Aligning the Organization for Principled Performance

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

By Carole Switzer

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.

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

GRC Illustrated

Align Your Business 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 OCEG®

WITH CONTRIBUTIONS FROM MetricStream THE Network A NAVEX Global Company

Set the Direction of the Pathway to Performance

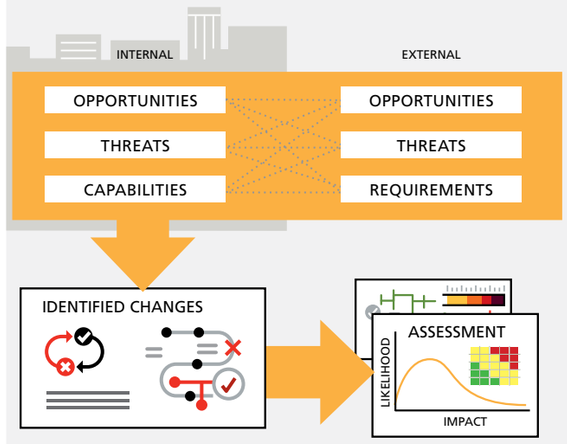
Leaders at all levels should articulate the goal of Principled Performance and demonstrate the pathway to its achievement in word and deed. Incorporate the goals of managing uncertainty and acting with integrity into stated objectives and decision-making guidance.

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

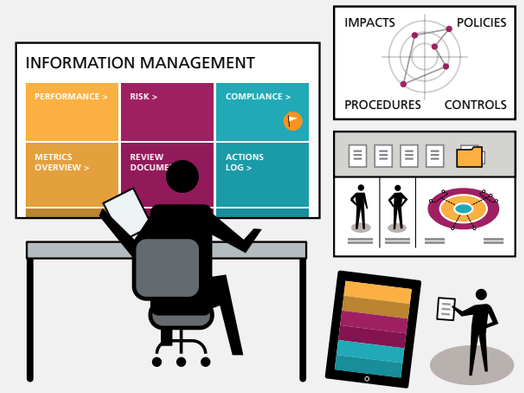
Changes in each factor may have different impacts and potential for cumulative or cascading effect. Be sure to map each factor to areas of management or business operations they might affect so that you can provide timely information to the right people.

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.

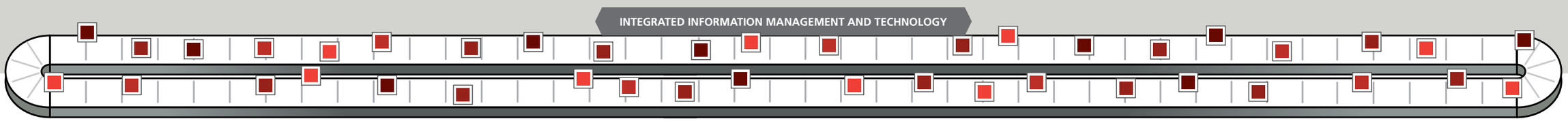
Ensure Technology and Information Management Support Objectives

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



[AN **OCEG ROUNDTABLE**]

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
Chief Evangelist
MetricStream

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

[GRC ILLUSTRATED]