

Deloitte.



**Building world-class ethics
and compliance programs**

Five ingredients to meet
global expectations

Regulatory Risk ●

Risk powers performance.



Risk has traditionally been viewed as something to be minimized or avoided, with significant effort spent on protecting value. However, we believe that risk is also a creator of value and, approached in the right way, can play a unique role in driving business performance.

Take the issue of reputation risk. Following the global financial crisis, how organizations approached ethics and compliance quickly came under the microscope of regulators and the markets. Those organizations that were slow to respond found themselves in a never-ending scramble to defend their integrity or navigate each new regulatory demand. But some organizations took the opportunity to address their corporate culture, introduced new approaches to ethics and compliance, and used their enhanced reputation as a competitive advantage.

This guide discusses five core ingredients for establishing a world-class ethics and compliance program:

- Tone at the top
- Corporate culture
- Compliance risk assessments
- The Chief Compliance Officer
- Testing and monitoring

Today's leading organizations are those that have learned how to protect their value through risk management. Tomorrow's leaders will be those that recognize the opportunity for risk to also create value. Deloitte's Risk Advisory professionals around the world can guide you on that journey and help you transform your organization into a place where risk powers performance.

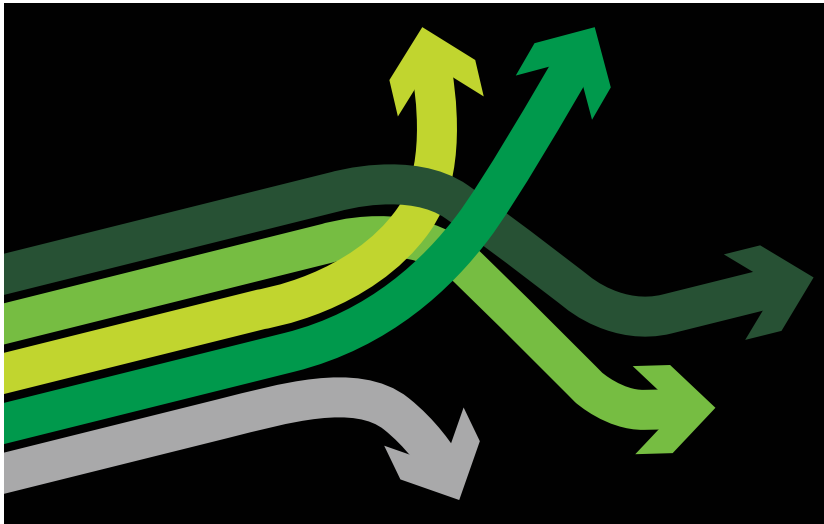
To learn more, please visit us at www.deloitte.com/risk.

Regards,

A handwritten signature in black ink that reads "Owen".

Owen Ryan
Global Risk Advisory Leader

How did we get here?



During the 1990s, the bulls were running wild. It was an era of unprecedented wealth creation, and global equity markets rose to stunning heights. During this same time, public and private sector gatekeepers took their eye off their fiduciary responsibilities to manage risk. When a number of high-profile corporate scandals broke, it exposed headline-grabbing issues of malfeasance. There was a devastating loss of trust in the equity markets, resulting in substantial declines. In the US alone, equity markets lost US\$7 trillion.¹ Painfully, these scandals evidenced widespread fraud, arrogance, conflicts of interest, and preferential treatment for people in high places.

In response, the US Congress passed The Sarbanes-Oxley Act of 2002, demanding greater accountability by boards and top executives. In particular, this law offered the platform to popularize the term “tone at the top,” clearly an element missing in the aforementioned scandals. In addition, the 2004 amendments to the US Federal Sentencing Guidelines created powerful incentives for corporations to “promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.”² Much of this legislation also emphasized the importance of assigning a high-ranking official to administer the organization’s ethics and compliance programs.

The focus on ethics and tone at the top that characterized legislation resulting from the financial crisis of the late 1990s was relatively US focused. Fast forward to 2008, when a global economic tsunami resulted in numerous bankruptcies, including failures in the financial services industry. The world stood as a powerless witness to the loss of more than 20 million jobs worldwide³ and a 37 percent decline in the value of global equities.⁴ In its wake, the meltdown exposed bribery and corruption, fraud, insider trading, conflicts-of-interest, money laundering, price fixing, and Ponzi schemes on an unthinkable scale. Then US President-elect Obama referred to it as an era of “reckless greed and irresponsibility.”

In response, the US Congress passed the expansive new requirements in the Dodd-Frank Wall Street Reform and Consumer Protection Act, coinciding with an unprecedented level of cross-border cooperation of regulators and prosecutors globally. Then, in March 2010, the Organisation for Economic Co-operation and Development (OECD) issued its Good Practice Guidance, which referenced that an effective system of internal controls must have “tone at the top, ethics standards, and a culture of integrity.” Forty-five nations are signatories to OECD. Then, in December 2014, promulgations by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) formally adopted provisions to its original guidance promoting tone at the top, ethics standards, and culture as integral to a comprehensive framework for reputation risk management. Other legislation, including the US Foreign Corrupt Practices Act of 1977 (FCPA) and the UK’s Bribery Act of 2010 address issues of corruption and have seen a significant increase in enforcement in recent years. Numerous other nations have adopted new anti-corruption laws, and there are significantly more prosecutions taking place worldwide.

Clearly, risks in today’s world are rising, as are the expectations from enforcement authorities. All told this adds up to a clear mandate for organizations everywhere: it’s time to get serious about developing a truly effective ethics and compliance program.

What are the ingredients of a great ethics and compliance program?

While there are a number of factors that separate the “good” from the “great,” in our experience, there are five ingredients that are key differentiators in the highest-performing ethics and compliance programs.

1

Tone at the top—The starting point for any world-class ethics and compliance program is the board and senior management, and the sense of responsibility they share to protect the shareholders’ reputational and financial assets. The board and senior management should do more than pay “lip service” to ethics and compliance. They need to empower and properly resource the individuals who have day-to-day responsibilities to mitigate risks and build organizational trust.

2

Corporate culture—A culture of integrity is central to any effective ethics and compliance program. Initiatives that do not clearly contribute to a culture of ethical and compliant behavior may be viewed as perfunctory functions instilling controls that are impediments to driving the “value change” of the enterprise.

3

Risk assessments—Ethics and compliance risk assessments are not just about process—they are also about understanding the risks that an organization faces. The risk assessment focuses the board and senior management on those risks that are most significant within the organization, and provides the basis for determining the actions necessary to avoid, mitigate, or remediate those risks.

4

The Chief Compliance Officer (CCO)—The CCO has day-to-day responsibility for overseeing the management of compliance and reputational risks, and is the agent for the board’s fiduciary obligations in this regard. A skilled CCO can create a competitive edge for their organization.

5

Testing and monitoring—A robust testing and monitoring program can help ensure that the control environment is effective. The process begins with implementing appropriate controls, which should be tested and ultimately monitored and audited on a regular basis.

On the following pages, we will explore each of these elements in greater detail.

Tone at the top

Tone at the top is what instills the organization with a culture of integrity.

Without question, reputation risks today are at least as great as strategic, operating, and financial risks. In fact, according to a Deloitte survey of more than 300 C-level executives worldwide, 87% rated reputation risk as more important than other strategic risks.⁵ Their concern is well founded: as we've seen again and again, once an organization's reputation is compromised, the impact can be devastating—from a plummeting stock price to a loss of customers.

Guarding against reputational risk begins with setting the proper tone at the top that the organization values and embraces a culture of integrity.

How can Chief Executive Officers (CEOs) create the right tone at the top? What role should the board play? How about the CCO? How does tone at the top cascade to the middle and beyond?

Who sets the tone?

In the context of an ethics and compliance program, the tone at the top sets an organization's guiding values and ethical climate. Properly fed and nurtured, it is the foundation upon which the culture of an enterprise is built. Ultimately, it is the glue that holds an organization together.

The board, the CEO, and the CCO play critical roles in setting the tone at the top.

The board

The starting point for setting the tone begins with the organization's governing authority—most frequently this means the board of directors. The board's most fundamental tasks would typically include hiring the CEO, approving strategy, monitoring execution of the plan, setting risk appetite, and exercising appropriate oversight regarding risk mitigations, all with the underlying goal of preserving and creating shareholder value.

“Sometimes, all it takes is a rumor, a hint of impropriety or malfeasance, or a social media post gone viral, to negatively impact shareholder value and damage—or worse, destroy—corporate and brand reputations in an instant.”

Nicole Sandford,
Deloitte Advisory National Practice Leader,
Enterprise Compliance Services, Deloitte & Touche LLP

The board sets the tone of the organization in the way that it executes each of these responsibilities. However, perhaps no single decision drives tone at the top more than the selection of the CEO. That process must necessarily focus on competence, character, and chemistry and raises questions such as the following:

- Does the prospective CEO have the requisite skills and experience to move the organization forward?
- Does the prospective CEO possess the character and moral fiber to model and contribute to the development of a values-centered enterprise and strategy?
- Does the prospective CEO have the chemistry and communication skills necessary to rally others to successfully and consistently deliver on the organization's value proposition to all stakeholders?

Boards must provide appropriate weight to each of these considerations. Too often, the CEO selection process focuses mostly on competence, with less thought given to character and chemistry.

Once selected, the board is accountable to monitor the CEO's performance based upon appropriate metrics for competence, character, and chemistry. In summary, the governing authority must ensure that ethical objectives are built into the actions and the strategy of the organization, and that they are not merely a statement of good intentions.

The CEO

Establishing the right tone at the top is much more than a system of compliance. Establishing the right tone is essential to fortifying the organization's reputation and its relationship with all stakeholders. The street is littered with corporate failures and sub-optimal performance from CEOs who have neglected to prioritize the development of a culture of integrity.

“People are suspicious of leaders who are closed about their values or standards. Stakeholders assume if you value nothing, you'll value anything.”

Philip Chong, Asia Pacific Governance, Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

The CEO is the face of the organization, the figurehead to whom employees ultimately look for vision, guidance, and leadership. A CEO's behavior tells employees what counts, and what's rewarded and punished. Leadership derives from trust, and trust is built upon a common understanding between people.⁶ Leadership, therefore, is relational, not transactional.

Tone at the top demands that leaders—and especially the CEO—find ways to connect with people inside and outside the organization. Leaders must openly and continually communicate their values, using different platforms and distribution systems. Unfortunately, many companies under-communicate values by a significant degree.

Developing a sense of shared values—a set of beliefs against which all decisions can be measured and tested—is increasingly the basis on which long-term strategies and successful implementations are built. Failure to align ethics and values to business strategies and operating plans bears potentially heavy costs.⁷

The CCO

Clearly, the Chief Compliance Officer plays a critical role in setting and reinforcing the tone at the top. The person selected for this role must be beyond reproach—someone whose integrity is clear and who can earn the respect of personnel at all levels. The character and stature of the person the board

and executive management team select to hold the CCO position is a powerful statement about the organization's commitment to ethics and compliance, as is the organizational positioning of the person within the executive leadership team.

The CCO contributes to tone at the top in both direct and indirect ways. The CCO has a built-in platform for reinforcing the organization's values; balancing the messaging related to sales and growth. The CCO is also the leader that employees seek out when they have ethical concerns. Therefore, he or she plays a crucial role in creating a “speak up” culture—an essential element of tone at the top.

In addition, the best CCOs seek out opportunities for the CEO to convey key ethics and compliance messages in both internal and external communications. He or she also proactively assists the board in both understanding and executing their role in setting the tone at the top.

Beyond the roles described above, the board and executive management help translate the “tone at the top” to a healthy “mood in the middle” by ensuring certain organizational practices are in place at all levels, including among others:

- **Recruiting and screening methodologies**—It begins with intake channels and screening for people's character, competence, and chemistry. Everyone in the hiring process should recruit for character first.
- **Socialization and training**—Organizations should create a seamless integration—beginning in orientation—to foster an ethical and compliant culture. Mentoring and additional training must offer consistent messages about what's valued.
- **Reward systems**—You get what you measure. Recognition and rewards should be aligned with desired values and behaviors. Everyone must be reviewed not only for what they do, but how they do it. Moreover, employees with the courage to step forward with ethical concerns must be appropriately recognized and rewarded to help encourage others to follow suit.
- **Employee exits**—People leaving the organization should be treated equal to how they were brought in. It sends a message regarding how people are valued.

Unique challenges

In creating the right tone, certain issues require special attention from the board and senior leaders. These unique challenges include:

- **Mergers and acquisitions**—Cultural integration is essential to a successful combination, especially in mitigating risks to the combined entity. Leaders must ensure that acquired employees don't feel plundered, exploited, or occupied.
- **Autonomous and decentralized operations**—The further away from headquarters, the greater the likelihood that something gets "lost in translation." Take time to understand and respect other peoples' cultures, and pay special attention to business units or individuals that operate with significant autonomy. Neither moral imperialism nor moral relativism works. Co-create a new understanding.
- **Discontents**—Nothing will undermine tone quicker than not addressing and dealing with individuals whose actions are contrary to the organization's beliefs.
- **Institutionalization**—Institutionalization of values is often the first step toward bureaucracy. The senior leadership helps set the tone at the top by keeping values and culture "fresh."

There is also another reality that must be recognized in developing tone. Given the proliferation of social media and mobile technologies, there are conversations going on between and among all stakeholders at any given moment. The world is becoming increasingly transparent. As a result, the gaps between a leader's words and actions can "go viral" in a nanosecond, thus undermining efforts to build a consistent message and tone. Where there are actions that cannot be spoken about, or words that cannot be put into action, the moral development of the enterprise can be undermined by cynicism.

Setting the right tone offers lasting benefits

At its most basic level, an organization is a community of people with common interests and shared values banded together to achieve a common goal.⁸ Increasingly, employees are saying they want to be identified with an organization that stands for something more than quarterly earnings and whose values align with their own. They want to take pride in what they produce. They want to admire the people with whom they work.⁹

Creating and maintaining the right tone at the top is an essential first step in creating an enterprise anchored to an effective ethics and compliance program. It also offers benefits that extend beyond compliance programs themselves—benefits that include both client and customer retention, increased employee engagement, and the establishment of an enduring brand.

Reinforcing tone at the top

- **Walk the talk:** Implement and publish board operating principles that align with the organization's values, and provide specific responsibilities for acting in an ethical manner at all times.
- **Remember the water cooler:** When making difficult decisions about unethical behavior involving anyone in a management role, assume both the ethical breach, and your response to it, will be widely known within the organization. Think about how the decision may reinforce—or conflict with—the company's stated values.
- **Keep an ear to the ground:** Use new technologies to monitor the corporate buzz. What are your employees, customers, and other stakeholders saying about the organization's culture in social media and other digital platforms?
- **Reward for principled performance:** Include ethics and compliance in performance goals for C-suite executives, and tie those goals to compensation.
- **Build an ethical corporate ladder:** Consider the ethics and compliance track record when promoting people into senior leadership roles, particularly as part of succession planning.

Corporate culture

A culture of ethics and compliance is at the core of a strong risk management program.

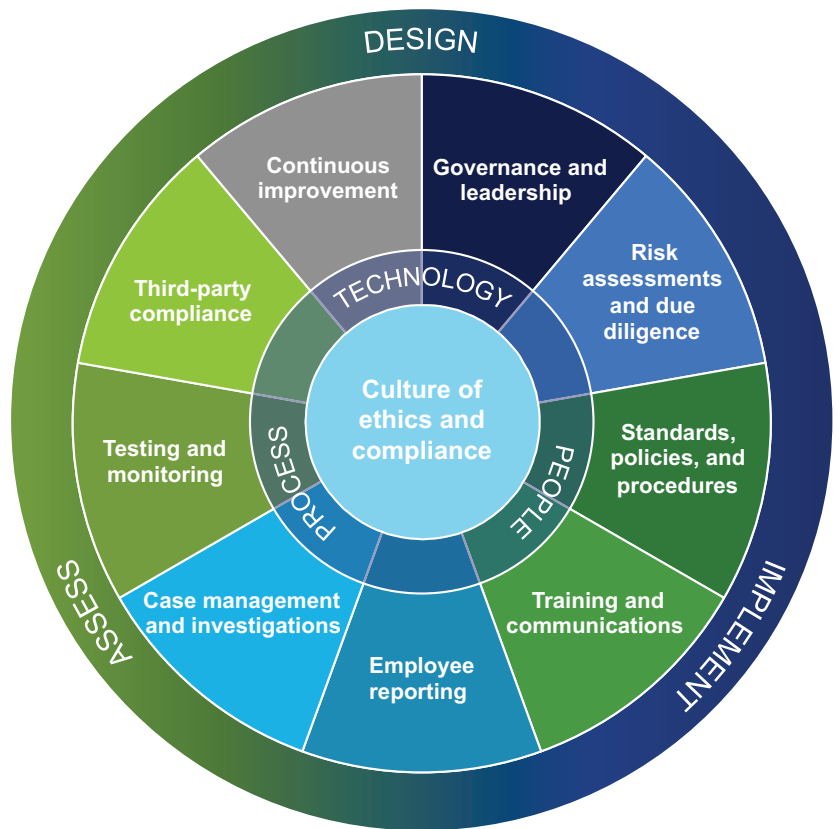
In a business environment where reputational threats lurk around every corner, a strong culture of ethics and compliance is the foundation of a robust risk management program. The lessons learned related to scandals and organizational crises that trace back to the early 2000s make one thing clear: without an ethical and compliant culture, organizations will always be at risk. In fact, more and more, culture is moving from a lofty, “squishy” concept to something that should be defined, measured, and improved (see Figure 1).

Culture has always been important to how organizations operate. So why is it getting so much attention lately? One reason is that regulators have come to the realization that without a culture of integrity, organizations are likely to view their ethics and compliance programs as a set of check-the-box activities, or even worse, as a roadblock to achieving their business objectives. In fact, organizations responsible for some of the most egregious acts of malfeasance have had quite impressive, formalized ethics and compliance guidelines. The problem was either leadership or a group of influential insiders operated outside of those guidelines.

What is a culture of integrity?

Culture is one of the biggest determinants of how employees behave. Strong cultures have two common elements: there is a high level of agreement about what is valued, and a high level of intensity with regard to those values. Of course, not all cultures encourage good or ethical behaviors. When it comes to developing world-class ethics and compliance programs, the starting point is a positive culture of integrity.

Figure 1: Culture is the foundation



The Deloitte Ethics and Compliance Framework recognizes that an ethical and compliant culture is the core element of an organization’s ethics and compliance program. If the culture of the organization does not support principled performance, then all of the people, processes, and technologies that are put in place to mitigate ethics and compliance risks are suboptimized.

A culture of integrity is generally characterized by:

- **Organizational values**—A set of clear values that, among other things, emphasizes the organization's commitment to legal and regulatory compliance, integrity, and business ethics.
- **Tone at the top**—Executive leadership and senior managers across the organization encourage employees and business partners to behave legally and ethically, and in accordance with compliance and policy requirements.
- **Consistency of messaging**—Operational directives and business imperatives align with the messages from leadership related to ethics and compliance.
- **Middle management carries the banner**—Front-line and mid-level supervisors turn principles into practice. They often use the power of stories and symbols to promote ethical behaviors.
- **Comfort in speaking up**—Employees across the organization are comfortable coming forward with legal, compliance, and ethics questions and concerns without fear of retaliation. When people believe that they will be heard, their level of trust in the organization increases. This in turn leads to higher-performing teams and increased employee engagement.
- **Accountability**—Senior leaders hold themselves and those reporting to them accountable for complying with the law and organizational policy.
- **The hire-to-retire life cycle**—The organization recruits and screens employees based on character, as well as competence. The on-boarding process steeps new employees in organizational values, and mentoring also reflects those values. Employees are well-treated when they leave or retire, creating colleagues for life.
- **Incentives and rewards**—The organization rewards and promotes people based, in part, on their adherence to ethical values. It is not only clear that good behavior is rewarded, but that bad behavior (such as achieving results regardless of method) can have negative consequences.
- **Procedural justice**—Internal matters are adjudicated equitably at all levels of the organization. Employees may not always agree with decisions, but they will accept them if they believe a process has been fairly administered and they have been treated as such.

Organizations with strong positive cultures create trusting relationships with stakeholders. In our experience, those relationships become reciprocal; that is, stakeholders trust the enterprise and the brand. This creates employee, customer, and supplier loyalty. A strong culture helps to build positive relationships with regulators and it helps attract long-term investors. Ultimately, a culture of integrity is reflected in superior, long-term performance.

Facing up to the challenges

More and more organizations are choosing to create additional structure around their ethics and compliance program. This can include the appointment of a Chief Ethics Officer (or expanding the Chief Compliance Officer's role to include specific responsibility for the ethics program), enhancing the code of conduct and related controls and procedures, and improving accountability for ethical behavior through training and performance assessments. In our experience, these actions are a great start toward the creation of a strong culture and will benefit the broader efforts around risk management and compliance.

Establishing a strong culture of integrity is not a discrete project with a beginning and an end, nor is it always smooth sailing. Despite best efforts, many organizations may run up against a number of obstacles.

“Culture sets expectations and guides behavior. When the organizational culture upholds integrity, people know that it needs to inform their actions.”

Philip Chong, Asia Pacific Governance,
Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

Defining the culture

Most leaders believe they understand and can define their organization's culture. However, often there is a gap between management's perception of the culture and how the rest of the enterprise views it. It is a mistake for leaders to assume they always have their finger on the pulse of the organization's culture. To get a more accurate picture, organizations can set up listening posts, such as cultural assessments using employee surveys and outside observers. It is especially helpful to offer avenues, such as focus groups, run by third parties, for employees to provide open-ended responses that truly reflect their perceptions of the enterprise.

Instilling culture and values throughout the organization

While executive leadership may work hard to establish a culture of integrity at headquarters, something often gets lost in translation as one moves farther away from the central office. This is why attention to culture needs to be active and continuous, especially in large organizations with distant outposts. Values—with ethics and integrity at their core—must be clearly and consistently communicated. Messaging needs to be explicit and repeated, so that it becomes embedded in how work gets done.

Communicating culture can be especially challenging when crossing borders. It is important that everyone understands the expected behaviors of the enterprise and the principles against which decisions will be made. Values need to be articulated in a manner that transcends nationality—for example, the concepts of honesty and trustworthiness are universally acknowledged. Nevertheless, it is important to recognize that cultural differences will influence how messages are heard and interpreted, and adjustments may need to be made in training, employee onboarding, and performance reviews.

Extending cultural values to mergers and acquisitions

Cultural fit is one of the biggest stumbling blocks in integrating a merged or acquired organization; in fact, it is one reason such transactions fail, despite the potential business benefits. This is why executives may want to conduct a cultural "audit" as part of the due diligence process. If the target acquisition diverges significantly from a buyer's values, this could be a red flag. A well-developed integration plan will ensure both entities understand and reinforce desired values. From day one, management needs to let new employees know that they are welcome. At the same time, leaders need to communicate how the organization expects them to behave and how they can expect to be treated in return.

Handling the naysayers

Nothing will damage culture more than the malcontents. When people get in the way of supporting the culture, they can cause roadblocks and undermine the efforts of the enterprise. They must be identified, counseled, and offered the opportunity to conform to expected behavior, or they should be separated from the organization. Training programs focusing on ethics and compliance are one way to communicate values to individuals who may need additional reinforcement. As a next step, performance reviews should be structured to include an evaluation of not just an individual's results, but should also reflect how results were achieved. Some organizations even make adhering to values part of the goal-planning process by setting objectives that are tied to specific cultural elements.

Battling values fatigue

While ongoing communication is essential, organizations should avoid delivering exactly the same message again and again. This is because messages can get stale, causing employees to ignore the underlying values and principles. Communicating values is much like a marketing campaign—it needs to capture people's attention and use different content, formats, and communication channels to remain fresh. One way to achieve this level of interest is through the power of stories. Stories can not only make values concrete, they connect people to those values in ways other forms of communication cannot.

Addressing leadership flux

When organizations experience rapid turnover of CEOs and other senior leaders, maintaining a consistent identity and set of values can sometimes be a challenge. Clearly, selecting the right individuals to lead the organization is critical. If everyone in the organization lives its values, then promoting from within is one way to ensure those values remain intact. But that is not always either practical or possible. The board is usually involved in external hiring of senior leaders, especially CEOs. They need to pay particular attention to cultural fit and consider candidates who are not only competent, but who have the chemistry, character, and moral capability to inspire and win the hearts and minds of all stakeholders. Regardless of the CEO selection, it is important that culture not be dependent on a single person or group. A robust ethics and compliance program—appropriately designed, positioned, and resourced—will survive executive changes at the top of the organization.

Appealing to a cross-generational workforce

Revolving leadership is not the only source of change that can undermine culture. Employee turnover can threaten it as well. Organizations today need to appeal to the most multi-generational workforce in history.¹⁰ For both financial and other reasons, baby boomers are not necessarily leaving work the minute they hit age the traditional retirement age. Many are choosing to remain employed, sometimes postponing promotional opportunities for younger, Generation X workers. At the same time, Millennials entering the workforce are often driven by a sense of purpose and crave a more collaborative culture. They are more likely to pursue portfolio careers in which they change jobs frequently to seek organizations that fit with their values. To create cultures with staying power, organizations must therefore foster an environment that balances a “something for everyone” appeal, with a set of consistent values that all generations will be able to embrace.

Reinforcing culture and values

- **Create listening posts:** Conduct cultural assessments that get at the core of how people behave and what they think.
- **Maintain a healthy mood in the middle:** Much hinges on middle management’s ability to translate tone at the top into the policies and practices that drive everyday behavior.
- **Keep it interesting:** Find new and innovative ways to communicate cultural values and reward values-based behavior. Encourage storytelling to bring values to life.
- **Play fair:** Reward the right behaviors and penalize the wrong ones. Don’t play favorites.
- **Shout it from the rooftops:** Leaders tend to under-communicate values and expectations. In this case, more is better.

Values: the building blocks of culture

Organizations that have a strong sense of shared values are primed for success. Building a culture of integrity not only fortifies them against risk, but also leads to employee engagement and strong loyalties from all stakeholders. In the long run, a positive culture of integrity is the foundation for an effective ethics and compliance program, which, when properly embedded into an organization, can create a competitive advantage and serve as a valuable organizational asset.

Compliance risk assessments

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

As global regulations proliferate and become more complex, and as stakeholder expectations increase, organizations are exposed to a greater degree of compliance risk than ever before. Global regulatory convergence and the expansion of businesses into new or adjacent industries have also increased the need for a broader view of compliance risk.

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 so that it fully incorporates compliance risk exposure. Nevertheless, according to a survey conducted jointly by Deloitte & Touche LLP and *Compliance Week*,¹¹ 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 corporate 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 are designed to specifically identify legal or regulatory compliance risks (see Figure 2). 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.

Figure 2: 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 non-compliance—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

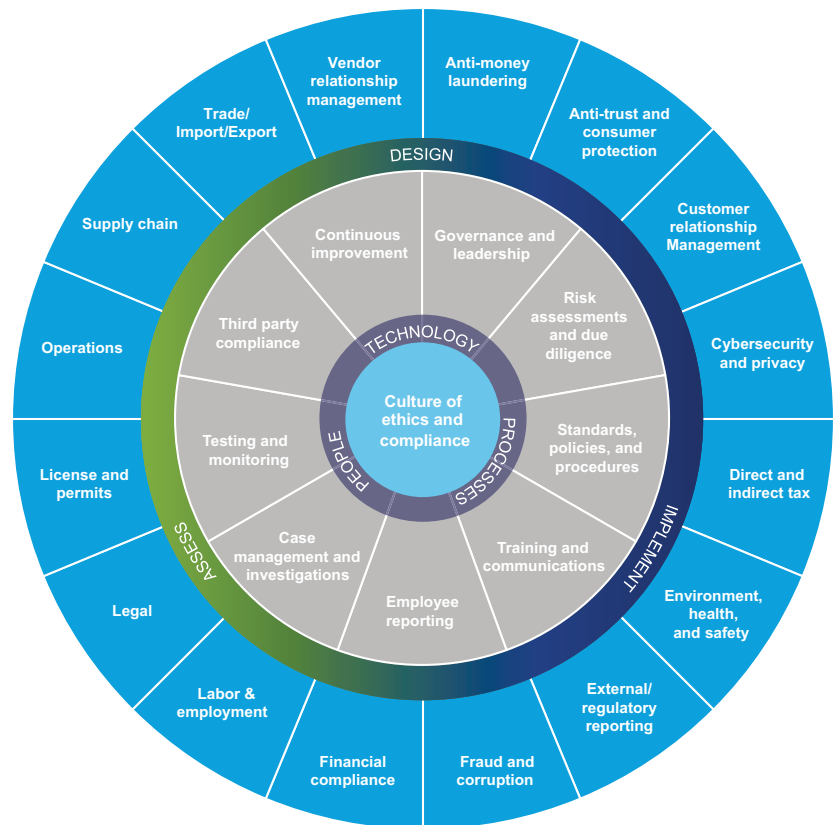
Understanding your top compliance risks

The compliance risk assessment can 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 3). 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 3: Enterprise ethics and compliance program and risk exposure framework



“Start by identifying what areas have the highest potential for violating the law. That way you can focus on preventing the most serious risks for your organization. To do that you need a solid understanding of the environment you are operating in.”

Marc Van Caeneghem, EMEA Governance, Regulatory & Risk Leader, Deloitte Touche Tohmatsu Limited

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 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 non-compliance 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 4).

Figure 4: An illustrative criticality scale



Rating	Reputational fallout/Brand damage	Civil or criminal fines or penalties	Loss of trust
	Sustained national (and international) negative media coverage (front page of business section), Social media news story gone viral	Major federal or state action/ Fraud or bribery investigation	Significant loss or harm of customer relationship(s), including customer shut downs
	Negative 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 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
	No press exposure	No regulatory or legal action	Limited, if any, impact on customers

“When it comes to risk assessments, some basic rules apply: always partner with business leaders, keep your methodology simple, but robust, and use documentation that is both intuitive and user-friendly.”

Henry Ristuccia,
Global Governance, Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

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.

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.

Assess for success

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 non-compliance event or ethics failure, setting themselves apart in the marketplace from their competitors.

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?

The Chief Compliance Officer

It takes an extraordinary leader to uphold the integrity of an organization.

Enterprise ethics and compliance executives represent a young, but rapidly maturing profession—one that began to emerge in the late 1980s when several government initiatives and high-level commissions began recommending that specific senior-level personnel should have responsibility for overseeing an organization's ethics and compliance program. These recommendations were reinforced by a host of new regulations and leading-practice guidance issued in the early 2000s.

In practice, the job responsibilities and the titles for these professionals vary, from Chief Compliance Officer (CCO)(with or without ethics responsibilities) to Chief Ethics Officer (with or without compliance responsibilities) to many models in between. Despite these variables in organizational design, individuals leading efforts to protect the company from ethics and compliance risks have a unique role and special importance within an organization. The principles discussed here apply to those leaders regardless of their title. Chief Compliance Officers now operate in a dynamic legal, regulatory, social, and economic environment that is often characterized by complex and sometimes conflicting rules and regulations. Regulatory expectations have risen globally placing tremendous pressure on organizations, particularly those with international operations. Designing programs that help ensure compliance with all of these regulations and guidelines falls squarely on the shoulders of CCOs.

Yet this is only a part of their responsibilities. CCOs must also respond to a host of rapidly emerging new risks. For example, enforcement authorities have reached an unprecedented level of cross-border cooperation in an effort to control bribery and corruption. Money laundering is no longer solely an issue for the banking sector, but for organizations across all industries. Cyber risk and digital crime represent enormous threats to businesses everywhere, and organizations need to step up their efforts to ensure compliance with internal policies designed to address those threats. In addition, a more aggressive focus on transparency has brought many previously hidden conflicts of interest to light.

“Risks are increasing and we are still in an environment of austerity. That’s a dangerous combination. To face the issue head-on, you need an astute CCO who can peer into the future and think strategically about tomorrow’s risks.”

Keith Darcy, Independent Senior Adviser to
Deloitte & Touche LLP

As a result of these developments, the CCO profession has begun to shift in ways that are subtle yet profound— an indication that organizations are acknowledging the significant role that CCOs play. In short, these key business leaders are responsible not only for maintaining compliance, but also for safeguarding what is arguably an organization’s most valuable asset: its reputation.

A profession in flux: Where the journey is heading

While for some organizations the CCO role remains frozen in time, for others, it has transitioned into one that is both strategic and value-adding. Companies with world-class ethics and compliance programs make sure they have a world-class CCO leading the charge. These individuals have helped to bring the profession to a new level. It’s a level that many aspire to—and it’s also an indication of where the profession is headed. Following are examples of how the role has evolved in some organizations over the last decade.

From compliance gatekeeper to risk manager

As the risk landscape continues to shift, and as ethics and compliance functions become more integrated into the fabric of organizations, CCOs are assuming a much more strategic role when it comes to helping organizations manage compliance and reputational risk. In the past, risk management was the purview of other areas of the organization, while the CCO focused primarily on routine compliance risk management activities. However, in more recent years, many organizations have begun to recognize that the risks CCOs mitigate—in particular, reputational risk—are critical. As a result, assessing and raising awareness of risks that could call the organization's integrity into question has become a key part of the CCO's job. Today's CCOs not only need an understanding of the full range of reputational risks, they need an instinct for what can go wrong and how their organizations can prepare.

“Leading CCOs are starting to crack the code on risk-sensing solutions that take familiar controls and technology and combine them in a ways that are brand new.”

Kevin McGovern, Americas Governance, Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

From legal program manager to senior-level adviser

Because a visible number of the CCO roles originated in response to enforcement activities, and because many of the more modern ethics and compliance functions evolved from regulatory compliance departments, many of the first CCOs came from legal backgrounds. These compliance officers either sat within, or reported to, the Chief Legal Officer (CLO). This has clearly begun to change.

In a recent survey of CCOs conducted jointly by Deloitte & Touche LLP and *Compliance Week*¹², only 21 percent of respondents said they reported to the General Counsel, while 36 percent said they reported directly to the CEO. Moreover, an additional 21 percent reported to the board of directors. From a governance perspective, especially in industries like financial services and health care, there is regulatory pressure for CCOs to move out from under the legal department: for money center banks, CCOs should report to the chief risk officer; in health care, The Department of Health and Human Services prefers to see an independent CCO, and one that is not subordinate in any way to the CLO. At issue, at least in part, is the concern that the CLO's fiduciary obligation is to its client, the company, but an independent CCO's obligation may be different. This compliance and legal restructuring is also reflected in the changing background of many who enter the profession today. Increasingly, these CCOs have broad-based experiences, including stints in operations where they have had profit and loss responsibilities. More and more, organizations seek dynamic CCOs who can think strategically, communicate and persuade effectively, and work cross-functionally. The most sought-after candidates for the CCO role have skills beyond the ability to design the necessary compliance architecture, assess risks from across the business, develop training and communication strategies, evaluate data, and conduct sometimes-critical investigations. These world-class leaders also have an aptitude for auditing and monitoring, the ability to influence organizational culture and behavior, and a solid grounding in public relations tactics, since a key part of their role is to clearly communicate the vision, mission, and strategy of the ethics and compliance program.

To be effective, CCOs need to be involved not just in day-to-day issues, but also in the strategic decisions facing the enterprise. As the importance and prominence of the role increases, some CCOs are moving to higher levels within their organizations, with a seat on the executive committee and unfiltered access to the board. The changing reporting structure for CCOs can send a strong signal to all stakeholders, including personnel and regulators, that the organization takes ethics and compliance seriously.

From checking boxes to asking questions

Fundamental to the CCO's role is designing programs that help to ensure compliance with laws, regulations, and enterprise policies. This requires spending considerable time on the nuts and bolts and making sure the right resources, systems, and controls are in place. But in the eyes of many, this is "Compliance 101." In today's global economy, where organizations are under pressure to achieve transparency across their entire supply chain, simply operating in compliance with the law may not be enough. Enforcement authorities require measures that go beyond what is legally required, including embedding a culture of integrity to achieve appropriate prevention and detection of improper behavior. CCOs need to be able to get out into the businesses and ask the hard questions in order to determine where the organization might be vulnerable or exposed.

"Today's CCO is a leader who can build alliances, enhance trust both inside and outside the organization, and work to strengthen brand and reputational value."

Henry Ristuccia, Global Governance, Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

From an expense to an asset

In organizations with more mature ethics and compliance programs, the CCO is viewed as a business enabler rather than a source of overhead. These organizations recognize that the CCO's efforts ultimately protect the organization's reputation—perhaps its most important asset. The value of a reputation can be quantified—it is quite simply the market capitalization of the enterprise. All it takes is a rumor or hint of malfeasance or a social media post gone viral and investor reaction can be swift and punishing. For companies that have suffered unfavorable news headlines, the value of maintaining integrity is more than apparent.

From living apart to building bridges

When the CCO role was in a more nascent state, many organizations kept their CCOs somewhat apart from the rest of the organization—perhaps in an effort to maintain structural and functional independence. As a result, many CCOs, positioned in the relative isolation of headquarters, would issue mandates, directives, and policies without an appreciation or understanding of the day-to-day business activities and pressures in the field. Eventually organizations began to realize the divisive and counterproductive effect of this arrangement, since it inhibited the CCO's ability to understand the organization's business processes, the risks to which their organizations were exposed, and the opportunities for greater compliance synergies and cost savings.

Over time, this began to change as CCOs emerged from behind their desks and started embedding with the businesses. Getting out and learning the business is especially important to gaining the trust of employees on the operational side, particularly when they are being asked to make changes to how they work. Today's CCO is a leader who can build partnerships, who can enhance trust within the organization and with all its stakeholders, and who can work to build brand and reputational value.

From no you can't, to yes we can

A common complaint and misperception about CCOs is that they are "police officers" or gatekeepers, whose primary duty is to point a finger at the activities that are disallowed by law or policy. In reality, CCOs in many organizations are viewed more and more as business partners, collaborators, strategists, and internal consultants. They add value by sitting down with the businesses and coming up with solutions for how to achieve objectives within the guidelines of what is permissible. Today's CCOs are more about starting conversations than shutting them down. When they can work hand-in-hand with the business to come up with a solution that works for everyone, this can become a competitive differentiator for the entire organization.

From down in the weeds to up in the trees

What began as a primarily administrative role— involving inventorying and understanding the detailed regulations and laws that applied to an organization— has changed. Today's CCOs are taking things to the next level—digesting and assessing risk information, determining what it means, and translating those insights into a consistent ethics and compliance program and framework for managing risks. In addition, the unprecedented velocity of change in the external environment means that CCOs must always be on the lookout for any new risks (for example, technological risks, customer information risks, emerging market risks) that are just over the horizon and may require enhanced policies or heightened enforcement. To prepare for these new and emerging risks, organizations need visionary CCOs who can view the entire risk landscape and “see around corners.”

From cleaning up to keeping clean

Over the years, a number of organizations have experienced the pain of an ethics or compliance crisis. In response, they have ramped up their compliance efforts for a specific period of time until the storm passed, later reducing the CCO's role to more of an administrative one. Clearly, this kind of short-term response is fraught with peril, and can send a strong negative message to employees and regulators about what matters most and how an organization conducts itself when it believes no one is watching. Organizations that take compliance seriously task their CCOs with developing processes and a mindset that weave integrity into the fabric of the organization.

A CCO for all seasons

As the volume and potential impact of compliance risks raining down on organizations threatens to overwhelm them, the CCO has emerged as a beacon in the storm. No longer seen as a functionary within the administrative branch of the legal department, a back-office indexer of regulatory requirements, or an obstructionist gatekeeper, today's CCO plays a strategic role within the organization. The CCO helps to shape organizational strategy, setting the “tone at the top” while gauging the “mood in the middle” and the “buzz at the base.” A visionary and activist, the CCO is instrumental to making compliance a dynamic, rather than a reactive, endeavor and establishing an ethics and compliance program that safeguards both the organization and its reputation.

Strategies for getting to world-class

Not every company has a world-class ethics and compliance program. But CCOs—whether they are new to the role or a more seasoned professional—who are intent on moving their organizations in a world-class direction, can start with a few leading practices:

- Cultivate the right stakeholder relationships
- Build your organization's and team's bench strength
- Define your legacy
- Separate out the urgent from the important
- Overcommunicate integrity and values so it's clear what matters most
- Become a trusted adviser to the businesses
- Develop a network of internal and external subject matter experts to support your growth and development
- Connect with your peers: sharing is common for CCOs across competitors and industries
- Stand up for what you believe is right
- Remember to stop, get out of the weeds, look up to the trees, and be strategic
- Manage your time and focus on priorities
- Be a lifelong learner: the best leaders are the best learners

Key considerations about the CCO role

Organizations intent on finding a world-class CCO and creating an environment where they can thrive should consider the following questions:

- Does the CCO have access to the board?
- Does the CCO occupy a sufficiently senior position (e.g., executive vice president, senior vice president, vice president)?
- How often does the CCO present to the board or a committee of the board?
- How is the CCO's performance measured?
- Does the CCO have sufficient oversight authority for compliance resources in the business units?
- Can the CCO drive or influence the organization's culture?
- Does the CCO have operational experience?
- Does the CCO have a good understanding of the business?
- Does the CCO have the knowledge and passion for the profession?
- Does the CCO communicate with people inside and outside the organization to see how others are experiencing the role?
- Is the CCO seen as a role model for integrity inside the organization?
- Does the CCO have an aptitude for understanding and managing current and emerging risks?
- Is the CCO viewed as an authentic leader?

Testing and monitoring

Testing and monitoring takes the pulse of the compliance program, ensuring its ongoing health.

Testing and monitoring is one of the most critical elements of an effective ethics and compliance program, and is a required program component in certain industries. Why? Because without testing, it is difficult or impossible to understand what is working and what needs enhancement. Similarly, robust monitoring programs serve as an early warning system that allows compliance professionals to identify—sooner rather than later—potential compliance issues.

As important as testing and monitoring are, they are often misunderstood and undervalued. Implementing and sustaining efficient and effective testing and monitoring programs continues to challenge organizations for many reasons, including the lack of skilled resources, the difficulty of design and of driving consistency across the enterprise, and the reliance on others in the organization for both the data and, in many cases, the execution of the programs.

The emphasis on other compliance program elements—such as risk assessments, training, or policies and procedures—has sometimes led to the undervaluing and under-resourcing of the testing and monitoring functions. As compliance programs mature, these elements serve as an invaluable source of information about deviations in expected behavior that might open the window to potential material or systemic compliance risks. What's more, companies often say that the implementation of new laws and regulations presents risk, yet this is an area that is often not tested, or not tested sufficiently, to determine whether the organization is complying with the requirements.

The lack of effective testing and monitoring can have a ripple effect on other areas of the compliance program. In a number of recent studies and surveys¹³, compliance professionals consistently indicated frustration with the quality of metrics used to measure the effectiveness of their compliance programs. The outcome of ongoing testing and monitoring programs—especially when considered over time—drives metrics that can point not only to the effectiveness of the program design, but also to the effectiveness of the program's operations. Although for some industries, particularly financial services, compliance metrics are already well established or even mandated, and for many companies these activities create new, more insightful metrics related to program performance than those compliance professionals have relied upon in the past.

Similarly, robust testing and monitoring—and the data associated with it—provides relevant and reliable information to stakeholders of the ethics and compliance program:

- **Regulators** view testing and monitoring activities as a demonstration of the company's commitment to ethics and compliance. Moreover, for some industries such as financial services, testing and monitoring programs are a regulatory requirement, and companies may face fines or penalties for failing to implement them.
- **Boards** require substantiated information on the effectiveness of the ethics and compliance programs in order to execute fiduciary duties.
- **Internal and external counsel** point to these activities as indicators of the company's diligence around ethics and compliance as part of their legal strategies.
- **Employees, customers, and investors** desire a deeper understanding of ethics and compliance programs and may even use this information to make employment, purchase, or investment decisions.

For all these reasons, and many others, we have identified a robust testing and monitoring program as the fifth distinguishing factor for a world-class ethics and compliance program.



Testing and monitoring: defined and contrasted

Many ethics and compliance professionals use the terms “testing” and “monitoring” interchangeably. While testing and monitoring may be two sides of the same coin, and one cannot be fully optimized without the other, they are not interchangeable. Many believe both their design and desired outcomes are quite different. Commonly recognized definitions of each are as follows:

- **Testing program:** A dynamic, risk-based, independent compliance oversight process designed to periodically select and review a sample of business products, services, communications, and other areas to gauge and report on the operating effectiveness of compliance controls and/or adherence to stated policies and procedures.
- **Monitoring program:** The ongoing surveillance, review, and analysis of key business performance and risk indicators that allows the organization to identify potential compliance violations. While many seek to implement “automated” monitoring programs, monitoring activities can be either automated or manual.

These definitions make the goals and objectives of testing and monitoring clearer; however, the specific steps for reaching these goals and objectives are not always easily defined. Even if regulatory expectations related to these critical elements are clear—as they may be in certain areas of the banking and pharmaceutical industries—detailed information about the specific testing and monitoring activities that will meet those expectations may not be. In other sectors, regulatory guidance related to the specific expectations of testing and monitoring activities may not be available at all. Even in cases where there is clarity around regulatory expectations, the design, implementation, and sustainment of an effective testing and monitoring program is one of the most challenging tasks facing those responsible for the risk and compliance functions.

In the next section, we will explore the distinguishing characteristics of “great” testing and monitoring programs.

“It is always a good idea to partner with subject matter specialists. A well-designed testing approach and a prior track record does not diminish the need for specialized knowledge when assessing the most critical compliance risks.”

Kevin McGovern, Americas Governance, Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

Great testing programs

Great testing programs have a number of common attributes:

Compliance is tested at the level of accountability.

In a great testing program, compliance testing is executed at each level of the organization. In this model, weak controls are quickly identified in the business where they are most likely to be quickly remediated.

- **The first line of defense:** At this level, the business unit leadership—which is primarily accountable for the development of controls and activities to prevent, detect, and respond to compliance failures—invests the time and resources to determine that such controls and activities are adequately designed and operating effectively.
- **The second line of defense:** Within the second-line testing program, the individuals who perform the testing must not be the same individuals who are responsible for the execution of the controls. Here, the compliance function—whether it be the “centralized” compliance function at headquarters, the compliance team within the business unit, or a combination of the two—should also invest time and resources to develop and execute independent compliance control testing. For purposes of executing the testing programs, these individuals are accountable to the independent compliance function, regardless of whether that function resides at “corporate” or within the business unit, under a federated compliance model.
- **The third line of defense:** Internal audit should be responsible for “testing the tests.” In some industries, internal audit plays a broader role. For example, in the financial services industry, internal audit functions go a step beyond testing the tests. Rather than rely on the results of second-line testing, they perform additional transactional and process-related testing.

In all instances, and at all levels, independence related to testing is an essential aspect of effective testing.

Regardless of industry sector, our experience indicates that a disproportionate number of compliance problems are identified by the third line of defense—internal audit. This may indicate that compliance testing in the business unit (the first line of defense) and in the compliance function (the second line of defense) is ineffective at identifying compliance vulnerabilities.

Programs draw on a range of skillsets. Outstanding testing programs involve professionals with specialized knowledge or skillsets that may be different from those found in a traditional corporate compliance and internal audit department. In many instances, professionals with knowledge of the applicable rules and regulations, expectations of regulators, and drivers of compliance risk are required to design and execute testing programs. This is not to say that existing compliance or internal audit staff cannot be trained to meet those needs. However, in the post-Sarbanes-Oxley world, many internal audit departments have focused on professionals with more traditional financial accounting controls experience. These individuals often do not have the deep regulatory and compliance subject-matter expertise required to execute effective compliance testing. Incorporating continuous training and including cross-training of personnel in different functional areas can further enhance the knowledge and effectiveness of the team.

The program is designed using a risk-based approach. Another distinguishing characteristic of a leading testing program is the process used to design the testing itself. As is almost always the case in compliance programs, it all starts with a robust compliance risk assessment. A great testing program takes the output of the risk assessment and goes an important step further: key compliance risks are mapped to the business units and business processes where those risks are most likely to present themselves. This is sometimes called an “applicability analysis.” The process flows within those operating areas are documented clearly, where both vulnerabilities and key controls are identified. This process drives the compliance testing, which is designed to be repeatable and to generate actionable results.

Great testing programs are repeatable and statistically valid. While it is good to know if a control is functioning well right now, great testing programs recognize that sustainable quality is achieved when key risks and the related controls are tested periodically using statistically valid sampling methodologies.

Great monitoring programs

Highly effective monitoring programs also have a number of key attributes in common:

The key risk and performance indicators the program monitors are meaningful. In the past, monitoring programs have relied too much on key risk indicators (KRIs) and key performance indicators (KPIs) that are easy to monitor, such as hotline call volume or ethics training completion rates. While this data is important, other data exists within organizations that can provide more meaningful insight from a testing and monitoring perspective. Admittedly, it is no small task to identify the transactions or other data (for example, gifts or entertainment expenditures) that will provide meaningful monitoring value. Nevertheless, organizations that take the time to do so will likely find the value generally makes up for the effort. Moreover, well-conceived KRIs and KPIs often provide meaningful operating insights, offering business unit leaders a powerful incentive to allocate resources to gather the information.

“An effective, well-designed testing program can not only help flag risks or transactions of interest, it can also identify areas where policies and controls can be improved.”

Marc Van Caeneghem, EMEA Governance, Regulatory & Risk Leader,
Deloitte Touche Tohmatsu Limited

Program owners understand how to harness the power of data. Monitoring programs sometimes rely on the availability of large amounts of data, and often that data exists in another function within the organization. The decentralized nature of data presents several challenges to ethics and compliance professionals. First, companies may need to invest in technology applications to efficiently manage the testing and monitoring processes, or in analytical tools that can process large datasets, ideally on an ongoing basis. Second, quality data is critical to this endeavor. Poor data quality and data governance must be addressed in order to implement a data-analytical approach to monitoring. Finally, the compliance function must collaborate with other internal teams—the ones that have the data—to obtain the needed information. If the company is operating with limited resources, this may require some diplomacy and a clear business case—answering the question, “What’s in it for me?”—to encourage participation. In making the “case for compliance” to the business, an important message is that compliance monitoring can improve business processes, reduce redundant and manually intensive controls, and enhance decision-making.



As with testing, repeatability is key. Monitoring activities—whether or not they are automated—are most valuable when they are performed on an ongoing basis. Trend data is critical for analyzing changes in underlying business processes, as well as emerging risks. When it comes to effective monitoring programs, a “once and done” approach simply does not work.

Putting it to the test

As organizations look to establish best-in-class ethics and compliance programs, testing and monitoring is one of the essential components they need to build

and leverage. With robust testing and monitoring programs, an organization can not only gather critical information on weaknesses in their compliance program, they can engage in risk sensing activities that may provide an advanced warning of any looming problems before they become significant and potentially damaging. Much like the other key elements of a great ethics and compliance program, testing and monitoring allows organizations to learn from the past and leverage people, process, and technology with an eye toward the future for continuous improvement of their ethics and compliance program’s maturity.

Figure 5: Testing and monitoring: How it works in practice

Testing and monitoring are often confused because they each can be performed on the same business processes and activities. The table below illustrates how the two differ.

Business process/Compliance risks	Testing example	Monitoring example
<p>Gifts and entertainment: Violations of Foreign Corrupt Practices Act, the UK 2010 Bribery Act, and/or industry-specific regulations related to customer entertainment</p>	<p>Risk-based, periodic testing of gifts and entertainment logs and individual employee expense reports</p>	<p>Involves the ongoing surveillance and analysis of a large number of G&E logs and expense reports to identify patterns and anomalies</p>
<p>Lending practices: Discriminatory or predatory lending practices prohibited by banking or consumer regulations</p>	<p>Perform “matched-pair” file reviews by comparing similarly situated protected class and non-protected class applicants who received different credit decisions or terms</p>	<p>Monitor distribution of applicants and customers from specific products and loan types to identify sales practices that may result in borrowers of protected classes receiving unfavorable terms</p>

Endnotes

- ¹ Seth W. Feaster. "The Incredible Shrinking Stock Market." The New York Times. July 21, 2002.
- ² http://www.ussc.gov/sites/default/files/pdf/amendment-process/official-text-amendments/20040501_Amendments.pdf
- ³ Verick and Islam. "The Great Recession of 2008-2009: Causes, consequences and policy responses." International Labor Office, 2010: 16. http://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_policy/documents/publication/wcms_174964.pdf.
- ⁴ Bartram and Bodnar. "No Place to Hide: The Global Crisis in Equity Markets in 2008/09." Presentation at the BSI Gamma Conference on Lessons from the Financial Crisis for Banking and Money Management, November 11, 2009: 9.
- ⁵ 2014 global survey on reputation risk: Reputation@Risk. www.deloitte.com/reputationrisksurvey
- ⁶ Darcy, K.T. A Companion to Business Ethics, edited by Robert E. Frederick, "Ethics and Corporate Leadership," Blackwell Publishers Inc., 1999: 405.
- ⁷ Ibid., 405.
- ⁸ Ibid., 407.
- ⁹ Ibid., 406.
- ¹⁰ Global Human Capital Trends 2014: Engaging the 21st-century workforce, Deloitte. http://dupress.com/wp-content/uploads/2014/04/GlobalHumanCapitalTrends_2014.pdf
- ¹¹ In focus: 2014 Compliance Trends Survey. http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us_aers_dcrs_deloitte_compliance_week_compliance_survey_2014_05142014.pdf
- ¹² 2015 Compliance Trends Survey, Deloitte and Compliance Week. <http://www2.deloitte.com/us/en/pages/regulatory/compliance-trends-report.html>
- ¹³ In Focus: 2015 Compliance Trends Survey Report and In Focus: 2014 Compliance Trends Survey Report.

For more information, contact one of our leaders:

Henry Ristuccia

Global Governance,
Regulatory & Risk Leader
+1 212 436 4244
hristuccia@deloitte.com

Kevin McGovern

Americas Governance,
Regulatory & Risk Leader
+1 617 437 2371
kmcgovern@deloitte.com

Nicole Sandford

Deloitte Advisory National
Practice Leader,
Enterprise Compliance Services,
Deloitte & Touche LLP
+1 203 708 4845
nsandford@deloitte.com

Philip Chong

Asia Pacific Governance,
Regulatory & Risk Leader
+65 6216 3113
pchong@deloitte.com

Marc Van Caeneghem

EMEA Governance,
Regulatory & Risk Leader
+33 1 55 61 65 88
mvancaeneghem@deloitte.fr

Keith Darcy

Independent Senior Adviser
to Deloitte & Touche LLP
+1 203 905 2856
kdarcy@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on [Facebook](#), [LinkedIn](#), or [Twitter](#).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.