Deloitte.

At the anti-corruption compliance crossroads

Deciding which way to turn in the face of converging stakeholder pressures, regulatory demands, and standard-setting and guidance initiatives

Many businesses feel a growing pressure to mitigate the risk of fraud, corruption, and other regulatory risks, while managing costs and reducing losses resulting from such activities. The pressure is coming from boards, management, shareholders, regulators, employees, and other constituents who are demanding that companies take these risks seriously. The consequences of not getting it right are growing more serious, too, including brand damage, imprisonment, lawsuits, fines, penalties, and potential suspension or disbarment from government contracting, among others. Compliance with growing regulatory and legal requirements, simply stated, is an inescapable duty.

Lately, another related factor is driving companies to take a closer look at their fraud and corruption risk programs: the convergence of various standard-setting and guidance initiatives outlined below, which are intended to help fight fraud and corruption globally. The confluence of these initiatives, with both overlapping and distinct requirements, presents companies with the challenge and opportunity for organizational moves that can strengthen and streamline fraud and corruption risk management, while considering the broader enterprise compliance program and initiatives they may have in place.

A closer look at the converging guidance

The push to establish standards and guidance for addressing fraud and corruption risk began with the Internal Control – Integrated Framework published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 1992 (Figure 1). Many of the framework concepts were derived from recommendations made a year earlier in the 1991 Federal Sentencing Guidelines Manual, issued by the US Sentencing Commission. The Guidelines were a landmark effort to outline broadly what is expected of corporations in terms of effective ethics and compliance. A decade later, the Sarbanes-Oxley Act of 2002 introduced stringent corporate governance and financial reporting requirements for publicly held companies, including Section 404, which focuses on internal controls for the mitigation of fraud.

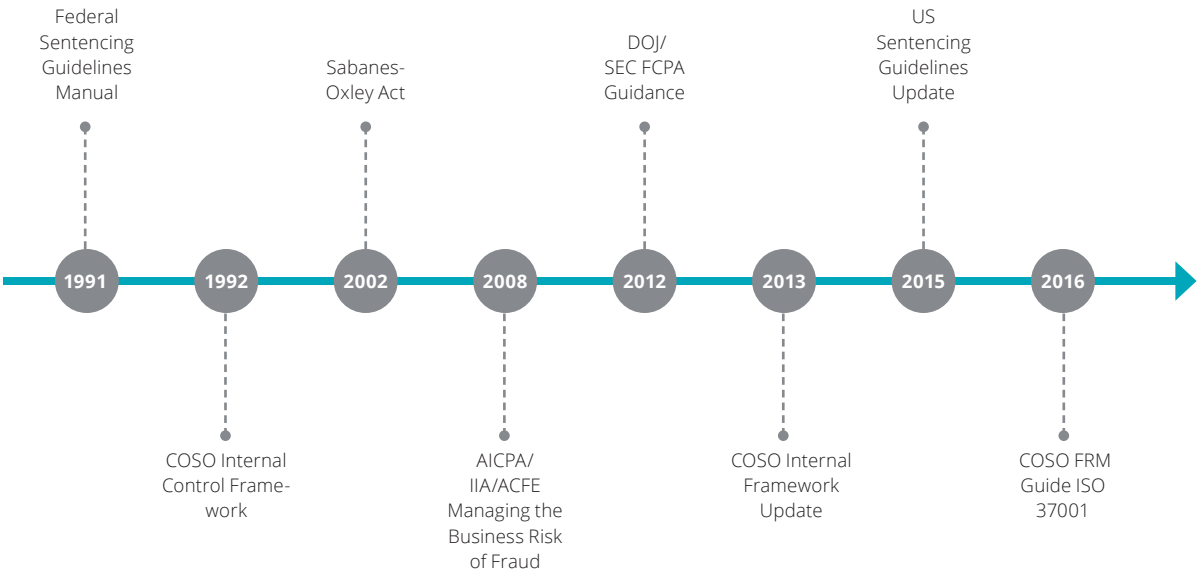
In 2008, the triumvirate of the American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), and Association of Certified Fraud Examiners (ACFE) published Managing the Business Risk of Fraud: A Practical Guide. In 2013, COSO updated its original 1992 framework, which included specific principles that dealt with fraud (namely, principles 7 and 8), and, in late 2016, released a supporting Fraud Risk Management Guide.

"Converging initiatives present companies with the challenge and opportunity to strengthen and streamline fraud and corruption risk management."

In 2012, the US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) issued "A Resource Guide to the U.S. Foreign Corrupt Practices Act" (FCPA). This Resource Guide, along with 2015 updates to US Sentencing Guidelines Manual, the "Yates Memo," and other authoritative guidance provides a compilation of information about the provisions and enforcement of the FCPA, as well as an essential resource on the foundational elements and characteristics of an effective anti-corruption compliance program. The 2015 Sentencing Guidelines refined the initial call in 1991 for establishment of appropriate corporate governance, increasing the focus on fraud, corruption, and regulatory compliance risk by mandating that "punishments more fairly reflect the harm suffered by victims and the intent of [fraud] offenders to cause harm."

And most recently, in October 2016, the International Organization for Standardization (ISO) published the final version of ISO 37001, a certifiable anti-bribery minimum standards program intended to help businesses address bribery risk across their enterprise, including their global supply chains.

Figure 1. Standards and guidance timeline



In the face of all these standards and guidelines, updates to existing documents, and increasingly detailed guidance, is it time to take a step back, analyze the various requirements, and reassess what is necessary to be compliant while keeping the business safe and managing related costs? Many companies can benefit from such an exercise.

Not surprisingly, company legal and compliance officers and other stakeholders might struggle to understand which requirements are similar, which are different, where they overlap, whether they are harmonious, and when the differences matter to their company's program. In fact, many relevant anti-corruption-related regulatory requirements and guidance have similarities (Figure 2), with some attempting to clarify or expand on previous ones. For example, the new ISO standard attempts to cover global expectations for anti-corruption programs, including those recommended by the DOJ and SEC Guidelines, as well as guidance under the U.K. Bribery Act. Other recent international anti-corruption laws have similarities and differences in both content and what is and is not expected and allowable. Examples include the US FCPA, the UK Bribery Act of 2010, and Brazil's Clean Company Act.

A challenge for companies, as discussed in the next section, is to understand how these requirements map to, and integrate into, their current and existing anti-fraud and anti-corruption compliance program(s), as well as the organization's enterprise compliance program, so they meet regulatory requirements while aligning with each company's risk profile and operating structure. Furthermore, each of the various standards and guidelines related to fraud and corruption, as well as the US Sentencing Guidelines, advocate and require consideration of basically the same elements. So another challenge for many companies is determining which requirements to follow and what is required under each to align not only with leading practices, but with specific requirements across various compliance risk domains.

Figure 2. Similarities between major frameworks and guidance

Requirements/Leading Practices	COSO Fraud Risk Management Guide	AICPA/IIA/ACFE Managing the Business Risk of Fraud	US Sentencing Guidelines	ISO 37001 Standard
Governance/leadership	X	X	X	X
Risk assessments/due diligence	X	X	X	X
Standards, policies, and procedures	X	X	X	X
Training and communications	X	X	X	X
Employee reporting	X	X	X	X
Case management/ investigations	X	X	X	X
Testing/monitoring	X	X	X	X
Third-party compliance				X
Continuous improvement	X	X	X	X

Source: Deloitte

Siloed efforts, redundant and missed opportunities

The responsibility for compliance with various standards and differing guidance pertaining to fraud and corruption, combined with the regulatory expectations, can and do often reside in different corporate functions:

- Internal auditors and finance professionals may tackle COSO-related initiatives, including oversight or ownership of a fraud risk management program and fraud risk assessment.
- Compliance and/or legal may address anti-corruption programs, including the new ISO standard.
- Legal and/or compliance may interpret and address the US Sentencing Guidelines.
- Internal audit may assist with the monitoring of specific programmatic elements related to fraud or corruption.
- Functions such as human resources, IT, and operations may also take on fraud and corruption issues on their own, often without visibility by the responsible department.

These silos are often necessary, but can create their own set of issues. Keeping certain types of activities and information cordoned off can also help protect sensitive employee information, maintain date security, and enable attorney-client privilege, as well as avoid internal conflict and inconsistency in the event of an investigation or required regulatory response.

However, a siloed approach can create gaps in critical information, communication, and efficient coordination between the various responsible parties. It is important to recognize and bridge these gaps so those parties can communicate clearly, share relevant information and effective compliance practices, and identify issues in the compliance program wherever possible with the goal of driving greater efficiency and value. When relevant information contained in various silos is not shared, critical risks are often missed because they are not identified and controlled.

A siloed approach can also create policy, procedural, process, and even personnel overlaps that, at best, result in inefficiency, duplicative efforts, and waste in the form of extra costs. At worst, it can give rise to contradictions and conflicts between compliance teams and confusion among other employees, third parties, and authorities.

Trying to find a balance when addressing these issues is difficult, and the effort to do so can cause its own inefficiencies as a company tries to "get it just right." It's an ongoing challenge for compliance teams to assess, coordinate, and ultimately resolve the problem.

Not surprisingly, company legal and compliance officers and other stakeholders might struggle to understand which requirements are similar, which are different, where they overlap, whether they are harmonious, and when the differences matter to their company's program.

An enterprise-wide view can help

To be sure, different priorities and circumstances are at play with an employee issue, a data security problem, or a legal matter. At the same time, teams tasked to address different fraud or corruption threats may not have the full complement of capabilities or resources needed for the job. Internal investigators can dig up the facts associated with a particular issue, but they might not be trained to understand which internal controls broke down or were circumvented. Internal auditors typically possess the skills to understand and recognize when internal controls have broken down, but they may not be trained on how to spot substantive missed red flags or failures, identify larger cultural issues, or effectively communicate controls to change employee behavior. The authors of policies and training programs may need to be involved in determining whether policies and training were too gray or otherwise inadequate to properly guide employee behavior.

Coordination and collaboration among various capabilities that exist within an organization related to fraud, corruption, and other compliance risk areas can help bring the right resources to a particular situation while avoiding unnecessary gaps and redundancy. The intent is not necessarily to centralize all compliance and risk management functions. Rather, the goal is to create an enterprise-level point of contact, which increasingly is a designated Chief Compliance Officer, who oversees and coordinates compliance activities related to fraud, corruption, and regulatory risk. That point of contact can also help bring efficiency by coordinating the design and use of basic compliance program elements by the various groups with more specific responsibilities for compliance activities rather than establishing their own policies and processes. Program elements include the code of ethics and other policies, the whistleblower helpline, an investigative response process and plan, and various control activities. In particular, establishing a consistent and efficient investigative response protocol across the business can facilitate a streamlined approach to a variety of fraud, corruption, and other risk issues.

Coordination and collaboration among various capabilities that exist within an organization related to fraud, corruption, and other compliance risk areas can help bring the right resources to a particular situation while avoiding unnecessary overlap and redundancy. The goal is to create an enterprise-level point of contact, such as the compliance function, to oversee distinct programs within various compliance risk domains such as anti-corruption and fraud.

Breaking down internal barriers

As noted above, various fraud and corruption activities may be siloed to protect employee information, trade secrets, competitive data, and other assets from compromise and misuse. But information and resources can be shared across different compliance domains while protecting privacy and confidentiality. For example, attorney-client privilege can be maintained in an internal investigation, while facts regarding what control issues arose can be shared to address deficiencies.

Technology and training can play important roles in effectively sharing relevant information. Programs and tools exist to capture data across silos so it can be shared, analyzed, and reported on within compliance parameters. With appropriate

training, employees can learn which activities, processes, and resources can be shared with other groups so everyone benefits from effective practices and learns from problems that have been identified.

Whatever way different companies choose to structure their fraud and corruption risk management programs, those programs generally should include the following high-level components:

- Governance and the control environment, including a code of ethics, whistleblower hotline, established oversight, and a clear tone at the top
- A sound, transparent culture supported with effective communication and awareness training
- A thorough, periodic risk assessment process
- The capacity and commitment to mitigate identified risks through the development and implementation of control activities
- Monitoring and timely incident response

Three keys for unlocking the potential of leveraged efforts

Different groups involved in mitigating and addressing fraud and corruption risks will face distinct issues and have tailored approaches to addressing them. However, taking several steps now, in a heightened enforcement and regulatory environment coupled with uncertainty at various levels of the geopolitical and economic environments, can help tap and harvest the potential of various stakeholders operating under the enterprise umbrella:

Share information. An objective that many companies often fail to achieve in establishing robust fraud and corruption compliance programs as part of a broader enterprise compliance program is to undertake a process to understand what is currently in place to identify, address, mitigate, monitor, and investigate a compliance breach. Identifying and understanding the root cause of a given issue is another common shortcoming. A lack of capabilities in this vital area of any mature compliance program may lead to similar matters arising again and again. Information is power, and the more people throughout the organization know about and share the risks related to fraud and corruption, the better equipped they can be to help respond to and mitigate those risks.

Understand what the government really wants. Regulatory authorities are not solely focused on how fraud and corruption compliance programs are structured. They want to know that these programs are addressing the organization's specific risks effectively. Whether functions are distributed or consolidated, the ultimate measure is how well they identify, understand, mitigate, and respond to risks.

Maximize assets. Substantial, diverse talent and capabilities exist in the various groups involved in establishing, conducting, and monitoring fraud and corruption efforts. Leveraging the strengths of these different resources can help in establishing and maintaining broad-based, effective risk management.

Heeding the call for coordination and communication

Standards and guidance will continue to converge on companies as they work to address fraud, corruption, and regulatory compliance risks. As a result, demands on compliance, legal, operations, finance, internal audit, and other company functions will likely continue to increase, along with the pressure to respond. Compliance activities and developments should not be looked at in isolation by any one group, but rather, they should be examined together by all respective functions in terms of how they can be most appropriately addressed. Achieving an effectively operating compliance program depends on communication and cooperation between groups and activities with a single point of contact at a high level providing leadership and guidance. Technology and employee training can reinforce the efforts of the various stakeholders, leading to improvements in program efficiency, transparency, and effectiveness.

Contacts:

Rob Biskup
Managing Director | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
rbiskup@deloitte.com
+1 313 396 3310

Bill Pollard
Partner | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
wpollard@deloitte.com
+1 773 640 0225

Holly Tucker
Partner | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
htucker@deloitte.com
+1 214 394 5352

Matt Queler
Principal | Deloitte Risk & Financial Advisory
Deloitte Financial Advisory Services LLP
mqueler@deloitte.com
+ 1 202 220 2156

Rebecca L. Burtless-Creps
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
rburtlesscreps@deloitte.com
+1 313 396 2542

Deloitte.