Originally Published January 12, 2016, 12:01 AM ET

Compliance Risks: What You Don't Contain Can Hurt You

As global regulations proliferate and stakeholder expectations increase, organizations are exposed to a greater degree of compliance risk than ever before. Specifically, compliance risk is the threat posed to a company's financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice.

To understand their risk exposure, many organizations may need to improve their risk assessment process to fully incorporate compliance risk exposure. The case for conducting robust compliance risk assessments can be made given today's business complexity, but it is also deeply rooted in the U.S. Federal Sentencing Guidelines for Organizations, which establish the potential for credit or reduced fines and penalties should an organization be found guilty of a compliance failure. Nevertheless, according to a survey conducted jointly by Deloitte & Touche LLP and *Compliance Week,* 40% of companies do not perform an annual compliance risk assessment.[1]

How do Compliance Risk Assessments Differ?

Organizations conduct assessments to identify different types of organizational risk. For example, they may conduct enterprise risk assessments (typically owned by the CFO or Chief Risk Officer) to identify the strategic, operational, financial, and compliance risks to which the organization is exposed. In most cases, the enterprise risk assessment process is focused on the identification of "bet the company" risks—those that could impact the organization's ability to achieve its strategic objectives. Many organizations also conduct internal audit risk assessments that likely consider financial statement risks and other operational and compliance risks.

While both of these kinds of risk assessments are typically intended to identify significant compliance-related risks, neither is designed to specifically identify legal or regulatory compliance risks. Therefore, while compliance risk assessments should certainly be linked with the enterprise or internal audit risk processes, they generally require a more focused approach. That is not to say that they cannot be completed concurrently, or that they ought to be siloed efforts—most organizations may be able to combine the activities that support various risk assessments, perhaps following an initial compliance risk identification and assessment process.

Table 1. The interrelationship among enterprise risk management (ERM), internal audit, and compliance risk assessments

	ERM	Internal audit	Compliance
Objective	Identify, prioritize, and assign accountability for managing strategic, operational, financial, and reputational risks	Determine and prioritize risks to aid in developing the internal audit plan, helping to provide the board and the executive team with assurances related to risk management efforts and other compliance activities	Identify, prioritize, and assign accountability for managing existing or potential threats related to legal or policy noncompliance—or ethical misconduct—that could lead to fines or penalties, reputational damage, or the inability to operate in key markets
Scope	Any risk significantly impacting the organization's ability to achieve its strategic objectives	Financial statement and internal control risks, as well as some operational and compliance risks that are likely to materially impact the performance of the enterprise or financial statements	Laws and regulations with which the organization is required to comply in all jurisdictions where it conducts business, as well as critical organizational policies—whether or not those policies are based on legal requirements
Typical owner	Chief Risk Officer/Chief Financial Officer	Chief Audit Executive	Chief Compliance Officer

Understanding Top Compliance Risks

The compliance risk assessment will help the organization understand the full range of its risk exposure, including the likelihood that a risk event may occur, the reasons it may occur, and the potential severity of its impact. An effectively designed compliance risk assessment also helps organizations prioritize risks, map them to the applicable risk owners, and effectively allocate resources to risk mitigation.

Building a Framework and Methodology

Because the array of potential compliance risks facing an organization is typically very complex, any robust assessment should employ both a framework and methodology. The framework lays out the organization's compliance risk landscape and organizes it into risk domains, while the methodology contemplates both objective and subjective ways to assess those risks.

The framework needs to be comprehensive, dynamic, and customizable, allowing the organization to identify and assess the categories of compliance risk to which it may be exposed. Some compliance risks are specific to an industry or organization—for example, worker safety regulations for manufacturers or rules governing the behavior of sales representatives in the pharmaceutical industry. Other compliance risks transcend industries or geographies, such as conflicts of interest, harassment, privacy, and document retention.

Figure 1. Enterprise ethics and compliance program and risk exposure program: An illustrative example

An effective framework may also outline and organize the elements of an effective risk mitigation strategy that can be applied to each compliance risk domain.
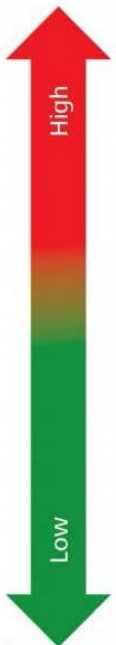
Applying the Methodology and Conducting the Risk Assessment

Using an objective methodology to evaluate the likelihood and potential impact of each risk can help the organization understand its inherent risk exposure. "Inherent risk" is the risk that exists in the absence of any controls or mitigation strategies. At the outset, gaining a preliminary understanding of inherent risk helps the organization develop an early view on its strategy for risk mitigation. And when organizations identify inherent risk, they should consider key risk drivers that can be organized into the following four broad categories:

- **Legal impact:** Regulatory or legal action brought against the organization or its employees that could result in fines, penalties, imprisonment, product seizures, or debarment.
- **Financial impact:** Negative impacts with regard to the organization's bottom line, share price, potential future earnings, or loss of investor confidence.
- **Business impact:** Adverse events, such as embargos or plant shutdowns, that could significantly disrupt the organization's ability to operate.
- **Reputational impact:** Damage to the organization's reputation or brand—for example, bad press or social-media discussion, loss of customer trust, or decreased employee morale.

It is important to provide both quantitative and qualitative measures for each category. However, as with all risk assessments, precise measurement may be elusive. In the case of risks with direct financial impact, an actual monetary value may be measurable with respect to the risk. Another way to evaluate risk is using a criticality scale that indicates the extent of impact should noncompliance occur. Extent of impact can be described in qualitative terms. For example, for reputational impact, low impact might be minimal to no press coverage, while high impact might be extensive negative press in the national media.

Figure 2. An illustrative criticality scale

Rating	Reputational fallout/ Brand damage	Civil or criminal fines or penalties	Loss of sales/ customer confidence
High	Sustained U.S. national (and international) negative media coverage (front page of business section)	Major federal or state action/ Fraud or bribery investigation	Significant loss or harm of customer relationship(s), including customer shut downs
	Negative U.S. national or international media coverage (not front page)	Federal or state investigations	Failure of ability to meet customer needs, e.g., significant quality issues, customer delays, or inability to deliver products to customer
	Negative media coverage in a specific U.S. region or a foreign country	Routine costly litigation	Ineffective products delivered to customers or delay in customer delivery
	Localized negative impact on reputation (such as a single large customer) but recoverable	Smaller actions, penalties/fines	Less than optimal acceptance by customers
Low	No press exposure	No regulatory or legal action	Limited, if any, impact on customers

Determining Residual Risk

While it is impossible to eliminate all of an organization's risk exposure, the risk framework and methodology help the organization prioritize which risks it wants to more actively manage. Developing a framework and methodology can help organizations determine the extent to which the organization's existing risk-mitigation activities (for example, testing and monitoring or employee training programs) are able to reduce risk.[2] Effective risk mitigation activities may reduce the likelihood of the risk event occurring, as well as the potential severity of impact to the organization.

When an organization evaluates inherent risk in light of its existing control environment and activities, the degree of risk that results is known as the "residual risk." If existing risk mitigation strategies are insufficient at reducing residual risk to an acceptable level, this is an indication that additional measures are in order.

Elements of a Leading Compliance Risk Assessment

While every compliance risk assessment is different, the most effective have a number of things in common. CFOs should consider the following leading practices when working with their Chief Compliance Officers to evaluate the assessment:

—**Gather input from a cross-functional team.** A compliance risk assessment requires the participation of deep subject matter specialists from the compliance department and across the enterprise. It is the people living and breathing the business—those in specific functions, business units, and geographies—who truly understand the risks to which the organization is exposed, and will help ensure all key risks are identified and assessed. In addition, if the methodology is designed in a vacuum without consulting the risk owners, the output of the process may lack credibility when it comes to implementing mitigation programs.

—**Build on what has already been done.** Rather than starting from scratch, look for ways to leverage existing material, such as enterprise risk assessments, internal audit reports, and quality reviews, and integrate compliance risk content where appropriate. Be sure to communicate the differences between the compliance risk assessments and other assessments to groups you seek to engage. Clearly, the output of each risk assessment process should inform and connect with each of the others.

—**Establish clear risk ownership of specific risks and drive toward better transparency**. A comprehensive compliance risk assessment can help identify those individuals responsible for managing each type of risk, and make it easier for executives to get a handle on risk mitigation activities, remediation efforts, and emerging risk exposures.

—**Make the assessment actionable**. The assessment both prioritizes risks and indicates how they should be mitigated or remediated. Remediation actions should be universally understood and viable across borders. Be sure the output of the risk assessment can be used in operational planning to allocate resources and that it can also serve as the starting point for testing and monitoring programs.

—**Solicit external input when appropriate.** By definition, a risk assessment relies on knowledge of emerging risks and regulatory behavior, which are not always well known within the organization. Tapping outside expertise can inform the assessment and ensure that it incorporates a detailed understanding of emerging compliance issues.

—**Treat the assessment as a living, breathing document.** Once you allocate resources to mitigate or remediate compliance risks, the potential severity of those risks will change. The same goes for events in the business environment. All of this should drive changes to the assessment itself.

—**Use plain language.** The assessment needs to be clear, easy to understand, and actionable. Avoid absolutes and complex legal analysis.

—**Periodically repeat the risk assessment.** Effective compliance risk assessments strive to ensure a consistent approach that continues to be implemented over time (e.g., every one or two years). At the same time, risk intelligence requires ongoing analysis and environment scanning to identify emerging risks or early warning signs.

—**Leverage data.** By incorporating and analyzing key data (e.g., hotline statistics, transactional records, audit findings, compliance exception reports), organizations can gain a deeper understanding of where existing or emerging risks may reside within the business. Many organizations are considering investments in technology, such as analytical and brand monitoring tools, to help leverage and analyze data to strengthen their risk-sensing capabilities. Additionally, organizations are considering investments in data, including traditional media/negative-mention monitoring, social-media data, surveying, and other data sources.

The constantly changing regulatory environment increases the vulnerability of most organizations to compliance risk. The complexity of the risk landscape and the penalties for non-compliance make it essential to conduct thorough assessments of compliance risk exposure. A good ethics and compliance risk assessment includes both a comprehensive framework and a methodology for evaluating and prioritizing risk. With this information in hand, organizations may be better able to develop effective mitigation strategies and reduce the likelihood of a major noncompliance event or ethics failure, setting themselves apart in the marketplace from their competitors.

— Produced by Nicole Sandford, Partner, National Practice Leader, Enterprise Compliance Services; Keith Darcy, Independent Senior Advisor; Maureen Mohlenkamp, Principal; and Nolan Haskovec, Senior Manager, all of Deloitte & Touche LLP

Endnotes

1. In focus: 2014 Compliance Trends Survey. http://www2.deloitte.com/us/en/pages/risk/articles/compliance-trends-survey-2014.html

2. For additional information on the components of a world-class ethics and compliance program. http://www2.deloitte.com/us/en/pages/risk/articles/building-world-class-ethics-and-compliance-programs-making-a-good-program-great.html

Related Resources:

How Assessing Compliance Culture Can Raise Ethical Standards

More Standalone CCOs Are Taking Compliance Reins: Survey

Designing Testing and Monitoring Components for Strong Ethics and Compliance

Email and Cyber Archiving: Regulatory Compliance Challenges

In Focus: 2015 Compliance Trends Survey