NORTON ROSE FULBRIGHT

COSO's new fraud risk management guidelines

What companies need to know

October 2016

Introduction

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") published its *Internal Control—Integrated Framework*, (the "COSO Framework" or the "Framework"), a set of guidelines designed to assist companies in evaluating the effectiveness of their internal control systems. Since that time, the Framework has gained broad international acceptance and is viewed as a leading template for designing, implementing, and assessing corporate internal controls. In fact, when the SEC adopted rules under Section 404 of the Sarbanes-Oxley Act ("SOX") requiring companies to include in their annual reports a certification by management regarding the effectiveness of their internal controls, it announced that the Framework "satisfies our criteria."[1] Accordingly, both the SEC and shareholder plaintiffs have seized on evidence that management failed to abide by the Framework or made a false certification of compliance with the Framework in SOX-mandated reports. These private suits and administrative enforcement actions have cast in stark relief the importance of management's understanding of, and compliance with, the Framework.

On September 28, 2016, COSO released a standalone Fraud Risk Management Guide. The Guide is intended to supplement the Framework and announce best practices for organizations seeking to assess fraud risks in accordance with Principle 8 of the Framework, which provides that "[t]he organization considers the potential for fraud in assessing risks to the achievement of objectives." Considering the weight accorded to the Framework by the SEC, the courts, and private civil litigants, companies are well advised to familiarize themselves with the Guide and ensure that both their fraud-risk-management practices and their SOX certifications relating to internal controls comport with this new guidance.

The internal control framework

COSO's internal control framework, which the organization revised in 2013, sets forth seventeen principles of internal control associated with five internal control components. For a system of internal control to be effective, according to COSO, each of the seventeen principles must be "present," "functioning," and operating "in an integrated manner."[2] The following table summarizes the internal control components and their corresponding principles:[3]

1 Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 68 Fed. Reg. 36,636, 36,642 (June 18, 2003).

2 Comm. of Sponsoring Orgs. of Treadway Comm'n, *Internal Control—Integrated Framework: Executive Summary 8 (2013)* [hereinafter *COSO Framework: Executive Summary*]. COSO has defined each of these terms: "present" describes "the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives"; "functioning" describes "the determination that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objectives"; and operating "in an integrated manner" describes "the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective." *Id.*

3 *Id.* at 4.

Internal control component	Internal control principles
Control environment	1. The organization demonstrates a commitment to integrity and ethical values.
	2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk assessment	6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
	8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
	9. The organization identifies and assesses changes that could significantly impact the system of internal control.
Control activities	10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	11. The organization selects and develops general control activities over technology to support the achievement of objectives.
	12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Internal control component	Internal control principles
Information and communication	13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
	14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.
Monitoring activities	16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

The Framework also lists three categories of objectives, which enable organizations to focus on different aspects of internal control.[4] Operations objectives "pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss."[5] Reporting objectives "pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies."[6] And compliance objectives "pertain to adherence to laws and regulations to which the entity is subject."[7] As COSO explains, "[a] direct relationship exists between *objectives*, which are what an entity strives to achieve, *components*, which represent what is required to achieve the objectives, and the *organizational structure* of the entity."[8]

SOX Section 404

In Section 404 of SOX, Congress directed the SEC to "prescribe rules requiring each annual report required by section [13(a) or 15(d) of the Exchange Act] to contain an internal control report," which must both: (1) "state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting"; and (2) "contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."[9] The SEC, in turn, promulgated Item 308, which sets forth the requisites of this internal control report,[10] and adopted Rules 13a-15 and 15d-15, which both define "internal control over financial reporting" ("ICFR") and require companies to complete their internal control assessments using "a suitable, recognized control framework that is established by a body or group that has followed due-process procedures."[11] The Commission defined "internal control over financial reporting" as the process designed by, or under the supervision of, the issuer's principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer's board of directors, management and

4 *Id.* at 3.
5 *Id.*
6 *Id.*
7 *Id.*
8 *Id. at 6.*
9 Sarbanes-Oxley Act of 2002 § 404(a), 15 U.S.C. § 7262(a) (2016).
10 17 C.F.R. § 229.308 (2016).
11 *Id. §* 240.13a-15(c), (f); *id. §* 240.15d-15(c), (f).

other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.[12]

As for the "suitable, recognized control framework," the Commission unambiguously endorsed the COSO Framework in the adopting release accompanying Rules 13a and 15d, writing: "The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements."[13] It emphasized, however, that its final rules "do not mandate use of a particular framework,"[14] and it noted in a later release that it "encourage[d] companies to examine and select a framework that may be useful in their own circumstances" and it supported "the further development of existing and alternative frameworks."[15] Nevertheless, in light of the Commission's express approval of the COSO Framework, most public companies specifically disclose that they use the Framework, and both the Commission itself and private litigants have used the Framework as a basis for pursuing claims against companies, certifying officers, accountants, and directors.

SEC enforcement actions

The SEC has brought a number of internal control-related enforcement actions in recent years, based either on inaccurate representations of compliance with the COSO Framework or on evidence that the company's controls in fact failed to satisfy the Framework.

In several cases, the Commission has charged executives under Exchange Act Sections 10(b) and 13(b), and their associated rules, for falsely certifying that they had assessed their companies' internal controls using the COSO Framework. In *Traci J. Anderson*,[16] the SEC instituted cease-and-desist proceedings against a defense contractor and its sole officer and director, contending that the company failed to evaluate its internal controls and falsely certified that its management had evaluated its ICFR in accordance with the COSO Framework.[17] The ALJ found the officer and director liable for violating Exchange Act Rules 13a-14 and 13a-15 in connection with the false certifications.[18] Similarly, in the companion cases *Marc Sherman*[19] and *Edward L. Cummings*,[20] the SEC instituted—and later settled—administrative and cease-and-desist proceedings against two executives of a computer company based on false SOX representations that the company's management had evaluated the company's ICFR using the COSO Framework, when in reality the CEO had not participated in the evaluation and in fact was unfamiliar with the Framework.[21] CEOs and CFOs who do not familiarize themselves with the new Fraud Risk Management Guide could face similar scrutiny after certifying future financial statements.

The Commission obtained a like result in federal court in *SEC v. Kovzan*.[22] There, the Commission brought an enforcement action against a CFO based in part on his false statements concerning internal controls in letters to the company's auditors.[23] The letters stated that they were "provided in connection with the auditors' opinions as to 'whether the Company maintained, in all material respects, effective internal control over financial reporting . . . based on the criteria established in [the COSO Framework].'"[24] The defendant moved to dismiss this claim and argued that, because the COSO Framework "relates in pertinent part to 'financial reporting,' that is, 'the preparation of reliable published financial statements,'" and the company had not made any false assertions in its financial statements, the letters were not false or misleading.[25] The District of Kansas found this argument unpersuasive, reasoning that "[i]t is possible . . . that [the company] did not have effective internal control relating to the preparation of financial statements . . . even if no financial statements were misstated," such that the letters nevertheless

12 *Id.* § 240.13a-15(f); *accord id.* § 240.15d-15(f).
13 Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 68 Fed. Reg. at 36,642.
14 *Id.*
15 Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, 72 Fed. Reg. 35,324, 35,326 n.23 (June 27, 2007).
16 Exchange Act Release No. 74273, 2015 WL 627340 (Feb. 13, 2015)
17 *Id.* at *1, *3–4.
18 SEC Release No. 930, 2015 WL 9297356, at *18 (ALJ Dec. 21, 2015).
19 Exchange Act Release No. 72723 (July 30, 2014).
20 Exchange Act Release No. 72722 (July 30, 2014).
21 See Marc Sherman, Exchange Act Release No. 74765, at 1 (Apr. 20, 2015); Edward L. Cummings, Exchange Act Release No. 72722, at 2.
22 807 F. Supp. 2d 1024 (D. Kan. 2011).
23 *Id.* at 1043.
24 *Id.* at 1044.
25 *Id.*

could have been false.[26] Accordingly, the court denied the motion to dismiss.[27]

The Commission has also used the COSO Framework to prove substantive ICFR deficiencies. Most recently, in *Laurie Bebo*,[28] the Commission instituted cease-and-desist proceedings against the CEO and CFO of a publicly traded assisted-living and senior-residence provider for maintaining inadequate internal accounting controls, among other charges.[29] The SEC's allegations centered on the efforts of the CEO and CFO to hide the company's noncompliance with certain occupancy and financial covenants in a lease to operate several assisted-living facilities.[30] At the administrative hearing, the SEC presented expert testimony on whether the company's ICFR, which encompassed the company's process for performing covenant calculations, comported with the COSO Framework.[31] The ALJ credited the SEC's expert in finding the company's ICFR ineffective to detect the misdeeds of the CEO and CFO, in violation of Exchange Act Section 13(b)(2)(B).[32]

Private securities fraud suits

Likewise, securities fraud suits have proliferated in the years since the SEC sanctioned the COSO Framework in connection with Rules 13a and 15d. As with the SEC actions, these suits generally involve either purportedly false SOX certifications or alleged internal control shortcomings that render SOX certifications or public statements materially false or misleading. The following cases, organized chronologically, provide a cross-section of the typical allegations and the federal courts' treatment of the COSO Framework.

In *Southeastern Pennsylvania Transportation Authority v. Orrstown Financial Services, Inc.*,[33] the Middle District of Pennsylvania granted the plaintiff's motion for leave to amend its securities fraud complaint to include the allegation that, "given the COSO standards that certifying officers are bound to follow, the SOX certifications and other statements in SEC filings regarding internal controls during the relevant reporting periods were false and misleading when made, as they omitted material information regarding the effectiveness of the Company's internal controls over loan underwriting, risk management, and financial reporting."[34] The plaintiff contended that the SOX omissions "demonstrate that Defendants did not properly assess the effectiveness of internal controls, in violation of the 'Internal Control Integrated Framework' issued by the COSO and required by the Sarbanes-Oxley Act."[35] The court held that it was unable to conclude that amendment of the complaint to include these statements and certifications regarding the effectiveness of internal controls would be futile, as "[t]hese statements are arguably the type of information that a reasonable investor would consider significant in making an investment decision."[36]

In *In re Energy Recovery Inc. Securities Litigation*,[37] the Northern District of California granted the defendants' motion to dismiss a securities fraud claim based on alleged misrepresentations regarding the compliance of the company's internal controls with the COSO Framework.[38] The plaintiffs claimed that the internal control certification in the company's Form 10-K was materially false and misleading because the certifying executive (1) "was forcing his subordinates into increasing internal sales projections" and (2) "was 'calibrating' his own sales projections 'all the time.'[39] Although the court rejected the defendant's argument that "the COSO frameworks are not the law," observing that "courts have imposed liability for non-compliance with COSO frameworks," it nevertheless found that the plaintiff had neither identified false or misleading statements nor explained how internal sales projections misled the public.[40]

In *North Port Firefighters' Pension-Local Option Plan v. Fushi Copperweld, Inc.*,[41] the Middle District of Tennessee denied the defendants' motion to dismiss a securities fraud suit alleging misrepresentations regarding internal controls, among other topics.[42] The plaintiffs alleged that Fushi "represented that its internal controls of financial reporting were effective because

of its utilization of [COSO] criteria in Fushi's 'Internal Control–Integrated Framework,'" but, in fact, "Fushi failed to comply with essential components of COSO."[43] Specifically, several executives "falsely stated that internal controls were in place to ensure the reliability of Fushi's financial reporting and that those internal controls were in accordance with COSO standards," and two executives signed SOX certifications despite "kn[o]w[ing] that Fushi's internal controls were inadequate and that Fushi failed to comply with COSO

26 *Id.*
27 *Id.*
28 SEC Release No. 893, 2015 WL 5769700 (ALJ Oct. 2, 2015).
29 *Id.* at *2, *74.
30 *Id.* at *2.
31 *Id.* at *20.
32 *Id.* at *75–76.
33 No. 1:12-cv-00993, 2016 WL 466958 (M.D. Pa. Feb. 8, 2016)
34 *Id.* at *3.
35 *Id.*
36 *Id.*
37 No. 15-cv-00265-EMC, 2016 WL 324150 (N.D. Cal. Jan. 27, 2016).
38 *Id.* at *15.
39 *Id.*
40 *Id.*
41 929 F. Supp. 2d 740 (M.D. Tenn. 2013).
42 *Id.* at 744–45.
43 *Id.* at 759.

requirements."[44] These allegations, the court held, plausibly stated actionable claims under Section 10(b), Rule 10b-5, and Section 20(a) of the Exchange Act.[45]

In *In re Ebix, Inc. Securities Litigation*,[46] the Northern District of Georgia denied the defendants' motion to dismiss a securities fraud suit based on the company's purported misrepresentations regarding the effectiveness of its internal controls.[47] The plaintiffs alleged that the corporate defendants "failed to comply with SEC regulations and the requirements of the [COSO Framework]," in that they 'failed to discover in a timely manner or recklessly disregarded deficiencies in Ebix's internal control' regarding revenues and related accounts receivable in connection with certain acquisitions, and they 'failed to maintain a proper tone and control awareness that focused on achieving consistent application of accounting policies and procedures and strict adherence to GAAP.'[48] The court found these allegations, coupled with specific examples of the company's problems with accounting and billing, sufficient to demonstrate the falsity of the company's statements to investors respecting internal controls, even under the PSLRA's heightened pleading requirements.[49]

Finally, in *In re Bear Stearns Companies, Inc. Securities, Derivative, & ERISA Litigation*,[50] the Southern District of New York denied the defendants' motion to dismiss a securities fraud claim premised on the falsity of the company's SOX certification regarding internal controls.[51] As the complaint alleged: "Management's assessment of internal control over financial reporting was a critical metric for investors because it provided assurance that the Company's financial statements were reliable and in compliance with applicable laws. However, during the Class Period, . . . Bear Stearns did not properly assess its internal controls over financial reporting, thus it violated the 'Internal Control–Integrated Framework' issued by COSO and various other requirements found in the SEC regulations and the Sarbanes–Oxley Act."[52] Taking these allegations as true, the court reasoned, the certification was materially false and misleading, and the complaint could not be dismissed under Rule 12(b)(6).[53]

The new fraud guidelines

COSO released its Fraud Risk Management Guide on September 28, 2016. The Guide is designed not only to supplement the COSO Framework—and in particular Principle 8, which obligates a compliant company to consider fraud in its risk assessments—but also to assist companies in establishing an effective fraud risk management program.[54]

For fraud risk management purposes, fraud is defined broadly to encompass a variety of misdeeds that can directly and indirectly affect a company's financial reporting.[55] First, fraudulent financial reporting itself, which includes inappropriate reporting of revenues and expenses, misleading disclosures, concealment of misappropriated assets, and concealment of unauthorized payments and receipts.[56] Second, fraudulent non-financial reporting, which includes manipulation or falsification of non-financial data, such as environmental, health, or safety records or customer or operational metrics.[57] Third, misappropriation of tangible or intangible assets.[58] And fourth, corruption or violations of consumer- or employee-protection statutes.[59]

The Guide sets forth five fraud risk management principles, each relating to one of the COSO Framework's five internal control components (i.e., Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities) and their corresponding principles.[60] The Guide also provides several targeted "points of focus" for each principle, which highlight important characteristics of that principle.[61] The following table lists the principles and their corresponding points of focus.

44 *Id.* at 759, 761.
45 *Id.* at 790.
46 898 F. Supp. 2d 1325 (N.D. Ga. 2012).
47 *Id.* at 1341–42, 1347–48.
48 *Id.* at 1330–31.
49 *Id.* at 1341–45.
50 763 F. Supp. 2d 423 (S.D.N.Y. 2011).
51 *Id.* at 470, 510.
52 *Id.* at 471.
53 *Id.* at 510.
54 *COSO Fraud Risk Management Guide*, *supra* note 2, at 3–4.
55 *Id.* at 23.
56 *Id.*
57 *Id.* at 24.
58 *Id.* at 25.
59 *Id.* at 25–26.
60 *Id.* at 5–6.
61 *Id.* at 7.
62 *Id.* at 9.

Fraud risk management principle	Points of focus
1. Control environment "The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk."	The board of directors and senior management institute the fraud risk management process by establishing an organizational commitment to deter, prevent, and detect fraud.
	The board of directors and senior management support fraud risk management as a "key element" of corporate governance.
	The board of directors and senior management establish a "comprehensive" fraud risk management policy.
	The board of directors and senior management identify the roles and responsibilities of all personnel with respect to fraud risk governance.
	The board of directors and senior management ensure that the fraud risk management program is fully documented and regularly updated.
	The board of directors and senior management maintain and communicate a continuous focus on fraud risk management throughout the organization[69].

Fraud risk management principle	Points of focus
2. Risk assessment "The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks."	The fraud risk assessment team includes appropriate levels of management
	The fraud risk assessment team is attuned to the entity, subsidiary, division, operating unit, and functional levels
	The fraud risk assessment team analyzes both internal and external factors and their effect on objectives
	The fraud risk assessment team considers various types of fraud
	The fraud risk assessment team specifically considers the risk of management overriding existing and otherwise effective controls
	The fraud risk assessment team evaluates the likelihood and significance of identified risks
	The fraud risk assessment team analyzes the personnel or departments involved in fraud and addresses all aspects of the "fraud triangle" (i.e., incentives and pressures, opportunities, and attitudes and rationalizations to commit fraud)
	The fraud risk assessment team identifies and evaluates existing controls for effectiveness
	The fraud risk management team's "ultimate goal" is to devise effective responses to all fraud risks
	The organization uses data analytics in its fraud risk assessments and responses
	The organization performs periodic reassessments that take into account changes affecting the organization, including changes in the external environment, operations, personnel, and leadership
	The organization carefully and thoroughly documents the fraud risk management process

Fraud risk management principle	Points of focus
3. Control activities "The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner."	The organization promotes fraud deterrence through preventive and detective control activities
	The organization ensures that the design and implementation of fraud control activities integrate with its fraud risk assessment
	The organization considers organization-specific factors and business processes in designing its fraud control activities
	The organization extends the application of control activities to all appropriate levels of the organization
	The organization uses a combination of preventive and detective fraud control activities
	The organization includes fraud control activities that take into account the possibility that senior management may circumvent or override fraud controls
	The organization uses data analytics in its fraud control systems
	The organization confirms that its fraud control activities are documented and implemented in organizational policies and procedures[73]
4. Information and communication "The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner."	The organization establishes, documents, and maintains a process for receiving, evaluating, and treating communications relating to potential fraud
	The organization conducts investigations into potential fraud, taking into account the scope, severity, plausibility, and implications of the reported matter
	The investigation team communicates the results of its investigation to the appropriate internal authority and, where necessary, to external third parties
	The organization takes appropriate corrective action upon discovering fraud, including discipline, remediation, asset recovery, training, civil action, and/or criminal referral
	The organization periodically evaluates its investigative performance

Fraud risk management principle	Points of focus
5. Monitoring activities "The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors."	Management includes a mix of ongoing and separate fraud risk management program monitoring evaluations to assess whether each of the five principles of fraud risk management is present and functioning effectively
	Management considers relevant factors in setting the scope and frequency of evaluations (e.g., changes in the organization, its operating environment, and its control structure)
	Management establishes appropriate measurement criteria to evaluate its fraud risk management program
	Management considers both known fraud schemes and novel frauds occurring in other organizations to assess the likelihood of recurrence or occurrence in the organization
	Management and the board of directors evaluate the results of fraud risk management program monitoring evaluations, communicate deficiencies to those tasked with corrective action, and ensure that appropriate remediation is implemented promptly

COSO recognizes that organizations implementing the Internal Control Framework can use the Fraud Risk Management Guide in one of two ways.[63] First, an organization can use the Guide's second fraud risk management principle (i.e., the risk assessment principle) "on a stand-alone basis" to perform a fraud risk assessment that complies with Principle 8.[64] "Under this approach," COSO writes, "an organization would overlay the fraud risk assessment process on its existing internal control structure by revisiting each component of internal control and addressing vulnerabilities to fraud."[65] Second, an organization can implement the Guide "as a separate, compatible, and more comprehensive process for specifically assessing the organization's fraud risk as part of a broader fraud risk management program or process."[66] Unlike the first option, this approach calls for an organization to assess fraud risk *in addition to* implementing fraud risk governance structures, fraud control activities, fraud investigations and corrective actions, and fraud risk evaluation and monitoring.[67]

COSO recommends the second approach, explaining that it "results in an ongoing, comprehensive fraud risk management process."[68] Further, the Guide observes, "[t]he second approach recognizes and emphasizes the fundamental difference between internal control weaknesses resulting in *errors* and weaknesses resulting in *fraud*"—namely, *intent*.[69] An organization that merely adds the fraud risk assessment to its existing internal control assessment "may not thoroughly examine and identify possibilities for intentional acts" designed to misstate financial or non-financial information, misappropriate assets, or perpetrate illegal acts.[70] In COSO's view, the second approach "provides greater assurance that the assessment's focus remains on intentional acts."[71]

63 *Id.* at 3.
64 *Id.*
65 *Id.*
66 *Id.*
67 *Id.*
68 *Id.* at 3–4. COSO visualizes this process as a cycle containing the following steps: (1) establish a fraud risk management policy as part of organizational governance; (2) perform a comprehensive fraud risk assessment; (3) select, develop, and deploy preventive and detective fraud control activities; (4) establish a fraud reporting process and coordinated approach to investigation and corrective action; and (5) monitor the fraud risk management process, report results, and improve the process. *Id.* at 4.
69 *Id.*
70 *Id.*
71 *Id.*

The following table illustrates the relationship between the Internal Control Framework and the Fraud Risk Management Guide:

Internal Control Component	Internal Control Principles	Fraud Risk Management Principles
Control Environment	1. The organization demonstrates a commitment to integrity and ethical values.	1. The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.
	2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
	3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
	4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
	5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
Risk Assessment	6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
	7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
	8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.	
	9. The organization identifies and assesses changes that could significantly impact the system of internal control.	

Internal Control Component	Internal Control Principles	Fraud Risk Management Principles
Control Activities	10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
	11. The organization selects and develops general control activities over technology to support the achievement of objectives.	
	12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	
Information & Communication	13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.	4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.
	14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
	15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.	
Monitoring Activities	16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.
	17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	

As the Guide bears the approval of all major self-regulatory bodies and was circulated broadly among various interest groups for public comment prior to publication, it is likely to meet the definition of an approved framework in Rules 13a-15 and 15d-15. And, in turn, the Guide is likely to become a standard for regulators and a target for shareholder plaintiffs. Companies therefore would be prudent to carefully study the Guide.

Lessons for Companies

As the SEC enforcement actions and private lawsuits described above demonstrate, COSO's guidance can serve both as a substantive standard governing the effectiveness of internal controls and as a basis for securities fraud liability when invoked injudiciously in public statements and filings. Given the strong probability that the Fraud Risk Management Guide will assume the same prominence as the Internal Control Framework, it is reasonable to anticipate regulatory and civil actions based on internal control failures relating to fraud. Although the Guide supplies more detailed guidance for companies seeking to mitigate the risks of fraud and resulting internal control-directed litigation, companies can draw several lessons from the actions rooted in the COSO Framework.

First, companies and executives should promptly familiarize themselves with the new fraud risk management principles and re-evaluate each of their internal control components with this guidance in mind. Once the principles become the industry standard, any deficiencies discovered later can create a risk of liability.

Second, executives completing SOX certifications should ensure that their review processes incorporate the new fraud risk management principles. Otherwise, they may be liable for making a false certification—either because the certification falsely represents that the company adhered to COSO's guidance in its assessment or because the certification does not accurately reflect a finding of compliance under COSO's standards.

Third, an executive should not cite the Guide in a public statement or filing unless he or she is knowledgeable about its contents and believes, in good faith and with a sound factual basis, that the company's internal controls satisfy COSO's principles.

Fourth, if is not feasible for a company to use the Fraud Risk Management Guide as COSO recommends (i.e., as "a separate, compatible, and more comprehensive process" for assessing fraud risk as part of a broader fraud risk management program), the company should nevertheless use the Guide on a standalone basis to conduct a Principal 8-compliant fraud risk assessment. Moving forward, it is not unreasonable to anticipate regulators and shareholder plaintiffs averring that a company's failure to conform its fraud risk assessments to the standards set forth in the Guide has led the company afoul of Principle 8.

Finally, companies and executives should adopt a broad view of fraud risks when completing their internal control assessments, taking into account risks and controls relating to fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets, corruption, and regulatory noncompliance.

Norton Rose Fulbright has extensive experience counseling clients in all industries on risk management and internal controls. As the only law firm represented on the COSO Task Force responsible for drafting the Fraud Risk Management Guide, Norton Rose Fulbright has a unique insight into COSO's process and priorities, as well as a deep understanding of the interplay between the Framework and the Guide.

NORTON ROSE FULBRIGHT

Key contacts

Gerry Pecht
Global Head of Dispute Resolution and Litigation
Tel +1 713 651 5243
gerard.pecht@nortonrosefulbright.com

Mark Oakes
Partner
Tel +1 512 536 5221
mark.oakes@nortonrosefulbright.com

Peter Stokes
Partner
Tel +1 512 536 5287
peter.stokes@nortonrosefulbright.com

Ryan Meltzer
Associate
Tel +1 512 536 5234
ryan.meltzer@nortonrosefulbright.com

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.