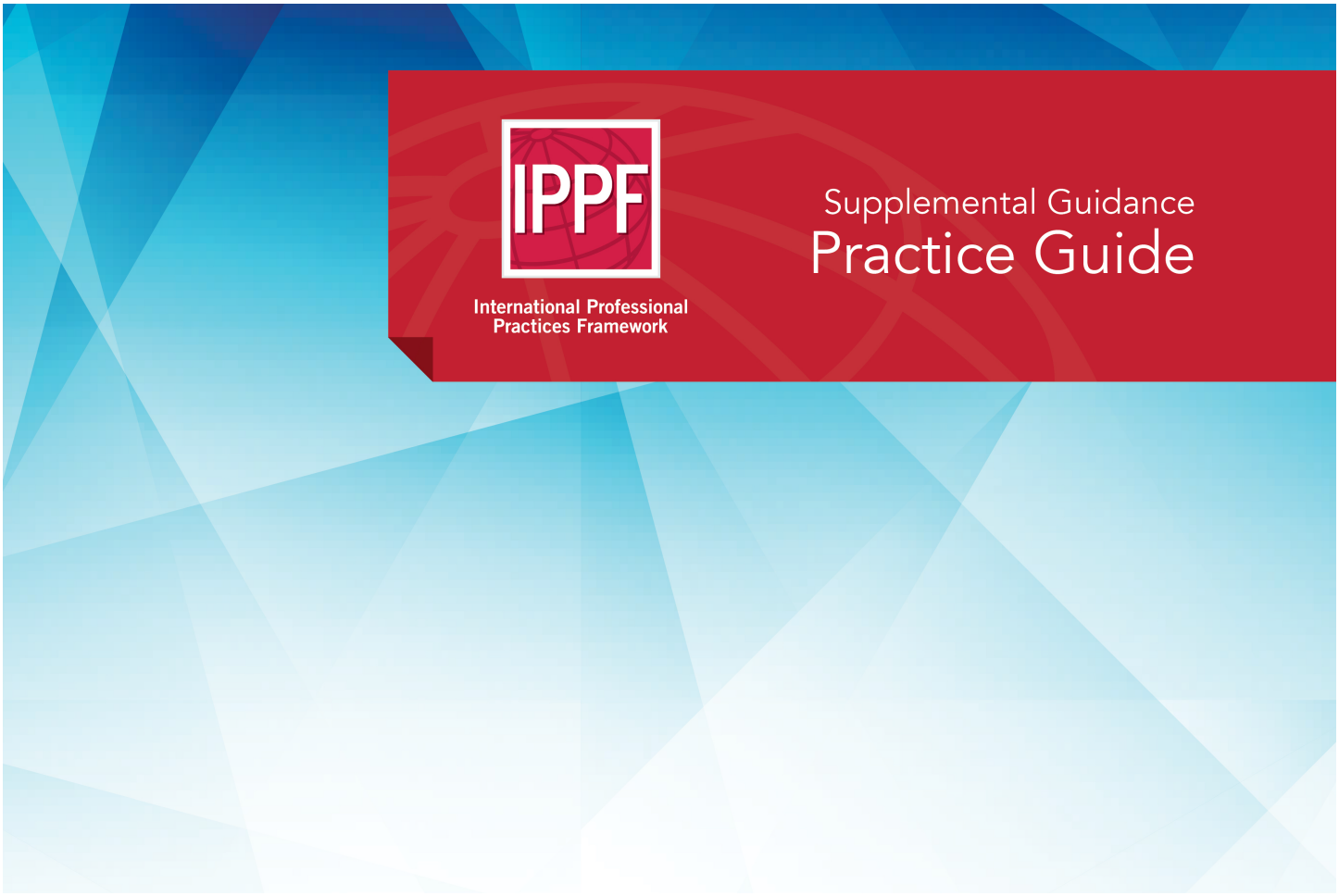


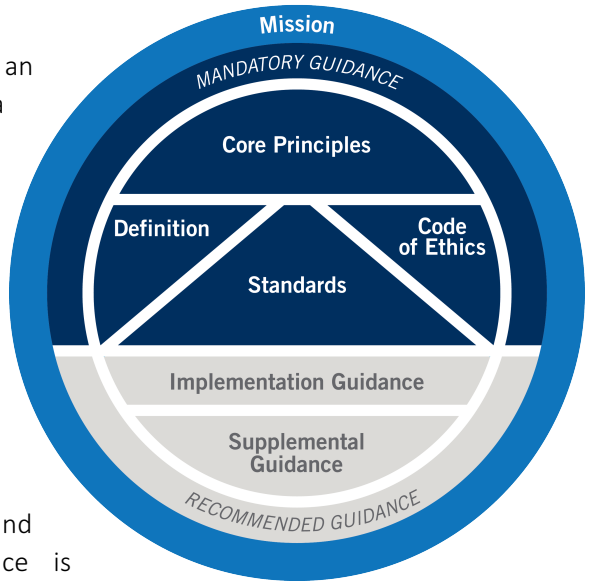
Supplemental Guidance
Practice Guide

Assessing the Risk Management Process

The Institute of Internal Auditors | Global

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.



Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.

Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance offers additional information, advice, and best practices for conducting internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

Table of Contents

Executive Summary

Around the world, risk management activities and initiatives are required and expected by regulators, rating agencies, and a host of other stakeholders in major industries including financial services, government, manufacturing, energy, health services, and more. However, risk management is driven by more than regulations and external forces. Implementing efficient and effective risk management benefits organizations of any type and size by helping them to achieve operational and strategic objectives and to increase value and sustainability, ultimately better safeguarding their stakeholders.

Internal auditors must evaluate the effectiveness and contribute to the improvement of risk management process (Standard 2120 – Risk Management). Benchmarking the current state of the organization's risk management against a risk management maturity model is a good place to start this type of assessment. Benchmarking may help the internal audit activity communicate with senior management and the board about the organization's level of risk management maturity and about aspiring to improve the process and advance in maturity. This information also enables internal auditors to appropriately tailor each engagement, taking into account the maturity of the area or process under review.

This guidance provides examples of risk management maturity models and a basic methodology internal auditors may use to provide independent assurance that the organization's risk management process is effective. Applying the guidance will help internal auditors protect and enhance organizational value and fulfill the expectations of the board and senior management.

Introduction

An organization's **risk management** efforts are often collectively referred to as its risk management program. However, the term "program" can be interpreted as limited, or finite. This practice guide treats risk management as a process, rather than a program, implying that it is a continuous effort and ongoing function.

Note: Terms in bold are defined in the glossary in Appendix B.

In many jurisdictions, the **board** is charged with overseeing that a risk management process is in place and effectively responds to the changing risk landscape. In turn, the **chief audit executive** (CAE) and the **internal audit activity** are expected to provide independent assurance that the organization's risk management processes are effective, according to Standard 2120 – Risk Management, which lists several criteria for making such an assessment.

Assessing an organization's risk management processes is a growing challenge as numerous risk management standards, frameworks, and models exist, and new ones are frequently introduced. Risk management may encompass the policies, procedures, and controls that ensure adequate,

timely, and continuous identification, assessment, treatment, monitoring, and reporting of risks to the organization.

While this guide does not advocate that an organization should use any particular risk management program, framework, or model, the following common attributes of mature risk management are discussed:

- Risk culture: Integration of risk into all decision-making, compensation, reward structures, and goal-setting.
- Risk governance: Participation in the risk management process throughout the entire organization by personnel that are knowledgeable, skilled, and competent in risk management.
- Risk management process: Aggregated risk identification, prioritization assessment, treatment, monitoring, and reporting throughout the organization.

Additionally, the maturity levels, approaches, strategies, and focus of risk management-related functions often depend on the organization's size and complexity and the industry and jurisdictions within which it operates. This guidance provides background information, methodology, and tools to enable internal auditors to provide assurance that the organization's risk management processes are effective and to contribute to the improvement of those processes.

This guidance will help internal auditors to:

- Apply The IIA's Code of Ethics principles and the *International Standards for the Professional Practice of Internal Auditing* to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.
- Understand the need to assess risk management activities.
- Understand the key components of an effective risk management process.
- Develop an assessment approach that takes into account the organization's business and regulatory environments and level of maturity.
- Collect the necessary information to determine the scope of an engagement to assess risk management activities.
- Evaluate the effectiveness of the risk management process.
- Contribute to the improvement of the risk management process.

Business Significance: Risks and Opportunities

Risk management as a discipline has long played a vital role in organizations. It has evolved into various forms and is known by many names, from "project risk management" to "enterprise risk management," or ERM. Risk management continues to garner attention as the world becomes more interconnected and disruption accelerates across all industries. However, the adoption of documented risk management as an organizationwide effort has yet to become the universal norm.

The failure of risk management governance, systems, and processes may lead to liabilities, fines, sanctions, and related exposures. Ongoing reviews and assessments of risk management will help organizations avoid the loss of assets, intellectual property, market share, revenue opportunities, customer loyalty, brand reputation, and more due to the occurrence of risk events that could have been prevented, avoided, or mitigated (shared or transferred). Appendix C describes risk scenarios related to the risk management process.

Well-governed and successful organizations use the risk management process to coordinate the direction and control of risk exposure in a way that enables the organization to meet its objectives. Measuring the benefits of a mature risk management process may be challenging because reliable data may be hard to obtain, if it is available at all. It may be difficult for organizations to objectively analyze the maturity of their own risk management process.

Standard 2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation:

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- *Organizational objectives support and align with the organization's mission.*
- *Significant risks are identified and assessed.*
- *Appropriate risk responses are selected that align risks with the organization's risk appetite.*
- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

However, a mature risk management process typically demonstrates benefits, such as:

- Enabling risk-based decision-making and strategy-setting.
- Increasing communication and consultation across the organization.
- Establishing connections and insights among risks, opportunities, and strategies via a common risk language.
- Enabling the documentation and timely reporting of risk management activities so senior management and the board are well informed of management's direction.
- Increasing the likelihood the organization will meet its strategic objectives.
- Creating and protecting value for stakeholders.

When proposing improvements to the risk management process, internal auditors may encounter objections, such as:

- Risk assessments take too much time.
- Risk information gathered is not relevant.
- Risk information is not used to make decisions.

When the internal audit activity designs an assessment of the organization's risk management process, understanding the organization's level of risk management maturity and its risk culture are important to developing appropriate questioning. If the organization has yet to fully develop its risk management outlook or philosophy, the internal audit activity should understand the reasons for this before formulating findings and recommendations. Opinions about whether the risk management process yields the right information are important. If management believes that the risk management process is a bureaucratic exercise that is not worth the resources needed to execute it, then recommending large-scale improvements may be premature and received with skepticism or rejected completely. Instead, internal auditors may be more effective by making recommendations related to the organization's risk culture.

Risk Management Maturity

Numerous risk management frameworks are available. Each offers principles organizations should consider when developing a comprehensive risk management process. Some frameworks focus on internal controls and their relationship to an organization's risks. Others focus solely on IT risks, strategic risks, or insurable risks, for example. An organization may recognize that no single risk management framework encompasses all the risk areas that it needs to consider. Instead of adopting a single framework, the organization may benefit from combining the elements of several frameworks to create one that is uniquely tailored to its specific characteristics and needs. Regardless of what framework is used as a foundation for a risk management process, certain elements may help the organization measure its maturity.

Figure 1 is an example of a risk management **maturity model**, illustrating five stages of development that may characterize a risk management process. Various elements within the same organization may be in different stages of maturity at any given time; for example, the maturity level of an organization's culture may differ from that of its governance and process. When planning audit engagements, internal auditors may use a maturity model to appropriately tailor each engagement to the maturity of the element under review.

Figure 1: Example of Risk Management Maturity Model

Stage	Culture	Governance	Process
1 – Initial	Risk belongs to the internal audit activity.	CAE/audit committee chair.	Risk-based auditing.
2 – Repeatable	Risk is considered on an as-needed basis.	Business managers.	As-needed risk and control self-assessment process.
3 – Defined	Risk information is shared among internal audit and control functions.	C-suite/board members.	Common risk language and risk assessment process are used by internal audit and control functions.
4 – Managed	Risk is integrated into strategic planning; risk appetite is stated and communicated.	All levels of management and the board.	Common risk language and consistent risk assessment process are in place throughout organization.
5 – Optimized	Risk is integrated into all decision-making, compensation, and goals.	Total participation.	Common risk language and aggregated risk reporting are established throughout organization.

To ascertain an organization's position on the risk management maturity model and to assess how effectively the risk management process is serving the organization, internal auditors should consider several elements.

Audit Considerations

How mature should an organization be? Consider a scale of 1 to 5, with 5 being the most mature. It is not necessarily optimal or practical for all organizations to be operating at the highest level of maturity. Achieving a solid 2 or 3 may be acceptable. Each organization should determine which level of maturity is optimal for its circumstances.

All organizations practice some form of risk management, though they may not be aware of it and may not be formally documenting their efforts. The simplest form of documented risk management is an annual exercise to create an organizational risk register at the top level. This may be referred to as a "strategic risk assessment" in which senior management develops and documents a list of risks, and the assessment is not addressed again until the following year. At the other end of the spectrum, organizations with the most robust, or mature, risk management process consider risk factors, including those of a cultural or governance nature, across the organization in a systematic, structured format.

Risk Appetite

The IIA's International Professional Practices Framework defines **risk appetite** as the level of risk that an organization is willing to accept. For many organizations, risk appetite is difficult to articulate for practical use in discussions. A common form of risk appetite is a statement of "loss tolerance" that may be approved by senior management and/or the board, with a caveat that the loss limit may be exceeded with approval by those with appropriate levels of authority.

Framing the risk appetite as a "loss tolerance" may be interpreted as an organizational plan to achieve the stated level of loss (monetary quantity) from its risk exposure, which could lead managers to take on levels of risk exposure that are higher than necessary or desired. Further, having a risk appetite stated in terms of broad strategies may lead to differing interpretations of how the tolerances work as the risk appetite statement is applied to lower levels in the organization.

Internal auditors should encourage the organization to adopt a risk appetite methodology and format that assist management and the board in prioritizing strategies and resource allocations. Risk appetite can be dynamic and is often a balance among strategies. Setting static levels for risk exposure from the top level of the organization may result in the risk appetite being overlooked as a tool in making informed decisions in a consistent manner across the organization.

Structure: Roles and Responsibilities

Depending upon the maturity level of the organization's risk management process and the resources to which the internal audit activity has access, roles and responsibilities for risk management will be distributed differently across the organization.

Based on its level of development and access to resources, an organization may find itself in various areas of the maturity continuum:

1 – Initial. In organizations where the risk management process is in early stages of development, the internal audit activity may be more actively involved than it would be when the process is more mature. At this maturity level, specific risk management activities may not be performed by the line/operational management or functions in the roles of control, compliance, legal, risk management, or internal quality assurance. Instead, those functions may rely on the internal audit activity's risk assessments and risk-based assurance and advice.

2 – Repeatable. At this level, the internal audit activity is better organized and resourced and plays an instrumental role by performing risk-based assessments, perhaps larger in scope. The internal audit activity may work with the control, compliance, legal, risk management, and internal quality assurance functions, adding internal audit expertise to assist risk owners in line/operational management functions to build and monitor operational controls. This stage is sufficient for many organizations if the process is operating consistently, efficiently, and delivering actionable results that aid in the attainment of the organization's goals and objectives.

3 – Defined. Organizations that rank toward the middle of the model may be a blend of maturity levels, with some business units operating at higher levels of maturity than others. In this structure, the organization's control, compliance, legal, risk management, and internal quality assurance functions may own the risk management process and have responsibilities that remain consistently within the Managed and Optimized levels, for example. The control and assurance functions may play an active role in assisting line/operational management to assess risks and perform other risk management activities. The internal audit activity may continue to operate functionally at the Repeatable level.

4 – Managed. Ascending the maturity model, in organizations that have achieved a significant level of maturity, line/operational management owns and manages risks organizationwide and are responsible for implementing corrective actions to address process and control activities. The internal audit activity acts primarily as an independent assurance function, assessing the effectiveness of the risk management process among the other management and assurance functions.

5 – Optimized. In organizations that have achieved this level of integration, sophistication, and maturity, line/operational management owns the risk management process. The organization's compliance and/or risk management functions conduct risk assessments for their own use. They may also monitor the risk assessments and reporting produced by line/operational management and may challenge the risk information as necessary. Risks are monitored and managed across various business processes.

The internal audit activity, as an independent assurance function, performs engagements to assess that risk management processes are effective in individual areas and overall throughout the entire organization. Additionally, the internal audit activity may compare its risk assessments to the risk information produced by management and verified by the internal assurance functions (compliance/risk management) to gauge the accuracy and completeness of management's assessment. Conversely, the internal audit activity may use management's risk information to inform internal audit's risk assessments, or they may do both as appropriate. The CAE should coordinate with other providers of assurance and consulting services and may consider relying on their work (Standard 2050 – Coordination and Reliance).

Resource

For more information on determining roles and responsibilities for risk management, see IIA Practice Guide "Coordination and Reliance: Developing an Assurance Map."

Culture

The effectiveness and comprehensiveness of a risk management process depends on the risk culture of the organization. If the culture is not conducive to open discussion and the consideration of risk in both the negative and positive senses of the word, then the risk management process will

fail. Internal auditors should ask, "If no policies existed, how would management operate?" An organization may have policies and procedures stating that risk management will be considered, but the culture may overshadow intent and negate any serious conversation or action.

Organizations may have sophisticated processes to measure and assess risk, yet the culture may not be conducive to risk management. In regulated industries, having an operational risk management process may be required, but if management's focus is simply ticking boxes on a checklist, the risk management process is unlikely to reach a maturity level where risk information is integrated into decision-making (and linked to compensation and incentives), aggregated, and reported widely throughout the organization.

If internal auditors are involved in designing a risk management process and determine that the organizational culture does not support the effort, they should bring the issue to the CAE, who can discuss the viability of the process with senior management and the board. Even if the tone at the top supports risk management, pressuring management in a resistant organization to cooperate with a risk management program is rarely worthwhile. Management must understand the value in risk management before they will champion the process.

Governance

For a risk management process to be successful, support from the top must be established from the beginning. To achieve buy-in and the proper allocation of resources, risk information must be used in decision-making at the highest levels of an organization. The interest of high-level entities, such as the audit committee of the board, is critical to create demand for the gathering, assessing, and providing of risk information. If the audit committee regularly requests risk information as they perform their supervisory role, then management must find a way to provide it.

In general, the risk management process is developed from the top down, with senior management and the board calling for risk assessments and reporting first, typically leading business management to adopt the same practices later as it must provide the risk information for senior management to use. Once key business managers, senior management, and the board are involved in the risk management process, the structure can be clarified, and policies, procedures, reporting, and escalation protocols can be implemented.

Process

The degree to which risk management activities are integrated with other business processes is a useful gauge of the organization's maturity level. If risk assessments are common throughout the organization, the risk appetite is communicated effectively at all levels, and risk information is used in key decision-making, the organization is considered to be more mature than an organization performing risk assessments once a year or only as mandated by regulations. **Figure 2** illustrates the differences. This example is representative but not exhaustive.

Figure 2: Sample Maturity Model Descriptions

1 – Initial	
Risk appetite	The organization's risk appetite is implied but not clearly stated or documented. Senior management may have similar ideas about the risk level the organization is willing to accept.
Risk assessment	Internal auditors may conduct risk assessments to gather risk information for their engagements, for use by the control/compliance/internal assurance functions, and/or for management's use. Management has not invested in hiring or training personnel with facilitation and risk assessment skills, and internal auditors may be the only personnel well-versed in assessing risks. Risks are assessed as needed; for example, senior management may assess risks related to their proposed strategies once a year. Large and expensive projects may warrant as-needed risk assessments.
Common language	Management uses risk information when they have it, but terminology is not consistent or is misinterpreted across the organization. Different risk registers and risk measurement criteria may exist, depending on the focus of the risk assessment. Risk measurement criteria is simplistic, such as ratings of high, medium, or low.
Use of risk information	Risk information is not aggregated or communicated beyond the specific group that performed the risk assessment.
2 – Repeatable	
Risk appetite	The organization's risk appetite has been addressed by senior management and the board and is documented, but is not shared organizationwide. The topic is inconsistently revisited for updates.
Risk assessment	Internal auditors conduct risk assessments to gather information for their engagements, for use by the control/compliance/internal assurance functions, and/or for management's use. Management has not invested in hiring or training personnel with facilitation and risk assessment skills. Risks are assessed consistently, but a strategic, comprehensive plan is lacking. Large and expensive projects may be treated as one-off risk assessments.
Common language	Management uses risk information when they have it, but terminology is inconsistent across the organization. Different risk registers and risk measurement criteria may exist, depending on the focus of the risk assessments. Risk measurement criteria may take likelihood and impact into account and be as simple as ratings of high, medium, or low.
Use of risk information	Risk information is sometimes aggregated or communicated beyond the specific group that performed the risk assessment.
3 – Defined	
Risk appetite	Senior management and the board have vaguely defined a risk appetite that may or may not be well understood throughout the organization.
Risk assessment	The control/compliance/risk management/internal assurance functions may perform risk assessments for their areas or for management's use. Management has not invested in hiring or training personnel with facilitation and risk assessment skills. Risk assessments may be conducted as needed. For example, senior management may request a risk assessment for a large capital project that presents significant risk exposure for the organization.
Common language	Management uses risk information when they have it, and the terminology is mostly consistent across the organization. Multiple risk registers and risk measurement criteria exist.
Use of risk information	Risks may be tied to the objectives of a department or project team but are not always overtly considered at the top levels of the organization.

Figure 2: Sample Maturity Model Descriptions (continued)

4 – Managed	
Risk appetite	Senior management and the board have defined a risk appetite that is well understood throughout the organization.
Risk assessment	Control/compliance/internal assurance functions regularly conduct risk assessments for their areas or for management's use. Management has invested in hiring and training personnel with facilitation and risk assessment skills. Risk assessments are conducted as needed and may addresses significant risks as they arise, rather than relying on a risk-based audit plan.
Common language	Senior management consistently requests and uses risk information, and the terminology is well known and used throughout the organization. Risk management criteria is understood and implemented organizationwide.
Use of risk information	Significant risks are tied to the organization's objectives. Risk information is communicated to senior management consistently, and management compensation and incentives may be linked to key performance indicators (KPIs) driven by identified and assessed risks. Information is used to contribute to improving the risk management process throughout the organization.
5 – Optimized	
Risk appetite	Once the risk appetite has been approved by the board, management and key employees implement it throughout the organization in a format and level of detail appropriate for decision-making.
Risk assessment	Management uses a common process to conduct risk assessments, document risk information, and monitor its performance against risk-adjusted KPIs. Management has protocols in place to ensure that significant risks are addressed when they arise, rather than during or after next scheduled risk assessment.
Common language	The entire organization, from the board to line/operational management and employees, has a common understanding of the terms used in the risk management process (e.g., risk, contributing factor, control, impact, likelihood) and uses a common language to discuss risk.
Use of risk information	Risks are tied to the organization's objectives at every level. Further, risk information is communicated throughout the organization on an ongoing basis, and compensation and incentives for management are linked to KPIs driven by identified and assessed risks.

Role of Internal Audit in Risk Management

Standard 2120 – Risk Management states that "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." Specifically, the standard requires the internal audit activity to assess whether:

- The organization's objectives align with its mission.
- Management assesses significant risks.
- Management's risk responses align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated timely throughout the organization, including to the board.

To accomplish this assessment, the internal audit activity may gather the information during multiple engagements and may consider the results of these engagements cumulatively to gain a complete understanding of the organization's risk management processes and make a judgment regarding their effectiveness. The internal audit activity also must assure that management has in place ongoing activities to monitor risk management processes.

The internal audit activity may be called upon to fulfill additional roles in risk management. If the internal audit activity is asked to help develop risk management processes (e.g., conducting and documenting risk assessments), questions regarding independence may arise. To be clear about appropriate roles, internal auditors should review the series of standards starting with 1100 – Independence and Objectivity, paying attention particularly to Standard 1130 – Impairment to Independence or Objectivity and its associated assurance and consulting standards. These standards provide distinctions between activities appropriate for assurance engagements and those appropriate for consulting engagements. For example, objectivity is presumed to be impaired if an internal auditor provides assurance services over an activity for which he or she had responsibility within the previous year (Standard 1130.A1).

Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing acknowledges that the CAE may be asked to take on roles and responsibilities beyond internal auditing, such as compliance or risk management activities. The standard states that "Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence and objectivity." Safeguards are oversight activities, often undertaken by the board, to address potential impairments. If the CAE has responsibility for risk management or related functions, then assurance over those functions must be overseen by a party outside the internal audit activity (Standard 1130.A2).

Some organizations may view internal audit's role in developing risk management processes as consulting services, which should have no impact on its independence. However, Standard 1130.C1 and Standard 1130.C2 should be taken into account, and internal auditors should disclose potential impairments if they exist. Another option is creating separate audit teams, having one team work on risk management processes while another assesses the effectiveness of those processes. Yet another option is to allow internal auditors to develop the risk management processes with a plan to turn over the operation and oversight of those processes to trained personnel in the compliance/risk management/internal assurance functions or in line/operational management.

Assessing Organizational Risk Management

According to Standard 2200 – Engagement Planning, internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.

This section is intended to guide internal auditors through the process of planning and executing an assessment of organizational risk management. The examples provided, while not exhaustive, should help internal auditors determine the key areas to include, the type of documents that may be requested, and evidence that may be obtained.

It may be difficult to assess an entire risk management process; instead, the scope of the engagement can be defined using criteria that meets a specific objective. For example, the scope may be defined by organizational units, locations, strategic objectives, or by other criteria that is meaningful to the organization.

Understand the Context and Purpose of the Engagement

As illustrated in the risk management maturity model (**Figure 1**), definitive governance structures and processes usually support the risk management process in an organization with a risk-focused culture. Conversely, an organization may have no structures or processes devoted to risk management.

In an assessment of organizational risk management, an internal audit engagement consists of two parts: first identifying the principles at work in the organization's risk management process, and then evaluating whether those principles are appropriate and effective.

In planning the assessment, internal auditors should refer to the Implementation Guide for Standard 2120 – Risk Management and consider the following elements:

- The organization's strategic and business plans, missions, and objectives.
- Any risk management frameworks used within the organization.

Typical Engagement Planning Steps

- Understand the context and purpose of the engagement.
- Gather information to understand the area or process under review.
- Conduct a preliminary risk assessment of the area or process under review.
- Establish engagement objectives.
- Establish engagement scope.
- Allocate resources.
- Document the work program.

The IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope" provides detailed guidance on how to plan and scope an audit engagement.

- Current methods and level of identification, assessment, and provision of oversight for risks.
- Processes that could be used to monitor, assess, and respond to risks and opportunities.
- Sophistication of the organization and its risk management processes, considering its size, complexity, life cycle, maturity, stakeholder structure, and legal and competitive environment.
- Robustness of risk management roles, responsibilities, and activities across the organization.
- Current results of risk monitoring activities, and identify and discuss risks and corresponding responses that have been chosen.
- Historically experienced risks.
- Any changes (regulations, staffing, processes, or products and services) that may have introduced new risks.
- Potential risk exposures and opportunities; including new developments, trends, emerging risks, and potential disruptions related to the organization (and its jurisdiction and industry).
- Any regulatory or other external requirements/expectations relevant to the organization and the jurisdictions within which it operates.
- Stakeholder expectations for the internal audit activity to provide assurance that the organization's risk management process is effective.

A key issue for the internal audit activity to explore is whether management has articulated objectives for risk management. Internal auditors should seek evidence that management is executing activities to accomplish those objectives. Also, internal auditors should gain clarity on, among other things, management's vision for the risk management process, their plans, and measurement methodologies they employ.

While developing the individual engagement plan, internal auditors gather information through procedures such as reviewing prior assessments (e.g., risk assessments, reports by assurance and consulting service providers), understanding and mapping of risk management process flows and controls, and interviewing relevant stakeholders. The information acquired through planning should be well documented, promptly updated, and taken into account throughout the engagement. The information may also be useful in the CAE's long-range planning for future engagements.

Gather Information to Understand the Risk Management Process

Once internal auditors have identified the departments, functions, and roles in the organization that are relevant to the engagement, they should gather information to support a preliminary risk assessment and plan the engagement, as outlined in Standard 2201 – Planning Considerations.

The following elements can help internal auditors identify the organization's risks and the strategies used to manage those risks:

- Charters, policies, and other mandate information for the governance entities responsible for establishing the risk management strategy.
- Risk management process documentation including policies, guidelines, and standards.
- Risk appetite statement(s).
- Strategy documents.
- Control reports or other management reports that contain performance information.
- Minutes of meetings of board/audit committee and other relevant committees (e.g., risk committee).
- Business cases for significant capital projects.
- Periodic external reports (i.e., 10K statements of public companies).
- Management's risk assessments.
- The organization's risk inventory including strategic, operational, human resources, financial, regulatory compliance, and IT risks.
- Documentation of all phases of the risk management process including risk identification, assessment, treatment, and monitoring.
- Results of risk monitoring activities.

As noted in The IIA's Practice Guide "Coordination and Reliance: Developing an Assurance Map," risk management in an organization is everyone's responsibility; therefore, risk information should be available in all business areas, though it may not be officially documented or readily apparent. Sometimes, risks can be overtly assessed, such as during strategic planning. However, risks may be identified in less obvious places, such as being cited in business cases (e.g., "This project may generate less revenue than desired because of these factors…."). To identify as many risks as possible, internal auditors should use more than just previous engagement reports or assessments limited to obvious risks.

Audit Consideration

Internal auditors may choose to assess risk management processes either in the context of individual engagements within the internal audit plan or as part of a special assessment of processes identified as risk related.

The IIA Practice Guide "Coordination and Reliance: Developing an Assurance Map" may help internal auditors to identify risk-related processes.

Conduct a Preliminary Risk Assessment

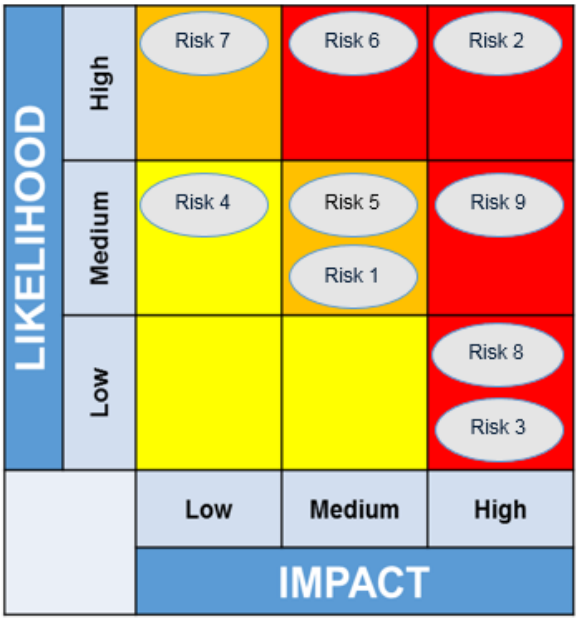
Standard 2210.A1 states that "Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review." The approach to assessing the risks associated with an organization's risk management process often differs from the approach to preliminary risk assessments conducted when planning other types of engagements.

An effective way to perform and document an engagement-level risk assessment is to create a risk matrix listing the relevant risks and then expand the matrix to include measures of significance. The format of the matrix may vary but typically includes a row for each risk and a column for each risk measure, such as impact and likelihood.

In organizations that have a mature and extensive risk management process, the internal audit activity may be able to review and use management's risk assessment, rather than having to recreate one. By tying the assessment of the risk management process to the maturity model, internal auditors make clear that the risk assessment is a key element in determining risk management maturity. If management has not already done so, internal auditors may develop a list of risks to the risk management process that fall into the maturity model categories of culture, governance, and process (See Appendix D for an example of a risk and control matrix that includes these categories). Those risks can then be rated in terms of impact and likelihood. A heat map, such as the example in **Figure 3**, is one tool used to visually represent risk significance on a simple scale of high, medium, and low.

In addition, the heat map may be retained as documented support of the engagement plan and work program, in conformance with Standard 2240 – Engagement Work Program.

Figure 3: Heat Map



Establish Engagement Objectives

Standard 2210 – Engagement Objectives states that "Objectives must be established for each engagement." Assurance standards 2210.A1 and 2210.A2 add that assurance engagement objectives must reflect the results of a preliminary risk assessment and must consider the probability (i.e., likelihood) of significant risk exposures including errors, fraud, and noncompliance.

The overall objective of an assessment of the organization's risk management process is typically to provide insight to senior management and the board regarding the maturity of the organization's risk management and whether it corresponds to their expectations. This type of assessment may also include benchmarking or comparison to best practices selected or endorsed by senior management and the board.

For an assurance engagement, according to Standard 2210.A3, adequate criteria are needed to evaluate risk management, and if internal auditors find that senior management and the board have already established adequate criteria (i.e., a risk management framework is in place), then that criteria should be used for the evaluation. If adequate evaluation criteria are not in place, then internal auditors work with management and/or the board to develop the measurements. Types of evaluative criteria may include:

- Internal (e.g., policies and procedures of the organization).
- External (e.g., laws and regulations imposed by statutory bodies).
- Leading practices (e.g., industry and professional guidance).

Internal auditors can adapt the previously introduced maturity model to reflect these criteria as appropriate to their organizations. External requirements may be combined with leading industry practices, integrated into the maturity model, and compared to the organization's internal policies and procedures.

For less mature organizations, a consulting engagement may be more appropriate, and the engagement objectives may be agreed upon with senior management and/or the board. In consulting engagements, the objective could be more advisory in nature; for example, to create awareness about the value of implementing more formal risk management processes.

Establish Engagement Scope

The CAE or internal auditors assigned by the CAE should be involved in meetings throughout the organization regarding risks and risk management, which may help drive the internal audit activity's approach to the assessment scope. As required by Standard 2220 – Engagement Scope, the scope must be sufficient to achieve the engagement objectives.

At a minimum, the scope of any assessment regarding risk management should confirm whether any identified risk-related processes are followed and comply with external criteria (e.g., laws, regulations, industry-related requirements). When scoping engagements, internal auditors may consider:

1. The sufficiency and operating effectiveness of the policies, procedures, and activities that support the risk management process, including alignment with the organization's risk appetite, stakeholder expectations, and industry standards.
2. The effectiveness of governance structures supporting the policies, procedures, and activities related to the risk management process.

3. The adequacy of resources dedicated to supporting the risk management process.
4. The inclusion of the following in the risk management process:

   - Clearly defined risk management and assurance roles and responsibilities throughout the organization.
   - Explicit consideration of risk in the strategy of the organization.
   - Risk lists/registers, risk-rating criteria, and risk assessment processes.
   - Expectations related to risk treatment.
   - Required reporting of risk exposures.
   - Processes for the classification, escalation, and tracking of findings that result from risk monitoring activities.

While all of these elements should be present in some form as part of the risk management process, internal auditors may customize the scope to fit the features and needs specific to the organization or the individual engagement.

Allocate Resources

Once an engagement's objectives and scope have been established, the CAE or the internal auditors assigned to the engagement must consider the engagement's nature and complexity, the time constraints, and the available resources and then determine whether the quantity of resources and mix of competencies available are sufficient to perform the engagement with due professional care (Standard 2230 – Engagement Resource Allocation).

To assess the effectiveness of a risk management process, internal auditors should know the requirements for risk management in the organization's industry as well as being familiar with a variety of risk and control frameworks and understanding the organization's culture and other soft controls in the organization's **control environment**.

Because assessing any organization's entire risk management process is a labor- and time-intensive exercise, the CAE should develop an engagement approach that is reasonable in terms of resources. To ensure resources are adequate, these engagements may be approached in several ways, as shown in **Figure 4**, depending on the structure of the organization. These examples are not exhaustive of those that may be appropriate.

Figure 4: Example of Engagement Approaches

Top-down Approach	
Most effective information-gathering method(s)	■ Interviews. ■ Document reviews.
Typical participants	■ Board members (e.g., audit committee and/or risk committee chairs). ■ Senior management. ■ Group/division management.
Limitations	■ Level of detail gathered is low. ■ The assessment may take on a governance focus as a function of the participant group. ■ The views of the board and senior management may not represent those of the rest of the organization, especially regarding culture.
Bottom-up Approach	
Most effective information-gathering method(s)	■ Interviews. ■ Surveys. ■ Document reviews. ■ Walk-throughs.
Typical participants	■ Line managers. ■ Supervisors.
Limitations	■ Surveys may generate confusion if they lack a common risk language or process. ■ Feedback may be inconsistently distributed across participants. ■ Many line managers and supervisors may be unable to participate due to time/resource restrictions (which may be indicative of the priority given to the risk management process).
Combination Approach	
Most effective information-gathering method(s)	■ Interviews (higher level personnel). ■ Surveys (lower level personnel). ■ Document reviews.
Typical participants	■ Board members (e.g., audit committee and/or risk committee chairs). ■ Senior management. ■ Group/division management. ■ Line managers.
Limitations	■ While this approach should provide a more comprehensive view, any of the previously mentioned limitations may still apply.

Document the Engagement Work Program

During planning, internal auditors document information in engagement workpapers. This information becomes part of the engagement work program that must be developed to achieve the engagement objectives (Standard 2240 – Engagement Work Program).

The process of establishing the engagement objectives and scope may produce any or all of the following workpapers:

- Process maps.
- Risk registers.
- Summary of interviews and surveys.
- Rationale for decisions regarding the organization's risk management maturity level.
- Criteria that will be used to assess the risk management process.

Perform the Engagement and Report the Results

Appendix E captures, at a general level, the activities that internal auditors may perform as part of an assessment of an organization's risk management process. The 2300 series of standards (Performing the Engagement) describes the requirements for identifying, analyzing, evaluating, and documenting sufficient information to achieve the engagement's objectives.

The engagement should culminate in recommendations appropriate to management's current and desired status according to the maturity model. Internal auditors should follow the internal audit activity's established procedures for communicating the results of the engagements, which are spelled out in the 2400 series of standards (Communicating Results) and associated implementation guides. Internal auditors should note that to conform with Standard 2410 – Criteria for Communicating and Standard 2410.A1, the final communication of engagement results must include the engagement's objectives, scope, results, applicable conclusions, recommendations, and/or action plans.

To conform with Standard 2440 – Disseminating Results, the CAE must ensure the results are communicated to the appropriate parties. For assessments of risk management processes, this may involve issuing a report to senior management, the board, and other parties they deem appropriate. Communications may be adapted for the audience receiving them.

Assess the Internal Audit Activity's Risk Management Process

To assess the efficiency and effectiveness of the internal audit activity and to identify opportunities for improvement, in conformance with Standard 1300 – Quality Assurance and Improvement Program, the CAE may apply lessons learned from the internal audit assessments of risk management throughout the organization. Applying a risk management maturity model (**Figure 1**) may help the CAE improve the internal audit activity's risk management process and work toward reaching higher levels of maturity across the spectrum of categories. Increasing maturity improves the internal audit activity's assurance and consulting service capabilities, enabling it to better protect and enhance organizational value.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency
Standards
Standard 1100 – Independence and Objectivity
Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing
Standard 1130 – Impairment to Independence and Objectivity
Standard 2050 – Coordination and Reliance
Standard 2120 – Risk Management
Standard 2200 – Engagement Planning
Standard 2201 – Planning Considerations
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program
Standard 2300 – Performing the Engagement
Standard 2400 – Communicating Results
Standard 2410 – Criteria for Communicating
Standard 2440 – Disseminating Results
Guidance
Practice Guide "Audit Reports: Communicating Audit Engagement Results," 2016.
Practice Guide "Coordination and Reliance: Developing an Assurance Map," 2018.
Practice Guide "Engagement Planning: Establishing Objectives and Scope," 2017.

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from the "Glossary" of *The IIA's International Professional Practices Framework*®, 2017 edition.

board* – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

chief audit executive* – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

control environment* – The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

internal audit activity* – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

maturity model – A gauge by which to measure an organization's current state of and progress toward mastery of a given area.

risk appetite* – The level of risk that an organization is willing to accept.

risk management* – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

Appendix C. Potential Risk Scenarios

To ensure organizational success and create value, all significant organizational risks, including the risk of missed opportunities, must be clearly understood, appropriately prioritized, and addressed. Properly assessing and providing assurance over the risk management process helps organizations implement suitable actions to prevent or address risk scenarios, such as those listed here, that may otherwise compromise their ability to achieve their goals and objectives:

- The independent assurance provided to the board and senior management is inadequate and leads to a false sense between both groups that risks are being managed within the organization's risk appetite and adequately support the organization's ability to achieve its objectives and strategies.
- Risk management governance, systems, and processes fail, resulting in poor corporate governance and related agency ratings, which are then communicated to stakeholders and the market.
- Preventable risk events occur, resulting in liabilities, fines, regulatory sanctions, and related exposures, as well as loss of assets, intellectual property, market share, revenue opportunities, customer loyalty, and brand reputation.
- Resource allocation and role assignments are not optimized; therefore, operationally sustainable risk management cannot be established.
- The organization's culture inhibits progress toward reaching a higher level of risk management maturity.
- Risks are either ignored, not prioritized properly, or not mitigated effectively, leading to the occurrence of risk events that prevent the achievement of business and organizational objectives and strategies.
- Timing constraints and opportunities are not met due to mismanagement of risks.
- Organizational priorities and strategies are not established with the proper awareness of risk or risk drivers behind the initiatives.
- IT, human resources, and funding risks are not considered and result in financial or operational losses or strategic failures.

Appendix D. Risk and Control Matrix

The following table lists some of the main risk areas and controls that internal auditors should consider when assessing the organization's risk management process. The list is neither exhaustive nor meant to be used as an engagement work program or checklist.

Culture Risks	
Risks	**Controls**
■ No resources have been allocated to expand risk management. ■ Risk is viewed as "owned" by the internal audit activity and control functions. ■ Scheduling interviews and receiving survey feedback timely is difficult. ■ Bad news does not travel upward in the organization. ■ The challenge to get whole organization on board is unanticipated or greater than anticipated. ■ The organization fails to recognize how people react to change. ■ The organization views risk management process as prescriptive. ■ The internal audit activity fails to effectively report and explain findings and risk ratings. ■ Management fears risk exposure. ■ Cultural traditions are opposed to risk management goals and objectives.	■ The internal audit activity conducts workshops or interviews to walk employees through the risk management process. ■ The board ensures effective tone at the top. ■ Confidential forums enable personnel to express cultural issues or blockages to communicating risk information. ■ Senior management encourages regular meetings and discussions and the exchange of information among all levels of management. ■ Management ensures that reporting risk information upward in the organization does not result in retaliation.
Governance Risks	
Risks	**Controls**
■ Entities (board, management, regulators) have disparate requirements for risk management. ■ There is no standard reporting system for risk management issues (e.g., timeliness, format). ■ Management does not talk about risk regularly in meetings. ■ The board does not perform its oversight role adequately.	■ Internal and external criteria for risk management are known and built into the process. ■ The organization invests in risk reporting software. ■ Board and senior management create demand for risk information throughout the organization.

Appendix D (continued)

Process Risks	
Risks	**Controls**
■ The risk assessment process is inconsistent across organization. ■ Too many risks are identified. ■ Risk outcomes are not monitored. ■ Impact and likelihood criteria differ, even for similar business lines. ■ Risk treatments are not reported beyond supervisor level. ■ The internal audit activity is the only entity completing an organizationwide risk assessment. ■ The risk management process involves language and terms that personnel do not understand. ■ The required level of quantification (in hard numbers) of risk exposure is not agreed upon. ■ The focus on emerging risks is insufficient.	■ The organization agrees on the risk management framework(s) to be used. ■ The organization invests resources in aggregating risk information and reporting at regular intervals. ■ Control functions (e.g., compliance; legal; environmental, health and safety) are well-trained in the risk assessment process and the risk management framework adopted by management. ■ A glossary of risk management related terms and a description of the risk assessment process are provided before risk assessments are conducted. ■ Impact and likelihood matrices are implemented consistently across the organization.

Appendix E. Assessing the Risk Management Process

At a general level, these tables describe activities that internal auditors may perform as part of an assessment of an organization's risk management process. These activities do not constitute a complete work program for such an assessment. Internal auditors may need to create more detailed analyses and test steps tailored to the policies and procedures that are unique to the organization. For a complete assessment of the risk management process, internal auditors may also need to create work programs specific to relevant areas (i.e., legal risk, compliance risk, strategic planning), especially if the assessment is broken down into smaller engagements as mentioned in this guide.

Risk Management Culture

Risk reporting

- Gather documentation including:
  - Charters, policies, and other mandated information for the governance entities responsible for establishing and overseeing the risk management process.
  - Documentation of all phases of the risk reporting process.
- Gain an understanding of the key risks identified as related to the organization's objectives.
- Determine whether risk reporting accurately communicates the status of risk exposure in the organization (e.g., is it too complicated, or is it too simple?).
- Rate risks in accordance with the organization's established risk assessment methodology.
- Review information obtained in the preliminary risk assessment to assess the impact and likelihood of risks related to risk culture.

Communication

- Follow risk reporting in various areas to ascertain whether risk information is communicated fluidly at all levels throughout the organization.
- Examine risk-related ethics and compliance investigations to determine whether retaliation for communicating risk information is a problem.
- Use surveys, interviews, or other methods to ascertain employees' participation in communication programs and their level of understanding of the organization's risk management objectives.

Accountability

- Confirm risk owners are held accountable for risk exposures in their sphere of authority.
- Confirm the board and senior management are held accountable for requesting and utilizing risk information in decision-making.

Appendix E (continued)

Risk Management Governance

Risk reporting

- Utilize reported risk information to assess culture and examine for appropriateness in terms of distribution, monitoring, and data retention.
- Review information obtained in the preliminary risk assessment to assess the impact and likelihood of risks related to risk management governance.

Board reporting

- Review risk-related reports that were prepared for the board. Ensure the reports contain all pertinent information needed by the board requires to make informed decisions.
- Review reports from senior management about the status of risk exposures in relation to strategies and risk appetite.

Risk appetite

- Review the organization's risk appetite profile for completeness and adequacy, including the following components:
  - Risk capacity: The maximum level of risk the organization can assume given its current obligations and constraints and its level of available resources.
  - Risk limits: The allocation of aggregate risk appetite limits to business lines, legal entities, specific risk categories, and other relevant granular levels.
  - Risk tolerance: The amount of variance the organization will accept around revenue and expenses, etc., given the parameters set for risk capacity and their associated risk limits.
- Review plans and processes to communicate the risk appetite to all employees.
- Ensure the plan covers the entire organization and is executed regularly.
- Use surveys, interviews, or other methods to ascertain both employees' participation in communication programs and their level of understanding regarding the organization's risk appetite.

Risk Management Process

Policies and procedures

- Verify that the policies and procedures are current and updated timely when procedural changes occur.
- Confirm that any updates requested by the board during the annual review have been made properly.
- Ensure the policies and procedures cover the entire risk management process in detail. Specific areas of importance include:
  - Relationship to strategies and risk appetite.
  - Governance overview.
  - Risk limits and tolerances with their associated triggers and escalation protocols (walk through the process from the identification of a breach to its resolution).
  - Roles and responsibilities.
  - Data considerations.
- Regulatory requirements.

Risk assessment process

- Identify where and how often risk assessments are conducted across the organization.
- Examine whether processes for risk identification, assessment, treatment, monitoring, and reporting are consistent.
- Review information obtained in the preliminary risk assessment to assess the impact and likelihood of risks related to risk management processes throughout the organization.

Appendix F. References and Additional Reading

References

International Professional Practices Framework (IPPF), 2017 edition. Lake Mary, FL: The Institute of Internal Auditors, 2017.

Additional Reading

Anderson, Richard J. and Mark L. Frigo. *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors.* Lake Mary, FL: Internal Audit Foundation, 2017. https://bookstore.theiia.org/assessing-and-managing-strategic-risks.

Anderson, Urton and Andrew J. Dahle. *Applying the International Professional Practices Framework, 4th Edition*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/applying-the-international-professional-practices-framework-4th-edition-2.

Baker, Larry L. *Practical Enterprise Risk Management: Getting to the Truth*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/practical-enterprise-risk-management-getting-to-the-truth.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *COSO Enterprise Risk Management – Integrating with Strategy and Performance*. COSO, 2017. https://bookstore.theiia.org/enterprise-risk-management-integrating-with-strategy-and-performance.

Committee of Sponsoring Organizations of the Treadway Commission. *COSO Enterprise Risk Management – Integrating with Strategy and Performance: Compendium of Examples*. PwC, 2018. https://bookstore.theiia.org/coso-enterprise-risk-management-integrating-with-strategy-and-performance-compendium-of-examples.

International Organization for Standardization (ISO). ISO 31000:2018, *Risk management – Guidelines*. ISO, 2018. https://www.iso.org/standard/65694.html.

Sobel, Paul J. *Auditor's Risk Management Guide: Integrating Auditing and ERM, 2015 Edition.* Wolters Kluwer, 2015.

Sobel, Paul J. *Managing Risk in Uncertain Times: Leveraging COSO's New ERM Framework.* Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/managing-risk-in-uncertain-times-2.

Acknowledgements

Guidance Development Team

Glenn Ho, CIA, CRMA, South Africa (Chairman)
Hans-Peter Lerchner, CIA, Austria (Project Lead)
Susan Haseley, CIA, United States
Rune Johannessen, CIA, CCSA, CRMA, Norway
Ian Lyall, CIA, CCSA, CGAP, CRMA, Australia
Michael Lynn, CRMA, United States
Denis Neukomm, CIA, CRMA, Switzerland

Global Guidance Contributors

Mohamed Ahmed Abdulla, Egypt
Lance Johnson, CIA, CRMA, United States
Cornelis Klumper, CIA, United States
Steven Nyakatuura, CFSA, South Africa
Tejinder Bob Shahi, CIA, Canada
Rita Thakkar, CIA, United States

IIA Global Standards and Guidance

Anne Mercer, CIA, CFSA, Director (Project Lead)
Jim Pelletier, CIA, CGAP, Vice President
Cassian Jae, Managing Director
Jeanette York, CCSA, FS Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

The IIA would like to thank the following oversight bodies for their support: Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

March 2019

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org