COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK

By

SCCE® Society of Corporate Compliance and Ethics

HCCA® Health Care Compliance Association

Authors

Society of Corporate Compliance and Ethics & **Health Care Compliance Association** (SCCE & HCCA)

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

Enterprise Risk Management

COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

November 2020

1234567890 PIP 198765432

Design and production: Sergio Analco.

Contents

	Page
1. Introduction	1
2. Governance and Culture for Compliance Risks	7
3. Strategy and Objective-Setting for Compliance Risks	11
4. Performance for Compliance Risks	15
5. Review and Revision for Compliance Risks	22
6. Information, Communication, and Reporting for Compliance Risks	27
Appendix 1. Elements of an effective compliance and ethics program	31
Appendix 2. International growth in recognition of compliance and ethics programs	37
Acknowledgments	39
About SCCE & HCCA	39
About COSO	40

1. INTRODUCTION

Why this publication is needed

Compliance risks are common and frequently material risks to achieving an organization's objectives. For many years, compliance professionals have used a widely accepted framework for compliance and ethics (C&E) programs to prevent and timely detect noncompliance and other acts of wrongdoing. The C&E program framework is described in Appendix 1 (if readers are not already familiar with the elements of a C&E program, consider reading Appendix 1 before proceeding). The COSO Enterprise Risk Management (ERM) Framework, meanwhile, has been used by risk and other professionals to identify and mitigate a variety of organizational risks, including compliance risks.

This publication aims to provide guidance on the application of the COSO ERM framework to the identification, assessment, and management of compliance risks by aligning it with the C&E program framework, creating a powerful tool that integrates the concepts underlying each of these valuable frameworks.

What are compliance and compliance-related risks?

Risk is defined by COSO as "the possibility that events will occur and affect the achievement of strategy and business objectives." Risks considered in this definition include those relating to all business objectives, including compliance. Compliance risks are those risks relating to possible violations of applicable laws, regulations, contractual terms, standards, or internal policies where such violation could result in direct or indirect financial liability, civil or criminal penalties, regulatory sanctions, or other negative effects for the organization or its personnel. Throughout this publication, "events" associated with compliance risks will be referred to as "noncompliance" or "compliance violations."

Although the underlying acts (or failures to act) are carried out by individuals, compliance violations are generally attributable to the organization when they are carried out by employees or agents of the organization in the ordinary course of their duties. The exact scope of acts attributable to an organization can vary depending upon the circumstances. In some cases, the employee may also bear liability as an individual.

Most compliance violations either inherently cause harm or have the potential to result in direct harm to individuals, communities, or organizations. Examples of parties that may be harmed through compliance violations include customers (e.g., violations of privacy or data security laws leading to a breach and theft of personal information, product safety violations resulting in injuries, antitrust violations resulting in inflated prices), employees (e.g., workplace safety regulation violations resulting in injury to a worker, antidiscrimination or whistleblower protection law violations), or the general public (e.g., environmental violations resulting in illness or death).

Although most compliance risks relate to specific laws or regulations, others do not. These other risks, referred to as "compliance-related risks," may include risks associated with failures to comply with professional standards, internal policies of an organization (including codes of conduct and business ethics), and contractual obligations. For example, conflicts of interest represent violations of laws or regulations only in limited instances (frequently involving government officials or programs). Conflicts of interest are frequently prohibited by professional standards, terms of contracts and grant agreements, or internal policies, and they are viewed as damaging to an organization if they are not disclosed and managed. As a result, conflicts of interest are commonly included within the population of compliance risks.

Accordingly, throughout this publication, the term "compliance risk" is used in reference to any risk that is either directly associated with a law or regulation or is compliance-related in that it is associated with other standards, organizational policies, or ethical expectations and guidelines.

As this discussion illustrates, the scope of what an organization considers to be compliance risks is not an exact science, although most organizations use a similar list of compliance risk areas within the universe of their programs (e.g., environmental, bribery, and corruption), even if the specific compliance risks within each area may differ. Determining the exact scope of a C&E program is typically

both an early step in developing the program and an ongoing exercise as the risk landscape changes, and input from compliance, legal, senior leaders, and the board are considered.

Compliance violations often result in fines, penalties, civil settlements, or similar financial liabilities. However, not all compliance violations have direct financial ramifications. In some cases, the initial impact may be purely reputational. However, reputational damage often leads to future financial or nonfinancial harm, ranging from loss of customers to loss of employees, competitive disadvantages, or other effects (e.g., suspension, debarment).

Most noncompliance stems from actions taken by insiders – employees, management, or members of an organization's board of directors. Increasingly, risks also result from contractors and other third parties whose actions affect an organization. The most common examples involve vendors in an organization's supply chain (e.g., when a supplier of Egyptian cotton bedding for several major retailers was found to be using a lesser grade of cotton that was not from Egypt, the retailers incurred significant liabilities to their customers) or third parties involved in the sales cycle (e.g., intermediaries that may pay bribes to government officials in order to obtain lucrative contracts for an organization).

A final consideration in determining the scope of a program is the potential for inherited risks resulting from merger and acquisition (M&A) activity. As M&A transactions take place, the universe of compliance risks to which an organization is exposed can change drastically and instantly. These risks may relate to events that took place prior to the merger or may simply result from unique risks faced by the merged entity that the acquiror had not previously faced.

The evolution of compliance and ethics programs

Although compliance with laws and regulations has been an expectation for many years, compliance and ethics as a profession and as a distinct function in organizations is a relatively recent development. It stems from the equally recent emergence of the C&E program as a valuable and frequently required element of organizational management.

A series of events in the 1980s in the United States led to the U.S. Sentencing Commission publishing guidelines in 1991 for the punishment of organizations for violations of the law. Among its provisions, the sentencing guidelines for organizations provide for very significant reductions in criminal penalties if an organization has an effective compliance program in place. Important amendments were made in 2004 and 2010 to clarify and expand on the characteristics of an effective program.

The current U.S. Federal Sentencing Guidelines (USSG) identify the following seven elements of an effective C&E program:

1. Standards and procedures
2. Governance, oversight, and authority
3. Due diligence in delegation of authority
4. Communication and training
5. Monitoring, auditing, and reporting systems
6. Incentives and enforcement
7. Response to wrongdoing

Separately, the USSG also require that organizations periodically assess the risk of noncompliance and continually look for ways to improve their C&E programs. This two-part requirement has often been referred to as the eighth element of an effective program. Each of these elements is explained in greater detail in Appendix 1.

The USSG also state that organizations should promote a culture that encourages ethical conduct and a commitment to compliance with the law. This acknowledgment that organizational culture and business ethics play integral roles in compliance risk management is one of the factors that led to the common use of the term "compliance and ethics program" or "C&E program".

The USSG do not mandate C&E programs for any organization; however, they provide an incentive for the establishment of such programs as a means of mitigating the significant penalties that can otherwise result when an organization is found to have violated federal laws. In criminal cases involving noncompliance with laws, an organization's penalty can be decreased significantly from a base amount determined, in part, on the existence of an effective C&E program. Developing case law related to the guidelines has added further weight to the importance of C&E programs, particularly in highly regulated entities, with courts concluding that the failure to implement an effective C&E program may represent a breach of fiduciary duty. Additionally, guidance issued by the U.S. Department of Justice and other agencies have emphasized the importance of C&E programs.

Although the USSG don't require organizations to have C&E programs, individual government agencies sometimes do. For example, certain healthcare organizations must have compliance programs as a condition for eligibility to participate in Medicare, and the Federal Acquisition Regulations require certain government contractors to have compliance programs.

Finally, a compliance department should be separate from the legal and regulatory affairs department. This independence is not generally required, but is rapidly emerging as a preferred practice due to the differing and sometimes conflicting responsibilities of the two functions. For example, guidance issued by the Office of Inspector General of the U.S. Department of Health and Human Services (HHS OIG) indicates that the compliance department should be independent. In its 2012 *A Toolkit for Health Care Boards*, the HHS OIG's Health Care Fraud Prevention and Enforcement Action Team (HEAT) stated: "Protect the compliance officer's independence by separating this role from your legal counsel and senior management. All decisions affecting the compliance officer's employment or limiting the scope of the compliance program should require prior board approval."

International guidance on compliance and ethics programs

Although the most extensive statutory, regulatory, and nonregulatory guidance on C&E programs has emanated from the United States, many other countries have issued various forms of requirements for and guidance on C&E programs. In some instances, guidance on C&E programs outside the U.S. is limited in application to specific areas of the law, such as bribery and corruption or antitrust/competition. In others, it is broader, like it is in the U.S., and applicable to many areas of the law. Much of the guidance issued globally mirrors many of the concepts and elements described in the USSG.

A sampling of some of the guidance from outside the U.S. reveals a mostly consistent picture of what regulators expect from C&E programs. For example, the United Kingdom's Ministry of Justice has provided guidance on the Bribery Act 2010, describing procedures that commercial organizations can put in place to minimize the risk of bribery. Those procedures are summarized into the following six principles, which that closely align with the USSG:

1. Proportionate procedures
2. Top-level commitment
3. Risk assessment
4. Due diligence
5. Communication (including training)
6. Monitoring and review

Guidance has also been issued by the International Organization for Standardization (ISO). Its 2016 ISO 37001 *Anti-bribery management systems* standard includes the following expectations of a program:

1. Performance of a bribery risk assessment
2. Leadership and commitment to the anti-bribery management system
3. Establishment of an anti-bribery compliance function
4. Sufficient resources provided for the anti-bribery management system
5. Competence of employees
6. Awareness and training on anti-bribery policies
7. Due diligence in connection with third-party business associates and employees
8. Establishment and implementation of anti-bribery controls
9. Internal audit of the anti-bribery management system
10. Periodic reviews of the anti-bribery management system by the governing body

Beyond bribery, ISO has also issued guidance more broadly on compliance management systems in the form of ISO 19600:2014. Most recently, ISO/DIS 37301 was proposed in 2020 to replace ISO 19600. The draft new standard describes the following five elements of a compliance management system:

1. Compliance obligations (identification of new and changed compliance requirements)
2. Compliance risk assessment
3. Compliance policy
4. Training and communication
5. Performance evaluation

A variety of other legal and regulatory developments that do not directly reference C&E programs nonetheless affect them. For example, 2019 European Union regulations aimed at providing new protections for whistleblowers help in supporting an important element of an effective C&E program. Similarly, data protection and privacy laws commonly differ from one country to another, but frequently have direct or indirect effects on C&E programs.

Additional examples of international guidance on C&E programs are provided in Appendix 2. What it shows is that global guidance on C&E programs has far more similarities than

differences, even if the scope of application of a C&E program may differ (i.e., limited to bribery and corruption in some jurisdictions and broader application in others). The common thread across these various guides is a shared appreciation for the elements on which this COSO guide is based.

The relationship between compliance, internal control, and enterprise risk management

COSO defines internal control in *Internal Control – Integrated Framework* (2013) and *Enterprise Risk Management – Integrating with Strategy and Performance* (2017) as follows:

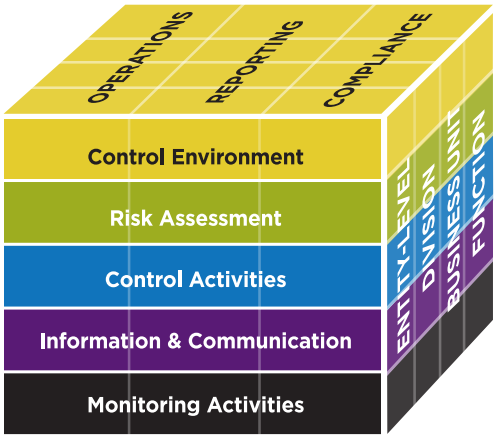
> *A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

As this definition clearly points out, internal control is not solely about accounting and financial matters. Compliance with laws and regulations is one of the three fundamental objectives of an organization's system of internal controls. The following five components of internal control support all three categories of objectives:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

The relationships between the three objectives, five components, and the entity are depicted in figure 1.1:

Figure 1.1 **The COSO 2013 Framework**



Source: COSO Internal Control Framework ©2013

COSO defines ERM as follows:

> *The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.*

The COSO ERM framework, like the internal control framework, comprises five interrelated components:

- Governance & culture
- Strategy & objective-setting
- Performance
- Review and revision
- Information, communication, and reporting

Figure 1.2 **Risk Management Components**

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance*

ERM is different than, but related to, internal controls. ERM incorporates some of the concepts of internal control. In fact, implementation of internal controls is the most common approach to reducing risk. But ERM also includes certain concepts that are not considered within internal control. For example, concepts of risk appetite, tolerance, strategy, and business objectives are set within ERM, but are viewed as preconditions of internal control. ERM is more closely aligned with strategy than internal control.

An important aspect of ERM is its focus on creating, preserving, and realizing value. The C&E program supports each of these three goals. An effective C&E program allows an organization to more confidently pursue new value creation opportunities. Further, value that has been created by an organization can quickly become impaired when accompanied by violations of laws or regulations. An effective C&E program can preserve this value and enable an organization to fully realize it.

Accordingly, the management of compliance risk is an important element of both the internal control and the broader ERM functions and processes of an organization.

The scope and positioning of the compliance function in an organization

As noted earlier, compliance risk generally involves the risk of violations of laws and regulations, but it may also address contract provisions, professional standards, organizational policy, and ethics matters. The laws and regulations that fall within the scope of a compliance program, however, can vary by industry and from organization to organization. For example, risk of violating the Foreign Corrupt Practices Act may fall clearly within the scope of a company's C&E program. But compliance with accounting standards required in filings with the U.S. Securities and Exchange Commission may be addressed within the accounting and finance functions and may be considered outside the scope of the C&E program. Human resources and employment law risks may be managed entirely within the human resources function, or the compliance function may also participate in managing these risks.

There is not a universally accepted definition for the scope of an organization's C&E program. It can vary from one organization to another. As a result, compliance with some laws and regulations may be primarily subject to the oversight of others, although the compliance function should always be prepared to serve an overarching role or to step in to assist or address issues if the others are unable or unwilling to properly manage the risk.

Another difference among organizations may involve where the compliance function "sits" within the organization. Although a C&E program is organization-wide, involving employees and managers from all functional areas, the compliance function, consisting of a dedicated team of compliance and ethics professionals, may be positioned in a variety of locations within an organization chart. In most organizations, it is an independent function, and this is considered the best practice. In others, it may be a part of, or report to, legal, internal audit, risk management, or another function. Regardless of where the compliance function is positioned on an organization chart, communication and collaboration with each of the preceding functions are essential to the success of a C&E program.

Likewise, ethics may be considered a function apart from compliance. In many organizations, however, compliance and ethics fall under a compliance and ethics officer.

It is important to understand that although virtually every employee plays a role in managing risk, the management/mitigation of compliance risk is primarily the responsibility of all management at all levels. The compliance function leads the development of the C&E program, but it is ultimately management's job to execute the program and for the board to provide oversight. The role of the compliance and ethics officer is to help management understand the risks; lead the development of the program to mitigate and manage those risks; evaluate how well the program is being executed; and report to leadership on gaps in coverage, execution, or material instances of noncompliance, including those by senior leaders.

In summary, management of compliance risk can be performed effectively under a variety of structural models. This publication provides guidance on the design and operation of an effective C&E program regardless of the organizational structure or how responsibilities are allocated.

About this Guidance

There are several target audiences for this publication, including the following:

1. Professionals such as risk managers, internal auditors, and others who are involved in applying an organization's ERM program to compliance risks.
2. Compliance professionals who are aiming to align their C&E program to, or integrate it with, an organization-wide ERM program.
3. The senior management team, to better understand compliance risk and the C&E program.
4. Members of the board of directors, to assist them in their oversight role.

When the USSG were developed, and as the elements of effective C&E programs have evolved, fitting the seven elements within the ERM framework was not a significant concern or objective. Indeed, much of this evolution occurred before the first ERM framework was published by COSO in 2004.

In the remaining portions of this guide, each of the 20 principles of the COSO ERM framework, depicted in figure 1.3, is mapped to the specific requirements and emerging practices of an effective C&E program. Section 2 starts with the governance and culture component and the related five principles. Sections 3 to 6 cover the other components and their related principles, respectively. In each, key steps are provided to implement and maintain an effective C&E program for each of the ERM principles.

Figure 1.3 Risk Management Components - The 20 principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance*

An example of the application of the guidance provided in this publication to a specific compliance risk can be found at corporatecompliance.org/coso.

Figure 1.4 Frequently used terms and abbreviations

	The following terms and abbreviations are used frequently throughout this publication
Board	The board of directors or, where appropriate, a board-level committee that has been delegated the responsibility for compliance oversight by the board of directors
C&E program	Compliance and ethics program
CCO	The chief compliance officer, chief compliance and ethics officer, or the equivalent title associated with the highest-ranking employee charged with oversight of the C&E program
Compliance committee	An internal committee composed of employees from various departments and functions within an organization whose mission is to advise, inform, and partner with the CCO in communicating and extending the compliance function throughout the organization's operations
Compliance risk	The possibility that violations of applicable laws, regulations, contractual terms, standards, or internal policies will occur and have a negative financial or nonfinancial impact on the organization
DOJ	The United States Department of Justice
USSG	The United States Federal Sentencing Guidelines

2. GOVERNANCE AND CULTURE FOR COMPLIANCE RISKS

This section describes the application of the governance and culture component of the COSO ERM framework to the management of compliance risks. The COSO framework describes the following five principles that underlie this component:

1. Exercises board risk oversight
2. Establishes operating structures
3. Defines desired culture
4. Demonstrates commitment to core values
5. Attracts, develops, and retains capable individuals

Principle 1 – Exercises board risk oversight

The board of directors is responsible for oversight of the organization's C&E program, and management is responsible for the design and operation of the program. The expectation of board oversight is reinforced in C&E program standards that have been promulgated in several countries. For instance, the USSG § 8B2.1(b)(2)(A)-(C) state that a company's "governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight."

Given the possible complexity of an organization's C&E program, it is often advisable for the board to delegate responsibility for this oversight to a board-level standing committee, much like audit oversight is commonly delegated to an audit committee. This enables a committee to devote sufficient time to oversight — time that may be unavailable for the entire board. As noted earlier, the term "board" is used in reference to either the board of directors or a board-level committee that has oversight responsibility for the C&E program.

For oversight to be exercised properly, there must be an open and direct line of communication between the CCO and the board. This communication should include regularly scheduled, periodic meetings, including sessions in which the board meets privately with the CCO without other members of senior management present.

Having compliance expertise on the board can be extremely valuable and can enhance oversight of the program. Ideally, this expertise comes from industry-specific experience with relevant compliance issues as well as experience developing and managing effective compliance programs.

The board should also ensure there is an effective compliance oversight infrastructure in place to support the C&E program, to include adequate staffing and resources, as well as appropriate authority and empowerment to achieve the objectives of the program. This infrastructure may also include an internal compliance committee. Often, an internal compliance committee composed of individuals from key functions or business units is an effective way for the CCO to maintain open lines of communication to facilitate timely awareness of emerging compliance risk areas and to obtain important input and buy-in on how to mitigate and address risks.

Table 2.1 **Exercises board risk oversight**

Key characteristics	• Require the board to oversee compliance risk management and the C&E program, including the approval of its charter • Ensure that the board is knowledgeable of and demonstrates oversight of the C&E program (regular part of agendas, monitors compliance metrics, holds regular executive sessions with CCO and others) • Require that the board includes a member who possesses compliance expertise • Document evidence of board oversight of the C&E program in minutes • Provide input or approve appointment/dismissal/reassignment of CCO and ensure independence • Ensure that sufficient resources are provided for the C&E program • Receive regular reports from the CCO • Ensure that the board is informed about material investigations and remediation efforts and provides input

Principle 2 — Establishes operating structures

The positioning of the compliance function within an organization has important implications for the effectiveness of the program. The compliance function should be led by someone who is positioned to be effective, which typically means being a peer of other senior leaders. Moreover, the compliance function must have the practical authority, resources, and tools to effectively fulfill its mandate. Finally, the compliance function should be functionally separate and distinct from other functions, particularly those that are frequently perceived by regulators as having conflicting obligations or priorities (e.g., legal, finance, etc.). Although it may be possible for the compliance and ethics function to be effective when housed within other departments, the preferred practice is for compliance to be functionally separate and — like internal audit — report to the board. If the function does not report to the board, extra care must be taken to ensure adequate resources and sufficient autonomy, including direct and unfiltered access to the board.

Operating structure should also include documented policies and procedures covering the governance and decision-making processes associated with the C&E program. From a governance standpoint, if oversight of the C&E program has been delegated by the board of directors to a board-level compliance committee, the committee should operate in accordance with a board-approved charter. The charter describes in detail the responsibilities and key operating procedures of the committee (e.g., frequency and nature of meetings, reporting to the board) as well as the qualifications for committee members.

Increasingly, regulators and the enforcement community consider the stature of the compliance function relative to other executive functions as a signal of how seriously the C&E program, and therefore compliance with laws and regulations, is viewed within an organization. Is the compliance function buried several layers down the organization chart? Or is it represented at a very high executive level? Stature also considers positioning of the CCO relative to other senior executives of an organization.

Operating structure should also include other key compliance policies and procedures, such as those that govern the methodology and performance of compliance risk assessments, consideration of forming an internal compliance committee with representation from across the organization, and procedures for escalation when significant risk events occur, among other procedures.

Table 2.2 **Establishes operating structures**

Key characteristics	• Maintain independence of the CCO and the compliance and ethics function • Ensure that the CCO directly reports to and regularly communicates with the board • Ensure that the CCO and C&E program have high stature relative to other functional leaders • Grant sufficient authority to the CCO to manage the program effectively • Provide sufficient resources for the C&E program to be effective • Address C&E program oversight in the charter (including delegation to a designated committee, if applicable) • Document policies and procedures specific to the operation of the C&E program • Establish protocol/procedures for escalation of significant compliance risk events

Principle 3 — Defines desired culture

It is critical for the organization to establish and maintain a culture of compliance and integrity. Without it, even the most carefully designed compliance controls will be vulnerable to failure. Culture begins with a sincere commitment to compliance and ethics at the leadership level. The commitment is reflected in several ways, beginning with its inclusion in a code of conduct or business ethics that is written in a manner that clearly articulates expectations of behavior. Leadership can also reinforce and clarify this culture through other communications. This commitment to culture should be further reflected through the adoption of important compliance metrics and by meaningfully incorporating compliance into the performance evaluation and compensation/incentive compensation processes, particularly at leadership levels.

An exercise that is helpful in setting expectations for culture is for senior management to have a robust discussion about the relationship between compliance risk and the organization's risk appetite and risk tolerance, which are discussed further in the next section. In particular, tolerance, which considers acceptable levels of variation in performance related to achieving business objectives, should consider the potential impact of compliance risk, because compliance with laws, regulations, and other requirements should itself be one of the primary business objectives for all organizations.

Another aspect in a culture of compliance is that of risk awareness. It is one thing to have a culture in which compliance is important. But an essential element of such an environment is a culture of risk awareness, where employees are vigilant and willing to raise concerns when they see warning signs of risk.

Communication and training are also important tools for promoting an ethical culture, because each reinforces an overall mindset of compliance and integrity, while also improving awareness of key compliance issues. Accordingly, training should include periodic discussion of the code of conduct, but it should also include training on specific compliance issues tailored to individual groups of employees exposed to these risks in connection with their work.

Table 2.3 **Defines desired culture**	
Key characteristics	• Ensure that the board is knowledgeable of and approves a code of conduct/ethics and other key compliance policies • Explain expectations relating to ethics and compliance in a code of conduct/ethics • Provide and require training on the code of conduct and on ethical decision-making for all staff (including board members) • Perform ongoing monitoring or assessment of organizational culture • Develop objectively measurable compliance metrics tied to performance evaluations and compensation, where appropriate • Adopt meaningful incentives to promote consistent execution of the C&E program • Include references to organizational values, expectations, and importance of ethics in communications from leadership

Principle 4 — Demonstrates commitment to core values

Commitment to core values should be represented in a value statement or other set of guiding principles that demonstrates a commitment to compliance and ethical business conduct. Increasingly, studies show a correlation between ethical culture and organizational performance, consistent with ERM's goal of creating value.

The tone from the top plays an important role in managing compliance risks. The tone set by the executive team must set an example of compliance and ethical behavior. This commitment must cascade throughout the organization, thus the term tone "from" the top rather than tone "at" the top. Each layer of leaders within an organization — the supervisors and managers of others — must communicate and pass this tone on to the next level.

Commitment to compliance and ethics, however, requires much more than setting the tone. Employees should be held accountable for their individual roles in managing compliance risks, and this should be reflected in job descriptions, performance evaluations, and incentives.

When allegations of noncompliance or unethical behavior emerge, they must be taken seriously. This means that individuals should be required to report wrongdoing and have multiple avenues for reporting. Once an allegation is received, sound investigative protocols should be followed in a timely manner to assess the credibility of the allegation. In addition, individuals who report concerns about wrongdoing must feel safe speaking up and be protected from retaliation in order for this system to operate effectively.

If wrongdoing is confirmed through the investigative process, disciplinary action should be taken in a degree that is appropriate to the level of wrongdoing. Discipline should be consistent based on the nature of the wrongdoing, without regard to the individual's level on the organization chart or level of influence within the organization.

Table 2.4 **Demonstrates a commitment to core values**	
Key characteristics	• Actively promote a culture of compliance risk awareness, including setting an ethical and compliant tone by leadership • Balance business incentives with material compliance incentives • Incorporate accountability for the management of (1) compliance risks and (2) compliance program implementation into employee performance measurement, promotions, and incentive programs, particularly at senior levels • Protect those who report suspected wrongdoing, with zero tolerance for retaliation • Take allegations of wrongdoing seriously and investigate in a timely manner • Promote organizational justice, including accountability for wrongdoing, fairness and consistency in discipline, and fairness in promotions • Communicate lessons learned from compliance and ethics failures across the organization in appropriate detail

Principle 5 — Attracts, develops, and retains capable individuals

An effective compliance function should be led by a CCO with appropriate experience and qualifications. The specifics of prior experience and other qualifications can vary based on the nature of the organization, its industry, and many other factors.

Throughout the entire organization, hiring individuals who respect compliance and make business decisions in an ethical manner is vital to the management of compliance risks. Indeed, being perceived as an organization that is committed to compliance and ethics helps companies attract and retain good people.

The USSG, which established the framework for what has become the global standard for C&E programs, state that an "organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program." As such, organizations should perform background checks appropriate to the responsibilities of the position and in compliance with relevant employment laws. The CCO may collaborate with human resources and others to identify positions considered to involve "substantial authority"— those that could create compliance risk for the organization.

The COSO ERM framework indicates that performance evaluation and the establishment of appropriate incentives are two important ingredients for developing and retaining individuals. These tools are critical for the management of compliance risks as well. The Department of Justice (DOJ) notes that a "hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance."

Just as training on a code of conduct and broad ethical issues helps to define an organization's desired culture (Principle 3), training on specific compliance risk topics further develops individuals' abilities to effectively recognize and manage compliance risks. Furthermore, the compliance team itself should continue to be developed with training on emerging practices for managing a C&E program and changes in the legal/regulatory environment.

In recent years, numerous compliance issues have been triggered by third parties (nonemployees), especially those that play integral roles in connection with supply chains, sales, delivery, and other key functions. Accordingly, the due diligence concepts described in this section should also be applied when engaging third parties to carry out activities on behalf of the organization (e.g., suppliers, sales agents, outsourcing partners), based on the level of compliance risk associated with each third party. The degree of background checking, other due diligence, and compliance-related performance measures should vary based on the assessed level of risk, and due diligence should be repeated periodically as part of maintaining ongoing relationships with high-risk third parties. Due diligence in engaging with certain third parties, as well as ongoing training and monitoring of compliance performance of third parties, have become expected by regulators and are integral elements of this principle.

Table 2.5 **Attracts, develops, and retains capable individuals**

Key characteristics	• Hire and retain a CCO with appropriate experience/expertise to lead the C&E program • Staff the compliance team with individuals that possess relevant expertise • Perform background checks aimed at screening for compliance risk, tailored to the level of risk associated with each position • Consider employee execution of and adherence to the requirements and expectations of the C&E program in the preparation of performance evaluations • Appropriately tailor compliance training based on the compliance risks encountered for specific roles in the organization • Perform risk-based due diligence on third parties

3. STRATEGY AND OBJECTIVE-SETTING FOR COMPLIANCE RISKS

This section describes the application of the strategy and objective-setting component of the COSO ERM framework, and the following four principles associated with the management of compliance risks:

6. Analyzes business context
7. Defines risk appetite
8. Evaluates alternative strategies
9. Formulates business objectives

Principle 6 — Analyzes business context

Context is critical to understanding and managing compliance risks. Business decision-making is one of the drivers of compliance risk; decisions can create new risks, change existing risks, or eliminate risks. Accordingly, the identification of a compliance risk universe should consider the organization's evolving strategy. The CCO should have an appropriate level of involvement in the strategy-setting process to enable the compliance function to be positioned to identify and develop plans to manage compliance risks that emerge from changes in strategy. Likewise, the CCO should be informed of sudden shifts in strategy that may occur as an organization responds to changes in its environment.

Context for effective compliance risk management includes consideration of other internal drivers of compliance risk — factors that can create new risks or change existing ones. Some of the most important internal drivers of compliance risk include changes in people, processes, and technology. Another driver of compliance risk is management pressure, particularly when such pressure is not coupled with reminders regarding the expectation of compliance and appropriate incentives to adhere to the C&E program. More broadly, changes in organizational culture can arise from many factors and can affect compliance risk.

External drivers of compliance risk also represent an important element of context in identifying and managing compliance risks. The most obvious external factors are those involving the legal, regulatory, and enforcement landscape. For example, recent changes in data privacy and security laws have created entirely new compliance risks for some organizations. External drivers also include competitive, economic, and other factors that may directly or indirectly affect compliance risk. External factors may be at a macro level (e.g., industrywide competition, economic conditions) or at a micro level (e.g., changes in local or regional laws and regulations).

Risk interdependencies may also affect how an organization manages compliance risks. An organization's responses to other risks (e.g., strategic, financial) may affect compliance risk in a positive or adverse way.

Table 3.1 **Analyzes business context**

Key characteristics	• Consider and reflect organizational strategy in performing compliance risk assessments and managing compliance risk • Consider how compliance risks are affected by internal changes, such as changes in people, structures, processes, technology, etc. • Evaluate effects of external factors (e.g., competitive, economic, enforcement trends, environmental, political, social forces) on compliance risks • Identify and consider risk interdependencies in the development of strategy • Give consideration to cultural and regional differences in legal frameworks based on locations where the organization operates

Principle 7 — Defines risk appetite

For those not familiar with the term, appetite for compliance risk often conjures up images of organizations willfully accepting known compliance violations. The very nature of compliance risk means that a law may be violated that could result in financial or nonfinancial consequences for the organization (e.g., fines, suspension or debarment, reputational damage). The level of acceptance of compliance risk in the pursuit of business goals and objectives is a topic for discussion among management and the board (being clear to point out that this discussion is not related to accepting known violations; it is about the realistic assumption that it is impossible to eliminate the possibility of a noncompliance event).

As defined by COSO, risk appetite refers to the types and amount of risk, on a broad level, that the organization is willing to accept in pursuit of value. Neither appetite nor risk tolerance — the acceptable levels of variation in performance related to business objectives — is typically defined at the risk-specific level.

Although neither appetite nor tolerance are expressed in terms of compliance risk, there may be separate risk-centric statements relating to individual compliance risk areas. More commonly, the potential impact of compliance risk on the achievement of business objectives should be considered in relation to determining and stating risk appetite and tolerance. As noted earlier, compliance with laws, regulations, and other requirements should itself be considered as a business objective of the organization.

A practical way of viewing compliance risk and its relationship to risk appetite and tolerance is by viewing it at the business unit or location level and by type of compliance risk. At the business unit (or functional) level, each group often has its own unique compliance risks, each with vastly different potential consequences for violations. For example, an international bribery violation may result in much more significant financial penalties than a building code violation.

Although a fire code violation may trigger only a rather small fine, however, the potential consequences of a fire code violation tragically resulting in the loss of life could be enormous. Seemingly immaterial compliance risks like this building code violation could lead to other risks, such as a request for a bribe from a building inspector. Examining risk appetite with consideration for the full range of potential consequences is an important element of compliance risk management.

As noted in COSO's May 2020 publication, *Risk Appetite – Critical to Success: Using Risk Appetite to Thrive in a Changing World*, three of the inputs to risk appetite are as follows:

1. Board and management perspectives on appetite
2. Understanding the existing risk profile
3. Organizational culture

Board and management perspective on risk appetite should be framed, in part, on a consideration of the relationships between compliance risk and the achievement of business objectives. This can be achieved only if the board and management have a sufficient understanding of compliance risk as a component of the organization's overall risk profile. Similarly, as noted earlier, maintaining a culture of compliance is an essential element of a C&E program and, therefore, should be considered in developing an organization-wide appetite for risk in general.

Understanding how much of a threat a compliance risk poses to the achievement of business objectives enables the CCO to effectively prioritize the deployment of preventive and detective resources. For example, if an organization has determined that a particular category of compliance risk poses a significant threat to the achievement of business objectives, the organization may allocate greater resources to managing that risk. More attention may be devoted to auditing and monitoring in this area, among other possible responses.

Organizations must also recognize that they cannot realistically eliminate all compliance risks or reduce the likelihood of occurrence to zero. This is simply not possible. As a result, engaging in discussions about risk appetite relating to compliance risks is a valuable tool in prioritizing efforts aimed at prevention and detection of specific compliance violations. Guidance from regulators is consistent with this concept: expecting organizations to reduce and manage, not necessarily eliminate, compliance risk.

Table 3.2 **Defines risk appetite**

Key characteristics	• Consider compliance risk as part of the organization's risk profile in determining risk appetite • Consider compliance risk by (1) type of risk (e.g., anti-bribery), (2) business unit or organizational function (e.g., human resources), and (3) location or region • Determine and evaluate the relationships between compliance risks and the achievement of business objectives • Discuss risk appetite on a regular basis and update as necessary based on changes in compliance risk • Consider developing specific risk-centric appetite statements associated with compliance risks in support of organizational risk appetite and tolerance

Principle 8 — Evaluates alternative strategies

The compliance function should be involved in strategy discussions from the standpoint of (1) understanding the strategy so that the C&E program can be designed to manage compliance risks appropriately and (2) advising strategic decision makers about possible compliance risks associated with strategies under consideration. Compliance risk assessment and management are most effective when the compliance function is fully informed prior to embarking on new strategic initiatives, enabling the C&E program to be prepared to proactively address new or changing compliance risks. The CCO should also play a role in developing new compliance risk mitigation approaches in the context of changing strategies and risk appetite, as well as assistance in evaluating compliance risk issues associated with alternative strategies under consideration.

If strategic decisions made by an organization involve merger or acquisition activities, it is important for compliance to be involved early in the process so that appropriate due diligence focusing on compliance risks can be performed. This due diligence is important to the decision-making process for mergers and acquisitions in order to understand the level of risk that may be inherited as a result of the transaction, as well as any C&E program integration needs and risks that may need to be addressed.

Once strategy has been decided, the compliance function should identify and understand the implications for the organization's C&E program. Begin by identifying and assessing compliance risks, as well as suggesting modifications to internal controls aimed at mitigating compliance risk. Consider changes to training, monitoring, and auditing plans for the C&E program, and the development of key compliance metrics or performance indicators.

As a strategy is being implemented, the organization may continue to make changes to the strategy based on an assessment of its successes and failures. This assessment is another opportunity for the CCO to provide valuable input based on the C&E program's monitoring and auditing activities, which may have revealed a level of compliance risk that differs from what was initially expected.

Table 3.3 **Evaluates alternative strategies**

Key characteristics	• Ensure that the CCO has a seat at the table in discussions of strategies • Solicit input and insight from the CCO regarding how strategy affects compliance risk • Perform risk-based due diligence on merger and acquisition targets prior to execution of the transaction • Consider implications of strategic decisions (including subsequent changes in strategy) in the design of the C&E program

Principle 9 — Formulates business objectives

Linked to strategy, business objectives are measurable criteria by which the organization and individual business units can be evaluated. Much like how adoption of strategy can affect compliance risk, development of business objectives also often creates or affects the likelihood of compliance violations. Additionally, complying with applicable laws, regulations, contract terms, and other requirements should be considered as its own business objective if compliance is not explicitly addressed through other stated business objectives.

Sometimes, performance metrics developed for business units can inadvertently create incentives to violate compliance requirements. Take the simple example of a manufacturing facility whose personnel are incentivized by aggressive new goals for increased production. This goal could lead to shortcuts in quality control and inspections, resulting in product safety violations if the production team views violating these compliance requirements as an acceptable means of achieving the new targets. The compliance function should be consulted as part of the establishment of business objectives, in much the same manner as described in Principle 8, to ensure that incentives are appropriately structured to minimize the promotion of bad behavior or that such incentives are balanced with appropriate compliance incentives. Ideally, compliance participates in the establishment of business objectives, but at a minimum, it is well informed of such objectives and the performance metrics that are used for individual evaluations.

Risk interactions should also be considered. As business objectives and performance metrics change in one area of the organization, compliance risks may be affected — either in the same business unit or in other areas of the organization.

Finally, just as performance metrics are an essential characteristic for business units, the compliance function itself should develop and monitor performance metrics. These metrics address and measure how well the C&E program and infrastructure is working in practice across the organization, and its overall effectiveness. Examples of measurable metrics — and key performance indicators (KPIs) — include such things as training completion rates, timeliness of responding to issues, investigations, and implementing corrective action plans, volume, frequency, and types of issues reported through the organizations' reporting mechanisms, culture survey responses over time, and metrics from monitoring various internal compliance controls such as vendor payments in high-risk operating locations. Although not all areas of the C&E program are easy to objectively measure, the compliance function should take steps to develop and monitor objective metrics wherever possible.

Table 3.4 **Formulates business objectives**

Key characteristics	• Identify and evaluate compliance risks associated with planned business objectives • Consider establishing compliance as a separate business objective • Incorporate compliance risk management and accountability into performance measures and related evaluations • Consider interactions between compliance and other risks based on changes in business objectives • Include objectively measured compliance metrics within business objectives, reflecting the management of compliance risk and the effectiveness of C&E program implementation, and carrying appropriate weight in incentive and other compensation decisions

4. PERFORMANCE FOR COMPLIANCE RISKS

This section describes the application of the performance component of the COSO ERM framework and the following five principles associated with the management of compliance risks:

10 Identifies risk

11 Assesses severity of risk

12 Prioritizes risk

13 Implements risk responses

14 Develops portfolio view

For C&E programs to be effective, it is expected by regulators and others that organizations periodically assess the potential threats of legal, regulatory, and policy noncompliance, as well as ethical misconduct, so that the organization can take steps to manage these risks to acceptable levels.

Principle 10 — Identifies risk

One of the most challenging tasks for the C&E program is the identification of the myriad compliance risks faced by the organization. Organizations are subject to thousands of laws and regulations ranging from antitrust, privacy, fraud, and intellectual property rights/obligations to local sales tax, licensing requirements, and environmental standards. Further, these threats constantly change with new and altered legal and regulatory requirements; with shifts in organizational strategies, such as a retailer entering the business of health care services; and with the emergence of new compliance risks as societal values evolve. To function effectively, the C&E program needs to have processes in place to identify and track these various risks across the organization.

Historically, many organizations approached compliance with laws and regulations in silos, developing programs to address specific issues where the organization or others in the industry had encountered significant challenges. For example, the business unit directly involved with the risk, such as antitrust or environmental or money laundering, would be responsible for most, if not all, aspects of compliance with those laws. As compliance programs have matured, they have moved to a more integrative, proactive approach based not on a particular past crisis that the organization wishes to avoid repeating, but on the systematic assessment of the organization and its environment to identify current and future threats to compliance. This same motive is what drives organizations to implement ERM.

Not all compliance threats will be considered priorities in the ERM context. For example, of the 10 most significant compliance risks identified by the C&E program, perhaps only 2 or 3 of them will be among the 10 most important identified by the ERM function at the organizational level, after consolidating compliance risks with all other risks. Yet for the C&E program, these are important, because they can emerge as serious threats through their impact on the compliance culture. Regulators expect a specific assessment of compliance risks as part of the C&E program. This suggests that even when an organization has a mature, well-developed ERM program, the C&E program should supplement the organizational-level ERM and should strive to identify and manage all compliance risks, regardless of whether all are material at the enterprise level.

Developing a risk inventory for compliance risk is similar to the process of developing the ERM risk inventory. As illustrated in figure 4.1, there are a number of approaches that can be taken, with some approaches being more effective in identifying new and emerging risks.

For compliance risk identification, some approaches have been found to be particularly useful. Many organizations start with a risk inventory identified by similarly situated organizations or industry associations. This inventory needs to be viewed as a starting place and should then be tailored to the organization, considering its unique operations. Another often-used approach is to interview key employees to better understand operations and determine applicable laws and regulations that they deal with on a regular basis. As noted in figure 4.1, this method is effective at identifying existing laws and regulations posing compliance risks and

Figure 4.1 **Approaches for Identifying Risks***

Types of Risk	Cognitive computing	Data Tracking	Interviews	Key Indicators	Process Analysis	Workshops
Existing	✓	✓	✓	✓	✓	✓
New	✓	✓			✓	✓
Emerging	✓		✓	✓		✓

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance,* Volume 1, p. 69

may provide an indicator of emerging risk, but it may not be as effective at identifying new risks or changing enforcement standards not yet apparent to employees. Surveys may also be used to ask key managers to identify applicable laws and regulations that they deal with regularly in their area.[1]

Regardless of the approaches taken, the variety and complexity of compliance risks create the need for operations managers and risk owners to be involved in the risk-identification process. One way of doing this is the development of compliance committees at various levels in the organization. Senior management and the board must also be involved by including the C&E program leadership in strategic planning so they can understand the organization's current and evolving strategies and the related compliance risk.

Information provided by regulators can also be helpful in identifying new and emerging risk, because many of these agencies issue alerts regarding where they see emerging risks and have compliance concerns. For example, the SEC Office of Compliance Inspections and Examinations issues special risk alerts, and the HHS OIG publishes its work plan to alert organizations to areas considered to be high risk.

Further, compliance risk extends beyond the legal boundaries of the organization. Third-party contractors, suppliers, and partners in strategic alliances can pose significant compliance and ethical risks. Concerns specifically related to third-party risks include the following:

1. The organization usually has a lessened ability to control or oversee the work of a third party than it would with its own employees.
2. Third parties often do not have as strong of an incentive to adhere to compliance and ethics expectations as employees do.
3. Third parties may operate in geographic areas that are distant from the organization's headquarters, sometimes with differing laws, norms, and customs.

For these reasons, assessing risk involving third parties can be complicated, but risk assessments should be performed at the time a third party is engaged and periodically thereafter. The extent of each risk assessment, due diligence process, and subsequent monitoring and auditing should consider the role the third party plays, materiality, and other factors that could affect the level of risk associated with each third party.

Not all compliance risks will rise to the entity level and appear in the ERM risk register; however, the risk of regulatory change would be included in such an entity-level inventory in most organizations.

Table 4.1 **Identifies risk**

Key characteristics	• Describe the compliance risk identification and assessment process in documented policies and procedures • Identify compliance risks associated with planned strategy and business objectives • Assess internal and external environments to identify risks • Create process for identifying new and emerging risks • Consider risks associated with use of third parties • Consider information gathered through hotlines, other reporting channels, and results of investigations

1 Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 21–25, https://compliancecosmos.org/compliance-risk-assessments-introduction.

Principle 11 — Assesses severity of risk

Severity of a compliance risk is usually assessed primarily on the basis of likelihood and impact. Other factors may also be considered and will be explained later.

Likelihood is the probability that the risk could occur. In the case of compliance, this means the probability of specific noncompliance with a law/regulation or ethical misconduct. Assessing the likelihood of compliance risk in most cases is a subjective judgment. Despite being subjective, systematic judgment can be made. One approach is to consider the frequency of noncompliance. Will the event (e.g., a salesperson making an illegal payment to a government official to gain a contract) occur once a year or once every five years? This judgment would be based on experience or perhaps the organization's historical data, if such data is available. Another factor that enters into this assessment is the organizational context. Typically, the assessor makes assumptions about controls in place, such as policies prohibiting such payments or the controls around the payments process. In theory, one would like the assessment to be made under the assumption of no controls at all being in place, but it is difficult for people to imagine such "no control" situations. They usually make the assessment assuming "normal controls" or some sort of "minimal controls." For greater precision, some assessment methods break the likelihood assessment in two parts: one for likelihood or frequency and the other for effectiveness of internal controls, as shown in figure 4.2. Some models may even consider preventive and detective controls as two separate factors, with preventive controls being more relevant to likelihood or frequency, and detective controls more likely affecting the impact of an event based on the timeliness of detection.

In figure 4.2, the likelihood of occurrence is measured on a five-point scale from "rare" to "almost certain." Control assumptions and frequency are given descriptive anchors that are then matched to the assessor's beliefs.

Figure 4.2 **Likelihood of Occurrence***

Scale	Existing controls	Frequency of noncompliance
5 Almost certain	• No controls in place • No policies or procedures, no responsible person(s) identified, no training, no management review	Expected to occur in most circumstances More than once per year
4 Likely	• Policies and procedures in place but neither mandated nor updated regularly • Controls not tested or tested with unsatisfactory results • Responsible person(s) identified • Some formal and informal (on-the-job) training • No management reviews	Will probably occur At least once per year
3 Possible	• Policies mandated, but not updated regularly • Controls tested only occasionally, with mixed results • Responsible person(s) identified • Training is provided when needed • Occasional management reviews are performed, but not documented	Might occur at some time At least once in 5 years
2 Unlikely	• Policies mandated and updated regularly • Controls tested with mostly positive results • Regular training provided to the identified responsible person(s), but not documented • Regular management reviews are performed, but not documented	Could occur at some time At least once in 10 years
1 Rare	• Policies mandated and updated regularly • Controls regularly tested with positive results • Regular mandatory training is provided to the identified responsible person(s), and the training is documented • Regular management reviews are performed and documented	May occur only in exceptional circumstances Less than once in 10 years

* Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 30, https://compliancecosmos.org/compliance-risk-assessments-introduction.

This approach is just one example. Every organization should customize its scale and measurement methodology to fit its particular needs. This customization would be done by a compliance committee or by the C&E program staff with input from management. Once the scale is determined, it should be applied consistently by the assessors.

The second component of risk severity is impact. Impact is the result or effect of risk in terms of the organization's strategy and business objectives. With compliance risk, one thinks immediately of civil and criminal fines and penalties, and the possible direct financial consequences of noncompliance. Another significant factor may be the reputational impact of compliance and ethical issues. This and other consequences (e.g., sanctions, suspension, and debarment) may have a material indirect financial impact, as well as an impact on morale and other factors that are difficult to measure.

Impact of noncompliance and ethical failures can be assessed using a variety of measurement categories.

- **Legal** — Consisting of civil and criminal fines and penalties
- **Financial** — Internal and external costs associated with investigating and remediation (e.g., legal fees, consultants, investigators)
- **Operational** — Potential disruption of business operations from plant shutdowns, suspensions, debarments, and loss of license
- **Reputation (image)** — Effect of media coverage; damage to organization's image/brand; and subsequent diminished attractiveness to current and potential future employees, business partners, vendors, and customers
- **Health and safety** — Employee, patient, customer
- **Ability to pursue strategic goals** — Prohibition to added new customers, loss of license

Figure 4.3 illustrates how these categories might be used to construct a scale for assessing the impact of compliance risks.

Figure 4.3 **Impact of Compliance Risks**

Scale	Legal*	Financial#	Operational (Potential Disruption)*	Reputation (Image)+	Health and Safety*	Ability to Pursue Strategic Goals*
1 Insignificant	In compliance	< $1 million	< 1/2 day	No press exposure	No injuries	Little or no impact
2 Minor	Civil violation with little/no fines	$1–$5 million	< 1 day	Localized negative impact on reputation (such as a single large customer) but recoverable	First aid treatment	Minor impact
3 Serious	Significant civil fines/penalties	$5–$25 million	1 day–1 week	Negative media coverage in a specific U.S. region or a foreign country	Medical treatment	Major impact
4 Disastrous	Serious violation, criminal prosecution probable	$25–$100 million	1 week–1 month	Negative U.S. national or international media coverage (not front page)	Death or extensive injuries	Significant impact
5 Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or licensure	> $100 million	> 1 month	Sustained U.S. national (and international) negative media coverage (front page of business section)	Multiple deaths or several permanent disabilities	Loss of accreditation or license

Amounts are examples only; each organization should set amounts to reflect its size and financial strength.

* Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 39, https://compliancecosmos.org/compliance-risk-assessments-introduction

\+ Adapted from Deloitte, *Compliance risk assessments: The third ingredient in a world-class ethics and compliance program*, Deloitte Development LLC, 2015.

As with the likelihood scale, each organization would adapt the impact scale and factors to its own environmental context. The organization's risk appetite would also be reflected in setting the values used in the anchor labels.

An additional factor that may enhance the evaluation of severity is the localization or regionalization of the assessment. For multilocation and multinational organizations, risk may vary from one location or region to another, based on a wide variety of factors. Rather than assessing severity at the organizational level, determining separate measures can add an additional level of precision to the assessment.

Assessment of each of the risks in the compliance risk inventory can be made by compliance staff or by a compliance committee and can be conducted at different levels of the organization. In conducting assessments, steps should be taken to minimize bias by avoiding self-assessment and using multiple assessors from varied disciplines and experience to ensure that risks are appropriately evaluated.

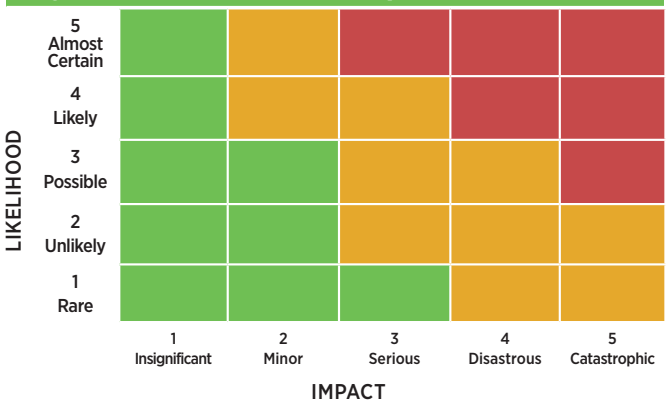
Table 4.2 **Assesses severity of risk**	
Key characteristics	• Adopt a uniform scale/scoring system for measuring severity of compliance risks • Consider qualitative and quantitative measures • Establish criteria to assess impact and likelihood of compliance risk event occurrence • Assess severity of risk at different levels (organizational, regional, affiliate, etc.) • Consider design and operation of internal controls intended to prevent or detect compliance risk events • Minimize bias and inadequate knowledge in assessing severity (e.g., minimize self-assessments, use multidisciplinary teams)

Principle 12 — Prioritizes risks

The assessments of compliance risks in terms of likelihood and impact allow for prioritization across the organization. One method used to capture and summarize the severity assessment is to construct a risk inventory matrix.

Using the example scales from the preceding section, the following matrix can be developed.

Figure 4.4 **Likelihood vs impact matrix**



This allows the organization to group risks in terms of how and when they will be addressed and the level of attention that each is given. Although it could be argued that the organization ideally could address all of its compliance risks, from a practical perspective, more direct and immediate attention is required for the most serious risks. How this is done will depend on the organization's risk appetite and tolerances and its available resources. For instance, in the example, risks in the green areas would be periodically reassessed, but no specific risk response action or extensive monitoring action would be taken. In the yellow areas, the risk owners would be required to develop a risk mitigation plan to reduce or eliminate them without the addition of significant resources. For those risks falling in the red areas, compliance committees would be assigned to work with risk owners to develop detailed response plans in which risk ownership is clearly identified, assign responsibility for risk responses, and develop monitoring and auditing plans for the remediation efforts.

In addition to severity and risk appetite, some organizations consider other factors in their risk prioritization. Adjustments might be made to the risks on the basis of velocity, persistence, and recovery. Velocity is the speed at which a risk affects the organization, such as a serious food safety violation that would require immediate closure of a food processing plant. Persistence is how long the risk affects the organization, such as media coverage from criminal violations lasting four or five years. Recovery refers to how long it takes to fix the problem (i.e., time needed to manage the risk to tolerable levels), such as how long it takes to implement improved vendor due diligence criteria and processes to reduce the risk of shell company transactions.

Table 4.3 **Prioritizes risks**	
Key characteristics	• Prioritize compliance risks based on assessed level of risk relative to meeting of business objectives • Use objective scoring based on assessment • Consider use of other assessment criteria (trend, velocity, etc.) in prioritizing compliance risks • Consider possible effects of planned changes in strategy and operations • Develop risk-based action plans for mitigation (risk responses, implemented in next step)

Principle 13 — Implements risk responses

Risk responses are designed to manage the assessed level of risk and can take many forms. The most obvious response to an elevated level of risk is the design and implementation of improved internal controls over compliance. Effective mitigation of a compliance risk involves consideration of all seven elements of a C&E program for each risk (e.g., policies, training).

Many risk-specific policies involve internal controls. Internal controls over compliance may be preventive or detective in nature, and ideally a blend of both is in place. Although

prevention of noncompliance and ethical misconduct is preferred, there may be practical considerations that result in an organization relying more heavily on timely detective controls for certain risks.

Effective improvement of internal controls requires an understanding of the principal drivers of a particular risk. If the likelihood or frequency of a risk drove the assessed severity higher, improvements to preventive controls may be particularly important. On the other hand, impact — especially when impact correlates to how long a risk goes undetected — may be mitigated by improving detective controls.

Risk responses may involve many actions other than improvements to procedural internal controls. For example, targeted training aimed at areas of vulnerability may be useful. Training is a form of internal control that is a particularly valuable response when the design of procedural controls is sound, but there are breakdowns in those controls based on a lack of understanding of how the controls are to be applied or a general lack of awareness of the controls.

Training may also be more general in nature. If the observed behavior involves a weak culture of compliance, general training on the importance of compliance may be useful. Regardless of type, training, by itself, rarely results in significant improvements. If coupled with improvements in control processes, however, improvements are much more likely to be observed.

Another possible risk response is to increase or improve the auditing and monitoring function related to the specific compliance risk assessed. This may be done through increased frequency or scope of monitoring and auditing. Or it may be achieved by implementing new methods of auditing and monitoring. For example, increased use of data analytics aimed at detecting red flags of noncompliance or red flags of breakdowns in internal controls (also discussed in connection with ERM Principle 18) can be powerful tools for the audit and monitoring function.

One aspect of risk response worth further consideration is the level of granularity of the response. Although some control responses are very broad and apply to an entire process, others may be much narrower. This is particularly pertinent for the design of improved internal controls and certain auditing and monitoring procedures. The assessment of risk and controls may reveal a vulnerability in one very specific part of a lengthy process. For example, an assessment of the risk of product safety violations for a toy manufacturer might reveal that new machinery installed on an assembly line has a particular vulnerability to improper operation that previous machinery did not have, leading to increased risk of the manufacture of unsafe products. The response in this instance may be equally narrow: to implement a different and more frequent inspection and maintenance schedule for the newer machinery.

Of course, the benefits of adding or improving internal controls and other risk responses should always be weighed against the financial and nonfinancial costs of these efforts. It may be possible to reduce a compliance risk to an extremely low level, but the cost of doing so in terms of slowing down productivity may be excessive. Accordingly, cost is a practical consideration when designing and implementing risk responses. This potential for tension between compliance-related controls and operational efficiency is often an important trade-off that requires attention.

For risk responses to be executed properly, accountability must be established. Responsibility for responses is often shared among a variety of groups, from the business unit directly affected by the risk to other units within the organization, such as internal audit, human resources, information technology, compliance, and others. For this reason, the exact nature of the risk response should be agreed upon by all parties that will play a role in the execution. Once this is accomplished, a specific timeline for the execution should be developed, with greater priority given to the risks identified as furthest above tolerable levels.

The final aspect of risk response involves following up to evaluate the implementation and operating effectiveness of those responses. An excellent response plan is only as good as its execution. Part of the response plan should include follow-up evaluations and ongoing monitoring to determine whether all actions in the plan have been properly carried out and are operating as planned.

Table 4.4 **Implements risk responses**

Key characteristics	• Consider potential need for modifications in each element of the C&E program when designing risk responses • Design compliance risk responses that consider the impact on other (non-compliance) risks and risk responses • Assign accountability for each compliance risk response (including timeline, etc.) • Follow up to determine whether compliance risk responses have been properly implemented as designed • Consider compliance risk responses when developing monitoring and auditing plans

Principle 14 — Develops portfolio view

It is important to recognize the interrelationship among compliance risks, as well as the relationships between compliance risks and other organizational risks. These interactions can be an important consideration in both the assessment of risk as well as the design and implementation of risk responses. This consideration can also lead to the identification of certain drivers of risk — factors that do not necessarily create a new risk, but that can increase the likelihood of one risk event as a result of some other action or event.

Here is a simple illustration: enhanced internal controls aimed at reducing the risk of a compliance violation could increase the risk of delays in certain operational or production processes. This concern would be amplified if the production team had also identified a slowness in its processes as a risk requiring a response. The two risk responses could potentially conflict with each other unless a portfolio view is taken in connection with both identifying and mitigating risk.

If risks are managed in isolation without consideration of other risks, inefficiencies — and possibly conflicts — can occur. For this reason, viewing risks as part of an organization-wide portfolio of risks is essential.

Another consideration in developing a portfolio view is the extent to which compliance risks increase or decrease in severity as they are progressively consolidated to higher levels within the organization. A compliance risk that at first appears to be significant at a business unit level may be rather minor by the time it is consolidated with other risks and rolled up to a higher level within the organization. Conversely, compliance risks that are minor in isolation may become much greater when consolidated with other seemingly minor risks.

Table 4.5 **Develops portfolio view**

Key characteristics	• Consider risk interactions (i.e., how mitigating a compliance risk can affect other risks) • Consider interactions of compliance risk responses with other risk responses • Integrate compliance risk management with ERM • Have regular meetings/communications between compliance and business units

5. REVIEW AND REVISION FOR COMPLIANCE RISKS

The legal, regulatory, and ethical environments of organizations are ones of constant change and, frequently, increased complexity. Technological advancements have increased the speed of communications and activity, expanding the number of individuals an organization can affect across the globe. Even small organizations may be operating in multiple countries and jurisdictions, and regulations in these places are proliferating. Stakeholder expectations regarding organizational conduct continue to rise. Thus, for compliance risk management to be effective, the organization must regularly review its compliance risk management practices and capabilities and take steps to continually improve its C&E program.

This section describes the application of the review and revision component of the COSO ERM framework and the following three principles associated with the management of compliance risks:

15 Assesses substantial change

16 Reviews risk and performance

17 Pursues improvement in enterprise risk management

Principle 15 — Assesses substantial change

Changes in the organization's internal and external environment can have significant impacts on the organization's compliance risk profile, often very quickly, which is why many compliance program standards require periodic re-evaluation and modification. The CCO needs to identify potential drivers of changing compliance risk. Broadly, these potential drivers include, but are not limited to the following:

- Changes to the organization's strategies and objectives
- Changes to people, process, and technology
- Changes in regulatory requirements and/or societal expectations

As Principle 6 discusses, the CCO should be involved in the strategy-setting process to allow the C&E program to identify and manage the change in compliance risk resulting from significant shifts in business strategy and objectives. For example, a technology company decides to start or acquire a new line of business in a highly regulated environment, such as providing cloud services for health systems' medical records, or an engineering firm seeks to begin contracting with the federal government. An organizational shift to the use of third parties for business processes may also result in potentially significant changes to compliance risk.

Changes in the internal environment in people, processes, and technologies can also result in changes to compliance risk. For example, a change in senior personnel can result in a significant shift in the level of risk tolerance as well as the compliance culture. Increased performance pressures (cost, sales, productivity, efficiency, etc.) can affect risk. Mergers and acquisitions can also drive change in compliance risk. Changes to processes and technologies may also lead to potential changes to compliance risk. For example, automation may result in the company being able to perform a task faster, but it may mean that the impact of a failure will also be magnified.

Changes in the external environment affect the organization's compliance risks through changes to laws, regulations, enforcement priorities, and societal norms and values. Assessing the impact on compliance risk has become increasingly complex due to the proliferation of laws and regulations across jurisdictions, often with conflicting requirements. The C&E program needs to keep abreast of changes to the regulatory environment through studying information from industry and professional groups as well as trends in enforcement and guidance provided by regulators. There are also increasingly sophisticated regulatory change management applications that can assist the C&E program with identifying and tracking.

Table 5.1 **Assesses substantial change**	
Key characteristics	• Identify drivers of change in compliance risk — internal and external • Consider how implementation of new strategic initiatives affects compliance risk • Consider how changes in senior personnel affect compliance risk and/or risk tolerance • Evaluate changes in laws and regulations • Consider developments in enforcement, guidance from regulators, and other trends • Assess changes in local/regional environments

Principle 16 — Reviews risk and performance

As noted in the discussion of Principle 1, the board of directors has oversight responsibilities for the performance of the organization's C&E program, and the CCO and management are responsible for the program's design and implementation. For the board and management to carry out their responsibilities, mechanisms are needed to provide assurance that compliance risks are being managed within tolerable levels.

The goal of the reviews of C&E program performance goes beyond just providing the needed assurance for the board and management to fulfill their responsibilities for managing compliance risk to acceptable levels; the goal is also to continually improve the C&E program. Regulators have become more explicit in their expectations regarding the review of C&E program performance as a critical element of an effective compliance program. As noted earlier, one of the seven elements of an effective compliance program under the USSG includes the expectation "to evaluate periodically the effectiveness of the organization's compliance and ethics program." Similar expectations for assessment of the C&E program's performance are found in guidance from various regulators across the globe.

The expectation is for two types of review: (1) a review of compliance risks that are considered to be a high priority based on their assessed likelihood and impact of noncompliance and (2) periodic review of the overall performance and effectiveness of the C&E program. In addition to reviews by auditing and monitoring, there is an expectation for the use of other mechanisms to provide feedback regarding C&E program performance, particularly a trusted system through which employees and others may report or seek guidance regarding potential misconduct.

For each high-priority compliance risk, in addition to developing an education and training strategy, the organization should develop a monitoring and auditing plan. Although the compliance function may take the lead in the development of such plans, it should not be the responsibility of compliance alone. Risk owners, internal audit, risk management, and potentially others should be involved in developing the plan. Role clarification for the plan is essential to minimize duplication of effort and assurance gaps. The plan should include a description of the planned risk responses, who is responsible for the response, how response effectiveness is measured, and who will be responsible for the performance review.

One model that can help establish role clarity is the Three Lines Model, formerly the Three Lines of Defense, updated July 2020 by The Institute of Internal Auditors. This framework distinguishes among the following three groups (or lines) involved in effective risk management:

First line roles (management):

- Leads and directs actions (including managing risks) and application of resources to achieve the objectives of the organization
- Maintains a continuous dialogue with the governing body, and reports on planned, actual, and expected outcomes linked to the objectives of the organization, and risk
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control)
- Ensures compliance with legal, regulatory and ethical expectations

Second line roles (management):

- Provides complementary expertise, support, monitoring, and challenge related to the management of risk, including the following:
  - The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, systems, and entity level
  - The achievement of risk management objectives, such as compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance
- Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control)

Third line roles (internal audit):

- Maintains primary accountability to the governing body and independence from the responsibilities of management
- Communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organizational objectives and to promote and facilitate continuous improvement
- Reports impairments to independence and objectivity to the governing body and implements safeguards as required

Above these three lines is the organization's governing body. The Three Lines Model describes the governing body's responsibilities to include,

> *Delegates responsibility and provides resources to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.*

Put more simply, the board is responsible for oversight of the compliance and ethics functions. The most senior level of management, where the CCO sits, is responsible for establishing structures and processes aimed at ensuring compliance. The next level of management is responsible for providing expertise, support and monitoring to achieve compliance and ethics expectations.

Figure 5.1 shows how this model can be used to design an auditing and monitoring plan for a high-risk area (conflict of interest in an academic medical center).

Figure 5.1 **Auditing and monitoring plan for a high-risk area**

	1st Line	2nd Line	3rd Line
Risk Area	**Management**	**Management**	**Internal Audit**
As Identified During Risk Assessment	Structures and policies	Monitoring and support	Independent auditing
Conflict of Interest (COI)	• Establish COI policies and procedures • Educate personnel about COI policies • Report non-compliance to COI Manager • Report unauthorized vendors representatives and displays • Advise personnel to contact Compliance with questions • Review annual COI disclosures	• Annual COI disclosure • Purchasing and Pharmacy vendor registrations • Open Payments database • Research conflict database cross-check	• Audit 10% of outside travel payments against Accounts Payable travel reimbursements • Level 2 review of COI disclosures • Audit 10% of "nothing to disclose" • "For cause" investigations

In addition to the auditing and monitoring of high risks, a review of the C&E program as a whole is necessary to provide the needed assurance for the board and executive management, and it is also part of Principle 17 and the effort to continually improve the C&E program. This review involves periodic assessment of the effectiveness of the C&E program as a whole. There are a number of approaches that could be taken. The review could be performed by members of the compliance and ethics function in a self-review, by the organization's internal audit function, or by external service providers. At a minimum, the review should look to see that the C&E program incorporates all of the elements of an effective compliance program described in the Appendix 1 (or other applicable standard) and that they are operating effectively.

An additional resource that could be used is the *Evaluation of Corporate Compliance Programs* guidance provided by DOJ to federal prosecutors for their use in assessing C&E program effectiveness.[2] This guidance asks the following three fundamental questions regarding the organization's C&E program:

1. Is the organization's C&E program well designed?
2. Is the program being applied earnestly and in good faith; in other words, is the program adequately resourced and empowered to function effectively?
3. Does the C&E program work in practice?

Determining the answers to these three questions requires further inquiry into each element of an effective program, as well as evaluating the C&E program as a whole.

2 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (updated June 2020), http://bit.ly/2Z2Dp8R.

One issue of note in the DOJ framework is that the overall review of the C&E program is expected to include a measurement of the organization's culture of compliance, including seeking input from all levels of employees to determine how they perceive senior and middle management's commitment to compliance.

Finally, in addition to monitoring and auditing, there are other mechanisms that provide feedback on the performance of the C&E program. A confidential reporting mechanism through which employees and others can report suspected misconduct involving the organization will identify specific instances where investigation and remediation are required and may identify opportunities to improve the program. Employees can also use this mechanism to seek guidance and ask questions about their work and the work environment.

When investigations of reported allegations of misconduct conclude that there is indeed misconduct, the organization should take appropriate steps to respond and to prevent further similar misconduct, including making appropriate modifications to the C&E program. Analysis of trends in the data from the confidential reporting system (including monitoring and auditing results and other data) should be used to identify gaps in the design or execution of the C&E program. Research has consistently found, however, that in many organizations, only a small portion of misconduct issues are reported through the confidential mechanism, so other feedback and data points must also be considered. For instance, many employees report misconduct to supervisors rather than use the confidential mechanism. In the majority of cases, these are handled by the supervisors and others in the organization; however, the data is not necessarily tracked or reported to compliance, so there is no feedback on C&E program performance. To get this feedback, some organizations have policies requiring supervisors to report such cases to compliance so they can be tracked and analyzed.

Other mechanisms are information from exit interviews — where employees are asked if they have observed instances of misconduct in the organization — periodic employee surveys, and feedback from participants in compliance training.

Table 5.2 Reviews risk and performance

Key characteristics	• Monitor performance against compliance and ethics metrics and report at the management and board levels • Update compliance risk assessments on a periodic basis • Develop monitoring plans for high-priority risks, assign assurance responsibilities clearly across the three lines, and set clear performance expectations • Ensure that internal audit considers compliance risk in connection with its review of entity risk and performance • Periodically assess the organization's culture of compliance • Ensure that annual C&E program work plans reflect risk assessment (cross-referenced) • Include appropriate audit rights clauses in third-party contracts to facilitate monitoring and auditing • Obtain feedback from participants in compliance training, hotline reports, employee surveys, and exit interviews • Require that implementation of corrective action plans is an important metric monitored by management and the board • Perform root cause analyses for compliance risk events experienced

Principle 17 — Pursues improvement in enterprise risk management

One of the key indicators of an effective C&E program is a commitment to continuous improvement. Principles 15 and 16 explain the importance of using a variety of mechanisms to identify substantial changes in the organization and its environment and to identify gaps in program effectiveness. Merely identifying issues is not enough, however. Action must be taken to adjust and improve the C&E program. Increasingly, regulators emphasize the importance of the organization demonstrating its efforts to review the program and take action to ensure that it does not become stale. For many regulators, proactive efforts by the organization may be rewarded with reduced fines and requirements in resolution agreements and prosecution decisions.

The CCO should meet periodically with the board, as well as with the organization's internal compliance committee, if one exists. Together, they should address the results of performance reviews and the C&E program's proposed action plan to address identified gaps in C&E program performance, as well as proactive improvements to the program. In addition, the results of investigations where misconduct was found should be analyzed to determine root cause and what adjustments need to be made to the C&E program and discussed with the respective committee.

Where adjustments and improvements to the C&E program are warranted, appropriate action plans should be developed with timelines and specific responsibilities assigned. Progress on the action plan should be tracked, and there should be appropriate follow-up.

Not all improvements to the C&E program are reactionary in nature. An important aspect of continuous improvement involves taking proactive measures. The organization should stay current on new or improved tools, as well as innovative approaches, that may improve program performance and effectiveness.

Another action that can contribute to the continuous improvement of the C&E program is benchmarking against the practices of other organizations. Often this is done within the same industry; however, this may be too narrow, as there are significant differences in the maturity of compliance programs within industries. There is much to be learned from looking at other industries, particularly ones that, because of their regulatory environments, have been dealing with heightened compliance risks for some time.

Table 5.3 **Pursues improvement in enterprise risk management**

Key characteristics	• Maintain awareness of current trends in compliance risk management (through training, review of regulatory guidance, etc.) • Ensure that compliance periodically self-assesses the C&E program's performance • Obtain feedback from the board on the quality and usefulness of compliance risk information shared • Consider obtaining periodic independent evaluation of the C&E program • Consider benchmarking the C&E program against similar organizations • Review efficacy of the compliance risk assessment process on a periodic basis • Ensure that internal audit plays an active role in periodically evaluating the effectiveness of the C&E program

6. INFORMATION, COMMUNICATION, AND REPORTING FOR COMPLIANCE RISKS

This section describes the application of the information, communication, and reporting component of the COSO ERM framework and the following three principles associated with compliance risks:

18 Leverages information and technology

19 Communicates risk information

20 Reports on risk, culture, and performance

Principle 18 — Leverages information and technology

For a compliance function to effectively manage a C&E program, it must have timely access to information pertaining to each of the elements of the C&E program. For example, to effectively carry out a monitoring and auditing function, the compliance function must have access to all information relevant to detecting noncompliance or breakdowns in compliance-related internal controls.

Technology can be a vital asset in connection with several aspects of a C&E program. For example, technology can be utilized to deliver compliance awareness training through a wide variety of methods and formats, with interactive features that improve learning in comparison with other methods, such as live classroom-based training. Technology-assisted training is often easy to update in order to rapidly address new issues or simply to keep training fresh.

Nowhere is technology more useful to compliance than in the monitoring and auditing component of the C&E program. Unlike with a sampling approach to auditing, properly designed data analytics can analyze 100% of a population of transactions or activities for red flags. These tests can target (1) breakdowns in internal controls designed to prevent noncompliance, (2) instances or patterns of noncompliance, (3) breakdowns in internal controls designed to detect noncompliance, or (4) other indicators or effects of noncompliance. Data analytics look through digital records to identify anomalies that are consistent with any of these four targets. Further, properly designed data analytics can be deployed in a manner that focuses on high-priority compliance risk areas based on the risk assessment.

For example, digital markers can indicate whether certain internal controls for compliance are functioning as designed (e.g., is digital evidence consistent with expectations of reviews and approvals performed by supervisors when this is done electronically?). Digital evidence can also reveal other anomalies that are consistent with noncompliance, such as indications of records being altered or substituted after a transaction has supposedly been completed. Analytics can also be applied to unstructured data in pursuit of the identification of compliance-related anomalies. Technology enables organizations to scan or actively monitor electronic communications (e.g., email, text messages, etc.) or other text (e.g., explanations on purchase orders, journal entries, etc.) for signs of nefarious activities. For example, communications between a manager and their subordinates could reveal signs of extreme pressure to meet deadlines, increasing the risk of employees overriding key compliance controls.

Another use of information and technology involves performing initial assessments of information provided through an organization's confidential reporting mechanism.

Table 6.1 **Leverages information and technology**

Key characteristics	• Ensure that compliance has access to all information relevant to effectively manage compliance risk • Provide compliance with relevant information technology/data analytics skills or access to such skills • Utilize data analytics in monitoring/auditing (monitor compliance and performance of internal controls) • Create automated dashboards/reports for monitoring compliance • Leverage technology to provide for the delivery of effective compliance and ethics training • Utilize technology to facilitate risk assessment process (scoring, reporting, etc.)

Hotline calls can be a valuable source of information relating to allegations of specific acts of noncompliance or unethical workplace behavior. Prior to launching a full investigation or interviewing employees, data analytics can be utilized to assess the credibility of the allegation or help focus the scope of the investigation.

Information and technology can also be used to provide managers with dashboards or other reports customized to each business unit (discussed further in Principle 20). Timely information about compliance-related activities and results of monitoring efforts enables managers to act quickly, minimizing the impact of any identified problems.

Principle 19 — Communicates risk information

Of all the characteristics that benefit a C&E program, communication is the most vital. The compliance function should interact with virtually every business unit and function within the organization, acting as a partner in identifying and managing compliance and ethics risks that threaten the organization, delivering quality training and information regarding compliance and ethics risks, and responding to allegations or concerns about compliance matters.

The partnership between compliance and individual business units is essential to the effectiveness of the C&E program. Just as the business units know their operations better than anyone, nobody is better positioned to help the business unit understand the ramifications of compliance and ethics issues than the CCO and the compliance team. Accordingly, the management of compliance risks is most effective when there is a regular dialogue between compliance and each business unit, resulting in a shared mission of balancing compliance with operational efficiency. This communication is a two-way street, not simply communication from compliance to operations. Operations must be able to engage with compliance in a way that ensures that solutions are both effective and practical, and built with the real-world insights that operations leaders bring to the table.

Effective compliance-related communication also has an important cascading effect. Broad statements about ethics and compliance awareness should come from the most senior levels of management and the board of directors. From there, communications that are more tailored to individual departments, functions, and even specific jobs should be developed and delivered by managers and supervisors — all aimed at personalizing the roles that various employees have in the C&E program. Throughout this process, the CCO and compliance team play an integral role, providing guidance and even assisting in preparing certain messages, including those addressing lessons learned from compliance failures the organization has experienced.

Communications may take a variety of forms, from emails, posters, and other recurring means to town halls, meetings, and other events. Informal communications from managers and supervisors are another effective means of articulating employees' roles and responsibilities in connection with the C&E program. Collectively, these different methods of communication should reinforce and make reference to the more formal compliance and ethics training explained in connection with Principle 5.

One commonly overlooked area of compliance communication pertains to an escalation policy or protocol. Certain allegations, issues, findings, or investigations should be disclosed beyond the team that is charged with looking into the matter. For example, if an allegation of improper conduct is aimed at a lower-level employee in an organization, the team responsible for investigating such matters likely does not need to inform many others within the organization; however, if the allegation was against a member of the executive team, or it involved very serious matters, some level of disclosure of the matter to the board of directors is necessary.

The final step in communications involves the board or its designated committee, as introduced in Principle 1. Much of this communication is done through the reporting described in Principle 20. An important aspect of compliance risk management is the discussion of risk that should take place between the board and the CCO, including the board challenging the CCO to ensure that all internal and external compliance factors have been considered. Simply delivering a report, no matter how thorough, is not sufficient and would not demonstrate program effectiveness. It fails to demonstrate the level of oversight that regulators expect or that is essential to effectively manage compliance risk. In-person explanation of issues addressed in the report, delivering meaningful information, and discussing actionable plans for improving the program are all steps that are important to effective management of compliance risk.

Table 6.2 **Communicates risk information**

Key characteristics	• Ensure that employees receive clear and regular communications on their roles regarding C&E • Require periodic reporting to the board by the CCO • Establish protocols and ensure a clear understanding of an escalation policy • Provide compliance risk communications that support and relate to training and job responsibilities • Engage in effective two-way communication between operations management and compliance

Principle 20 — Reports on risk, culture, and performance

Closely related to the communication of risk information is reporting on risk, culture, and performance associated with compliance-related risks. These stakeholders include the board of directors, any board-level committee delegated the responsibility of compliance risk oversight (if one exists), the senior executive team, any internal compliance committee (if one exists), and appropriate managers/heads of departments or functions within the organization. Reporting to these groups should be tailored to the unique needs and responsibilities of each, as should the frequency of reporting.

For example, reporting to the board should focus on what is needed for the effective oversight of the entire C&E program — information about the risk assessment process, identification of the most material risks and actions being taken in response to those risks, meaningful compliance metrics addressing both the structural and substantive performance of the program, information about compliance-related investigations, resource allocations and needs, etc. Reporting to the board should also periodically address culture as it pertains to compliance and ethics. Culture can be a difficult area to assess; however, efforts should be made to provide the board with some perspective and trends on organizational culture associated with compliance and ethics. This may be accomplished through employee surveys; data associated with culture; and other less formal methods, such as interviews and focus groups.

As reports are designed for each level in the organization chart, the information included should be more granular and customized to the needs of each layer. By the time the reporting gets to the department head/manager level, information should focus on what is needed to manage compliance risk in that area, although periodic reporting on organization-wide risk may provide helpful context.

Reports on compliance risk management should address externally generated risks as well as those that result from the internal risk universe (e.g., employee acts). Third-party risk management is an important element of a C&E program. Accordingly, reports should be prepared and distributed to appropriate stakeholders on the status of third-party suppliers, sales agents, and others who could create risk for the organization. These reports should focus on the results of third-party due diligence efforts in the selection or continued use of vendors and other third parties, site visits, auditing and monitoring procedures, training provided to third parties, and any other matter associated with managing this area of risk.

One final aspect of reporting that is critical to C&E program effectiveness is documentation. Typically, documentation involving investigations is maintained and reviewed only by the compliance, legal, and/or investigations team. It is crucial to properly handle, preserve, and maintain these materials and records in the event of legal action or government inquiry. Each compliance-related investigation should be well documented, include a timeline of events and key steps/actions taken along the way, and summarize any remedial steps. Whether a formal case management software tool is used or something simpler is utilized, maintaining this record is an important part of a C&E program. From these records, useful reports can be generated that provide insight into the needs and effectiveness of the investigations element of compliance risk management.

Table 6.3 Reports on risk, culture, and performance

Key characteristics	• Provide periodic reports on compliance and ethics risk assessments and related remediation efforts tailored to key stakeholder needs • Develop and report on meaningful operational and substantive metrics associated with the effectiveness of the C&E program • Provide managers with reports on completion and results of training of their direct reports • Use a case management and reporting system for investigations and outcomes • Establish and follow a policy that clearly articulates the nature of reporting on all significant remediation efforts

APPENDIX 1.
Elements of an Effective Compliance and Ethics Program

Introduction

The seven elements of an effective compliance and ethics program are described in the U.S. Federal Sentencing Guidelines (USSG), ¶8B2.1, subsection (b) as follows:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an a ppropriate subgroup of the governing authority.

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

¶8B2.1, subsection (c) follows by stating:

In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

This final provision requiring periodic compliance risk assessments and continuous improvement of the C&E program, which was added in 2004, is often referred to as the eighth element of a C&E program.

All seven elements of a C&E program, along with periodic risk assessments and ongoing program improvement, must be in place and functioning well in order for the program to be considered effective. It should be noted that the USSG, which set forth the seven elements, are guidelines for federal judges, but they may be much more than "guidelines" for organizations. The word "shall" appears 17 times in connection with the elements, and many believe the guidelines represent the minimum standards for building an effective C&E program, at least for U.S. organizations and others operating in the U.S., as well as U.S.-based multinational companies.

This appendix is devoted to an overview of each of these elements, forming the basis for understanding the guidance on its application to ERM found in earlier sections of this publication.

Standards and procedures

Standards of conduct demonstrate an organization's commitment to an ethical workplace and a culture of compliance with laws and regulations. This begins with a code of business conduct and ethics. The code should be designed to apply to all employees, management, and the board. The code is supported by many policies and procedures. A code should also apply to certain third parties, such as vendors and suppliers, although this code is often different and more abbreviated than the code that applies to employees.

Two types of policies and procedures are essential to a C&E program: structural and substantive. Structural policies create the framework for how the program operates. Substantive policies address the organization's positions on the key laws, regulations, and standards that apply to its business activities.

Examples of structural policies and procedures are those that define the roles and responsibilities of the compliance officer, compliance committee, and the board; methods for reporting suspected wrongdoing; processes used for auditing and monitoring; investigative responsibilities and procedures; and many others.

Substantive policies focus on preventing and detecting specific compliance violations (e.g., bribery, false claims, antitrust, environmental, record retention) by communicating the organization's expectations for employee behavior in connection with individual risk areas.

Governance, oversight, and authority

The compliance and ethics function should be subject to effective oversight at the board, management, and compliance officer level.

The board has a clear responsibility to ensure that an effective C&E program is in place and to provide adequate oversight of the program by being knowledgeable about the content and operation of the program. The board must also ensure that the CCO is positioned at a senior level within the organization and has adequate resources and authority to effectively manage the program.

In some instances, compliance oversight at the board level is delegated to a committee, such an audit or compliance committee. In other cases, compliance oversight is handled by the board as a whole. Either way, the CCO should have a reporting relationship with the board or a committee of the board, even if there is also a reporting line to another executive position, such as to the CEO.

In this respect, the compliance function is similar to an internal audit function, where independence and autonomy are important. From a day-to-day operational standpoint, the top compliance professional may report to another member of the senior management team, but there should always be a direct reporting line to the board as well so that the compliance officer can have candid discussions without interference from other members of management.

Although the board provides oversight, management is responsible for executing the program — ensuring that employees complete training, report concerns, fix problems, or perform work activities consistent with program requirements. The USSG recognized that it is ultimately management that is responsible for the ensuring the program is effective.

The CCO has day-to-day responsibility for operating the C&E program and must have the necessary resources and access to information to operate the program. Sufficiency of resources was added to the list of factors the DOJ considers when evaluating compliance programs in the June 2020 revision to its Evaluation of Corporate Compliance Programs guidance.

There may also be an internal compliance committee, with representatives from major functional areas and/or operating divisions. Although the CCO may be the most visible leader of a C&E program, an internal compliance committee can be a very effective method of program management, ensuring that

each operating division approaches compliance similarly. An additional benefit of such a compliance committee is the value created by collaboration and input across functional areas to support the overarching objectives of the C&E program.

The final critical element of compliance oversight involves making sure there is a clear and written understanding of the roles and responsibilities of each of these functions or committees. This may be documented in the form of a charter or policy.

Due diligence in delegation of authority

Organizations should perform background checks before hiring new employees and additional periodic checks when permitted or required by law. In addition, the organization should consider the person's past support of (or failure to support or execute) the organization's C&E program when promoting employees to positions of greater authority. The level and type of background check should correspond to the position of each employee, based on the role that person has, or will have, in relation to compliance risks.

The USSG refer to this expectation in connection with "substantial authority personnel," a term defined in the application notes as "individuals who within the scope of their authority exercise a substantial measure of discretion in acting on behalf of an organization," noting that these individuals may or may not be considered management. The clear inference is that the scope of diligence should grow as the level of responsibility grows. Compliance may wish to work with human resources and other functions to make these determinations.

Though not explicitly stated in the USSG, regulators have grown to expect that organizations perform appropriate levels of due diligence on third parties that create or involve compliance risk for the organization. For example, if a company utilizes a third party located in another country to represent the organization, or to sell to customers in that country, an appropriately scaled background check — based on the assessed level of compliance risk involved — would be expected.

Communication and training

Communication and training, when done effectively, contribute to the prevention and detection of compliance issues. Every employee and member of the board of directors should receive training on general topics that are important to the program, and more focused training on specific compliance matters should be provided to personnel involved in activities relevant to each compliance risk.

General training, done on at least an annual basis, for all employees and the board of directors is a hallmark of a robust and effective program. General training covers the code of conduct, maintaining a culture of compliance and ethics, how to seek guidance and report suspected problems, the organization's nonretaliation policy, what the organization does when suspected compliance issues are reported, and any other relevant aspect of the program that affects everyone.

Focused training dives deeper into specific compliance risk areas, critical internal controls, and other procedures associated with specific risks. Consequently, only those employees who play key roles involving those risk areas are typically required to participate in this type of training. An example of focused training is a program aimed at sales personnel of an international company on compliance with the Foreign Corrupt Practices Act. It is not necessary for every employee to understand what constitutes a violation of the act, but it is critical for individuals involved in international sales (and relevant support and finance teams) to have a sound understanding of this risk as well as the controls and procedures the organization has implemented to prevent misconduct.

To be effective, training must be more than simple delivery of educational content. In its June 2020 guidance, DOJ emphasized the importance of (1) allowing employees to ask questions during training and (2) evaluating whether training affected employee behavior.

Although much of the training that involves compliance topics is in the form of either traditional classroom style presentations or online, web-based programs, training may also involve other forms of education and communication. For instance, an email message or a company newsletter may be used to inform the workforce or reinforce traditional training on new or changed compliance requirements. Communications may also address lessons learned from compliance failures the organization has experienced.

Organizations can sometimes be held accountable for compliance failures of third parties. Accordingly, training should be considered for each third party based on an assessment of the associated type and level of compliance risk.

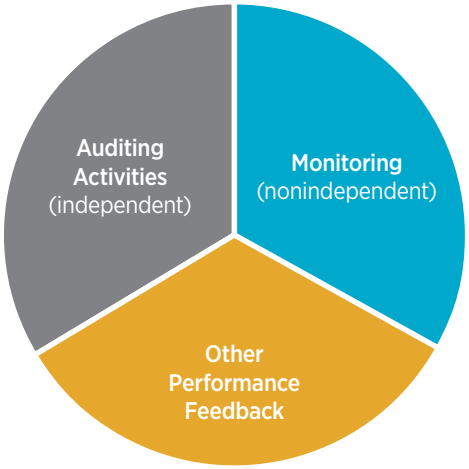
Finally, other forms of general communications also help to create and maintain a culture of compliance and ethics. Examples include supportive messages from the CEO, informative articles in company newsletters, and many others.

Monitoring, auditing, and reporting systems

Monitoring, in the broad sense, refers to the assessment of whether processes are operating as intended in pursuit of the system's improvement. Sometimes the term "monitoring" is used more narrowly to contrast with "auditing," where auditing refers to an assessment by individuals independent of the system. Both auditing and monitoring draw on the same set

of methods and techniques, with a goal of obtaining assurance on the quality of the system's performance over time and contributing to its continuous improvement (see figure A.1).

Figure A.1 **Auditing, monitoring and reporting**



Accordingly, auditing is performed by individuals independent of the function being reviewed. Auditing may be performed by an internal audit department, other third parties, or by individuals within the compliance function if structured so as to maintain their independence. Monitoring is often performed by a quality assurance function or managers, supervisors, and other employees within the function being reviewed.

A monitoring and auditing plan is an important driver of compliance program effectiveness, and it should be designed and updated based on periodic risk assessments. Monitoring and auditing activities should be aimed at both (1) detecting noncompliance (or signs of noncompliance) and (2) identifying breakdowns in internal controls over compliance, such as areas in which a preventive or detective control is not functioning as designed. A wide variety of techniques may be used in monitoring and auditing. Examples include observation and site visits, surveys, questionnaires and checklists, interviews, reviewing transactions and documentation, data analytics, and reviewing digital evidence. The audit function may also provide assurance to the board regarding the overall effectiveness of a C&E program.

Another important mechanism of an effective C&E program involves maintaining a trusted system for seeking guidance and reporting suspected wrongdoing by employees (and others). Employees should have multiple avenues for seeking guidance regarding compliance and ethics issues and for reporting what they perceive as potential violations of laws, regulations, or the organization's policies and procedures.

Although employees may be encouraged to report matters to their supervisors, organizations must recognize that there may be situations in which that is not desirable or practical. Accordingly, making employees aware of other options for reporting is important. Other options may involve telephone- or email-based systems (internal or operated by independent third parties) or direct reporting to others within the organization, such as human resources, compliance, internal audit, an investigations unit, certain members of senior management, or even the board or audit/compliance committee.

Characteristics of an effective reporting system include user options that allow for the following:

1. **Anonymous reporting** — The reporter's identity is not known (where allowed by law), often achieved through a hotline or similar mechanism
2. **Confidential reporting** — The reporter's identity is known only to a select few, and those few are expected to take reasonable steps to maintain that confidentiality while pursuing the matter
3. **Open reporting** — The reporter is willing or desires to have their identity disclosed without limitations

These and any other methods of reporting should be developed with consideration for federal, state, and local laws in the countries and regions in which the reporting system operates.

For any reporting to be effective, it must be trusted. Trust is driven by many factors, but the most important two are (1) a belief that the organization will take allegations and concerns seriously and perform a proper assessment in response and (2) that reporters can expect to be free from retaliation after they have reported their observations and concerns in good faith.

Finally, DOJ encourages publicizing reporting systems to third parties, in addition to employees. Vendors, suppliers, and other third parties are often in a unique position to observe signs of possible violations that might not immediately be observable by employees.

All matters reported should be reviewed and assessed in a timely manner. The assessment of a report should consider whether further investigation is necessary based on the information provided by the reporter, the nature and seriousness of the possible violation, and any other information known that is relevant to the report.

Even in the most trusted of systems, some employees may not feel comfortable reporting wrongdoing until they are leaving an organization. As a result, exit interviews of departing employees should provide one final opportunity for the employee to report suspected wrongdoing and to provide feedback in other areas related to the C&E program.

Investigations may result from information obtained via the reporting system, but may also stem from an organization's

auditing and monitoring activities or even outside parties (e.g., customers, competitors, suppliers). Regardless of what event triggered the concern, an investigation should be prompt, thorough, and independent of the affected function or person, and it should be performed in accordance with written policies and procedures. Case files or other documentation should be maintained and protected to ensure the integrity of each investigation. Investigations are described further in the section on responding to wrongdoing.

It is important to note that the investigation and resolution of allegations are not the only goals of these reporting mechanisms. An equally important goal is the feedback provided on the C&E program's performance so that the program can be improved. This requires tracking and analysis of the trends in issues being reported and the areas where guidance is being sought so that appropriate steps can be taken to increase the C&E program's effectiveness.

Incentives and enforcement

Noncompliance can be entirely unintentional — often the result of ineffective controls, ineffective training or new employee orientation, misunderstanding of procedures, a deteriorating culture, or simply carelessness. A natural deterioration in processes and internal controls occurs over time, unless the processes or internal controls are consistently enforced. Noncompliance can also be intentional — carried out by employees who know they are violating organization policies and who may understand that they are violating laws and regulations in the process.

The USSG require the use of incentives and similar tools to promote consistent participation in and/or execution of the C&E program. Just as boards and executives use financial and recognition incentives to promote sales, safety outcomes, customer or employee satisfaction, and other strategic goals, the USSG state that incentives should be a component of an organization's compliance efforts. Incentives can be particularly effective in motivating leaders to embrace and execute on the compliance program but can also be used effectively at all levels in the organization. Incentives can be financial or nonfinancial in nature and can be effectively integrated with an organization's performance management system.

In its explanation of enforcement, the USSG recommend appropriate consequences for ignoring compliance obligations or violations of law or policy. Such discipline should consider whether acts of noncompliance, or the failure to act, was intentional or unintentional, as well as the severity of the noncompliance. The organization should provide for a range of potential disciplinary actions, from verbal and written warnings up to termination of employment.

Organizational justice is critical to the success of a C&E program. Accordingly, enforcement and discipline must be consistent across all levels of the organization, perhaps most importantly at the highest levels. If the noncompliance of a highly successful salesperson, an executive, or an influential employee is tolerated while another employee is disciplined for the same violation, the C&E program's credibility will be undermined, and the organization's culture can be harmed.

As with all elements of a C&E program, discipline should always consider the local/regional legal environment, as well as contractual or labor union provisions.

In connection with incentives and enforcement involving vendors, suppliers, and other third parties that may create liability, the organization should ensure that there are appropriately tailored contract provisions imposing relevant compliance obligations and addressing the consequences of noncompliance, including penalty provisions and contract termination clauses.

Response to wrongdoing

No C&E program guarantees a lifetime of compliance for an organization. If an organization is around long enough or is large enough, noncompliance is inevitable regardless of how effective the program is.

What an organization does in response to noncompliance is an important factor that distinguishes effective programs from ineffective programs. There are two key aspects of responding to wrongdoing: investigating and remediating.

A compliance investigation must be prompt and thorough, fair to all parties, and conducted by individuals who are independent from the subjects and not otherwise conflicted. Other key considerations in conducting a compliance investigation include the following:

1. **Notifications** — Who should be informed about the investigation (e.g., leaders, legal, outside parties)?
2. **Expertise** — Does the organization have all the expertise needed to conduct the investigation, or should outside assistance be brought in?
3. **Involvement of compliance** — Regardless of whether the compliance officer is conducting the investigation, the compliance officer should be informed and involved along the way.
4. **Documentation** — Collect, protect, and preserve evidence and other documentation gathered as part of an investigation.
5. **Oversight and management** — The larger the investigation, the more important it is to establish an appropriate chain of command (including the involvement of legal counsel where appropriate), for all parties involved to have their work overseen and reviewed, and for the scope of the investigation to be well managed.

6. **Scope** — Understand what the scope of an investigation is from the outset and gear the investigation plan accordingly.

There are many steps to an investigation (e.g., gathering documents, identifying electronic records, conducting interviews of personnel). And in the end, there may or may not be any need or desire for a written report. But the case file should always be closed out properly.

If the investigation uncovers compliance failures, a root cause analysis should be performed to fully understand where any breakdowns or omissions in internal controls occurred, or whether weaknesses in the design of internal controls were identified. Once this is done, the organization must turn its attention to remediating the underlying problems. In cases in which existing policies and procedures were well designed, but the execution of those controls failed, remediation may require nothing more than training (or retraining) certain groups of employees on those controls and the reinstatement or introduction of the appropriate monitoring processes.

In other cases, remediation involves significantly more effort. Modifying policies and procedures, improving preventive controls, changing business processes or incentives, and any other remediation efforts should all be aimed at making sure a particular act of noncompliance does not happen again. In cases where prevention is costly or impractical, remediation might involve adding or modifying detective controls so that if noncompliance occurs in the future, it will be detected and corrected sooner, resulting in reduced losses or penalties. Regardless of the nature of planned actions, accountability for fully implementing remediation plans should be established and monitored.

Risk assessment and program improvement

Regulators consistently emphasize the importance of taking a risk-based approach to training, monitoring and auditing, and the other elements of a C&E program. As such, a sound risk assessment process is critical. Approaches and considerations for assessing the risk of compliance and ethics events are generally very similar to assessing other types of risks. For example, a typical approach would include the following steps:

1. Identify compliance risks that are inherent to the organization's activities
2. Map compliance risks to existing internal controls
3. Assess the effectiveness of internal controls
4. Assess the likelihood and impact of each compliance risk
5. Prioritize (via scoring, heat maps, or other methods) compliance risks based on the assessment
6. Design risk responses (e.g., improvements to internal controls, training) to reduce risk to an acceptable level
7. Assign responsibility and monitor implementation of risk responses

Although these are the core elements of a typical risk assessment, many additional factors can be considered to further enhance the quality of a risk assessment. Risk assessments should be updated periodically, either on a fixed time interval or when relevant new information comes to light indicating a change may have occurred that affects a risk.

Another 2004 addition to the USSG involves an expectation that efforts are made to continuously improve the C&E program. Periodic risk assessment is one method of identifying needed improvements to the program. But there are many other ways of identifying improvements: a thorough root cause analysis at the conclusion of an investigation, feedback mechanisms, auditing and monitoring, and others. Benchmarking against other organizations is also an effective method of assessing program effectiveness. Assessing program effectiveness can be performed internally or by third parties (e.g., consulting firms). Additionally, looking outside the organization — attending conferences, reading publications, and monitoring government guidance — is an excellent way to identify emerging practices that can be adopted to improve a program.

APPENDIX 2.

International Growth in Recognition of and Requirements for Compliance and Ethics Programs

As described in section 1, global recognition of C&E programs has grown considerably in recent years. In this appendix, a few additional examples are provided.

France

Guidance on anticorruption compliance programs from the French Anticorruption Agency (AFA) in conjunction with the 2016 French Sapin II Law was issued in 2017 and then updated in December 2019. The guidance notes that the compliance officer's mission may go beyond anticorruption to include other laws, such as anti-money laundering, antitrust, data privacy and others deemed appropriate for the scope of the program. The following eight expected areas of a program are described in the AFA's guidance:

1. Commitment by top management, including policies and procedures, governance over the program that extends to the highest level of the organization, and communication about the program with employees and external partners
2. A code of conduct
3. An internal whistleblowing system
4. Risk mapping, including risk assessment, prioritization and management
5. Third-party due diligence
6. Accounting controls
7. Risk training for managers and other employees exposed to risks
8. Internal monitoring and assessment

Brazil

Brazil's Clean Companies Act, which took effect in 2014, provides for penalties for the commission of certain acts, including bribery, money-laundering, and fraud in public bidding for contracts, and other offenses. The law required the government to issue a regulation on the act, which it did in the form of a 2015 decree (8.420/15). The decree states that a program will be evaluated for its existence and application, according to the following parameters:

1. Commitment by the top management of the legal entity, including the councils, evidenced by the visible and unequivocal support for the program
2. Standards of conduct, code of ethics, policies, and procedures applicable to all employees and administrators, regardless of their position or function
3. Standards of conduct, code of ethics and policies extended, when necessary, to third parties, such as suppliers, service providers, intermediary agents, and associates
4. Periodic training on the program
5. Periodic risk analysis to make necessary adaptations to the program
6. Accounting records that fully and accurately reflect the transactions of the entity
7. Internal controls that ensure the prompt elaboration and reliability of reports and financial statements of the entity
8. Specific procedures to prevent fraud and illicit activities in the context of bidding processes, in the execution of administrative contracts or in any interaction with the public sector, even if intermediated by third parties, such as payment of taxes, subjection to inspections, or obtaining authorizations, licenses, permits, and certificates
9. Independence, structure, and authority of the internal body responsible for implementing the program and monitoring compliance with it
10. Channels of whistleblowing, open and widely disseminated to employees and third parties, and mechanisms designed to protect whistleblowers
11. Disciplinary measures in case of violation of the program
12. Procedures that ensure the prompt interruption of detected irregularities or infractions and the timely remediation of the damages generated
13. Appropriate procedures for contracting and, as the case may be, supervision of third parties, such as suppliers, service providers, intermediary agents, and associates
14. Verification, during mergers, acquisitions, and corporate restructuring processes, of the commission of irregularities or illicit acts or of the existence of vulnerabilities in the entities involved
15. Continuous monitoring of the program aiming at improving it in preventing, detecting, and combating the occurrence of acts prohibited under the law

16. Transparency of the entity regarding donations to candidates and political parties

The decree states that in evaluating the compliance program, consideration will be given to the unique features of the organization, including the number of employees, number of locations, countries in which it operates, it industry, its complexity, and its use of third parties.

This provision is consistent with U.S. guidance stating that there is no "one size fits all" approach to C&E programs. Every program should be tailored to fit the unique needs of the organization.

Costa Rica

Costa Rica is another Latin American country (along with Argentina, Peru, and Chile in 2018) to recently enact a law addressing compliance programs. The scope of the 2019 Costa Rican law is domestic and international bribery and corruption, as well as falsifying books and records to conceal such corruption. Significant penalties can be reduced if a company has a compliance program in place. Expectations of the C&E program as described in the law include the following:

1. Conduct a risk assessment for the business activity in Costa Rica
2. Implement a code of conduct and adopt specific rules and processes that prevent the commission of crimes
3. Establish specific policies and procedures to prevent crimes relating to public bidding contracts, obtaining licenses, or any other activity related to the public administration
4. Determine the scope of these policies for third parties
5. Establish adequate financial controls and financial records aimed at the prevention of wrongdoing
6. Periodic anti-corruption training, including training for third parties
7. Perform periodic risk assessments and modify the program accordingly
8. Establish a disciplinary model for noncompliance
9. Appoint a compliance officer and provide adequate capacity and resources for the program
10. Conduct an external accounting audit

New Zealand

The Anti-Money Laundering and Countering Financing of Terrorism Act took effect in July 2013. One of the requirements of the act is the appointment of a compliance officer and development of a reporting and compliance program.

The key elements of a compliance program must include the following:

1. A comprehensive risk assessment
2. Vetting and training obligations for managers
3. Reporting procedures
4. Recordkeeping
5. Due diligence
6. Other processes for minimizing the risk of abuses

Singapore

Singapore's Corrupt Practices Investigation Bureau in 2017 published "PACT – A Practical Anti-Corruption Guide for Businesses in Singapore" to assist organization's in complying with The Prevention of Corruption Act. The guide describes the following four steps (thus the acronym, PACT) that companies can take to prevent corruption:

1. **Pledge** — Tone from the top, anti-corruption policies, and a code of conduct
2. **Assess** — Conduct periodic risk assessments
3. **Control and communicate** — Internal controls, audit checks, training and communication, and a robust reporting system
4. **Track** — Evaluate and improve the anti-corruption system

Spain

Amendments to Spain's Criminal Code that took effect on July 1, 2015, provide for the regulation of corporate compliance programs. The amended code provides companies with an exemption from criminal liability for crimes committed by their officers or employees if the company has adopted a compliance program that includes the following six elements:

1. Risk assessment
2. Standards and controls to mitigate any criminal risks detected
3. Financial controls to prevent the crimes
4. Obligation to report to the compliance body any violations of the standards and controls (a whistleblowing channel)
5. Disciplinary system to sanction violations of the compliance program by officers and employees
6. Periodic review of the compliance program, making the necessary adjustments when serious violations occur or when the company undergoes organizational, structural, or economic changes.

Summary

The summary in this appendix is far from complete and is provided only to illustrate some of the similarities and differences among a handful of the many nations that have promulgated some form of requirement or guidance relating to compliance and ethics programs. Organizations should always consult the laws and regulations of each jurisdiction in which they operate for further guidance.

ACKNOWLEDGMENTS

Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA)

corporatecompliance.org

This publication is the product of the SCCE & HCCA Working Group on the Application of ERM to Compliance Risk:

Co-chairs
Urton Anderson, Director and EY Professor, Von Allmen School of Accountancy, University of Kentucky
Gerry Zack, CEO, SCCE & HCCA

Contributing editors
Dan Roach, Chief Compliance Officer, Optum360
Greg Triguba, Principal, Compliance Integrity Solutions, LLC

Contributors
Thanks to the following individuals for their input, feedback, and contributions:

Deborah L. Adleman, Ernst & Young LLP
Joseph Agins, Institutional Compliance Officer, Sam Houston State University
Jeffrey Driver, Faculty, Arizona State University & Principal, Soteria Risk Works
Margaret Hambleton, President, Hambleton Compliance LLC
Samantha Kelen, Chief Ethics and Compliance Officer, Cardinal Innovations Healthcare
Gwendolyn Lee Hassan, Managing Counsel – Global Compliance & Ethics, CNH Industrial
Walter Johnson, Assistant Privacy Officer, Regulatory Compliance, Inova Health System
Caroline McMichen, Principal, McMichen Consulting and former Vice President, Global Ethics and Compliance, Molson Coors (Retired)
Robert Michalski, Chief Compliance Officer, Baylor Scott & White Health
Rebecca Walker, Kaplan & Walker LLP

ABOUT THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS & HEALTH CARE COMPLIANCE ASSOCIATION

The Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA) was founded in 1996 to serve the health care compliance profession and expanded in 2004 to serve the global compliance and ethics community across all industries. With 20,000 members in 100 countries, SCCE & HCCA is the largest association furthering the interests of the profession. Headquartered in Minneapolis, Minn., SCCE & HCCA exists to champion ethical practice and compliance standards and to provide the necessary training, publications, certifications, and other resources for ethics and compliance professionals.

ABOUT COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK

COSO

Committee of Sponsoring Organizations of the Treadway Commission

coso.org