Assessing the Risk Management Process

2nd Edition

Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GENERAL GUIDANCE

Acknowledgements

Global 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 Council Reviewers

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

2nd Edition Reviewers

José Carlos Peñaloza Rojas, CIA, Peru
Tichaona Zororo, CIA, CRMA, South Africa
Ana Cristina Zambrano Preciado, CIA, CCSA, CRMA, Colombia

International Internal Audit Standards Board Reviewers

2nd Edition Reviewers

Fábio de Figueiredo Pimpão, CIA, CCSA, CRMA, Brazil
W. Charles Johnson, Jr., CIA, QIAL, CFSA, CGAP, CRMA, United States

IIA Global Standards and Guidance

Benito Ybarra, CIA, CFE, CISA, CCEP, Executive Vice President
Katleen Seeuws, CIA, CGAP, CRMA, CFE, CIAS, Vice President
Andrew Cook, CIA, Director (Project Lead)

The IIA thanks the following oversight bodies for their support: Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council.

About the IPPF

International Professional Practices Framework® (IPPF)

A framework provides a structural blueprint and coherent system that facilitate the consistent development, interpretation, and application of a body of knowledge useful to a discipline or profession. The International Professional Practices Framework® (IPPF)® organizes the authoritative body of knowledge, promulgated by The Institute of Internal Auditors, for the professional practice of internal auditing. The IPPF includes Global Internal Audit Standards™, Topical Requirements, and Global Guidance.

The IPPF addresses current internal audit practices while enabling practitioners and stakeholders globally to be flexible and responsive to the ongoing needs for high-quality internal auditing in diverse environments and organizations of different purposes, sizes, and structures.

Global Guidance

Global Guidance supports the Standards by providing nonmandatory information, advice, and best practices for performing internal audit services. It is endorsed by The IIA through formal review and approval processes.

Global Guidance provides detailed approaches, step-by-step processes, and examples on subjects including:

- Assurance and advisory services.
- Engagement planning, performance, and communication.
- Financial services.
- Fraud and other pervasive risks.
- Strategy and management of the internal audit function.
- Public sector.
- Sustainability.
- Global Technology Audit Guides® (GTAG®) provide auditors with the knowledge to perform assurance or advisory services related to an organization's information technology and information security risks and controls.

Global Guidance is available as a benefit of membership in The IIA.

Contents

Executive Summary

Globally, risk management initiatives and activities are required by regulators and rating agencies and expected by other stakeholders in major sectors and industries, including financial services, government, manufacturing, energy, health services, and more. However, risk management is driven by more than regulations and external forces. Managing risks efficiently and effectively benefits organizations of any type and size by helping them to achieve operational and strategic objectives and increase value and sustainability, ultimately better serving their stakeholders.

Standard 9.1 Understanding Governance, Risk Management, and Control Processes states: "To develop an effective internal audit strategy and plan, the chief audit executive must understand the organization's governance, risk management, and control processes." Benchmarking the current state of enterprise risk management against a risk management maturity model is a good place to start. Benchmarking may help the internal audit function communicate with the board and senior management about the maturity of the organization's risk management process and potential improvements. This information also enables internal auditors to tailor each engagement appropriately, considering the maturity of the activity 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

The **risk management** process generally encompasses the policies, procedures, and **control processes** that ensure the organization's **risks** are identified, assessed, treated, monitored, and reported adequately, timely, and continuously.

In many jurisdictions, the **board** is charged with ensuring the organization implements a risk management process that effectively respond to risks. The board may rely on the **internal audit function** to provide independent **assurance** that the organization's risk management process is effective. Standard 9.1 Understanding Governance, Risk Management, and Control Processes requires the **chief audit executive** to consider how the organization identifies and assesses significant risks and selects appropriate control processes. This includes understanding how the organization identifies and manages risks in key areas.

Note

Terms in **bold** are defined in the glossary in Appendix B.

The Global Internal Audit Standards use certain terms as defined in the glossary. To understand and implement the Standards correctly, it is necessary to understand and adopt the specific meanings and usage of the terms as described in the glossary.

The Standards use the word "must" in the Requirements sections and the words "should" and "may" to specify common and preferred practices in the Considerations for Implementation sections.

Assessing an organization's risk management process is a growing challenge because risk management standards, frameworks, and models are numerous and continue to be introduced.

This guide does not advocate the use of any particular risk management standards, framework, or model. Rather, it discusses the following common attributes of mature risk management:

- Risk culture: Risk considerations are integrated into all structures and processes for decision-making, compensation, rewards, and goal setting.
- Risk **governance**: Personnel who are competent in risk management participate in risk management processes throughout the organization.
- Risk management process: Aggregated risk identification, prioritization, assessment, treatment, monitoring, and reporting occur 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 process is effective and to contribute to its improvement.

This guide will help internal auditors to:

- Apply the Global Internal Audit Standards to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.
- Understand the benefits of assessing risk management activities.
- Understand the key components of an effective risk management process.
- Develop an assessment approach that considers the organization's business and regulatory environments and level of maturity.
- Collect the information needed to determine the scope of an **engagement** that assesses risk management activities.
- Evaluate the effectiveness of the risk management process.
- Contribute to the improvement of the risk management process.

Business Significance

Risk management plays 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.

The failure of risk management governance, systems, and processes may lead to liabilities, fines, sanctions, and related exposures as well as the inability to achieve organizational goals and objectives. 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, transferred, or treated). 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 of the difficulties involved in obtaining reliable data. It may be difficult for organizations to analyze the maturity of their own risk management process objectively.

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 and strategies via a common risk language.
- Enabling the documentation and timely reporting of risk management activities so the board and **senior management** are well informed of management's direction.
- Increasing the **likelihood** that the organization will meet its strategic and performance objectives.
- Enhancing the organization's ability to act on emerging opportunities.
- 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 function designs an assessment of the organization's risk management process, understanding the organization's level of risk management maturity and its risk culture is important to developing appropriate questioning. If the organization has yet to fully develop its risk culture, the internal audit function 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

Figure 1 is an example of a maturity model illustrating five stages, or levels, of risk management maturity. 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 risk culture may differ from that of its risk governance. When planning audit engagements, internal auditors may use a maturity model to appropriately tailor each engagement to the maturity of the element being considered.

Internal auditors should consider several elements when ascertaining an organization's position on the risk management maturity model and assessing the effectiveness of its risk management process.

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 2 or 3 may be acceptable. Each organization should determine which level of maturity is optimal for its circumstances.

Figure 1: Example of Risk Management Maturity Model

Stage	Culture	Governance	Process
1 – Initial	Risk belongs to the internal audit function.	chief audit executive board/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.	The board and senior management.	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.	The board and all levels of management.	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.

All organizations practice some form of risk management, though they may not be aware of it and may not formally document their efforts. The simplest form may be a "strategic risk assessment" through which senior management develops and documents a list of risks annually to create an organizational risk register at the top level. At the other end of the spectrum, organizations with a very robust or mature risk management process consider risk factors, including those related to risk culture and governance, across the organization in a systematic, structured format.

Risk Appetite

The Global Internal Audit Standards define **risk appetite** as the types and amount of risk that an organization is willing to accept in the pursuit of its strategies and objectives. 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 the board and/or senior management, 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 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 the board and management in prioritizing strategies and resource allocations addressing all risks including nonfinancial ones. 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 for making informed decisions consistently across the organization.

Structure: Roles and Responsibilities

How roles and responsibilities for risk management will be distributed across the organization depends upon the maturity of the organization's risk management process and the resources to which the internal audit function has access.

The continuum of risk management maturity may be described in stages, for example:

1 – Initial. In organizations where the risk management process is in the early stages of development, the internal audit function 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 function's risk assessments and risk-based assurance and advice.

2 – Repeatable. At this level, the internal audit function is better organized and resourced and plays an instrumental role by performing risk-based assessments, perhaps larger in scope. The

internal audit function 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 and efficiently and delivering actionable results that help the organization attain its 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 function may continue to operate functionally at the Repeatable level.

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

5 – Optimized. In organizations that have achieved this level of integration, sophistication, and maturity, line/operational management owns the risk management process. The compliance and 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 challenge the risk information as necessary. Risks are monitored and managed across various business processes.

The internal audit function provides independent assurance by performing engagements to assess the effectiveness of risk management processes in individual areas and throughout the entire organization. The internal audit function may compare its risk assessments to the risk information produced by management and verified by other internal assurance functions (compliance/risk management) to gauge the accuracy and completeness of management's assessment. Conversely, the internal audit function may use management's risk information to inform its own risk assessments, or it may do both. The chief audit executive must coordinate with internal and external providers of **assurance services** and consider relying upon their work (Standard 9.5 – 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."

Risk Culture

The effectiveness and comprehensiveness of a risk management process depend on the organization's risk culture. Culture can affect the intent of risk management policies and

procedures. For example, if the culture is not conducive to an open discussion about risk, one that considers negative and positive aspects, then appropriate conversations and actions may not be taken, causing the risk management process to fail.

Organizations may have sophisticated processes to measure and assess risk, yet the culture may not be conducive to mature 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 determine that the organizational culture does not support the effort of designing an effective risk management process, they should bring the issue to the chief audit executive, who can discuss the process's viability with the board and senior management. Successful implementation of the risk management process requires not only a supportive tone at the top but also management's understanding of its value.

Risk Governance

Achieving buy-in and proper resourcing for a risk management process starts with risk information being used in decision-making at the highest levels of an organization. The interest of high-level entities, such as the board (or more specifically, the audit committee), is critical to create demand for gathering, assessing, and providing risk information. If the audit committee regularly requests risk information as part of its supervisory role, management must find a way to provide it.

In general, the risk management process is developed from the top down, with the board and senior management first calling for risk assessments and reporting. This typically leads management to adopt the same practices to provide the risk information. 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.

Risk Management 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 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 available risk information, but terminology is not consistent or understood across the organization. Different risk registers and risk measurement criteria may exist, depending on the focus of the risk assessments. Risk measurement criteria are 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 board and senior management have addressed the organization's risk appetite, which is documented but not shared throughout the organization. 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 available risk information, but terminology is inconsistent across the organization. Risk registers and risk measurement criteria may differ, 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	The board and senior management have vaguely defined a risk appetite that 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 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 available risk information, 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.

4 – Managed	
Risk appetite	The board and senior management 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 address significant risks as they arise, rather than relying on a risk-based internal 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 are 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, senior management, and key members of management at various levels 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 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 the 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. 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 Auditing in Risk Management

Standard 9.1 Understanding Governance, Risk Management, and Control Processes describes the requirements for the chief audit executive to understand the organization's governance, risk management, and control processes. It requires the chief audit executive to consider how the organization:

- Establishes strategic objectives and makes strategic and operational decisions.
- Oversees risk management and control.
- Promotes an ethical culture.
- Delivers effective performance management and accountability.
- Structures its management and operating functions.
- Communicates risk and control information throughout the organization.
- Coordinates activities and communications among the board, internal and external providers of assurance services, and management.

Additionally, to gain a complete understanding of the organization's risk management and control processes, the chief audit executive must consider how the organization identifies and selects appropriate control processes, including how it manages four key risk areas:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws and/or regulations.

Standard 11.3 describes the requirements for the chief audit executive to communicate the **results of internal audit services** to the board and senior management. The results can include **engagement conclusions**, themes, and conclusions at the level of the business unit or organization. Standard 11.3 provides specific language for each type of communication.

To develop themes and conclusions about the organization's risk management process and its effectiveness, the chief audit executive may rely on information gathered during multiple engagements and may consider the results of these engagements cumulatively. The findings and conclusions of multiple engagements, when viewed holistically, may reveal patterns or trends. Internal auditors should look for patterns, trends, and gaps related to the effectiveness of the

risk management process and effectively communicate them to the board and senior management.

The internal audit function may be called upon to fulfill additional roles in risk management. Some organizations may want the internal audit function to develop the risk management process as an advisory service. If the internal audit function is asked to help develop the risk management process (e.g., conducting and documenting risk assessments), questions regarding internal auditors' **objectivity** may arise.

To be clear about appropriate roles, internal auditors should review Principle 2 Maintain Objectivity. Standard 2.1 Individual Objectivity states, "Internal auditors must be aware of and manage potential biases." Standard 2.2 Safeguarding Objectivity clearly defines requirements for maintaining objectivity under various circumstances and describes how to avoid actual, potential, or perceived impairments. For example, objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous 12 months.

If the internal audit function is to provide assurance services related to the risk management process it developed, the chief audit executive must assign resources in a way that manages individual objectivity. If impairments exist, internal auditors should disclose them, according to Standard 2.3 Disclosing Impairments to Objectivity.

To handle this situation, the chief audit executive could create separate audit teams, having one team work on the risk management process while another assesses its effectiveness. Another option is to allow internal auditors to develop the risk management process with a plan to turn over the operation and oversight of the process to trained personnel in the compliance/risk management/internal assurance functions or line/operational management.

Standard 7.1 Organizational Independence acknowledges that the chief audit executive may be asked to take on roles and responsibilities beyond **internal auditing**, such as compliance or risk management activities. The standard states that "When the chief audit executive has one or more ongoing roles beyond internal auditing, the responsibilities, nature of work, and established safeguards must be documented in the internal audit charter. If those areas of responsibility are subject to internal auditing, alternative processes to obtain assurance must be established, such as contracting with an objective, competent external assurance provider that reports independently to the board."

Assessing Enterprise Risk Management

According to Standard 13.3 Engagement Objectives and Scope, internal auditors must establish and document the objectives and scope for each engagement. The **engagement objectives** must articulate the purpose of the engagement and describe the specific goals to be achieved, including those mandated by laws and/or regulations. The scope must establish the engagement's focus and boundaries by specifying the activities, locations, processes, systems, components, period to be covered in the engagement, and other elements to be reviewed, and be sufficient to achieve the engagement objectives.

This section is intended to guide internal auditors through the process of planning and executing an assessment of enterprise 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 meet a specific objective. For example, the scope may be defined by organizational units, locations, strategic objectives, or other criteria that are 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.

Assessing enterprise risk management involves identifying the principles at work in the organization's risk management process and evaluating whether those principles are appropriate and effective.

Typical Engagement Planning Steps

- Understand the context and purpose of the engagement.
- Gather information to understand the **activity under review**.
- Conduct a preliminary risk assessment.
- 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.

In planning the assessment, internal auditors should consider the following elements:

- Sophistication of the organization and its risk management processes, considering the organization's size, complexity, life cycle, maturity, and stakeholder structure, along with the macro environment in which the organization operates.
- The organization's mission, strategic and business plans, and objectives.
- Current methods and processes for identifying, monitoring, assessing, and responding to risks, including relevant risk management frameworks.
- Methods for overseeing risk management.
- Robustness of risk management roles, responsibilities, and activities across the organization.
- Current results of risk monitoring activities and the identification and discussion of risks and corresponding responses.
- Historically experienced risks.
- Any changes (regulations, staffing, processes, or products and services) that may introduce new risks.
- Potential risk exposures, 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 function to provide assurance that the organization's risk management process is effective.

Internal auditors should understand management's vision for the risk management process and consider whether management has articulated relevant objectives and plans. Auditors should seek evidence that management is executing activities to achieve the objectives and should understand how outcomes are measured.

While developing the individual engagement plan, internal auditors gather information through procedures such as reviewing prior assessments (e.g., risk assessments and reports by assurance and advisory service providers), understanding and mapping risk management process flows and controls, and interviewing relevant stakeholders. The information acquired through planning should be well documented, promptly updated, and considered throughout the engagement. The information may also be useful in the chief audit executive'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 described in Standard 13.2 Engagement Risk Assessment.

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

- Charters, policies, and other mandated 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 board/audit committee meetings and other relevant committees (e.g., risk committee).
- Business cases for significant capital projects.
- Periodic external reports (such as published financial statements of public companies).
- Management's risk assessments.
- The organization's risk register 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.

Standard 9.1 also describes considerations and evidence of conformance related to understanding risk management processes.

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 business cases; for example, "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.

Conduct a Preliminary Risk Assessment

Standard 13.2 Engagement Risk Assessment states that "Internal auditors must develop an understanding of the activity under review to assess the relevant risks." 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.

Audit Consideration

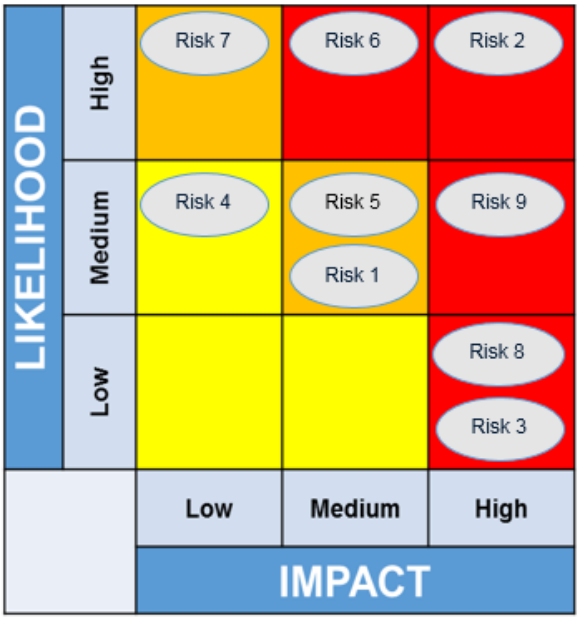
Internal auditors may choose to assess risk management processes either in the context of individual engagements within the **internal audit plan** or as part of a special assessment of processes identified as risk related.

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

In organizations that have a mature and extensive risk management process, the internal audit function 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 13.6 – Work Program.

Figure 3: Heat Map



Establish Engagement Objectives

Standard 13.3 Engagement Objectives and Scope states that "Internal auditors must establish and document the objectives and scope for each engagement. The **engagement objectives** must articulate the purpose of the engagement and describe the specific goals to be achieved, including those mandated by laws and/or regulations."

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

Standard 13.4 Evaluation Criteria requires internal auditors to use the most relevant **criteria** to evaluate whether objectives and goals have been accomplished. Internal auditors start by assessing whether the board and senior management have established such criteria. When evaluating risk management, internal auditors should determine whether a relevant risk management framework is in place to provide adequate criteria. If the criteria are inadequate, internal auditors must identify appropriate criteria through discussion with the board and/or senior management.

Types of evaluative criteria may include:

- Internal (policies, procedures, key performance indicators, or targets for the activity).
- External (laws, regulations, and contractual obligations).
- Authoritative practices (frameworks, standards, guidance, and benchmarks specific to an industry, activity, or profession).
- Established organizational practices.
- Expectations based on the design of a control.
- Procedures that may not be formally documented.

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 with the organization's internal policies and procedures.

For less mature organizations, an advisory engagement may be more appropriate, and the engagement objectives may be agreed upon with senior management and/or the board. For example, the objective of an advisory engagement may be to create awareness about the value of implementing more formal risk management processes.

Establish Engagement Scope

The chief audit executive or designated internal auditors should be involved in meetings throughout the organization regarding risks and risk management, which may help drive the

internal audit function's approach to the assessment scope. As required by Standard 13.3 Engagement Objectives and 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:

- The effectiveness of governance structures supporting the policies, procedures, and activities related to the risk management process.
- 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.
- The adequacy of resources dedicated to supporting the risk management process.
- 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 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 internal auditors assigned to the engagement must consider the engagement's nature and complexity, the time constraints, and the available resources. This will include determining whether the number of resources and mix of **competencies** available are sufficient to perform the engagement with due professional care (Standard 13.5 Engagement Resources).

To assess the effectiveness of a risk management process, internal auditors should know the requirements for risk management in the organization's industry. They should also be familiar with a variety of risk and control frameworks and understand the organization's culture and other soft controls in the organization's control environment.

Assessing any organization's entire risk management process is a labor- and time-intensive exercise. Therefore, the chief audit executive 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	• The 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 13.6 Work Program).

The process of establishing the engagement objectives and scope may produce any or all 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. Principle 14 Conduct Engagement Work 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 requirements for communicating the results of the engagements, which are spelled out in Principle 15 Communicate Engagement Results and Monitor Action Plans. Internal auditors should note that to conform with Standard 15.1 Final Engagement Communication, the final communication of **engagement results** must include the engagement's objectives, scope, recommendations and/or action plans, if applicable, and conclusions.

To conform with Standard 15.1 Final Engagement Communication, the chief audit executive must ensure the results are communicated to the parties that can ensure the results are given due consideration. Assessments of the risk management process may involve issuing a report to senior management, the board, and other appropriate parties. Communications may be adapted for the audience receiving them.

Assess the Internal Audit Function's Risk Management Process

To assess the efficiency and effectiveness of the internal audit function and to identify opportunities for improvement, in conformance with Standard 8.3 Quality, the chief audit executive 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 chief audit executive improve the internal audit function's risk management process and work toward reaching higher levels of maturity across the spectrum of categories. Increasing maturity improves the internal audit function's assurance and advisory service capabilities, enabling it to

better protect and enhance organizational value. The chief audit executive should also consider including internal audit risk management assessments in performance measurement to properly monitor progress and "promote the continuous improvement of the internal audit function" (Standard 12.2 Performance Measurement).

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide.

Standards
Standard 2.1 Individual Objectivity
Standard 2.2 Safeguarding Objectivity
Standard 2.3 Disclosing Impairments to Objectivity
Standard 7.1 Organizational Independence
Standard 8.3 Quality
Standard 9.1 Understanding Governance, Risk Management, and Control Processes
Standard 9.5 Coordination and Reliance
Standard 11.3 Communicating Results
Standard 12.2 Performance Measurement
Standard 13.2 Engagement Risk Assessment
Standard 13.3 Engagement Objectives and Scope
Standard 13.4 Evaluation Criteria
Standard 13.5 Engagement Resources
Standard 13.6 Work Program
Standard 15.1 Final Engagement Communication
Global Guidance
Practice Guide "Coordination and Reliance: Developing an Assurance Map"
Practice Guide "Engagement Planning: Establishing Objectives and Scope"

Appendix B. Glossary

Definitions are taken from the "Glossary" within The IIA's publication, *Global Internal Audit Standards*, *2024 edition*, unless otherwise noted.

activity under review – The subject of an internal audit engagement. Examples include an area, entity, operation, function, process, or system.

assurance – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria.

assurance services – Services through which internal auditors perform objective assessments to provide assurance. Examples of assurance services include compliance, financial, operational/performance, and technology engagements. Internal auditors may provide limited or reasonable assurance, depending on the nature, timing, and extent of procedures performed.

board – Highest-level body charged with governance, such as:

- A board of directors.
- An audit committee.
- A board of governors or trustees.
- A group of elected officials or political appointees.
- Another body that has authority over the relevant governance functions.

In an organization that has more than one governing body, "board" refers to the body/bodies authorized to provide the internal audit function with the appropriate authority, role, and responsibilities.

If none of the above exist, "board" should be read as referring to the group or person that acts as the organization's highest-level governing body. Examples include the head of the organization and senior management.

chief audit executive – The leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services in accordance with Global Internal Audit Standards. The specific job title and/or responsibilities may vary across organizations.

competency – Knowledge, skills, and abilities.

compliance – Adherence to laws, regulations, contracts, policies, procedures, and other requirements.

control – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

control processes – The policies, procedures, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance.

criteria – In an engagement, specifications of the desired state of the activity under review (also called "evaluation criteria").

engagement – A specific internal audit assignment or project that includes multiple tasks or activities designed to accomplish a specific set of related objectives. See also "assurance services" and "advisory services."

engagement conclusion – Internal auditors' professional judgment about engagement findings when viewed collectively. The engagement conclusion should indicate satisfactory or unsatisfactory performance.

engagement objectives – Statements that articulate the purpose of an engagement and describe the specific goals to be achieved.

engagement results – The findings and conclusion of an engagement. Engagement results may also include recommendations and/or agreed upon action plans.

engagement work program – A document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools necessary, and the internal auditors assigned to perform the tasks. The work program is based on information obtained during engagement planning.

finding – In an engagement, the determination that a gap exists between the evaluation criteria and the condition of the activity under review. Other terms, such as "observations," may be used.

governance – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

impact – The result or effect of an event. The event may have a positive or negative effect on the entity's strategy or business objectives.

internal audit charter – A formal document that includes the internal audit function's mandate, organizational position, reporting relationships, scope of work, types of services, and other specifications.

internal audit function – A professional individual or group responsible for providing an organization with assurance and advisory services.

internal audit plan – A document, developed by the chief audit executive, that identifies the engagements and other internal audit services anticipated to be provided during a given

period. The plan should be risk-based and dynamic, reflecting timely adjustments in response to changes affecting the organization.

internal auditing – An independent, objective assurance and advisory service designed to add value and improve an organization's operations. It 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.

likelihood – The possibility that a given event will occur.

methodologies – Policies, processes, and procedures established by the chief audit executive to guide the internal audit function and enhance its effectiveness.

objectivity – An unbiased mental attitude that allows internal auditors to make professional judgments, fulfill their responsibilities, and achieve the Purpose of Internal Auditing without compromise.

results of internal audit services – Outcomes, such as engagement conclusions, themes (such as effective practices or root causes), and conclusions at the level of the business unit or organization.

risk – The positive or negative effect of uncertainty on objectives.

risk and control matrix – A tool that facilitates the performance of internal auditing. It typically links business objectives, risks, control processes, and key information to support the internal audit process.

risk appetite – The types and amount of risk that an organization is willing to accept in the pursuit of its strategies and objectives.

risk assessment – The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed in terms of impact and likelihood.

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.

senior management – The highest level of executive management of an organization that is ultimately accountable to the board for executing the organization's strategic decisions, typically a group of persons that includes the chief executive officer or head of the organization.

significance – The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

stakeholder – A party with a direct or indirect interest in an organization's activities and outcomes. Stakeholders may include the board, management, employees, customers,

vendors, shareholders, regulatory agencies, financial institutions, external auditors, the public, and others.

workpapers – Documentation of the internal audit work done when planning and performing engagements. The documentation provides the supporting information for engagement findings and conclusions.

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 function 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 the whole organization on board is unanticipated or greater than anticipated. • The organization fails to recognize how people react to change. • The organization views the risk management process as prescriptive. • The internal audit function 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 function 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.

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 function 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 engagement 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 engagement 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.

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: Acceptable variations in performance related to achieving objectives.
- 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. Additional Reading

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *COSO Enterprise Risk Management – Integrating with Strategy and Performance*. COSO, 2017. https://www.theiia.org/en/products/bookstore/coso-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://www.theiia.org/en/products/bookstore/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.

Page, W. Scott. "Global Knowledge Brief: Governance, Risk, and Control, Part 1: Rethinking Risk Appetite from a Non-Financial Risk Perspective," The IIA, 2023. https://www.theiia.org/globalassets/site/content/articles/global-knowledge-brief/2023/grc_part_1_risk_appetite.pdf.

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

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 245,000 global members and has awarded more than 195,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance.

For more information, visit theiia.org.

Disclaimer

Copyright

July 2024 (This version supersedes "Auditing the Risk Management Process," published in 2019.)

The Institute of Internal Auditors

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