FROM BOLT-ON TO BUILT-IN

Managing Risk as an Integral Part of Managing an Organization

IFAC International Federation of Accountants®

The mission of IFAC is to serve the public interest by: contributing to the development of high-quality standards and guidance; facilitating the adoption and implementation of high-quality standards and guidance; contributing to the development of strong professional accountancy organizations and accounting firms and to high-quality practices by professional accountants, and promoting the value of professional accountants worldwide; and speaking out on public interest issues.

The IFAC Professional Accountants in Business (PAIB) Committee serves IFAC member bodies and professional accountants worldwide who work in commerce, industry, financial services, education, and the public and not-for-profit sectors. Its aim is to promote and contribute to the value of professional accountants in business. To achieve this objective, its activities focus on:

- increasing awareness of the important roles professional accountants play in creating, enabling, preserving, and reporting value for organizations and their stakeholders; and
- supporting member bodies in enhancing the competence of their members to fulfill those roles. This is achieved by facilitating the communication and sharing of good practices and ideas.

The PAIB Committee extends its appreciation and thanks to Grant Purdy, Associate Director, Broadleaf Capital International, and Matthew Leitch, Tutor, Researcher, Author, and Consultant, for assisting the committee in developing this paper.

For questions or comments about this thought paper, please contact Vincent Tophoff (vincenttophoff@ifac.org) or see the Risk Management and Internal Control section of the IFAC Global Knowledge Gateway.

ISBN: 978-1-60815-230-8

Published by:

Table of Contents

Introduction

With the increased volatility in the modern business environment and the financial and economic crises, the effective management of risk in organizations—including good internal control—has taken on even greater importance. Effective risk management facilitates the achievement of an organization's objectives, while complying with legal, regulatory, and societal expectations, and enables the organization to better respond and adapt to surprises and disruptions.

In some organizations the approach to management of risk and internal control has deviated from its original purpose: to support decision making and reduce uncertainty associated with achieving objectives. Instead, risk management in these organizations has become an objective in itself, for example, through the institution of a non-integrated, stand-alone risk management *function*.[1] This typically removes responsibility for the management of risk from where it primarily belongs: incorporated into line management. A separate risk management function, even though established with the best intentions, may hamper rather than facilitate good decision making and subsequent execution. Managing risk in an organization is everyone's responsibility.

This Paper contends it is time to recognize that managing risk and establishing effective control form natural parts of an organization's system of management that is primarily concerned with setting and achieving its objectives. Effective risk management and internal control, if properly implemented as an integral part of managing an organization, is cost effective and requires less effort than dealing with the consequences of a detrimental event. It also generates value from the benefits gained through identified and realized opportunities. On the other hand, a potential adverse impact of a poorly implemented risk management framework or an overemphasis on internal control is that employees may become so risk adverse that they no longer advance their organization.

This Thought Paper positions risk management and internal control as it was originally intended in the organization—as a highly relevant and useful process for decision and execution support, and as a process that boards and management naturally use to ensure their organization makes the best decisions and achieves its objectives. This Thought Paper is, therefore, applicable to all organizations, regardless of their size or structure, private or public, that want to improve how they manage risk.

This Paper: a) demonstrates the benefits of properly integrating the management of risk, including internal control, into the governance, management, and operations of an organization; b) provides ideas and suggestions on how such integration can be achieved; and c) furnishes practical examples of how professional accountants in business can support their organizations with this integration.

This Paper is intended for professional accountants in business and other participants in the governance, management, and operations of an organization who are responsible for:

- Establishing, evaluating, or improving risk management in an organization;
- Managing risk as integral part of managing an organization; or
- Overseeing the strategic direction and management of an organization, including the effective management of risk.

[1] For example, the Basel Committee on Banking Supervision's consultation paper, *Corporate Governance Principles for Banks* (2014), elaborates mainly on the risk management function, largely forgoing the business line, which is first and foremost responsible for the management of the risk to business objectives.

The Roles of Professional Accountants in Business

Worldwide, more than one million professional accountants support organizations in commerce, industry, financial services, education, and the public and not-for-profit sectors, making those organizations more successful and sustainable. They form a very diverse constituency, and can be found working as employees, consultants, and self-employed owner-managers or advisors.

As further explained in *Competent and Versatile—How Professional Accountants in Business Drive Sustainable Organizational Success* (2011), the roles professional accountants in business perform can broadly be described as creators, enablers, preservers, and reporters of sustainable value creation for organizations.

Professional accountants in business are also generally concerned with the collection, analysis, interpretation, and provision of information for decision-making processes in setting and achieving the organization's objectives. In this way, they are helping internal and external stakeholders to understand and influence drivers of performance, and what might happen in the future under alternative plans. They can also link risk to business performance indicators, providing relevant information from risk assessments that can help manage sources of risk in the internal and external environment.

Evaluating and improving risk management and internal control are among the core competencies of professional accountants in business. This Thought Paper supports professional accountants in business in integrating the management of risk as an inseparable part of their organization's system of management.

Some professional accountants in business might find themselves in an organization with poor risk management and/or internal control. Embarking on a journey toward integration contributes to enhancing the effectiveness of risk management and internal control while simultaneously improving the performance of the organization.

The Importance of Managing Risk Effectively

Organizations face a wide range of internal and external sources of uncertainty, both positive (opportunities) and negative (threats), that may affect achievement of their objectives. Risk—the effect of uncertainty on objectives—can, of course, be viewed as beneficial or detrimental depending on how the organization's objectives are affected. For example, agricultural businesses may regard extreme weather events as detrimental, while firms who specialize in rebuilding roads and repairing buildings after storms may see them as beneficial. Organizations face inherent risk in all their activities, including their strategy setting, operations, and financial management. *Risk management* provides a systematic way to manage such risk more effectively.

Risk management assists organizations in making informed decisions about:

- objectives they want to achieve;
- the level, nature, and amount of risk that they want to assume in pursuit of those objectives; and
- the controls required to support achieving their objectives.

However, neither risk management nor internal control are objectives in themselves; instead, they are an integral part of setting and achieving the organization's objectives.

This Paper is predicated on the basis that internal control is best achieved when it is considered to be part of the risk management process. This is in line with the widely-accepted definition of risk management—"coordinated activities to direct and control an organization with regard to risk"—from the International Organization for Standardization (ISO)'s standard 31000 on risk management that incorporates internal control as part of the risk management process.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) publication *Enterprise Risk Management (ERM)—Integrated Framework* (2004) makes a similar point by arguing that as the ERM framework "incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process."

Risk management should never be implemented in isolation; it should always be fully integrated into the organization's overall system of management. This system should include the organization's processes for good governance, including those for strategy and planning, making decisions in operations, monitoring, reporting, and establishing accountability.

The Importance of Integrating Risk Management

Because employees in organizations automatically think of issues that might either prevent or facilitate achieving objectives when they decide how to act, some form of managing risk will already be "integrated" in organizations. However, the approach adopted may not be coherent, consistent, comprehensive, or communicated effectively, which means that its outcomes are likely to be unreliable.

Key to ensuring effective and integrated management of risk is the employment of a properly formed risk management framework as an integral part of the organization's system of management. If this contains the necessary elements, is appropriate, and works effectively, it will help ensure that risk is managed at all times to create the maximum net benefit for the organization.

Unilever: Embedded Risk Management

"At Unilever, we believe that effective risk management is fundamental to good business management and that our success as an organization depends on our ability to identify and then exploit the key risks and opportunities for the business. Successful businesses take/manage risks and opportunities in a considered, structured, controlled, and effective way. Our risk management approach is embedded in the normal course of business. It is 'paper light—responsibility high.' Risk management is now part of everyone's job, every day! It is no longer managed as a separate standalone activity that is 'delegated to others."

—Unilever, one of the world's leading suppliers of fast-moving consumer goods with operations in 100 countries and sales in more than 190 countries

Information provided by Unilever for a case study in Integrating Governance for Sustainable Success *(IFAC 2012).*

SERIOUS FLAWS

Some organizations have not yet established a formal framework for the management of risk, nor integrated it into their overall system of management. In these cases, organizations may rely on ad-hoc crisis management that attempts to recover the status quo after an event. Others have some sort of framework, but it may be plagued by serious flaws (see Serious Risk Management Flaws and Additional Examples). Both instances may result in missed benefits or larger than necessary detrimental consequences.

Serious Risk Management Flaws

Standalone or poorly implemented risk management, or internal control, usually leads to higher costs and sub-optimal performance. Examples of poorly integrated and ineffective risk management in organizations and how to counter these include:

A. Having a ***compliance-only mentality*** in covering issues such as formal roles and responsibilities, prevention and detection of fraud, and compliance with laws and regulations, but ignoring the need to address both the compliance and performance aspects of risk management.

B. Treating ***risk as only negative*** and overlooking the idea that organizations need to take risks in pursuit of their objectives. Effective risk management enables an organization to exploit opportunities and take on additional risk while staying in control and, thereby, creating and preserving value.

C. Internal control that is ***overly focused on external financial reporting***. Providing control in relation to financial reporting is important in the detection and prevention of fraud, as well as ensuring financial reports are accurate, and may be a major focus of corporate regulators. However, effective controls should address all material organizational risk to help it achieve its objectives, create value, and avoid loss.

D. Regarding ***risk management as a separate function or process***. Line managers should be aware that they are managing risk as part of their everyday roles and responsibilities, in line with the organization's intentions as expressed in its policies, goals, and objectives. This problem is exacerbated when line managers are not directly responsible for maintaining risk within established limits for risk taking but are allowed to choose their own limits for risk taking over those of the organization.

These flaws were informed by IFAC's interviews with 25 key business leaders, summarized in Integrating the Business Reporting Supply Chain (2011), on what went wrong in the various financial crises and what should be done to further enhance governance, risk management, and internal control.

Additional Examples of Risk Management Flaws

Bad practice		Good practice
Risk management as objective in itself	vs.	Risk management to help achieve objectives
Auditor / staff driven	vs.	Driven from top down, supported by exemplary behavior
Rules based	vs.	Performance and principles based
Off-the-shelf systems	vs.	Tailored to the organization
Focused on loss minimization only	vs.	Also focused on the creation of value
Mainly hard controls	vs.	Recognizing influence of culture and attitude
Imposed	vs.	Implemented through management of change
Stand-alone / "bolt-on"	vs.	Integrated / "built-in"
Static, out-of-date	vs.	Dynamic, evolving
Seen as a cost	vs.	Seen as a sound investment

MATURITY

Effective risk management supports management's attempts to make all parts of an organization more cohesive, integrated, and aligned with its objectives, while operating more effectively, efficiently, ethically, and legally. Figure 1 shows a typical pathway of the development stages of risk management that many organizations have followed. Ideally, however, organizations should integrate risk management, including internal control, from the start.

The maturity stages of risk management and internal control in organizations can be summarized as:

1. **Non-existent or ad hoc**—often characterized by reactive crisis management once something has gone wrong;
2. **Internal control only**—formal internal controls, often mainly focused on external financial reporting;
3. **Stand-alone risk management and internal control**—functioning as a siloed system next to, and not necessarily in tandem with, an organization's management system; and
4. **Integrated risk management**—risk management, including internal control, as a natural and integral part of an organization's system of management.

Integrating effective management of risk across all of an organization's decision making processes and subsequent execution will help ensure that its objectives are achieved and maximum value is created for all stakeholders. Various risk management standards, frameworks, or guidelines can support organizations in this process (see appendix B).

The following section provides a number of guiding principles for effective management of risk as part of the organization's overall system of management. The final section provides a practical model for how organizations can effectively integrate the management of risk into their system of management.

Figure 1: Typical Risk Management and Internal Control Development

Considerations for Integrating the Management of Risk

It is not always easy to get governing bodies and top management, and sometimes even risk committees and risk management functionaries, to consistently implement a framework and processes that ensures risk is managed effectively. And in cases where they do so, the attention to risk may weaken over time, particularly when crucial people rotate in or out their function. The following considerations provide guidance for effectively integrating the management of risk as an integral part of managing an organization.

A. Organizations should primarily focus on setting and achieving their objectives to create sustainable value and growth; managing risk is an integral part.

The main objective of an organization is not to have effective controls, nor to effectively manage risk, but to properly set and achieve its goals; to be in compliance and capable of managing surprises and disruptions along the way; and to create sustainable value.

JC Penney: No Adequate Testing

A useful example is the case of JC Penney, an American chain of mid-range department stores, which almost toppled after a disastrous reorganization. "One of the big mistakes was perhaps too much change too quickly without adequate testing on what the impact would be," according to Bill Ackman, the principal shareholder of JC Penney's.

The management of risk in pursuit of these objectives should be an inseparable and integral part of all these activities.

In some organizations, the risk management process is applied only *after* objectives are set, overlooking that setting objectives itself can be one of the greatest sources of risk. This may apply both to strategic objective setting and to all other decision-making processes within the organization, from the board level down. In addition, not all organizations perform formal risk assessments to stress test their top strategic objectives while in draft. Therefore, risk should be considered at all stages of the objective setting process, as well as in the subsequent planning, execution, monitoring, and review stages.

Also, because most people in an organization, especially those in line functions, are primarily focused on doing their job well and achieving their objectives, establishing an explicit connection between how risk affects their jobs and their objectives makes them more inclined to manage the related risk as well.

B. Risk should always be identified, assessed, treated, reported, monitored, and reviewed in relation to the objectives an organization wants to achieve, while giving consideration to the organization's ever changing internal and external context.

As risk is the effect of uncertainty on achieving objectives, it would be inadvisable to manage risk without taking into account the effect on objectives. Unfortunately, in some organizations the linkage between the risks periodically reported to the board and the strategic objectives that are most critical to the long-term success of the company is at best opaque and at worst, missing completely. As a consequence, risk is insufficiently understood or controlled, even though the organization devotes some attention and resources to the management of risk. Risk management without taking into account the effects on objectives is thus ineffective.

Risk is also best dealt with before a decision has been made or actions have been started to achieve a certain objective in the place and by the people where it originated, irrespective or their position in the business.

Last but not least, as the context in which an organization sets its objectives and tries to achieve them is continuously changing, so does risk. Therefore, organizations should constantly evaluate progress and, if necessary, adjust their objectives or their planning—including risk treatment—in light of the changed circumstances.

C. While risk management is a body of knowledge with global frameworks, standards, and guidance, the application of risk management needs to be tailored to the organization.

Because effective risk management is inextricably linked with the organization's strategy and operations, it follows that the approach to risk management is as individual as that organization. And just as the organization's strategy should be tailored to its specific organizational circumstances, so should its risk management strategy.

An organization's risk to setting and achieving its objectives is influenced by many factors, such as its size, structure, business model, IT systems, financial flexibility, its employees, and its environment—that is, its customers, suppliers, competitors, and regulators as well as political, social, economic, and technical drivers of change, etc. Ergo, it is all of these factors together that determine how the management of risk can be applied most effectively for a specific organization at a specific point of time.

Most guidelines explicitly pay attention to some of these characteristics, for example, by pointing out that application of risk management in smaller organizations can be less formal and less structured—even though smaller organizations also need all elements of good risk management to be properly integrated.

D. Those responsible for setting and achieving the organization's objectives should also be responsible for effectively managing the related risk.

As an organization's risk is inextricably connected to its objectives, the responsibility for managing risk cannot lie with anyone other than the person who is responsible for setting and achieving those objectives. Good risk management is, in this sense, everybody's responsibility in the organization as everyone is, in one way or another, responsible for ensuring the organization achieves its objectives.

The governing body and senior management should formulate, approve, and implement the organization's strategy for governance and any particular policies with respect to risk management and internal control. The governing body should also ensure that everyone in the organization, including themselves, acts accordingly.

Line management needs to accept its responsibility and not delegate risk management and internal control to specialized staff departments. Placing responsibility within the line also implies that staff or support functions should not, or no longer, be the "owner" of risk management in organizations. However, these support functions nevertheless play a crucial role in supporting line management in the effective management of risk.

Where risk management is an integral part of the organization's system of management, the risk management function plays a number of important roles, such as:

- facilitator of good risk management and internal control processes in the organization;

- custodian of the overall risk management and internal control framework; and
- internal assurance provider on the effectiveness of risk management and internal control in the organization.

E. Decisions should be informed by an appropriate assessment of risk.

Sustainable organizational success can only be achieved through informed and structured decision making while setting the organization's objectives and planning, implementing, executing, evaluating, and improving the organizations strategy. Decision making needs to consider risk from both external and internal sources as organizations and their objectives are affected by many factors, often outside their direct control. Risk management should, therefore, be an integral part of these decision making processes at every level of an organization and across all operations ("built-in").

Special attention should be given to decision making by the governing body, as some of the biggest risk management failures have been caused by emotion, greed, or fear. In such cases boards often forget about the basics of sound decision making, including adequate risk assessment. This also sets a bad example for the rest of the organization ("tone at the top"). For example, an organization might have a policy explicitly requiring all decisions be supported by risk assessments. However, if top management is prepared to make significant decisions—such as those involving organizational change, investments, or acquisitions—without a proper risk assessment, a clear signal is sent to the organization that leadership is not committed to its own policy and substandard practices are tolerated.[2] This inevitably results in decisions lower down in the organization also being made without adequate risk assessment, despite whatever official policy there might exist.

F. High-quality information is crucial to good decision making as it reduces uncertainty.

The organization must ensure that it has access to timely, reliable data on which to base the decision, as well as the technical resource/expertise to analyze data and turn them into useful information, including a note of any limitations in the data or analysis.

Often, there is a need to use professional judgment in reaching a decision. Perhaps there is not enough data, evaluation techniques provide contradictory answers, or there are multiple risk responses available. However, professional judgment must always be *professional*—meaning, exercised by those who are suitably trained, qualified, and experienced to use it and based on the best available information.

G. Effective management of risk is equally important to all managerial steps following the decision-making process.

Once a decision has been made, numerous follow-up steps need to be taken to actually achieve the desired outcomes, such as designing, planning, executing, monitoring and reviewing, and providing accountability to the various stakeholders. Obviously, all these steps require additional decision making. However, as internal and external circumstances change—or additional information becomes available—so does risk. The effects of these changes in risk subsequently need to be taken into account.

[2] For example, see the analysis of the takeover of ABN AMRO Bank by RBS characterized as "willing to bet the bank on a risky takeover with surprisingly little insight into what it wanted to buy."

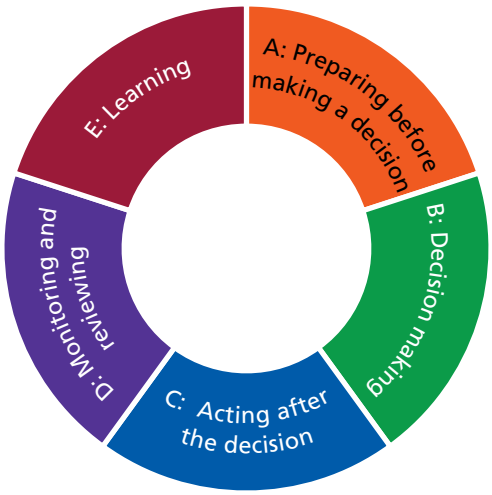
H. Organizations need to remain sufficiently agile to make the changes needed to continue to create and preserve value.

As the effects of risk can never be completely eliminated, organizations need to build both resilience and agility in all their activities, enabling them to adequately respond to changes in circumstances or deal with the consequences of unforeseen events. After all, over the long term it is not the strongest of the species that survives or the most intelligent, but rather the one most adaptable to change.

Managing Risk as an Integral Part of Managing an Organization

Integrating risk management should mean adopting ways to influence the managerial processes that already exist—to enhance and improve them but not necessarily replace or increase them. To that end we have to work from the inside out by first understanding how decisions are made and implemented, and then determining how the management of risk should be integrated therein.

This section first provides a technical underpinning and then a practical model of how organizations effectively integrate the management of risk into their system of management. For this purpose, a simple representation of an organization's system of management is chosen as the starting point, based on the managerial planning and control (or "Plan-Do-Check-Act"[3]) cycle:



Using this cycle, discussed in detail below, a model of how the effective management of risk could naturally be integrated into these already existing managerial steps is provided.

How does a managerial planning and control cycle work? Suppose we want to shoot an arrow at a moving target. Risk is the effect of uncertainty on hitting the target and is larger if the target is further away or moving faster. Control helps the organization modify that risk so the arrow is launched in the right direction, at the right speed, and on the right course—and/or returns to course or is redirected at a target that has shifted (see figure 2).

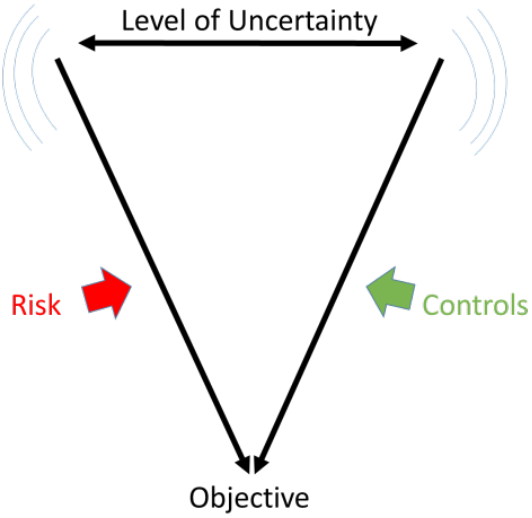


Figure 2: Balance between objectives, risk, and controls

[3] The "Plan-Do-Check-Act Cycle," also called the P-D-C-A or Deming Cycle, is an iterative, four-step management process typically used in organizations for the planning, control, and continuous improvement of processes and products.

The course from setting an objective to achieving an objective is typically managed through a series of interconnecting planning and control cycles, each with its own interval and informed by the progress of the activities and the changes in the environment. Think, for example, of an overall strategic planning and control cycle, consisting of several tactical planning and control cycles and including many more operational planning and control cycles. In addition, most organizations work with rolling planning and control cycles in which, for example, a four-year strategy is being updated annually to reflect the revised objectives and activities in light of the changes in the circumstances (see figure 3).

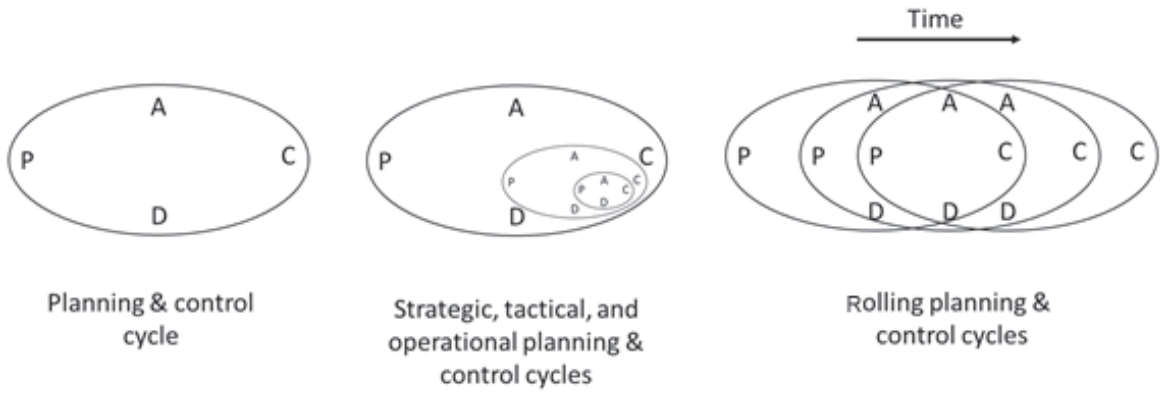


Figure 3: Planning & control cycles

Typically, initial strategic planning and control cycles in which the objectives are set and the course to achievement is charted must handle the maximum level of uncertainty, and, therefore, consist of many more steps than subsequent cycles. Through a series of iterative planning and control processes, an organization progressively reduces its level of uncertainty as it gets closer to achieving its specific objectives.[4] Consequently, the number of steps will also be significantly less and more of an operational nature (see figure 4).

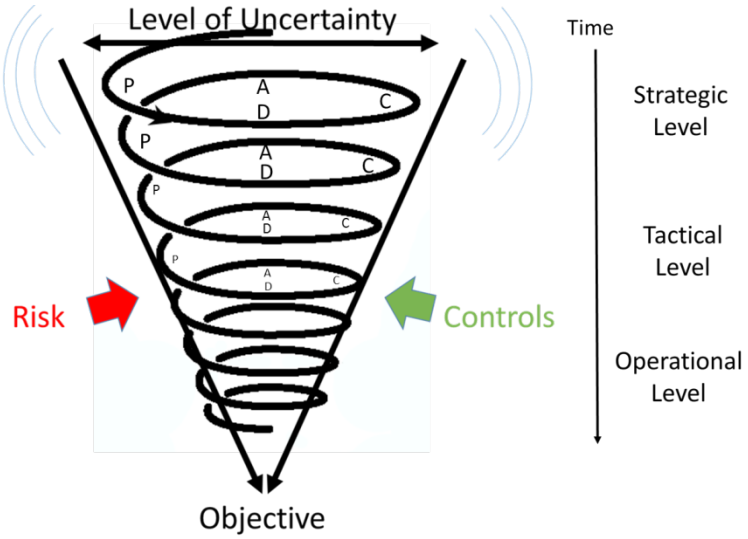


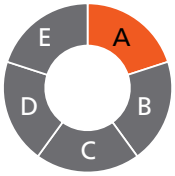
Figure 4: Combination of Planning & Control Cycles and Risk Management Triangle

[4] This is not to say that a significant risk event can also thwart/cross achievement of objectives in the later stages of the process, like a ship wrecking in sight of the harbor.

MODEL

Once the management of risk is fully embedded as an integral part of managing an organization, it becomes virtually invisible—so implicit in everything the organization does, and no longer identifiable as separate steps (see example below).

In practice, many of the activities in these steps will be executed intuitively. The point is, however, that good intuitive decisions and actions are underpinned by sound decision making, which equals good risk management. The model below does not serve as a "checklist" for every planning and control cycle. Rather, it demonstrates how risk can be managed as an integral part of managing an organization.



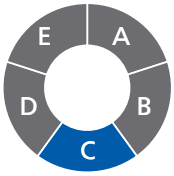
A: Preparing before making a decision

- Understand broad scope and purpose of what we are trying to achieve. What will it involve?
- Define what outcomes we are trying to achieve and their relation to the organization's overall objectives. Define how we will measure them.
- Consider who will need to be involved in the decision and the actions that follow. Will they be inside or outside the organization?
- Consider the major sources of uncertainty for what we are trying to achieve. Are they internal or external to the organization? What are their implications for our overall objectives?
- Determine the criteria we will use to make the decision. What is the basis and how we will know if it is the correct decision in the light of our overall objectives?
- Decide how we will make the decision—the process and steps. What will be considered and what will be irrelevant?

B: Decision making

- Clarify and agree on key assumptions and presumptions about the decision and the outcomes.
- Consider the range of things that might occur or are already present that would prevent us from achieving the outcomes we require.
- Consider the range of things that might occur or are already present that would enhance achieving the outcomes we require.
- Consider—in all cases—the effect of those things that might occur or are already present on our overall objectives.
- Consider our recent performance in the area under discussion. What does it say about the effectiveness of the existing controls that are intended to enable the achievement of the organization's objectives?
- Consider the results of any recent reviews that are pertinent to what we are trying to achieve. What lessons can be learned?

C: Acting after the decision



- Once the decision to act has been made, decide what actually needs to be done, by whom, and by when.
- Consider what other things need to be done, including implementing controls, to limit uncertainty associated with the outcomes we wish to achieve.
- Consider the costs and benefits of alternative courses of action and decide which create the most value and provide the highest chance that the outcomes we desire will be achieved.
- Consider the sequence of all actions and the critical path to achieving outcomes.
- Allocate resources and accountabilities for all actions.
- Record and communicate the outcomes of the decision-making and planning processes and ensure that everyone involved knows what they are responsible for.
- Set up the process for monitoring progress and completion of all actions.

D: Monitoring and reviewing

- Track progress and actions and provide management oversight. Question any delays in actions that fall on the critical path to achieving outcomes. Provide or re-allocate resources if required.
- Monitor the previously identified major sources of uncertainty and asses the environment for new sources of uncertainty. Understand the implications of any changes on what we are trying to achieve and on our overall objectives.
- Monitor the existing controls that are intended to enable the achievement of the organization's objectives.
- Conduct periodic reviews of those controls by management and propose appropriate evolution.
- Monitor decision making and implementation as part of each employee's performance evaluation, emphasizing and encouraging sound decision making.
- Validate the continuous monitoring and periodic reviews using competent and sufficiently independent assurance providers (such as internal audit).

E: Learning

- Agree on the extent to which the outcomes were achieved.
- Agree on whether the outcomes were successes or failures in terms of the organization's objectives.
- Agree on whether any consequential effects were successes or failures.
- Agree on the causes of the successes or failures and the role of the existing controls.
- Consider the implications for future decisions and define what the organization should learn.
- Disseminate the learnings across the organization.
- Codify and capture the learnings in policies and procedures and cycle into management processes.

The most important feature of this model is the almost total invisibility of risk management and internal control terminology, as risk is managed as an integral part of managing the organization (i.e., built-in). This also corresponds with the main objective of an organization, which is *not* to effectively manage risk, *nor* to have effective controls but to ensure that it makes the best decisions and achieves its objectives.

Appendix A: Definitions

Governance: the set of responsibilities and practices exercised by the governing body with the goal of: a) providing strategic direction; b) ensuring that objectives are achieved; c) ascertaining that risks are managed appropriately; and d) verifying that the organization's resources are used responsibly. This is aligned with the definition of governance in *Board Briefing on IT Governance, 2nd Edition* (IT Governance Institute, 2003)**.**

Governing body: the person(s) or body (e.g., a board of directors) with primary responsibility for overseeing the strategic direction, operations, and accountability of the organization, including the financial reporting process. Governing bodies can be made up of independent and non-independent directors and can have various subcommittees, such as the audit, remuneration, and ethics committees. In some entities in some jurisdictions, the governing body may include management personnel, executive members of a governance board of a private or public sector entity, or an owner-manager.

Integrated governance system: the governing body and subsequent levels of management integrating governance into strategy, management, oversight, and accountability in order to achieve sustainable organizational success.

Internal control: IFAC recognizes that the term "internal control" can have multiple meanings, including:

1. A system or process: the entirety of an organization's internal control system, i.e., an organization's internal control system.
2. An activity or measure: the actual measure to treat risk and to effectuate internal control, i.e., individual controls.
3. A state or outcome: the outcome of the internal control system or process, i.e., an organization achieving or sustaining appropriate or effective internal control.

Risk: ISO *Standard 31000:2009—Risk Management* defines risk as "effect of uncertainty on objectives."

Risk management: ISO Standard 31000:2009—Risk Management defines risk management as "coordinated activities to direct and control an organization with regard to risk."

Risk management framework: ISO *Standard 31000:2009—Risk Management* defines risk management framework as a "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."

Risk management process: ISO *Standard 31000:2009—Risk Management* defines the risk management process as the "systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk."

Stakeholder: any person, group, or entity that has an interest in an organization's activities, resources, or output, or that is affected by that output. Stakeholders can include regulators, shareholders, debt holders, employees, customers, suppliers, advocacy groups, governments, and society as a whole.

Stakeholder value: organizational value that is generated for stakeholders by creating, implementing, and managing effective strategies, processes, activities, assets, etc. Sustainable value creation for stakeholders occurs when the benefits to them are greater than the resources they expend. Value is generally measured in financial terms, as in the case of shareholders, but it can also be measured as a societal or environmental benefit, as in the case of both shareholders and other stakeholders.

Tone at the top: the words and deeds of an organization's governing body and senior management that determine its values, culture, and the behavior and actions of individuals; synonymous with "leading by example."

Appendix B: Resources

Risk management is a dynamic area and no list can cater for all needs; therefore, these resources may not be sufficient for the needs of all users. Additional resources from IFAC, its member bodies, and third parties can be found through the *IFAC Global Knowledge Gateway*.

Your Portal to Global Accountancy Knowledge, Resources, and News

www.ifac.org/Gateway

IFAC Resources

- *Defining and Developing an Effective Code of Conduct for Organizations* (IFAC, 2007) helps organizations encourage an ethics-based culture and define and develop a code of conduct. It also refers to the most significant resources in this area.
- *Internal Control from a Risk-Based Perspective* (IFAC, 2007) includes ten senior-level professional accountants in business who share their experiences and views on establishing effective internal control systems.
- *Evaluating and Improving Governance in Organizations* (IFAC, 2009) includes a framework—consisting of a series of fundamental principles, supporting guidance, and references—for how professional accountants can contribute to evaluating and improving governance in organizations.
- *Global Survey on Risk Management and Internal Control—Results, Analysis, and Proposed Next Steps* (IFAC, 2011) contains over 600 responses from around the globe and provides an analysis of survey results and summarizes respondents' recommendations for the next steps in this area.
- *Competent and Versatile: How Professional Accountants in Business Drive Sustainable Organizational Success* (IFAC, 2011) outlines the diverse roles of professional accountants in business and the many ways they serve their employers and the public interest.
- *Evaluating and Improving Internal Control in Organizations* (IFAC, 2012), establishes a benchmark for good practice in maintaining effective internal control in response to risk, and help professional accountants in business and their organizations create a cycle of continuous improvement for their internal control systems.
- *Integrating Governance for Sustainable Success* (IFAC, 2012) analyzes how professional accountants in business can support their organizations and increase performance by integrating governance into the key drivers of sustainable organizational success. Using case studies from around the world, the report illustrates that good governance is about more than the protection of stakeholders' interests or compliance with regulatory requirements.

Third Party Resources

- *Enterprise Risk Management—Integrated Framework* (COSO, 2004) expands on internal control and provides key principles and concepts on the broader subject of enterprise risk management.
- *Internal Control—Integrated Framework* and companion documents (COSO, 2013) help organizations design and implement internal control in light of many changes in business and operating environments.
- *Standard 31000:2009—Risk Management* (International Organization for Standardization, 2009) sets out principles, a framework, and a process for the management of risk that are applicable to any type of organization in the public or private sector.
- *King Code of Governance for South Africa* (King III) recommends companies maintain effective governance, risk management, and internal control; it came into effect in 2010.
- *Risk Management Guidelines—Companion to AS/NZS ISO 31000:2009* (Standards Australia,

Standards New Zealand, 2013) expands on and explains the elements included in the ISO Standard 31000 and provide advice about applying the standard, taking a similar approach to risk management as this Thought Paper.

- *Improving Organizational Performance and Governance: How the COSO Frameworks Can Help* (COSO, 2014) relates the COSO Enterprise Risk Management and Internal Control frameworks to an overall business model and describes how the key elements of each framework contribute to an organization's long-term success.
- *Mixing Strategy with Risk* (*CGMA Magazine,* 2014) provides a practical example on how risk management naturally fits into strategic planning, as well as the role of the finance function in that process.
- *Guidance on Risk Management, Internal Control, and Related Financial and Business Reporting* (UK Financial Reporting Council, 2014) argues, among other things, that risk management and internal control should be incorporated within the company's normal management and governance processes, not treated as a separate compliance exercise.
- *A Risk Challenge Culture* (Association of Chartered Certified Accountants and the Institute of Management Accountants, 2014) identifies nine areas critical to designing and implementing an environment that encourages, requires, and rewards enquiries that challenge existing conditions.

International Federation of Accountants
529 Fifth Avenue
New York, NY 10017
USA
T +1 212 286 9344
www.ifac.org