INTEGRATED THINKING AND SUSTAINABILITY

Applying Key Governance Tools and Frameworks

COSO

The Institute of Internal Auditors

Contents

Purpose

Organizations of all sizes and from all sectors are experiencing growing pressure to demonstrate how they manage sustainability risks and opportunities and report them publicly.

Demands from internal and external stakeholders for organizations to consider the impacts of a wide array of issues, such as climate change, intangible drivers of enterprise value, diversity, and social justice, are redefining value creation and organizational success. Increasingly, the spotlight is focusing on the critical step that comes before the issuance of a report — the alignment of how organizations are managing risk, with how they are reporting risk. This has made the concepts of integrated thinking and integrated reporting increasingly more relevant, particularly as organizations strive to succeed in an ethical and transparent way. An important part of organizational success is holistically understanding and effectively managing risk and working with internal audit to incorporate objective and independent assurance and advice on the efficacy of risk management processes and controls.

The focus of this paper is to show how integrated thinking and reporting, effective internal control, enterprise risk management (ERM), and independent assurance provided by internal audit functions align to help organizations achieve their objectives and meet stakeholder expectations. It is critical to long-term value creation to apply ERM broadly, including to environmental, social, and governance (ESG)-related risks, to understand their impacts and interdependencies throughout the value creation process, and to embrace the value of independent assurance.

The paper's objectives are to:

- Increase understanding and awareness of integrated thinking and reporting.
- Demonstrate parallels among the COSO frameworks (Internal Control and ERM), The Institute of Internal Auditors' (IIA's) Three Lines Model, and the International Integrated Reporting Framework, in terms of:
    - Informing the content, preparation, and presentation of an integrated report.
    - Reinforcing the role internal audit plays in ensuring the integrity of information underpinning integrated thinking and reporting by providing independent assurance over that information.
    - Helping organizations embed integrated thinking into their approach to ERM.

A useful matrix reflecting those parallels is included in the section titled "Integrated Thinking Matrix" on page 19.

Introduction

Most organizations focus on internal operations and finances for the purpose of planning and decision-making. This focus is typically reflected in the organizational reporting on which investors, taxpayers, regulators, and other stakeholders rely. Increasingly, however, organizations recognize they have broader value, wider impacts, and greater interdependencies than reported in customary financial statements.

Defining Sustainability

For the purposes of this paper, sustainability should be understood to mean the ability to provide value that sustains the organization and the context within which it exists. This incorporates the historical focus on profit with acknowledgement, understanding, and accountability for the organization's impact on people and the planet.

There is growing understanding that many of the diverse resources that feed organizations are finite, and that sustainability matters are inextricably linked to performance over time. While an organization can consume resources to turn a profit, it may simultaneously deplete overall value when the wider impacts on people, society, and the environment are considered. This is because organizations are interconnected, joined by overlapping value chains and shared, limited resources. They have stakeholders in common who want success, but not at any price. Stakeholders expect results to be achieved efficiently, effectively, ethically, and sustainably. Organizations' interests lie not just in outcomes and impacts, but also in the decisions, actions, and behaviors adopted to achieve them.

In other words, financial success is not the only measure by which to understand performance, position, and potential. Value must be defined and recognized in ways other than purely financial terms. Accordingly, increasing attention is being paid to improving external reporting so that it accurately communicates long-term views of performance and the interconnectedness of both financial and nonfinancial elements. These more fulsome representations address matters that haven't been adequately captured by traditional reporting models. Often reflected in sustainability or ESG reporting, they consider the organization's impact not just on its own resources, but also on resources held by others and those held in common.

This acknowledgment of value being driven by measures beyond the bottom line is clearly articulated in the International Integrated Reporting Framework (Integrated Reporting Framework), which facilitates the publishing of periodic "integrated reports" about value creation over time. Indeed, integrated reporting:

- Encourages more holistic thinking about a broader range of resources beyond purely financial.
- Encourages the inclusion of sustainability matters into overall business strategies.
- Provides greater context for performance data and clarifies how relevant information integrates into operations.
- Ultimately encourages organizational decision-making to consider long-term impacts on value across a wider range of stakeholders.

Even so, while public ESG and sustainability reporting is becoming more common, often sustainability strategies and approaches, while well intentioned, are developed and reported on independently of the overall business strategy. This lack of integration prevents users of corporate reports from getting the complete picture of an organization's strategy, governance, performance, and prospects over time.

Competing public reporting frameworks and standards and the lack of requisite assurance needed to be confident in the quality and integrity of information can create confusion and inconsistency in the quality of reporting. However, promising developments over the past year — principally the creation of the International Sustainability Standards Board (ISSB) and its commitment to issuing general and climate-related reporting standards — likely will help to alleviate such confusion and inconsistency (see box on page 6).

Despite such progress, angst over public reporting can overshadow the need for organizations to undergo a fundamental transformation to genuinely embrace a holistic view of value creation and become a sustainable organization. While different types of reports, including ESG, corporate sustainability, and integrated, are valuable, the real value arises when an organization successfully integrates long-term thinking into all aspects of its strategy, operations, governance, risk management, and internal control.

This integration — basing business decisions on interconnected information across multiple capitals — is “integrated thinking.” The Integrated Reporting Framework describes integrated thinking as “the active consideration by an organization of the relationship between its various operating and functional units and capitals that the organization uses or affects. It leads to integrated decision-making and the creation of value over the short, medium, and long term.”[1]

This paper sets out how an organization can benefit from integrating sustainability into its governance, risk management, and internal control frameworks and processes. In doing so, the paper connects four key dimensions:

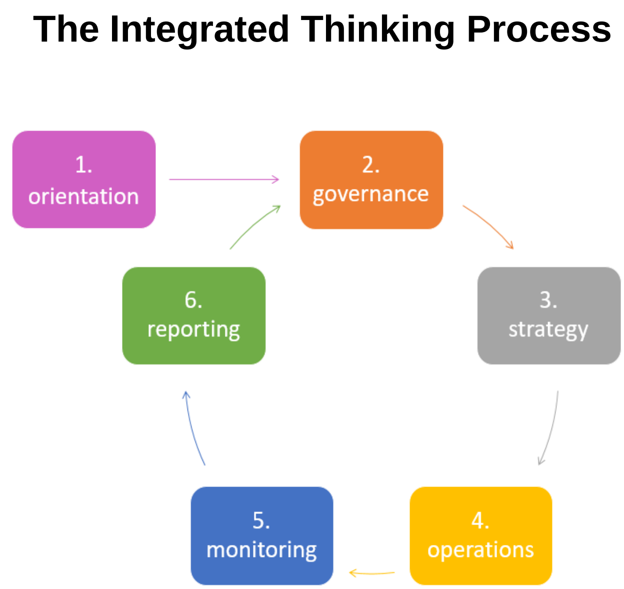
- Integrated thinking and reporting (with reference to the Integrated Reporting Framework and The IIA’s Three Lines Model).
- Internal control (as exemplified by COSO’s Internal Control – Integrated Framework).
- Risk management (as exemplified by COSO’s Enterprise Risk Management – Integrating with Strategy and Performance Framework).
- Independent and objective assurance and advice through the services of the internal audit function (in accordance with The IIA’s International Professional Practices Framework (IPPF)).

To glean the greatest benefit from understanding and using these valuable tools, organizational leaders must understand and embrace the concept of integrated thinking.

1 International Integrated Reporting Framework, https://www.integratedreporting.org/resource/international-ir-framework/

The Integrated Thinking Process

It is important to acknowledge that organizations may approach integration differently. No two organizations will have the same journey or rate of progress in their integrated thinking and reporting journey, nor necessarily the same starting point.[2] Some may begin with an effort to produce an integrated report. Others, such as The World Bank, begin with an effort to have a single line of sight across the organization through an integrated thinking approach.



It is useful to consider integrated thinking as an ongoing process that begins with initial orientation, then follows steps to build upon its holistic approach to **governance** → **strategy** → **operations** → **monitoring** → and **reporting**. The reporting step should facilitate a continuous process to enhance and improve overall governance by informing governing boards, executive management, stakeholders, assurance providers, regulators, and other interested parties about the organization's overall performance.

It should be clearly stated that governance serves as an overarching principle that drives all aspects of the organization. Ultimately, integrated thinking is all about sound governance and effective, holistic decision-making. Prototype Integrated Thinking Principles[3] have been developed to provide a structured approach, rooted in the Integrated Reporting Framework, to embed integrated thinking into an organization year-round.

Applying Integrated Thinking to Management and Governance

Six fundamental ideas are helpful to understanding integrated thinking and integrated reporting:

1) All organizations are interconnected; their actions affect each other; their affairs are interdependent; and they are joined by overlapping and complementary value chains.

2) All organizations draw from and contribute to the same, and in some cases, finite, store of global resources.

3) All organizations impact the interests of overlapping stakeholder groups, including future generations.

4) All organizations share responsibility for achieving common objectives as expressed by the United Nation's Sustainable Development Goals (SDGs).

2 *Transition to integrated reporting: A guide to getting started* is a supplement to the Integrated Reporting Framework and helps report preparers develop a custom-fit transition plan to integrated reporting. Like the Integrated Reporting Framework, the Guide is written in the context of private sector, for-profit companies of any size, but can also be applied by public sector and not-for-profit organizations. https://www.integratedreporting.org/wp-content/uploads/2022/08/Transition-to-integrated-reporting_A-Getting-Started-Guide.pdf

3 Integrated Thinking Principles, https://www.integratedreporting.org/integrated-thinking/

5) Doing good and doing well are two complementary sides of the same coin; they are not diametrically opposed.

6) Integration of sustainability risks and opportunities into business planning, performance, and reporting is a central component of effective governance.

Beyond recognition of these ideas, applying them across an organization requires a broad mindset about how and why organizations operate. An expanded view of the impacts of actions throughout organizations requires integrated thinking in specific and varied ways. In addition to applying integrated thinking across the six capitals (financial, manufactured, human, social and relationship, intellectual, and natural) included in the Integrated Reporting Framework, organizations must instill an integrated thinking mindset throughout their entire business and across components of organizational governance, risk, and control, including:

- Strategic and operational planning and decision-making over the short, medium, and long term.
- Broader stakeholder interests.
- Assurance from multiple internal and external providers.
- Internal and external reporting.

Critical to successful integrated thinking is that this approach must be applied consistently across an organization and driven by those charged with governance to encourage organizational commitment. When implemented successfully, integrated thinking can break down siloed or fragmented work efforts and instill greater collaboration, cooperation, and efficiency. The more that integrated thinking is embedded into an organization's activities, the more naturally the connectivity of information will flow into management reporting, analysis, and decision-making. It also leads to better integration of the information systems that support internal and external reporting and communication, including preparation of the integrated report.

Yet, decision-making in any organization is inherently complex, with influencers that can be dynamic, uncertain, and reliant on second- and third-hand reports that are potentially skewed by subjectivity and self-interest. Therefore, organizations must mitigate this unpredictability with greater transparency, unwavering integrity, enhanced oversight, solid risk management, and independent assurance.

Progress on Unifying Reporting Standards

An integrated mindset is essential for a modern, responsible, and successful organization. The concept of integrated thinking has gained traction as comprehensive approaches to organizational governance and risk management have evolved over the past two decades in support of sustainability. Over time, a plethora of frameworks and tools to measure and report on sustainability matters developed, creating confusion and frustration for organizations as well as their stakeholders.

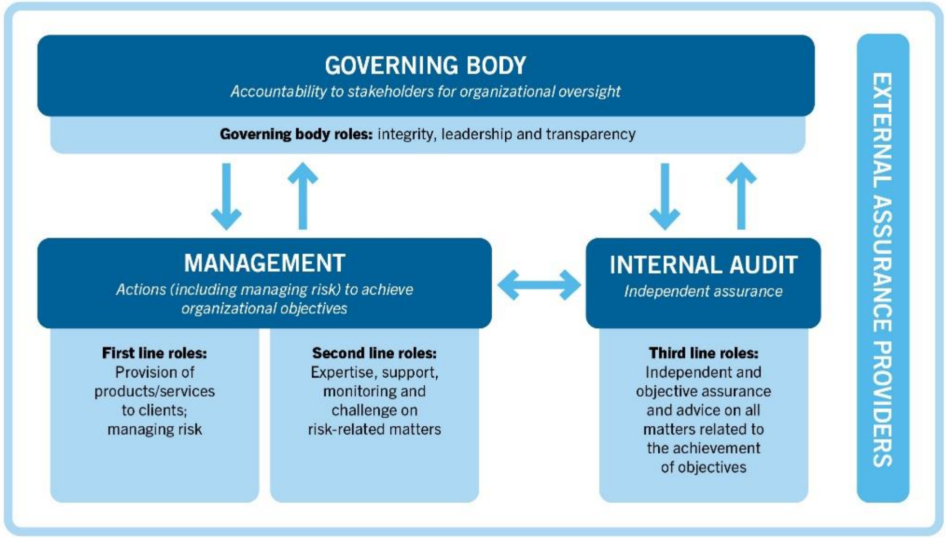
However, recent influential mergers among distinct groups involved in sustainability and related reporting have set the groundwork for creating a complementary set of tools that embrace both integrated reporting and sustainability reporting. These mergers led to the formation of the ISSB in November 2021 by the International Financial Reporting Standards (IFRS) Foundation. The IFRS Trustees announced three major developments designed to improve the quality of disclosures relating to climate and other sustainability issues:

- The formation of the new ISSB, tasked with developing comprehensive global disclosure standards to meet investors' needs.
- A commitment to consolidate two leading investor-focused groups — the Climate Disclosure Standards Board (CDSB) and the Value Reporting Foundation (VFR) — with the IFRS Foundation.
- The publication of prototype climate and general disclosure requirements developed by the Technical Readiness Working Group (TRWG), formed to undertake preparatory work for the new ISSB.

The ISSB unveiled its first proposed general disclosure standards and climate-related disclosure standards in March 2022.

The IIA’s Three Lines Model

The IIA’s [Three Lines Model](), a 2020 refresh of the Three Lines of Defense, provides a foundation to help organizations understand governance structures and roles that support transparency, integrity, oversight, risk management, and independent assurance. The principles-based model begins by identifying three fundamental concepts of sound governance in its first principle.



Principle 1:

GOVERNANCE OF AN ORGANIZATION REQUIRES APPROPRIATE STRUCTURES AND PROCESSES THAT ENABLE:

- ACCOUNTABILITY BY A GOVERNING BODY TO STAKEHOLDERS FOR ORGANIZATIONAL OVERSIGHT THROUGH INTEGRITY, LEADERSHIP, AND TRANSPARENCY.
- ACTIONS (INCLUDING MANAGING RISK) BY MANAGEMENT TO ACHIEVE THE OBJECTIVES OF THE ORGANIZATION THROUGH RISK-BASED DECISION-MAKING AND APPLICATION OF RESOURCES.
- ASSURANCE AND ADVICE BY AN INDEPENDENT INTERNAL AUDIT FUNCTION TO PROVIDE CLARITY AND CONFIDENCE AND TO PROMOTE AND FACILITATE CONTINUOUS IMPROVEMENT THROUGH RIGOROUS INQUIRY AND INSIGHTFUL COMMUNICATION.

Source: The IIA’s Three Lines Model: An update of the Three Lines of Defense

Applying the Three Lines Model

The Three Lines Model addresses how accountability, actions, and assurance should operate within the organization, who within the organizational structure is tasked with their application, who provides oversight and assurance, and the value of coordination and alignment.

Structures, roles, and responsibilities

The Three Lines Model is most effective when it is adapted to align with the objectives and circumstances of the organization. How an organization is structured and how roles are assigned are matters for management and the governing body to determine. The governing body may establish committees to provide additional oversight for particular aspects of its responsibility, such as audit, risk, finance, planning, and compensation. Within management, there are likely to be functional and hierarchical arrangements and an increasing tendency toward specialization as organizations grow in size and complexity.

Oversight and assurance

The governing body relies on reports from management (comprising those with first and second line roles), internal audit, and others in order to exercise oversight and achievement of its objectives, for which it is accountable to stakeholders. Management provides valuable assurance (also referred to as attestations) on planned, actual, and forecast outcomes, on risk, and on risk management by drawing upon direct experience and expertise. Those with second line roles provide additional assurance on risk-related matters. Because of the internal audit function's independence from management, the assurance it provides carries the highest degree of objectivity and confidence beyond that which those with first and second line roles can provide to the governing body, irrespective of reporting lines. Further assurance may also be drawn from external providers.

Coordination and alignment

Effective governance requires appropriate assignment of responsibilities as well as strong alignment of activities through cooperation, collaboration, and communication. The governing body seeks confirmation through their internal audit function that governance structures and processes are appropriately designed and operating as intended.

Source: The IIA's Three Lines Model: An update of the Three Lines of Defense

Understanding structures, roles, and responsibilities enables an organization to approach integrated thinking and the integration of sustainability into business processes and systems in a holistic and considered way. The Three Lines Model does not direct how an organization assigns those structures, roles, and responsibilities to the board, executive management, and internal audit, but clear definition thereof ensures that duplication of effort and gaps in control can be avoided. These benefits also apply to integrated thinking, sustainability risk, and opportunity management efforts. Similarly, oversight and assurance provide critical feedback on internal control, strategy, operations, and overall governance. This aligns with monitoring and reporting requirements for integrated thinking and sustainability.

COSO's Internal Control - Integrated Framework

COSO's Internal Control – Integrated Framework (Internal Control Framework) is a tool that "enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision-making and governance of the organization."[4]

While commonly used as an external financial reporting compliance instrument (particularly in the United States for the Sarbanes-Oxley Act of 2002), it is equally useful for nonfinancial reporting. This is articulated clearly in a paper produced by leaders from the Institute of Management Accountants (IMA) and SASB in 2017:

"The [Internal Control] framework specifically references nonfinancial reporting objectives, suggesting that sustainability reporting objectives can be integrated into an organization's existing internal control framework. COSO defines internal control as 'A process, affected 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.'

"While the framework was always intended to apply to nonfinancial measures (for internal and external reporting), to some extent the U.S. Sarbanes-Oxley Act of 2002 (SOX), particularly Section 404, typecast the framework as one aimed at providing reasonable assurance over external financial

COSO Internal Control – Integrated Framework: Five Components

COSO's Internal Control – Integrated Framework describes the five components of internal control and their direct relationship with the organization's objectives.

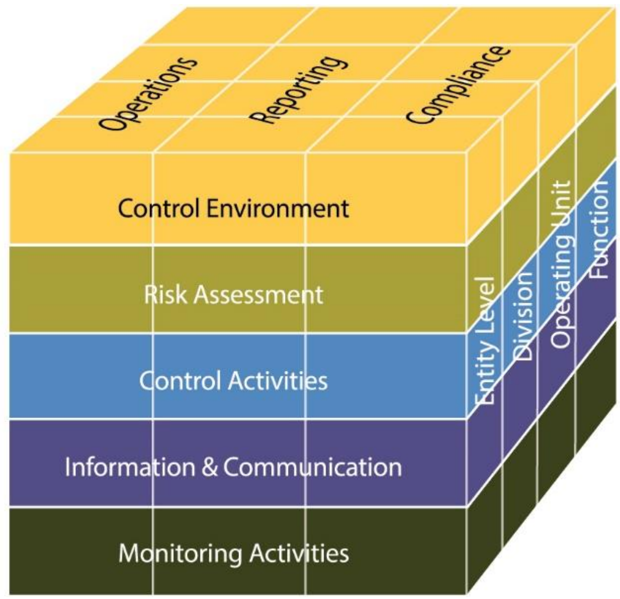
- **Control Environment** – The Control Environment encompasses the standards, processes, and structures that allow internal control to be carried out across the organization. This includes the tone at the top set by boards and executive management about the importance and enforcement of internal control and the accepted standards of conduct to achieve primary objectives. The control environment includes:
  - Integrity and ethical values
  - Management's philosophy and operating style
  - Organizational structures
  - Assignment of authority and responsibility
  - Human resource policies and practices
  - Competence of personnel
- **Risk Assessment** – Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives.
- **Control Activities** – Control activities are the actions established through policies and procedures that help ensure management's directives to mitigate risks to the achievement of objectives are carried out.
- **Information and Communications** – Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously.
- **Monitoring Activities** – Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning.

Source: COSO Internal Control – Integrated Framework

4 *COSO Internal Control – Integrated Framework: Executive Summary*, page 1, May 2013

reporting only. One complementary aim of this paper is to reaffirm that, from its inception in 1992, the framework was always intended to facilitate the achievement of both financial and nonfinancial objectives, including those related to reporting for both internal and external stakeholders. As organizations consider the application of internal control to material sustainability information, they do not need to start over with newly created controls. It may be more efficient to leverage many existing activities, controls, and established internal expertise as well as existing and proven methodologies, approaches, and concepts from internal control over financial reporting (ICFR), such as IT controls or monitoring techniques.[5]

"The Internal Control Framework provides numerous advantages to executive management and the board, including employing a principles-based approach designed to provide maximum flexibility for user judgement in designing, implementing, and facilitating internal controls. Importantly, these principles can be applied across the organization at the entity, operating, and functional levels."[6]



Recognizable by its trademark multicolored cube graphic, the Internal Control Framework is a popular and widely used means to support effective internal control. Its five interrelated components — control environment, risk assessment, control activities, information and communication, and monitoring activities — are identified as essential for effective internal control.

The Internal Control Framework further acknowledges that all processes are ultimately designed to achieve objectives relating to operations, reporting, and compliance. It is within these three objective categories where the framework's practical application to integrated thinking becomes clearer.

- Operational Objectives – These pertain to the effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
- Reporting Objectives – These pertain to internal and external financial and nonfinancial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
- Compliance Objectives – These pertain to adherence to laws and regulations to which the entity is subject.[7]

The Internal Control Framework's cube graphic depicts the tie between objectives, which the organization strives to achieve, and the components, which address what is required to achieve those objectives. The graphic further ties in the organizational structure and its varying levels, from organizationwide to function level.

The Internal Control Framework's components lay out a process that aligns closely with the integrated thinking process, and the related principles provide guidance for maximizing internal control effectiveness (see page 19, Integrated Thinking Matrix).

5 *Leveraging the* COSO Internal Control—Integrated Framework *to Improve Confidence in Sustainability Performance Data*, pages 8-9, IMA/SASB, September 2017.

6 ibid

7 *COSO Internal Control – Integrated Framework: Executive Summary*, https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf

Applying the Internal Control Framework

Control Environment

Creating an atmosphere conducive to effective internal control is also fundamental to the sound governance required for successful integrated thinking. Generally, boards must demonstrate commitment to integrity and ethical values, and exercise appropriate oversight responsibilities that support effective internal control over sustainability efforts. As with general internal control, boards should direct executive management to establish and monitor processes that nurture and support integrating thinking. From a C-suite perspective, management must establish appropriate reporting lines, structures, and responsibilities that promote integrated thinking. What's more, executive management must demonstrate commitment to competence and enforcing accountability in pursuit of related sustainability objectives.

Risk Assessment

As with any risk assessment, executive management should clearly articulate objectives for integrated thinking and sustainability, then identify and analyze risks to achieving those objectives.

Control Activities

Management should craft policies and procedures that nurture and promote integrated thinking and mitigate risks to effectively deploying those policies and procedures.

Information and Communication

Under the Internal Control Framework, communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Communication is particularly crucial to successful integrated thinking and sustainability efforts. One of the Integrated Reporting Framework's Guiding Principles recognizes the need for effective communication through improved connectivity of information: "An integrated report should show a holistic picture of the combination, interrelatedness, and dependencies between the factors that affect the organization's ability to create value over time."

Monitoring Activities

As with the overall Internal Control Framework, organizations should conduct ongoing and/or separate evaluations of internal controls related to integrated thinking and sustainability and report any identified deficiencies.

COSO’s Enterprise Risk Management Framework

There are various definitions of risk:

The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. (IIA IPPF glossary, 2017)

The effect of uncertainty on objectives. (ISO 31000:2018 Risk Management)

The possibility that events will occur and affect the achievement of objectives. (Enterprise Risk Management – Integrating with Strategy and performance, COSO 2017)

What these definitions have in common is recognition that uncertainty prevents organizations from accurately predicting future events. This leads to the inevitable conclusion that there is always a possibility of positive or negative deviation from stated objectives. Many factors contribute to that uncertainty, including complexity, interconnectedness, constant change, unreliable evidence, subjectivity, and other limitations on the capacity to anticipate and eliminate risk.

For organizations, setting goals and taking actions to achieve them are synonymous with risk-taking. Uncertainty creeps in even through the strategizing process itself, as it is based on expectations, judgments, and assumptions. Risk management is the deliberate attempt to anticipate and prepare for the range of events that may occur in order to optimize outcomes — maximizing beneficial impacts and minimizing or mitigating adverse ones — but it can never be failsafe. The only surefire way to eliminate uncertainty regarding an objective is to abandon the objective altogether.

COSO’s Enterprise Risk Management – Integrating with Strategy and Performance Framework

The Framework is built on a set of principles organized into five interrelated components:

- **Governance and Culture:** Governance sets the organization’s tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
- **Strategy and Objective-Setting:** Enterprise risk management, strategy, and objective-setting work together in the strategic planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
- **Performance:** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
- **Review and Revision:** By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
- **Information, Communication, and Reporting:** Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

These principles cover everything from governance to monitoring. They’re manageable in size, and they describe practices that can be applied in different ways for different organizations regardless of size, type, or sector. Adhering to these principles can provide management and the board with a reasonable expectation that the organization understands and strives to manage the risks associated with its strategy and business objectives.

Source: COSO Enterprise Risk Management Framework – Integrating with Strategy and Performance

Enterprise risk management (ERM) calls for a holistic organizationwide approach to managing risk, starting with the determination of strategic objectives. COSO's Enterprise Risk Management – Integrating with Strategy and Performance Framework (ERM Framework) provides boards and management with a tool to build on existing risk management processes and demonstrates how integrating it across the enterprise can help accelerate growth and enhance performance. Like the Internal Control Framework, the ERM Framework contains principles that apply to five components: governance and culture; strategy and objective-setting; performance; review and revision; and information, communication, and reporting. The similarities to the components of the Integrated Thinking Process should also be noted (see Integrated Thinking Matrix, page 19).

An additional similarity between the two frameworks is that ERM is not intended to be a function or department. Instead, it is "the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value," according to the ERM Framework's executive summary. Importantly, ERM goes beyond simple internal control by addressing strategy setting, governance, communicating with stakeholders, and measuring performance.[8]

The ERM Framework anticipates that its greatest benefit may be helping organizations build traits that support and drive an effective response to change, including "agile decision making, the ability to respond in a cohesive manner, and the adaptive capacity to pivot and reposition while maintaining high levels of trust among stakeholders."[9]

COSO's ERM Framework: Core Components and Guiding Principles

8 *Enterprise Risk Management – Integrating with Strategy and Performance: Executive Summary*, page 3, COSO, June 2017

9 *Enterprise Risk Management – Integrating with Strategy and Performance: Executive Summary*, page 7, COSO, June 2017

Applying the Enterprise Risk Management Framework

A more recent contribution from COSO, *Enterprise Risk Management: Applying enterprise risk management to environmental, social, and governance-related risks*, addresses how a sound ERM approach can support sustainability efforts, specifically as they apply to environmental-, social-, and governance-related risks. Developed with the support of the World Business Council for Sustainable Development (WBCSD), this guidance has five chapters that mirror the five components of COSO's ERM Framework.

"**Governance and culture for ESG-related risks**: Governance, or internal oversight, establishes the manner in which decisions are made and how these decisions are executed. Applying ERM to ESG-related risks includes raising the board and executive management's awareness of ESG-related risks and their potential business impact – supporting a culture of collaboration among those responsible for risk management of ESG issues.

Strategy and objective-setting for ESG-related risks: All entities have impacts and dependencies on nature and society. Therefore, a strong understanding of the business context, strategy, and objectives serves as the anchor to all ERM activities and the effective management of risks. Applying ERM to ESG-related risks includes examining the value creation process to understand these impacts and dependencies in the short, medium, and long term.

Performance for ESG-related risks:

- Identifies risks: Organizations use multiple approaches for identifying ESG-related risks: megatrend analysis, SWOT analysis, impacts and dependency mapping, stakeholder engagement, and ESG materiality assessments. These tools can help identify and express ESG issues in terms of how a risk threatens achievement of an entity's strategy and business objectives. Applying these approaches through collaboration between risk management and sustainability practitioners elevates ESG-related risks to the business risk inventory and positions them for appropriate assessment and response among all other risks identified.
- Assesses and prioritizes risks: Companies have limited resources, so they cannot respond equally to all risks identified across the entity. For that reason, it is necessary to assess all risks, regardless of type, for prioritization. Applying ERM to ESG-related risks includes assessing risk severity in a language management can use to prioritize identified risks. Leveraging ESG subject-matter expertise is critical to ensure emerging or longer-term ESG-related risks are not ignored or discounted, but instead assessed and prioritized appropriately.
- Implements risk responses: How an entity responds to identified risks will ultimately determine how effectively the entity preserves or creates value over the long term. Adopting a range of innovative and collaborative approaches to risk responses that consider the source of a risk as well as the cost and benefits of each approach supports the likely success of those responses.

Review and revision for ESG-related risks: Ongoing review and revision of ERM activities are critical to evaluating their effectiveness and modifying approaches as needed. Organizations can develop specific indicators to alert management of changes that need to be reflected in risk identification, assessment, and response. This information can be reported to a range of internal and external stakeholders.

Information, communication, and reporting for ESG-related risks: Applying ERM to ESG-related risks includes consulting with risk owners to identify the most appropriate information to be communicated and reported internally and externally to support risk-informed decision-making."[10]

10 *Enterprise Risk Management: Applying enterprise risk management to environmental, social, and governance-related risks*, COSO and WBCSD, October 2018.

While the COSO/WBCSD guidance is aligned to the five components and 20 principles of COSO's ERM Framework, shown on page 13, it also offers a practical approach to entities using other risk management frameworks, such as ISO 31000 – Risk Management.

The COSO/WBCSD guidance is designed to help organizations achieve:

- Enhanced resilience: An entity's medium- and long-term viability and resilience will depend on the ability to anticipate and respond to a complex and interconnected array of risks that threaten the strategy and business objectives.
- A common language for articulating ESG-related risks: ERM identifies and assesses risks for potential impact to the strategy and business objectives. Articulating ESG-related risks in these terms brings ESG issues into mainstream processes and evaluations.
- Improved resource deployment: Obtaining robust information on ESG-related risks enables management to assess overall resource needs and optimize resource allocation.
- Enhanced pursuit of ESG-related opportunities: By considering both positive and negative aspects of ESG-related risks, management can identify ESG trends that lead to new opportunities.
- Realized efficiencies of scale: Managing ESG-related risks centrally and alongside other entity-level risks helps to eliminate redundancies and better allocate resources to address the entity's top risks.
- Improved disclosure: Improving management's understanding of ESG-related risks can lead to greater transparency and integrated disclosure of financial and nonfinancial information to both meet investors' needs and comply with jurisdictional reporting requirements.

The Integrated Reporting Framework

The changes occurring in the corporate reporting landscape are unprecedented. While there have been positive developments, a change in mindset is necessary if an organization is to experience the full benefits of efforts to create a cohesive reporting system suitable for the 21st century and beyond. An organization must have a long-term view of its purpose, one that fosters greater collaboration and integration, and a holistic view of value creation.

To this point, we have seen how The IIA's Three Lines Model, COSO's Internal Control Framework, and COSO's ERM Framework provide approaches that parallel the integrated thinking process. It is valuable to consider how the Integrated Reporting Framework fits in.

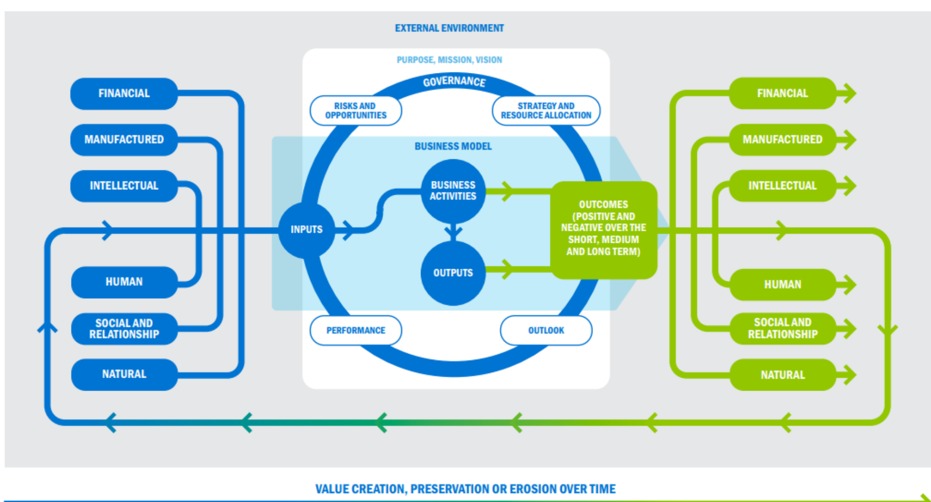
The Integrated Reporting Framework provides a comprehensive tool to monitor and report on an organization's actions and operations, made more effective when integrated thinking practices have been embedded throughout the organization. Ultimately, "The cycle of integrated reporting and thinking, resulting in efficient and productive capital allocation, will act as a force for financial stability and sustainable development," according to the Integrated Reporting Framework.

As noted earlier, the Integrated Reporting Framework's definition of integrated thinking stresses the importance of understanding relationships among various operating and functional units. Integrated thinking leads to integrated decision-making and actions that consider the creation, preservation, or erosion of value over the short, medium, and long term.[11] Integrated reporting is a process founded on integrated thinking that results in a periodic public integrated report by an organization about value creation over time and related communications regarding aspects of value creation.

The Integrated Reporting Framework is underpinned by the fundamental concepts of value creation for the organization itself and for others, and how that value is created, preserved, or eroded, as well as the six capitals. The capitals, or resources and relationships of the Integrated Reporting Framework, are critical components in an organization's efforts to create value. Understanding the role each capital plays in how organizations create value is critical to integrated thinking. Further, examining and monitoring how those capitals interact provides even greater insight to understanding value creation.

Value Creation Model

Organizations exist to create value, and various models attempt to capture the individual factors that influence an organization's ability to do so. The Integrated Reporting Framework's value creation model is underpinned by the six capitals, which provide inputs to an organization's business model. The focus is not just on value creation, but also value preservation and erosion over time. (See the Integrated Reporting Framework on page 16.) The process to create, preserve, or erode value over time considers an organization's inputs, business activities, outputs, and outcomes, which all make up the business model, the external environment the



11 Integrated Reporting Framework, https://www.integratedreporting.org/integrated-thinking/

organization operates in and its impacts on the organization's goals and objectives, risks and opportunities, strategy and resource allocation, governance, outlook, and performance. Importantly, outcomes of the organization's business model (both positive and negative, and over the short, medium, and long term) feed back into the value creation process in a continuous loop.

Internal Audit's Role in Integrated Thinking

Strong governance, sound reporting, and embracing independent, objective assurance are all fundamental to a modern organization that applies integrated thinking. They equally describe the characteristics of a successful internal audit function. Indeed, the mission of internal audit as articulated in The IIA's International Professional Practices Framework (IPPF) embraces key aspects of sustainability: "To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight."

The internal audit function's role as an independent, yet internal, assurance provider affords it a unique opportunity to become familiar with all areas of the organization, including nonfinancial aspects. This positions it well to provide assurance over the relevance and accuracy of data used in integrated and sustainability reporting. What's more, internal audit standards specifically require internal audit functions to evaluate the adequacy and effectiveness of internal control and governance within their organizations.

Applying Internal Audit to Sustainability Information

A properly resourced and independent internal audit function can make valuable contributions to help incorporate sustainability information into organizational performance and act as a catalyst for innovation and change by:

- Helping an organization prepare for making reliable and accurate external nonfinancial disclosures by advising and providing assurance on the content, design, and implementation of appropriate structures, systems, and processes for strategic and operational planning; goal setting; data collection, creation, and validation; decision-making; and reporting.
- Driving the necessary conformity to standards and processes over data collection, creation, and validation at the business unit level for the organization's use in internal and external reporting.
- Providing independent assurance through audit and assessment of both financial and nonfinancial data accuracy.
- Consulting on the establishment of measurement and evaluation processes; definition of materiality and listing of relevant key performance indicators (KPIs); and the introduction of reporting methods, guidelines, and tools (both internal and external).
- Participating in project teams to provide guidance to implementation plans and performance.
- Reviewing reporting processes and recommending process improvements based on business assessments, and the financial and nonfinancial information that should be contained in internal and external reports.
- Brokering strong relationships within business units, between management functions, and among organizations.
- Assessing whether the risks associated with sustainable organizational performance are considered and addressed — risks that may have an impact on stakeholder evaluation and support, and value creation.
- Collaborating with external auditors to provide assurance on the accuracy, reliability, and consistency of the information being reported, and to ensure the engagement is performed in a cost-effective manner.

Previously published content from The IIA on internal audit's role in ESG reporting provides additional clarity to the benefits and value that an internal audit function offers, particularly in effective public-facing statements about an organization's sustainability efforts.

"As ESG reporting becomes increasingly common, it should be treated with the same care as financial reporting. Organizations need to recognize that ESG reporting must be built on a strategically crafted system of internal controls and accurately reflect how an organization's ESG efforts relate to each other, the organization's finances, and value creation.

The internal audit function should play a significant role in an organization's ESG journey. It can add value in an advisory capacity by helping to identify and establish a functional ESG control environment. It also can offer critical assurance support by providing an independent and objective review of the effectiveness of ESG risk assessments, responses, and controls. Additionally, internal audit functions that operate in compliance with The IIA's globally recognized standards are well-positioned to help their organizations apply established, credible internal control frameworks to their ESG efforts.

Seeking out objective assurance on all ESG-related risk management processes from a qualified, independent, and properly resourced internal audit function should be part of any ESG strategy. While this paper outlines how and why internal audit functions must play a critical role in an organization's sustainability reporting efforts, it bears repeating that reporting comprises only part of an effective ESG strategy. Internal audit should provide assurance and advice over all aspects of ESG risk management."[12]

12 *Internal Audit's Role in ESG Reporting: Independent assurance is critical to effective sustainability reporting*, The IIA, Lake Mary, FL, USA, May 2021.

The Integrated Thinking Matrix

This Integrated Thinking Matrix demonstrates parallel structure among key governance frameworks and tools. Understanding and leveraging these parallels can help organizations embrace integrated thinking and sustainable approaches to governance, strategy, and internal controls.

Integrated Thinking Process	Components/Principles COSO ERM Framework	Components/Principles COSO Internal Control Framework	Integrated Reporting Framework's Seven Guiding Principles	Role of Internal Audit
Orientation				Provide assurance and advice on strategic and operational planning, goal setting processes and structures.
Governance	**Governance and 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	**Control Environment** 1. Demonstrates commitment to integrity, ethical values 2. Board exercises oversight responsibilities 3. Management establishes reporting lines, structures, responsibilities 4. Demonstrates commitment to competence 5. Enforces accountability in pursuit of objectives	**3C Stakeholder Relationships** 3.10 An integrated report should provide insight into the nature and quality of the organization's relationships with its key stakeholders, including how and to what extent the organization understands, considers, and responds to its legitimate needs and interests.	Provide independent assurance over governance and culture issues and keep board informed on strength and health of both.
Strategy	**Strategy and Objective Setting** 6. Analyzes business context 7. Defines risk appetite 8. Evaluates alternative strategies 9. Formulates business objectives		**3A Strategic Focus and Future Orientation** 3.3 An integrated report provides insight into the organization's strategy; how it relates to the organization's ability to create value in the short, medium, and long term; and its use of and effects on capitals.	Provide assurance on content, design, and implementation of structures, systems, processes for strategic and operational planning; goal setting; data collection, creation, validation; decision-making; reporting.
Operations	**Performance** 10. Identifies risk 11. Assesses severity of risk 12. Prioritizes risk 13. Implements risk responses 14. Develops portfolio view	**Risk Assessment/Control Activities** 6. Identifies objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change 10. Selects and develops control activities 11. Selects and develops control over technology 12. Deploys controls through policies and procedures	**3B Connectivity of Information** 3.6 An integrated report should show a holistic picture of the combination, interrelatedness, and dependencies between the factors that affect the organization's ability to create value over time.	Drive conformity of data collection, creation, and validation standards and processes at the entity level for data aggregation at an organizational level. Through audit and assessment, provide independent assurance of nonfinancial data accuracy.
Monitoring	**Review and Revision** 15. Assesses substantial change 16. Reviews risk and performance 17. Pursues improvement in enterprise risk management	**Monitoring Activities** 16. Conducts ongoing and/or separate evaluation of internal control 17. Evaluates and reports deficiencies		Consult on establishment of measurements and evaluation processes; definition of materiality and listing of relevant indicators (KPIs); introduction of reporting methods, guidelines, and tools (both internal and external).
Reporting	**Information, Communication, and Reporting** 18. Leverages information and technology 19. Communicates risk information 20. Reports on risk, culture, and performance	**Information/Communications** 13. Uses relevant information to support internal control 14. Communicates internally 15. Communicates externally	**3D Materiality** 3.17 An integrated report should disclose information about matters that substantively affect the organization's ability to create value over the short, medium, and long term. **3E Conciseness** 3.36 An integrated report should be concise. **3F Reliability and Completeness** 3.39 An integrated report should include all material matters, both positive and negative, in a balanced way and without material error. **3G Consistency and Comparability** 3.54 The information in an integrated report should be presented: • On a basis that is consistent over time. • In a way that enables comparison with other organizations to the extent it is material to the organization's own ability to create value over time.	Review reporting processes and recommend needed process improvements based on business assessments, and what should be contained in internal and external reports. Collaborate with external auditors to provide assurance on the accuracy, reliability, and consistency of the information being reported, and ensure the engagement is performed cost-effectively.

Conclusion

Undoubtedly, mounting investor activism, public concern over climate change, growing social movements, and the COVID-19 pandemic's disruptive magnification of risk have raised the stakes for all organizations to effectively manage sustainability risks and opportunities. Yet, it is challenging for an organization to develop the complexity, sophistication, and maturity in its internal control and governance practices to become truly sustainable. What's more, the fundamental shift in culture and mindset away from measuring success strictly on financial measures is equally challenging for many organizations. The integrated thinking process addressed in this report, coupled with the tools examined, provide a significant starting point.

The holistic mindset necessary for successful integrated thinking opens the door to internal benefits, such as breaking down silos, understanding how risks manifest across all areas of the organization, and acknowledging the critical relationship between sustainability and long-term organizational success. It also provides external benefits, such as enhanced reporting on those matters relevant to value creation over time, forging stronger connections with stakeholders, and doing good in addition to doing well.

The holistic approaches found in COSO's Internal Control and ERM frameworks can be applied to the six capitals underlying integrated thinking and integrated reporting, which can help an organization begin to incorporate a more integrated approach into its governance, strategy, operations, and risk management. The Integrated Reporting Framework provides direction for capturing progress and value creation. The IIA's Three Lines Model offers additional clarity on roles and responsibilities that promote appropriate action, accountability, and assurance. Finally, the internal audit function contributes the essential ingredients of independent and objective assurance and advice, which add value by providing the governing body with critical assessments of governance, risk management, and control.

Identifying, understanding, and executing a business strategy that properly integrates sustainability will inevitably drive an organization to create and preserve value in the short, medium, and long term. The dynamic and volatile risk landscape, growing social justice movements, and increasingly knowledgeable stakeholders, including investors, regulators, employees, and the general public, demand that organizations embrace sustainability. Anything less will place an organization behind the competition and eventually threaten its continued existence.

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 218,000 global members and has awarded 180,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world. For more information, visit theiia.org.

ABOUT COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, 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).

Acknowledgment

Professionals working for the Value Reporting Foundation provided foundational content to this report on the Integrated Reporting Framework and Integrated Thinking. The VRF consolidated into the IFRS Foundation, effective August 2022.