and controls on a daily basis. That requires knowing what the KPIs for those objectives are, and mapping KRIs and KCIs to those objectives.

Of course, the business environment is dynamic—objectives change, and new risks and rules emerge, so this is a continuous process, not just something that is done once a year during the strategic planning exercise. So continuous scanning and communications is required throughout the organization. GRC has to become pervasive. Pervasive GRC is the next stage of evolution to achieve our purpose—the 3Ps of protect, preserve, perform.

LIN: Understanding your risk landscape through assessments is a good starting point, but to execute on risk mitigation and compliance culture building activities is much more difficult. And this comes back to alignment. As executives set goals for various departments, we need to train our organizations to think about risk in the context of those objectives. For example, is your sales goal for emerging markets so lofty that you will inadvertently incent rogue behaviors, like bribery, in order to achieve those objectives? When I think about alignment, I also think about balance. You have to take a balanced approach to provide clear goals and objectives for middle management. Once you start executing on your tactics, it is important to be aware of changes and ensure your objectives continue to stay in line. This is where continuous measurement is key. I think compliance professionals are often overwhelmed when we refer to continuous measurement or monitoring, but an integrated GRC platform makes reporting easier while also helping you identify shifts in trends. Work together, as a GRC ecosystem team to monitor these metrics and determine if shifts in tactics are necessary to achieve principled performance.

ROUNDTABLE PARTICIPANTS



MODERATOR
Carole Switzer
Co-Founder & President,
OCEG



French Caldwell
CEO, Chief Evangelist,
MetricStream



Jimmy Lin
VP of Product Mgmt & Corporate
Development, The Network,
a NAVEX Global company

What Do We Need to Align for Principled Performance?

Leaders must align an organization's objectives to its defined mission, vision and values but that is not enough to guarantee success. Objectives and strategies also must be based on consideration of the business environment within which the organization operates and the internal culture regarding governance, risk, workforce and ethical conduct. Management of risk and compliance must align to the objectives for performance. Start by establishing alignment so that you set, maintain and achieve appropriate goals while addressing uncertainty and acting with integrity.

DEVELOPED BY



WITH CONTRIBUTIONS FROM



Set the Direction of the Pathway to Performance

Leaders at all levels should articulate the goal of Principled Performance and demonstrate the pathway to its achievement in word and deed. Incorporate the goals of managing uncertainty and acting with integrity into stated objectives and decision-making guidance.

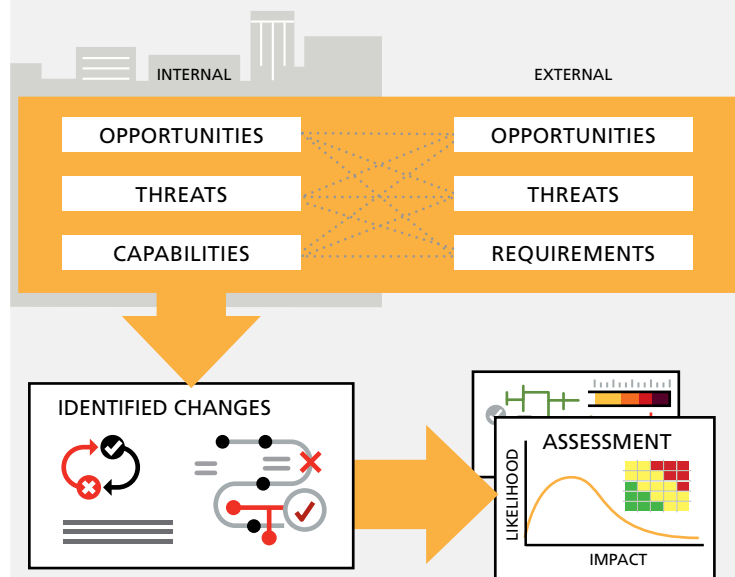


KEY STEPS

1. Prepare statements about risk appetite, tolerances and capacity, along with decision-making guidance, for use in setting objectives and strategies.
2. Consider the impact analyses for influencing factors in the external business environment and internal business context, then set or adjust objectives and strategies.
3. Ensure objectives are measurable and consistent with the criteria set for acceptable levels of risk, performance and compliance in light of the stated mission, vision and values.
4. Issue instructions that limit and guide management as it sets detailed objectives and strategies throughout the organization.

Assess Threats, Opportunities and Requirements

There are many factors that affect the ability to achieve established objectives or that may compel the organization to conduct itself in a particular way. It is essential to establish integrated management of performance, risk and compliance aligned with the stated objectives, but to do so you must determine priorities for management actions and controls.

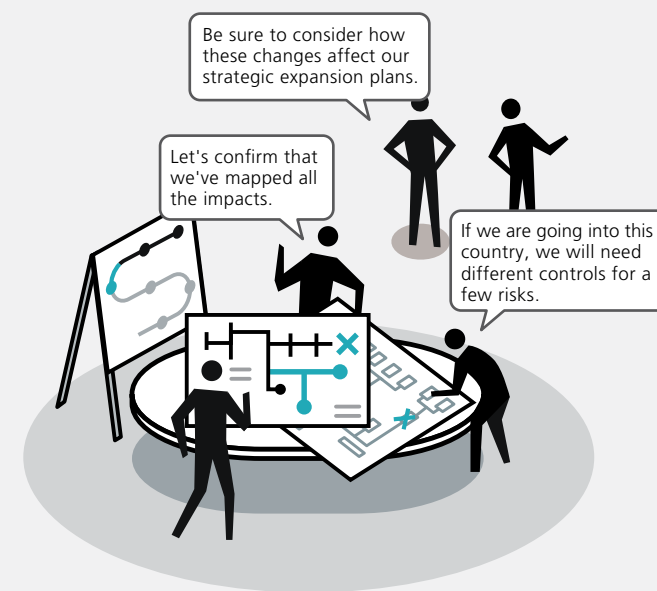


KEY STEPS

1. Regularly consider results from evaluation of external business environment and internal business context that identify a requirement, find a threat to achievement of objectives or highlight an opportunity.
2. Evaluate existing capabilities (people, process, technology and information) and how they affect ability to achieve objectives while addressing uncertainty and acting with integrity.
3. Identify how opportunities, threats and requirements relate to one another and prioritize them.
4. Assess current and planned approach to address threats, opportunities, and requirements, taking into consideration the possible need to revise objectives or strategic direction.

Develop Integrated Strategic and Tactical Plans

Changes in each factor may have different impacts and potential for cumulative or cascading effect. Be sure to map each factor to areas of management or business operations they might affect so that you can provide timely information to the right people.

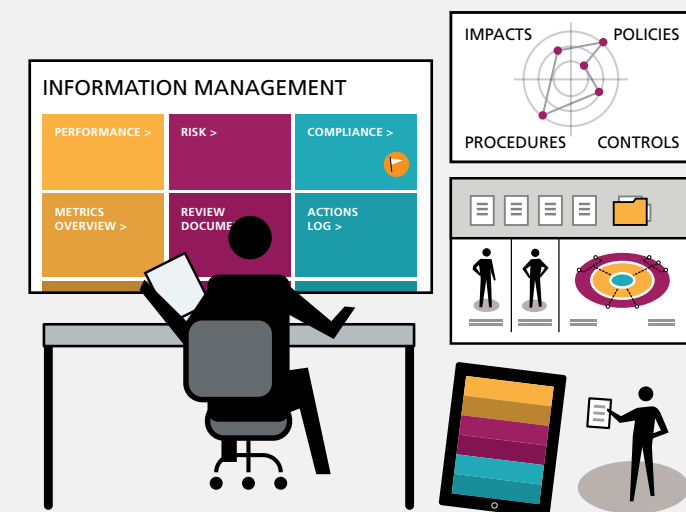


KEY STEPS

1. Determine strategies and tactics for achievement of objectives while addressing uncertainty and acting with integrity that include risk and compliance management aspects.
2. Design actions and controls to address each opportunity, threat and requirement according to the impact each may have on objectives as identified in assessments.
3. Develop Key Indicators - Develop key indicators that inform management about the effectiveness of actions and controls including level of reward, risk and compliance.
4. Integrate and embed the management of performance, risk and compliance within mainline operations to enhance ownership and accountability throughout the organization.

Ensure Technology and Information Management Support Objectives

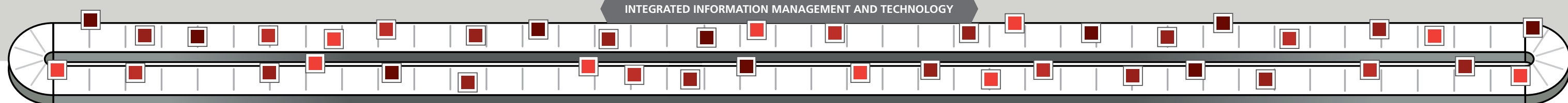
Today's technologies aid in management of performance, risk and compliance by providing a repository for all relevant information and reporting capabilities for a variety of needs. Having consistent and reliable information, metrics and triggers for review of established management actions and controls makes the organization more agile, resilient and responsive to change.



KEY STEPS

1. Evaluate where technology use is appropriate based on priorities and complexity and establish triggers for re-evaluation.
2. Identify needed changes in existing technologies (or how they are used) and any additions or substitutions after establishing GRC processes and taking inventory of current approaches.
3. Establish information and communication plans and policies.
4. Integrate plans with change management activities

INTEGRATED INFORMATION MANAGEMENT AND TECHNOLOGY



[GRC ILLUSTRATED] AN OCEG ROUNDTABLE, PART 3: PERFORM

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 gamechanger 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 Csuite 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

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

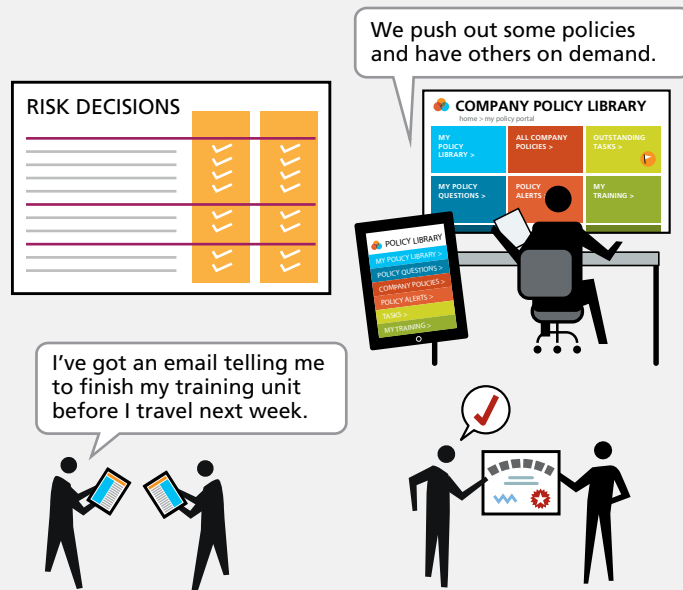


WITH CONTRIBUTIONS FROM



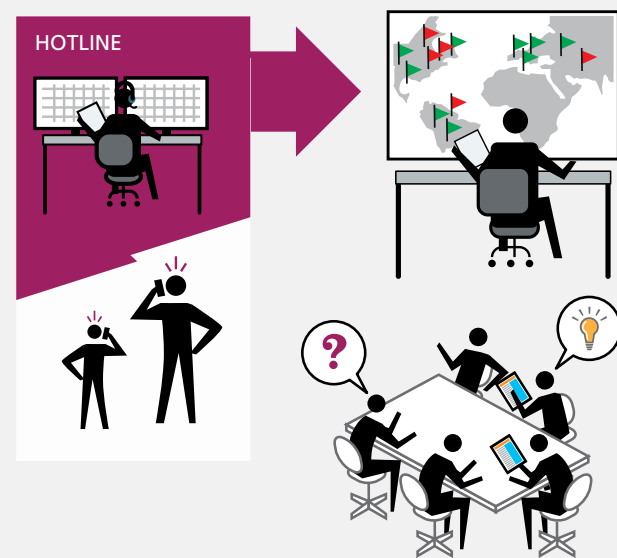
Proactive Actions and Controls

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.



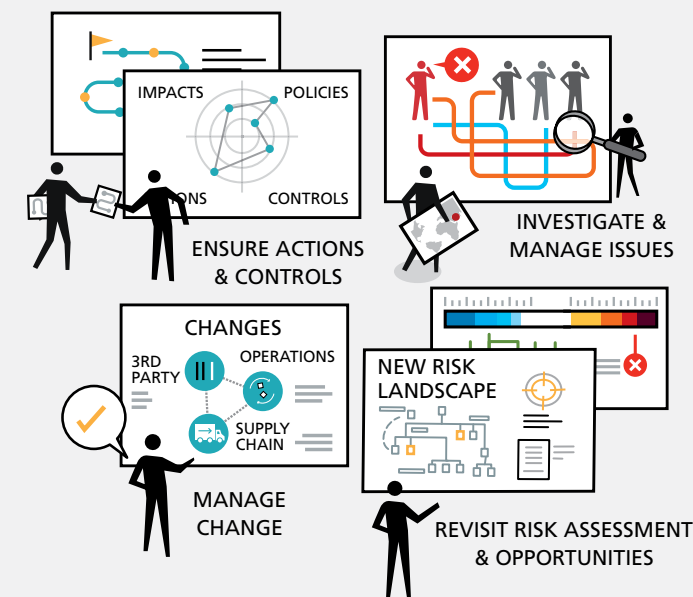
Detective Actions and Controls

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.



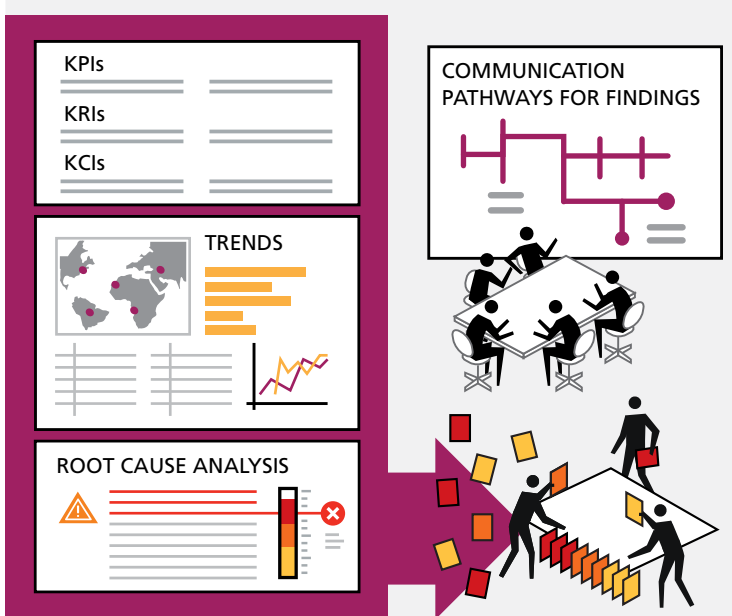
Responsive Actions and Controls

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.

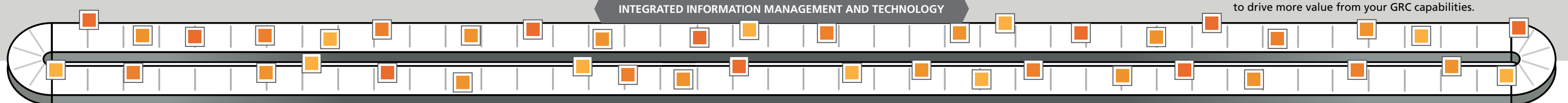
KEY STEPS

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.

INTEGRATED INFORMATION MANAGEMENT AND TECHNOLOGY



Let's Change the Way We Talk About Controls

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

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.

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.

The GRC Audit Quandary

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.

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.

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?

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 reperforming 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.

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

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

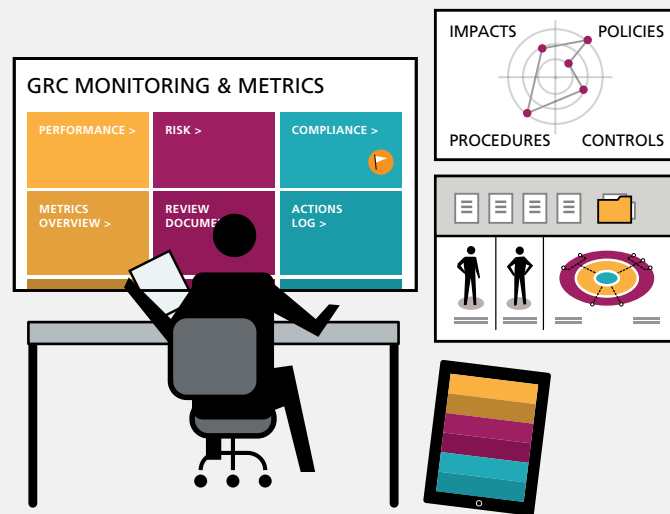


WITH CONTRIBUTIONS FROM



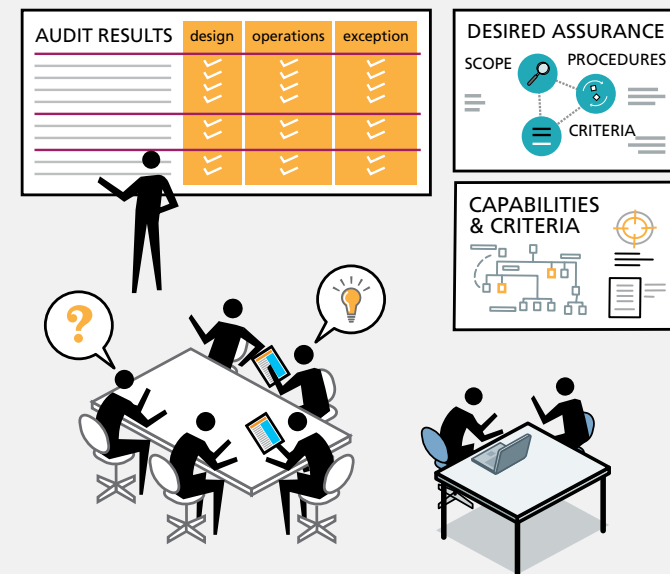
Monitor Defined Actions and Controls

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.

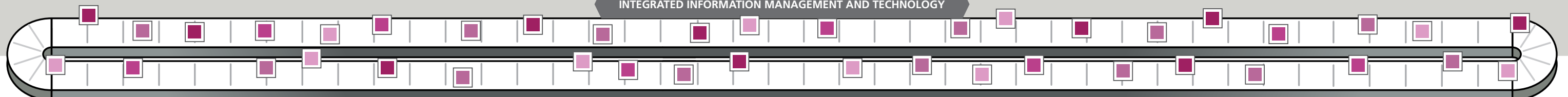
KEY STEPS

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.

INTEGRATED INFORMATION MANAGEMENT AND TECHNOLOGY





FUTURE-PROOF YOUR CAREER

Level up your skills and get the GRC Professional (GRCP) certification by OCEG, the nonprofit think tank that invented GRC

Everything is included in a single fee:

Online preparation

Online exam

Online continuing education

www.oceg.org/cw-ebook

