Deloitte.

Compliance risk assessments
The third ingredient in a world-class ethics and compliance program

You can't mitigate a risk if you don't know it's there

As global regulations proliferate, and as stakeholder expectations increase, organizations are exposed to a greater degree of compliance risk than ever before. Compliance risk is the threat posed to an organization'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 is deeply rooted in the U.S. Federal Sentencing Guidelines for Organizations, which establishes the potential for credit or reduced fines and penalties should an organization be found guilty of a compliance failure. In today's environment of global regulatory convergence, ever-increasing complexity, and the expansion of businesses into new or adjacent industries, the need for a broader view of compliance risk has never been greater. Nevertheless, according to a survey conducted jointly by Deloitte and *Compliance Week*,[1] 40 percent of companies do not perform an annual compliance risk assessment.

Many ethics and compliance officers will likely agree that new ethics, compliance, and reputational risks appear each day. At the same time, the recent global recession forced many organizational functions to closely examine their budgets and resources. Together, these factors have created a tension between growing regulatory obligations and the pressure to do more with less. To help resolve this situation and continue to add value to their organizations, ethics and compliance professionals need to be sure they understand the full spectrum of compliance risks lurking in each part of the organization. They then need to assess which risks have the greatest potential for legal, financial, operational, or reputational damage and allocate limited resources to mitigate those risks.

How is a compliance risk assessment different from other risk assessments?

Organizations conduct assessments to identify different types of organizational risk. For example, they may conduct enterprise risk assessments 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. Most organizations also conduct internal audit risk assessments to aid in the development of the internal audit plan. A traditional internal audit risk assessment is likely to 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 (see illustrative table). 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.

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

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 your 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 these risks to the applicable risk owners, and effectively allocate resources to risk mitigation.

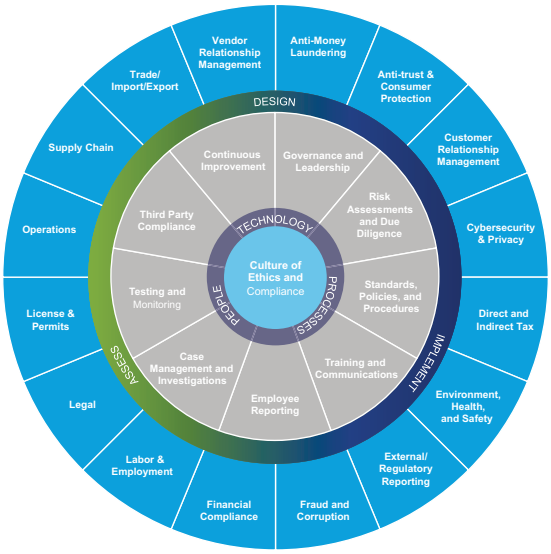
Building a framework and methodology

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 (see Figure 1). 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.

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.

Figure 1: Enterprise ethics and compliance program and risk exposure framework – An illustrative example (© Deloitte Development LLC)



Applying the methodology and conducting the risk assessment

Using an objective methodology to evaluate the likelihood and potential impact of each risk will 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 prove to 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 (see Figure 2).

Figure 2: An illustrative criticality scale (© Deloitte Development LLC)

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 helps 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. 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.

Some key questions about your exposure

There are a number of critical questions organizations should ask related to compliance risks and the program(s) in place to mitigate those risks:

- What kinds of compliance failures would create significant brand risk or reputational damage? Could the failures arise internally, in the supply chain, or with regard to third parties operating on the organization's behalf? What is the likely impact of that damage on the organization's market value, sales, profit, customer loyalty, or ability to operate?
- What kinds of compliance missteps could cause the organization to lose the ability to sell or deliver products/services for a period of time?
- How should the compliance program design, technology, processes, and resource requirements change in light of growth plans, acquisitions, or product/category/service expansions?
- Is the organization doing enough to inform customers, investors, third parties, and other stakeholders about its vision and values? Is it making the most of ethics, compliance, and risk management investments as potential competitive differentiators?
- What are the total compliance costs—beyond salaries and benefits at the centralized level—and how are costs aligned with the most significant compliance risks that could impact the brand or result in significant fines, penalties, and/or litigation?
- How well-positioned is the compliance function? Does it have a seat "at the table" in assessing and influencing strategic decisions?
- What are the personal and professional exposures of executive management and the board of directors with respect to compliance?

What makes a compliance risk assessment world class?

While every compliance risk assessment is different, the most effective ones have a number of things in common. To build a world-class assessment, consider the following leading practices:

- **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 will 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 will 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 that speaks to a general business audience:** 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, etc.), 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.

Conclusion

The constantly changing regulatory environment increases the vulnerability of most organizations to compliance risk. This is particularly true for those organizations that operate on a global scale. The complexity of the risk landscape and the penalties for non-compliance make it essential for organizations to conduct thorough assessments of their 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 will be 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.

Contacts

Please contact one of our Enterprise Compliance Services leaders for more information.

Nicole Sandford
Partner | Deloitte Advisory
National Practice Leader,
Enterprise Compliance Services
Deloitte & Touche LLP
+1 203 708 4845
nsandford@deloitte.com
Stamford, CT

Keith Darcy
Independent Senior Advisor to
Deloitte & Touche LLP
+1 203 905 2856
kdarcy@deloitte.com
Stamford, CT

Maureen Mohlenkamp
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 212 436 2199
mmohlenkamp@deloitte.com
Stamford, CT

Brian Clark
Partner | Deloitte Advisory
Deloitte & Touche LLP
+1 816 802 7751
bclark@deloitte.com
Kansas City, MO

Laurie Eissler
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 313 396 3321
leissler@deloitte.com
Detroit, MI

Nolan Haskovec
Senior Manager | Deloitte Advisory
Deloitte & Touche LLP
+1 212 436 2973
nhaskovec@deloitte.com
New York, NY

Kevin Lane
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 214 840 1577
kelane@deloitte.com
Dallas, TX

Thomas Nicolosi
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 215 405 5564
tnicolosi@deloitte.com
Philadelphia, PA

Holly Tucker
Partner | Deloitte Advisory
Deloitte Financial Advisory Services LLP
+1 214 840 7432
htucker@deloitte.com
Dallas, TX

Additionally, feel free to reach out to our team of former compliance officers who are located across the country and experienced in a wide variety of industries.

Martin Biegelman
Director | Deloitte Advisory
Deloitte Financial Advisory Services LLP
+1 602 631 4621
mbiegelman@deloitte.com
Phoenix, AZ
Industry: Technology

Rob Biskup
Director | Deloitte Advisory
Deloitte Financial Advisory Services LLP
+1 313 396 3310
rbiskup@deloitte.com
Detroit, MI
Industry: Consumer & Industrial Products

Timothy Cercelle
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 216 589 5415
tcercelle@deloitte.com
Cleveland, OH
Industry: Insurance

Michael Fay
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 617 437 3697
mifay@deloitte.com
Boston, MA
Industry: Investment Management

Howard Friedman
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 713 982 3065
hfriedman@deloitte.com
Houston, TX
Industry: Energy & Resources

George Hanley
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 973 602 4928
ghanley@deloitte.com
Parsippany, NJ
Industry: Insurance

Peter Reynolds
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 973 602 4111
pereynolds@deloitte.com
Parsippany, NJ
Industry: Investment Management

Thomas Rollauer
Director | Deloitte Advisory
Executive Director, Deloitte Center for
Regulatory Strategies
Deloitte & Touche LLP
+1 212 436 4802
trollauer@deloitte.com
New York, NY
Industry: Financial Services/Banking
& Securities