Learning Lessons 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

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.

Switzer

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.

COMPLIANCE WEEK

GRC Illustrated

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.

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.

DEVELOPED BY oceg®

WITH CONTRIBUTIONS FROM hiperos THOMSON REUTERS workiva

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.

THIRD-PARTY RELATIONSHIPS
REGULATORY & LEGAL ENFORCEMENT
ECONOMICS / GEO-POLITICS
EXTERNAL STAKEHOLDER VIEWS
SOCIETAL / ENVIRONMENTAL STANDARDS
MARKET DEMANDS
TECHNOLOGY ADVANCEMENTS

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.

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.

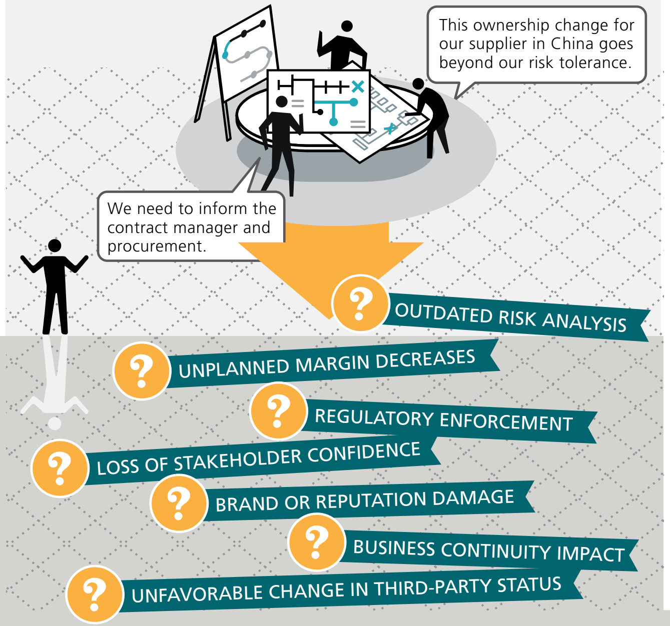
RISK TOLERANCE
GOVERNANCE AND TONE
STRATEGIC AND OPERATING PLANS
TRAINING AND COMMUNICATION
WORKFORCE CULTURE
POLICIES
THIRD-PARTY RISKS AND PERFORMANCE
POLICIES AND CONTROLS

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.

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.


This ownership change for our supplier in China goes beyond our risk tolerance.
We need to inform the contract manager and procurement.
OUTDATED RISK ANALYSIS
UNPLANNED MARGIN DECREASES
REGULATORY ENFORCEMENT
LOSS OF STAKEHOLDER CONFIDENCE
BRAND OR REPUTATION DAMAGE
BUSINESS CONTINUITY IMPACT
UNFAVORABLE CHANGE IN THIRD-PARTY STATUS

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.

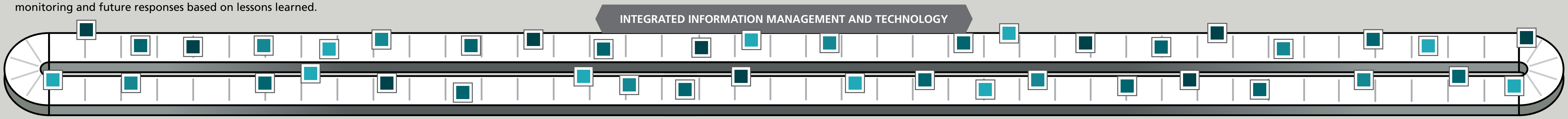
Establish the Priorities & Process

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.

MONITOR & REPORT
PLAN
ENSURE ACCOUNTABILITY
CHANGES
3RD PARTY
OPERATIONS
SUPPLY CHAIN
MAP IMPACTS
DEVELOP CHANNELS
IMPACTS
POLICIES
PROCEDURES
CONTROLS
NEW RISK LANDSCAPE

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.



[AN **OCEG ROUNDTABLE**]

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