Heads Up | Volume 30, Issue 5
April 21, 2023

In This Issue

#DeloitteESGNow — Using the COSO Framework to Establish Internal Controls Over Sustainability Reporting (ICSR)

Overview

In a market in which entities are expected to provide an increasing number of disclosures about environmental, social, and governance (ESG) matters,[1] organizational governance and internal controls are top of mind. On March 30, 2023, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a landmark interpretive report[2] on how the COSO *Internal Control — Integrated Framework* (the "COSO Framework") can apply to sustainable business activities and information. The report illuminates how the COSO Framework's 5 components and 17 principles can help companies establish an effective and integrated system of internal control over their material or decision-useful sustainable business information.

[1] According to Deloitte's December 2022 Sustainability Action Report, 89 percent of executives have reported proactively making strides to drive trust with stakeholders by holding themselves accountable.

[2] COSO Report, *Achieving Effective Internal Control Over Sustainability Reporting (ICSR): Building Trust and Confidence Through the COSO* Internal Control — Integrated Framework.

How Companies Can Use COSO's ICSR Report

The report serves as a **resource for companies** working toward more complete and accurate sourcing, measurement, compilation, review, and disclosure of ESG information. It considers the more **varied, qualitative, forward-looking, and multidisciplinary nature of sustainable business data** to support practical applications of the COSO Framework to sustainability reporting. Because input is often required from professionals of diverse backgrounds at all levels of an organization, COSO's report serves as a **valuable tool for facilitating interdisciplinary cooperation**[3] as stakeholders' demands for high-quality, trustworthy, and transparent ESG information continue to rise.

Most recently refreshed in 2013, the COSO Framework (ICIF-2013) is the "generally accepted" framework for compliance with the Sarbanes-Oxley Act of 2002 in the United States as well as for similar internal control requirements internationally. The COSO Framework is fundamental to high-quality disclosure that promotes efficient functioning and reliability of the capital markets. While the 2013 revision expanded the COSO Framework to include all forms of reporting (e.g., internal, external, financial, and sustainability), this 2023 ICSR report comes at a timely moment when ESG and climate-related disclosure requirements and regulations are accelerating. The SEC's proposed climate-related disclosure rule[4] and the recent adoption of the E.U. Corporate Sustainability Reporting Directive (CSRD)[5] serve as two recent examples. Deloitte's December 2022 Sustainability Action Report findings highlight that while nearly all companies (99 percent) are considering investment in new technologies and a majority (81 percent) of executives continue to create new roles and responsibilities to accommodate additional disclosure requirements, it is paramount that organizations take the right steps to prepare. Companies can start working to develop not only scalable and cross-functional governance and accountability structures related to their sustainable business information, but also robust policies and procedures; business process and information technology (IT) controls; and risk assessment, mitigation, and monitoring practices that reliably address the rapid pace of change.

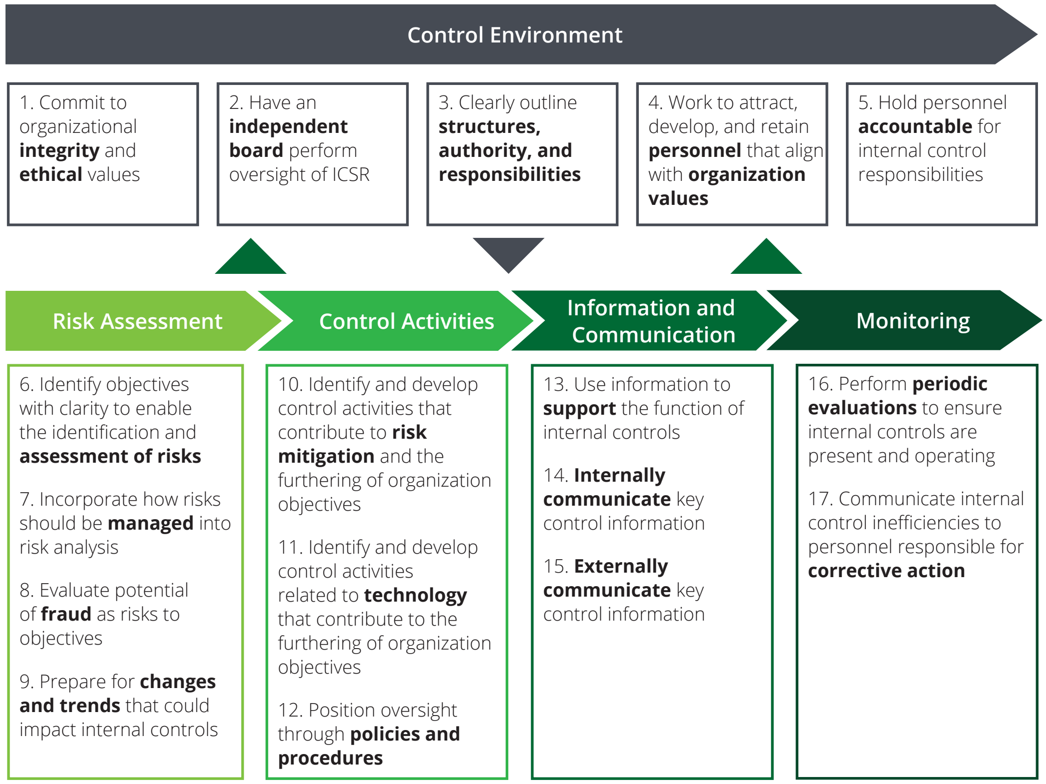
Key Takeaways

The time to act is now. COSO's report provides evidence that companies can consider in designing and implementing ICSR that are similar to internal controls over financial reporting. The COSO Framework is intended to be leveraged at the entity, division, operating unit, and functional levels. Companies can begin customizing and adapting their governance structures and system of internal control to meet their unique sustainable business reporting objectives as well as their stakeholders' growing expectations. The report indicates that much like financial reporting, sustainability and ESG reporting is not intended to be an "annual and manual" activity but instead needs to be thoroughly integrated into a business's strategy and operational practices.

Applying the Five COSO Components to Sustainable Business Information

The COSO Framework consists of five components (encompassing 17 principles) that are interrelated with operational, reporting, and compliance objectives throughout an organization. When all principles are present and functioning, an effective system of internal control is achieved. COSO's comprehensive application of ICIF-2013 to sustainable business information is summarized below with respect to the five components.

[3] See COSO's report for further details.
[4] See Deloitte's March 29, 2022, *Heads Up* for more information about the SEC's proposed rule on climate disclosure requirements.
[5] See Deloitte's January 9, 2023, *Heads Up* for more information about the CSRD.



1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring Activities

Component 1 — Control Environment

An organization's control environment is important to a sustainable infrastructure that supports effective ICSR. A strong "tone at the top" establishes expectations and helps companies form the necessary governance and accountability structures to achieve sustainability reporting objectives. To be successful, an organization's control environment needs to have clearly established standards of conduct that help it achieve its mission and objectives at all levels. Practices that emphasize integrity and ethical values as well as investment in human resource development and retention — and that hold employees accountable when communicated policies, roles, responsibilities, and expectations are not adhered to — can all aid in maintaining effective ICSR.

Principle	ICIF-2013 Description	COSO's Sustainability Application
1. Demonstrates commitment to integrity and ethical values	The organization demonstrates a commitment to integrity and ethical values.	An organization furthers its objectives by demonstrating to its stakeholders that it is trustworthy and acts in the public interest. An entity demonstrates its **commitment to acting sustainably**.

(Table continued)

Principle	ICIF-2013 Description	COSO's Sustainability Application
2. Exercises board of directors' oversight responsibilities	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Oversight by an independent board of directors serves as a **check that management is acting in accordance with the organization's sustainable business objectives**.
3. Establishes structures, authority, and responsibilities	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	As it endeavors to meet its sustainable business objectives, an organization's management, with the oversight of the board of directors, establishes **internal structures that set out authority and responsibilities**.
4. Demonstrates commitment to competent human resources	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	To meet its sustainable business objectives, an organization depends on its **human resources**.
5. Enforces accountability	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	To meet its sustainable business objectives, an organization needs to **establish and implement meaningful ways to support its human resources and**, at the same time, **monitor performance**.

Connecting the Dots

Governance is a central component of the COSO Framework. Executives are already reporting rapid changes in governance structures and promoting further alignment with strategic priorities. From March 2022 to December 2022 alone, progress on establishing cross-functional working groups — made up of executives (e.g., finance, accounting, risk, legal, sustainability) and other business leaders to drive strategic attention to ESG for the business — nearly tripled from 21 percent to 57 percent (according to Deloitte's December 2022 Sustainability Action Report). To continue this progress, companies can take steps to:

- **Align organizational purpose** with sustainability commitments and objectives, develop oversight **structures and standards** associated with that purpose, and consider leveraging the Three Lines Model of the Institute of Internal Auditors when defining governance structures.
- Consider **change management** practices and the necessary commitments that must be made to ESG investment, oversight, action, and ongoing improvement by the board, management, and broader organization.
- Prioritize **human resources** who not only share company values but also possess the necessary skills to advance strategic ESG objectives.
- Provide ongoing and **meaningful support to and investment in** those human resources through **training and development**, performance **incentives and rewards**, and succession planning.
- Clearly **define and communicate expectations** and find ways to **maintain accountability** and **evaluate performance**.
- Establish or expand **cross-disciplinary teaming** (i.e., involve and upskill personnel throughout accounting, internal audit, legal, human resources, communications, investor relations, and operations) and cross-business representation to contribute **diverse perspectives** and insights to

sustainability matters to more effectively translate risk and opportunity prioritization in the context of market trends, requirements, and conditions; hold the appropriate stakeholders throughout the organization accountable; and promote consistent data collection practices, controls, and reporting infrastructure.

Component 2 — Risk Assessment

Organizations today are familiar with risk assessment activities, particularly those related to financial reporting processes. Incorporating ESG-related risks into an existing enterprise risk management (ERM) framework is becoming increasingly common. In 2018, COSO released a publication[6] to provide guidance on expanding or creating ERM frameworks that include ESG considerations. The COSO ICIF and ERM frameworks offer complementary benefits — the ERM framework helps entities develop and apply their ERM activities (e.g., assessing risk appetite and tolerance), while the COSO report indicates that ICIF-2013 offers "the means for carrying out objectives throughout an organization" and "is an integral yet narrower part" of ERM. A robust risk assessment process for ESG information includes, but is not limited to, sustainable business objective setting and materiality considerations, cross-functional collaboration, management involvement, and assessing incentives and pressures for fraud.

Principle	ICIF-2013 Description	COSO's Sustainability Application
6. Specifies suitable objectives	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks related to objectives.	With clarity, an organization expresses its sustainable business objectives. These objectives are a means to tie the organization's purpose or mission, values, and sustainability goals to strategy. An **organization's sustainable business objectives follow from its commitment to integrity and ethical values and are integrally linked to** its **operations** objectives, **external financial reporting** objectives, **external nonfinancial reporting** objectives, **internal reporting** objectives, and **compliance objectives**. Explicit expression of these objectives is a predicate to considering risks (i.e., the likelihood that events will occur that may be detrimental to the organization's ability to satisfy them).
7. Identifies and analyzes risks to meeting sustainable business objectives	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.	To meet its sustainable business objectives, an organization needs to establish and implement **meaningful ways to support its human resources** and, at the same time, **monitor performance**.
8. Assesses fraud risk	The organization considers the potential for fraud in assessing risks to the achievement of objectives.	In identifying and assessing the risks to achieving its sustainable business objectives and developing an effective response, an organization **considers the risk that actors**[7] **will engage in fraudulent activities** such as intentional misstatements or misappropriation of valuable resources.

[6] *Enterprise Risk Management — Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks.*
[7] Actors may include the employees, human resources, and process performers within an organization.

(Table continued)

Principle	ICIF-2013 Description	COSO's Sustainability Application
9. Identifies and analyzes significant changes and emerging trends	The organization identifies and assesses changes that could significantly affect the system of internal control.	As part of identifying and assessing risks to the achievement of its sustainable business objectives, **an organization considers emerging trends**. **Sustainability-related risks are evaluated in an ongoing manner or periodically** to respond to regulatory trends and economic drivers.

Connecting the Dots

The risk assessment process is imperative to staying focused on what matters. As we have seen with the CSRD, performance of an **ESG materiality assessment**[8] remains an important first step to narrowing focus and can inform future risk assessments. Though often segregated, ESG risk and more traditional risk assessment procedures (e.g., ERM) are inherently linked to an organization's strategic, financial, business, and operational risks. Risk-related issues that companies should consider in these situations include whether any reputational risks arise from environmental and social inaction, what financial risks extreme weather and climate events pose to company assets, and the regulatory risks of noncompliance with upcoming sustainability reporting standards. Ways companies can expand and integrate ESG risks into their existing ERM processes include:

- Defining **sustainable business objectives** (e.g., establishing greenhouse gas reduction targets) and determining the level of **risk tolerance** management is willing to accept if objectives are not met.
- **Identifying risks** related to the achievement of objectives and **assessing the significance of each risk**, considering all operating units and functional levels of the organization (e.g., lack of knowledgeable personnel that can quantify and report greenhouse gas emissions).
- Considering potential risks of **fraud** and assessing related incentives and pressures (e.g., omission or underreporting of greenhouse gas emissions by specialists or management to meet reduction targets or receive ESG-linked compensation).
- Factoring in **emerging trends** and how they could affect the system of internal control (e.g., adapting the business strategy, changing leadership, redefining the accountability structure).
- Determining how to appropriately **adapt and respond to the risk** whether through acceptance, avoidance, reduction, or risk sharing (e.g., accepting and choosing to invest in hiring or upskilling greenhouse gas reduction and reporting specialists).

Component 3 — Control Activities

Once risks are identified and understood, risk mitigation is key. Tailored, documented, and tested business processes and IT control activities applied at the appropriate level can help organizations develop the necessary layers of oversight to meet business objectives. With respect to sustainability information, clear roles and responsibilities need to be established for process owners through well-defined and regularly updated policies and procedures. When

8 An ESG materiality assessment is a process in which companies engage with key stakeholders to understand ESG priorities and align with the business strategy and leading measurement and reporting standards. See Deloitte's May 26, 2022, *Heads Up* for more information about ESG materiality considerations.

possible, management may seek opportunities to automate and digitize processes to promote consistency, standardization, and development of an audit trail. A well-maintained technology infrastructure that accommodates the unique needs of sustainable business data can support the completeness, accuracy, and integrity of such data.

Principle	ICIF-2013 Description	COSO's Sustainability Application
10. Selects and develops control activities	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Once an organization has identified and assessed risks to achieving its sustainable business objectives, **it designs, develops, and implements means to counter these risks, partly or completely**. This helps ensure that oversight activities are responsive to sustainable business objectives, including reporting and related risks.
11. Selects and develops general controls over technology	The organization selects and develops general control activities related to technology to support the achievement of objectives.	An organization **designs its control activities to respond to risks** to achieving its sustainable business objectives. In doing so, it **considers the extent to which it will rely on technology**. This includes leveraging existing IT systems to the collection, processing, reporting, and security of sustainable business information, such as greenhouse gas emissions, energy usage, water usage, waste management, supply chain management, and diversity.
12. Deploys oversight through policies and procedures	The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	An organization uses **various means of oversight** to direct its sustainable business objectives. **Primary among these means is established policies and procedures**. These policies and procedures promote clarity in how the organization will meet its sustainable business objectives.

Connecting the Dots

Control activities related to sustainability reporting are akin to traditional financial reporting control activities and processes and can be integrated with them to support internal decision-making. As ESG governance is formalized, procedures are established, roles are defined, and systems that can make reporting automated, efficient, and continuous are identified, businesses should:

- Keep in mind **operations and compliance objectives**, the resulting risks created, and the activities required to achieve effective internal control in these areas.
- Consider defined materiality while undergoing a **readiness assessment** to identify available information, evaluate and document ESG business process controls (e.g., flowcharts, standard operating procedures, and risk and control matrices), and establish a basis for assurance (see the Center for Audit Quality's March 2021 report[9]).
- Prioritize **IT and security considerations** to include controls over infrastructure; centralized and decentralized data and security management;

[9] *The Role of Auditors in Company-Prepared ESG Information: A Deeper Dive on Assurance.*

technology acquisition, development, and maintenance; and the availability of competent professionals to intervene if system controls are not designed or functioning as intended.

- Assess whether (1) control activities are **applied at the right level**, are sufficiently **aligned with the outcome of risk assessment**, and support **data completeness and accuracy** and (2) **internal checks and balances** (e.g., segregation of duties) are in place. If third-party service organizations are relied upon for sustainability data and information, companies should consider evaluating their qualifications and certifications.

Component 4 — Information and Communication

The main purpose of information and communication systems is to measure, collect, and report informative, timely, and high-quality data. An effective system of internal control preserves the reliability and integrity of information as it flows through various processes from source to decision makers who are both internal and external to the organization.

Principle	ICIF-2013 Description	COSO's Sustainability Application
13. Uses relevant information	The organization obtains or generates and uses relevant, high-quality information to support the functioning of internal control.	An organization needs **high-quality data indicating whether its processes are facilitating its ability to meet its sustainable business objectives**.
14. Communicates internally	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Once an organization establishes oversight structures and expresses policies and procedures, it **communicates these structures and policies throughout the organization**. This communication **facilitates the understanding of all actors regarding their responsibilities** for meeting the organization's sustainable business objectives.
15. Communicates externally	The organization communicates with external parties regarding matters affecting the functioning of internal control.	Once an organization establishes oversight structures and expresses policies and procedures, it **communicates these structures and processes to external parties**, such as debt and equity investors and other stakeholders, **that are relying on these processes** for the delivery of reliable sustainable business information.

Connecting the Dots

Information and communication systems (both automated and manual) should effectively collect, measure, and present ESG-related information in a manner that is understandable to process owners, relevant to external users, and supportive of effective ICSR. At a time when "35% of executives reported that their greatest [ESG] challenge is the accuracy and completeness of data, and another 25% cited access to quality data as the greatest challenge," information management and communication processes help uphold proper implementation of controls and disclosure of high-quality ESG data. Companies should:

- Prioritize preparation and maintenance of ESG-related information and **evaluate whether communication methods, internally and externally**, are **relevant** to objectives.

- Promote **timely** collection and dissemination of data; support an effective **flow of information**; and emphasize **data integrity**, end-to-end **completeness, and accuracy** (e.g., whether existing procedures provide clear direction to ESG data process owners and stakeholders; whether information systems enable establishment of effective and evidenced review over data quality; whether the controls within the systems are designed, implemented, and operating effectively; how necessary data are summarized for the board).
- **Consider risks posed by communications** by assessing whether external parties can rely on the information today and looking forward (e.g., whether sustainability commitments are reliable, whether information in press releases about ESG can be validated).

Component 5 — Monitoring Activities

Monitoring activities underpin the maintenance of present and functioning ICSR. Implementing ongoing and/or separate evaluations by competent personnel to detect and remediate internal control deficiencies will demonstrate a commitment to transparency and accountability. Proper communication of assessment results, including identified deficiencies, facilitates the alignment or realignment of activities in accordance with the organization's sustainable business objectives.

Principle	ICIF-2013 Description	COSO's Sustainability Application
16. Conducts ongoing and/or separate evaluations	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Once implemented, an organization **revisits its oversight structures and processes to ensure that they are effective** in facilitating its ability to meet its sustainable business objectives. These reassessments may be scheduled and ongoing, or they may be performed as specific needs arise.
17. Evaluates and communicates deficiencies	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 an organization reassesses its structures, policies, and procedures related to its sustainable business activities, it **communicates its findings so that actors better align their activities** with the organization's sustainable business objectives.

Connecting the Dots

The aim of developing, integrating, and prioritizing ICSR is to deliver complete, accurate, and reliable data to stakeholders in an environment in which sustainability information is increasingly critical to decision-making. Governance is the foundation, and readiness will rely on the following:

- **Ongoing evaluation and improvement** — Organizations should continually assess the effectiveness of their governance structure and control activities and should invest in knowledge and skills development through ESG-related training and development so that **deficiencies** can be properly **addressed and remedial actions** appropriately **deployed**.
- **Cross-functional collaboration** — Companies will need to communicate with and **facilitate interaction** between relevant stakeholders — at all levels and disciplines — to **continually align** activities with sustainability objectives and implement remedial actions.

- **Internal audit and external assurance** — When possible, organizations should involve the internal audit function, or a similar compliance function, in control monitoring activities and should use insights raised by external auditors and stakeholders. Obtaining both internal and external ESG assurance will help **instill the necessary discipline and internal infrastructure** to manage risk and drive value through sustainability.

Next Steps

Deloitte's December 2022 Sustainability Action Report states that almost all (96 percent) of executives indicated that their organization plans "to seek external assurance for the next reporting cycle." Of these, 61 percent are "already seeking external assurance" and 35 percent are "seeking external assurance for the first time." However, only one in three executives (37 percent) say their companies are starting to apply the COSO Framework to their sustainability reporting process and have begun to identify a path toward a reasonable level of assurance. Just over one in ten (12 percent) said they have not started to evaluate the steps within their own company. As COSO's report supports, the time has come for organizations to establish or enhance ICSR. Consider the following next steps and prepare by using ICIF-2013 for ESG starting today.

1	**Governance is foundational.** Encourage cross functionality. Bring together relevant stakeholders across departments (e.g., internal audit, communications and IT alongside ESG) to delegate responsibilities, create an implementation roadmap, and prepare for upcoming regulation, assurance, and reporting demands.
2	**Prioritize ICSR** by incorporating ESG risks and opportunities into your existing risk management processes to appropriately identify areas where control activities are needed. Design processes, internal controls, and governance structures which support complete, accurate, and reliable data measurement and disclosure. Internal evaluation of controls is a necessary first step prior to engaging in external assurance.
3	**Risk assessment and determining materiality** are key activities to focus on what matters. Consider conducting or refreshing your ESG materiality assessment to identify overlap between your sustainability, climate, and ESG-related risks and enterprise risks and impacts.

Other Resources

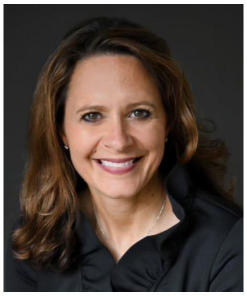
Deloitte resources such as the following may help companies as they implement ICSR and prepare for required climate disclosures:

- *Heads Up — #DeloitteESGNow — Global Reach of the E.U. Corporate Sustainability Reporting Directive and the Impact on U.S. Companies*
- *Heads Up — #DeloitteESGNow — Setting the Standard: When ESG and Climate Reporting Meet Financial Reporting*
- *Heads Up — #DeloitteESGNow — The Disclosure Heat Is On: The Move Toward International Standardization of Sustainability and Climate Reporting*
- *Heads Up — Comprehensive Analysis of the SEC's Proposed Rule on Climate Disclosure Requirements*
- *Heads Up — #DeloitteESGnow — Enhancing Trust in ESG Disclosures*

- *Defining the Role of the Audit Committee in Overseeing ESG*
- *Financial Reporting Alert — Financial Reporting Considerations Related to Environmental Events and Activities*

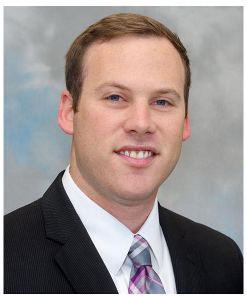
Contacts

For information about Deloitte's service offerings related to ESG matters, please contact:



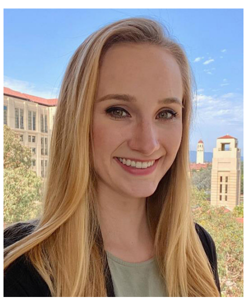
Kristen Sullivan
Partner
Deloitte & Touche LLP
+1 203 708 4593
ksullivan@deloitte.com

Kajal Shah
Partner
Deloitte & Touche LLP
+1 408 857 6186
kajshah@deloitte.com



Stefan Ozer
Partner
Deloitte & Touche LLP
+1 763 670 7797
sozer@deloitte.com

Meadow Rutenbar
Senior Manager
Deloitte & Touche LLP
+1 215 341 8731
mrutenbar@deloitte.com



Sarah Husted
Senior
Deloitte & Touche LLP
+1 240 538 5079
shusted@deloitte.com

Elise Hess
Senior
Deloitte & Touche LLP
+1 248 766 4319
elhess@deloitte.com

Dbriefs for Financial Executives

We invite you to participate in Dbriefs, Deloitte's live webcasts that give you valuable insights into important developments affecting your business. Topics covered in the Dbriefs for Financial Executives series include financial reporting, tax accounting, business strategy, governance, and risk. Dbriefs also provide a convenient and flexible way to earn CPE credit — right at your desk.

Subscriptions

To subscribe to Dbriefs, or to receive accounting publications issued by Deloitte's Accounting and Reporting Services Department, please register at My.Deloitte.com.

The Deloitte Accounting Research Tool

Put a wealth of information at your fingertips. The Deloitte Accounting Research Tool (DART) is a comprehensive online library of accounting and financial disclosure literature. It contains material from the FASB, EITF, AICPA, PCAOB, and SEC, in addition to Deloitte's own accounting manuals and other interpretive guidance and publications.

Updated every business day, DART has an intuitive design and navigation system that, together with its powerful search and personalization features, enable users to quickly locate information anytime, from any device and any browser. While much of the content on DART is available at no cost, subscribers have access to premium content, such as Deloitte's *FASB Accounting Standards Codification Manual*. DART subscribers and others can also subscribe to *Weekly Accounting Roundup*, which provides links to recent news articles, publications, and other additions to DART. For more information, or to sign up for a free 30-day trial of premium DART content, visit dart.deloitte.com.