Coordination and Reliance

Developing an Assurance Map

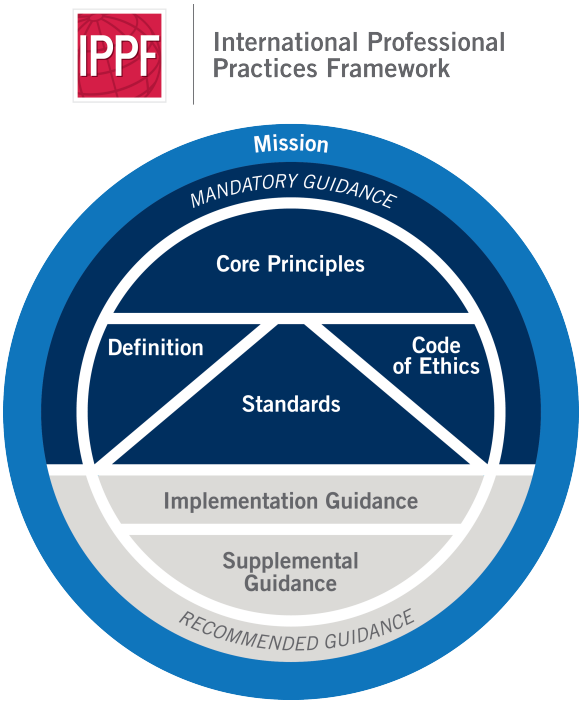
The Institute of Internal Auditors | Global

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA. A trustworthy, global, guidance-setting body, The IIA provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as Mandatory Guidance and Recommended Guidance.

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*.



About Supplemental Guidance

Supplemental Guidance is part of the IPPF and provides additional recommended, nonmandatory guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is intended to address topical areas, as well as sector-specific issues, in greater procedural detail than the *Standards* or Implementation Guides. Supplemental Guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed step-by-step approaches, featuring processes, procedures, tools, and programs, as well as examples of deliverables.

Practice Guides are intended to support internal auditors. Practice Guides are also available to support:

- 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

One of the key responsibilities of a board of directors is to obtain assurance that an organization's processes operate within the parameters established to achieve the defined objectives. This occurs when risk management processes are working effectively, addressing significant risks to acceptable levels. The board relies on information from multiple providers of assurance services, including internal providers (e.g., risk management, compliance, and other control functions as well as the internal audit activity) and external providers (e.g., external auditors and consultants).

An assurance map is a matrix comprising a visual representation of the organization's risks and all the internal and external providers of assurance services that cover those risks. This visual depiction exposes coverage gaps and duplications. Assurance providers may use the map to coordinate the timing and scope of their services, preventing audit fatigue within areas and processes under review, except in cases where senior management or the board may need a second opinion or a double check from another assurance provider on a high risk area.

An assurance map would be used by various departments throughout the organization as follows:

- Internal audit may use an assurance map as a basis for discussion to determine whether reliance on the work of other assurance providers would be appropriate.
- Senior management may use the map to ensure that risk management and internal control functions are properly aligned and effectively monitored.

Thus, an assurance map can enhance a comprehensive, organizationwide risk management process, advance the maturity of assurance functions, and strengthen the control environment.

The primary purpose of this practice guide is to assist internal auditors in developing an assurance map to document assurance coverage and enable efficient use of assurance resources through minimizing duplication of efforts.

Introduction

Various providers of **assurance services** contribute to an overall, organizationwide risk and control structure, together assuring that **risks** are identified and addressed to an acceptable level. However, the providers differ in their reporting responsibilities, their level of **independence** from the activities over which they provide assurance, and the reliability of the assurance provided.

Note: Terms in bold are defined in the glossary at the end of this practice guide.

With the responsibility for assurance activities shared among the three lines of defense[1], it is important for the organization to document assurance activities. A clear understanding of risk coverage throughout the organization can provide benefits, including reduced duplication of effort among assurance providers and avoidance of audit fatigue among auditable entities. If assurance coverage is inadequate, significant risks may be overlooked or misjudged. By coordinating and aligning their risk coverage, assurance providers can build a robust assurance framework. The mandate to prepare an assurance map may come from senior management or the **board**; specifically, audit or risk committees or through self-initiative of internal audit.

Developing an Assurance Map

The development of an assurance map should be a collaborative effort, involving each assurance service provider. Internal audit may have the best perspective to initiate the creation of a holistic, organizationwide assurance map. Once the map is created, it may reside in whatever assurance function is most appropriate for the organization. Any of the risk management functions — risk management, compliance, legal, finance, or internal audit — would be suited to maintain the assurance map.

Assurance Activities

The purpose of assurance activities is to provide an objective examination of evidence from an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Since internal audit is the most likely function to utilize the assurance map in its audit planning, it would follow that they are the most logical entity to task with the responsibility of creating and maintaining the assurance map. Other assurance providers are not as likely to utilize the map in their planning activities, as their activities are largely mandatory assessments required by regulation or some other external entity. If the organization has an Enterprise Risk Management

[1] IIA Position Paper, "The Three Lines of Defense in Effective Risk Management and Control," Jan. 2013.

function or an active Strategic Planning function involved in annual risk assessment activities, these functions may be additional logical homes for the assurance map.

In its simplest form, an assurance map may be formatted as a matrix that lists the organization's risk categories in the first column, with additional column headings for each assurance provider, enabling assurance coverage for each risk category to be identified throughout the organization. The assurance map may be as simple or as complicated as suits the organization; however, the key steps to constructing an assurance map remain consistent irrespective of the design.

Assurance mapping steps include:

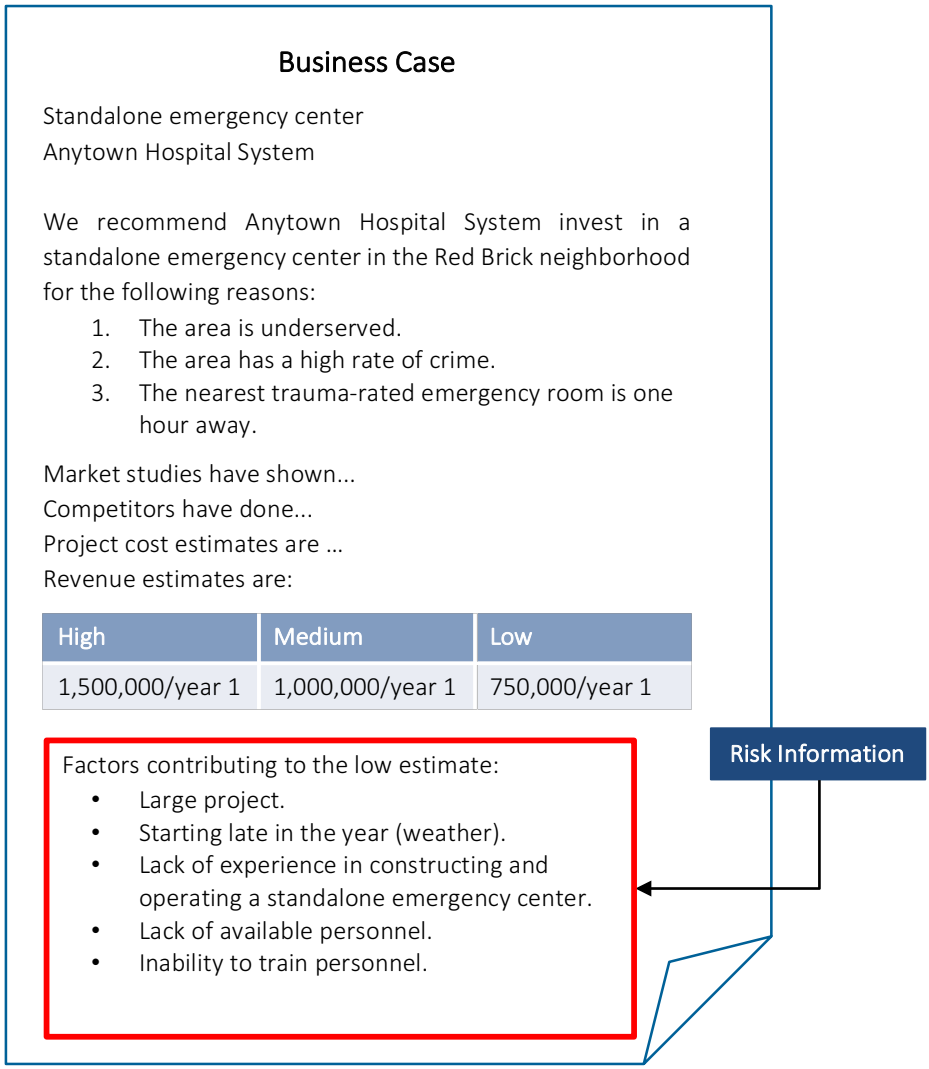
1. Identifying sources of risk information.
2. Organizing risks into risk categories for consolidated viewing.
3. Identifying assurance providers.
4. Gathering information and documenting assurance activities by risk category.
5. Periodically reviewing, monitoring, and updating the assurance map.

Identify Sources of Risk Information

Risk management in an organization is everyone's responsibility; therefore, risk information will be present in nearly all areas whether it looks like risk information or not. Risks can be overtly assessed in processes such as strategic planning. They can be cited in business cases (e.g., "this project may generate less revenue than desired because of these factors…."), as shown in **Figure 1**. Internal auditors should avail themselves to more than just audit reports or obvious assessments of risks. Key documents in an organization to be reviewed could include:

- **Risk appetite** statement(s).
- Strategy documents.
- Risk assessments.
- Policies.
- Control reports or other management reports that contain performance information.
- Board minutes.
- Audit committee minutes.
- Business cases for significant capital projects.
- Periodic reports (e.g., 10K statements of public companies).

Figure 1: Sample Business Case



Internal audit should rely on more than its own experience to identify risk information. While internal audit's auditable risk universe is useful, it may fail to offer a complete picture of an organization's significant risks. Developing an assurance map is meant to be a collaborative process; therefore, internal auditors should involve personnel from management and relevant control functions at an early stage.

Organize Risks into Risk Categories

All the risks that could occur within an organization may collectively be called the risk universe. There are myriad perspectives and measures of risks, many of which are unique to individual business units or functions in the organization. To avoid gaps or duplication in the provision of assurance to the board, however, the organization's risks must be organized in a way that enables a holistic, cohesive overview. Organizations often categorize risks according to business functions,

units, processes, or programs, and some may employ an organizationwide risk management framework. (See Appendix C for a list of potential frameworks to guide this process if one is not in use at your organization.)

At a high level, risk categories should align with the organization's strategic objectives. Additional risk categories may cover operational areas or processes, and compliance and reporting risks. This ensures that all significant areas are included. Regardless of the approach used, individual risks must be categorized to summarize the information and make it accessible for reporting to the board and senior management as needed.

As described above, the first column of an assurance map typically lists categories of risks that have been identified from risk assessments throughout the organization, as shown in Figure 2. If neither a formal risk assessment and reporting system nor a common perspective on risks exists, then assurance providers should meet to develop a shared understanding and agree on the risk categories.

Figure 2: Sample of Risk Categories

Strategic	
	Crisis Management
	Competitive Environment
	Resource Allocation
	…
Operational	
	Product Quality
	Production Capacity
	Suppliers & Key Relationships
	…
Human Resources	
	Succession Planning
	Training
	Turnover
	…
Financial	
	Financial Reporting
	Accounts Payable
	Accounts Receivable
	…
Regulatory Compliance & Reporting	
	Disclosure
	Environmental
	Information Privacy
	…
Technology	
	Data Security
	Hardware Availability & Effectiveness
	Software Usability & Efficiency
	…

Identify Assurance Service Providers

A concept that may assist internal audit in identifying assurance providers within their organization is the Three Lines of Defense model, which distinguishes sources of risk management into three main internal groups (or lines of defense) based on essential roles and responsibilities. The first two lines of defense include internal risk owners who report to senior management. The third line of defense — the internal audit activity — has a dual reporting relationship to senior management and the board. Additional assurance services may be provided by external sources such as consultants.

First Line of Defense – Operational Management

Operational management, or line management, is responsible for maintaining effective internal controls within the systems and processes. As the "risk owners," this group ensures that business risks are addressed and business objectives are met.

This line of defense may lack independence and objectivity but provides valuable input as it reflects insights from the personnel closest to the business and daily challenges. This risk owner should assist with populating the assurance map relevant to their roles and responsibilities. Internal audit should communicate with senior management if risk owners cannot be identified for any key risks.

Senior management can be confident that the first line is fulfilling its responsibilities to manage risks through the development and implementation of good policies and practices, performance metrics, and/or dashboards, which can be updated and monitored according to the organization's risk appetite. Coupled with the assurance opinions provided by the second and third lines of defense, this forms the basis for a comprehensive risk management program. The management tools that provide useful information to risk owners are also useful to incorporate into assurance maps.

Second Line of Defense – Risk and Compliance

The organization's risk and compliance functions provide oversight of management activities performed by the first line of defense. Risk and compliance functions also provide assurance that regulatory, environmental, ethical, and quality requirements, and perhaps others, are met. Compliance functions monitor regulatory requirements related to health and safety, the environment, supply chains, etc. Second line activities could also include assessing the accuracy and completeness of reports provided by the first line of defense and reviewing automated monitoring processes and organizational databases.

Functions that provide second line assurance typically are more objective than operational management, but they are still part of management, and therefore, they are not organizationally independent. Information from risk areas covered by second line functions, including the results of their evaluations and the extent and quality of their work, provide valuable input for the assurance map and help internal auditors evaluate how well the assurance activities are managed.

Third Line of Defense – Internal Audit Activity

As the third line of defense, the internal audit activity provides senior management and the board with an independent and objective assessment of the organization's governance, risk management, and control processes and contributes to the improvement of those processes (Standard 2100 – Nature of Work). In conformance with Standard 1000 – Purpose, Authority, and Responsibility, and Implementation Standards 1000.A1 and 1000.C1, the nature of assurance and consulting services are defined in the internal audit charter, which is approved by senior management and the board. In creating the internal audit charter, the chief audit executive (CAE) works with senior management and the board to determine their assurance needs.

External consultants and specialists:

- Risk management consultants.
- Law firms.
- CPA/accounting firms.
- Finance/forensic accounting specialists.
- Environmental, health, and safety consultants.
- Information Technology consultants (benchmarking, software vendors, virus protection, maintenance).
- Market consultants.
- Joint venture partners.
- Private security monitoring.

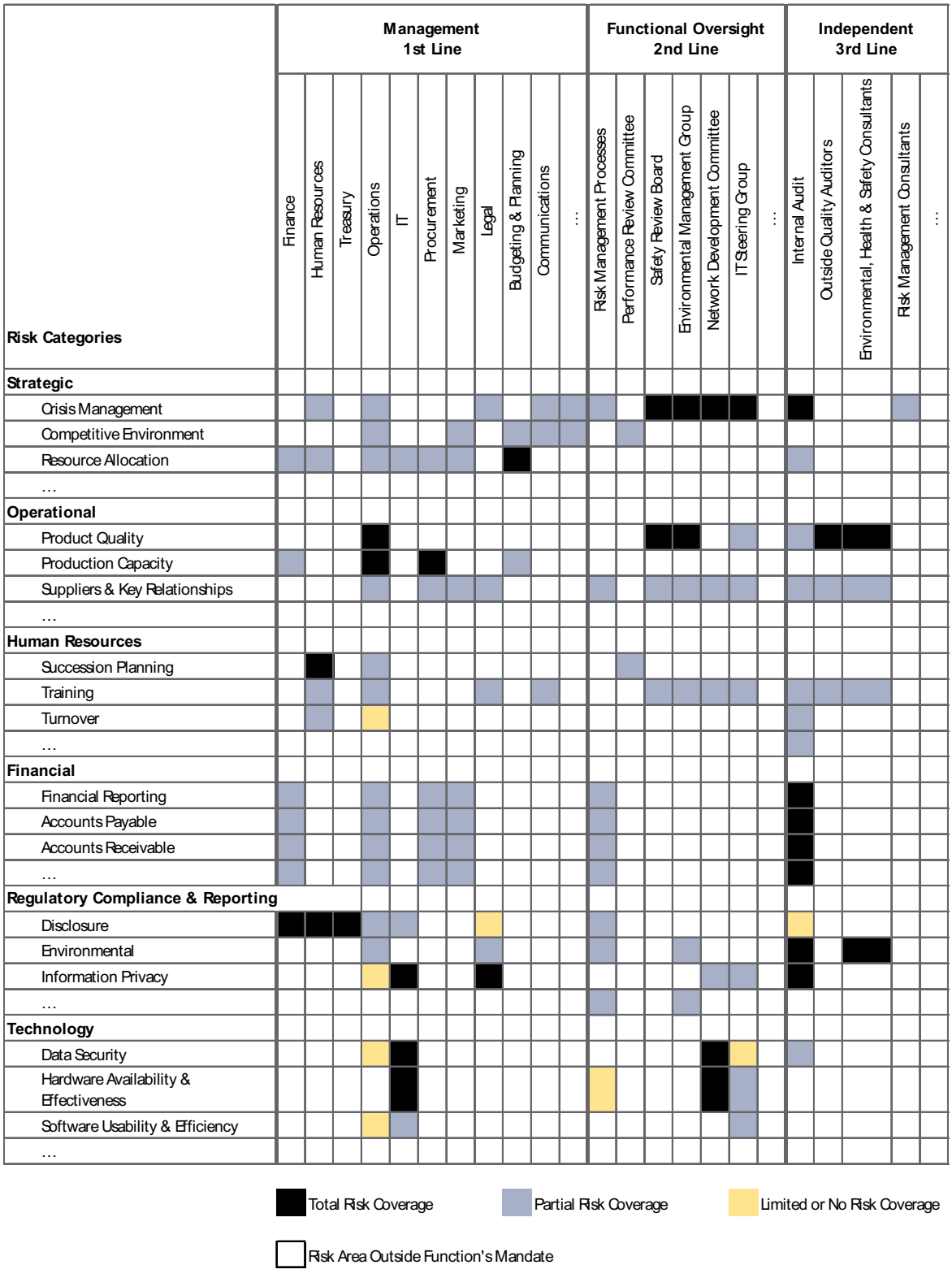
External Providers of Assurance Services

An organization may engage various external consultants and specialists to provide assurance in areas as required by regulation or because they require an outside opinion. These consultants may have vital risk information and/or they may need to be included in the assurance map. Internal audit should investigate the organization's use of external assurance providers and determine to what extent the external assurance provider's activities should be included in the assurance map.

Gather Information and Document Assurance Coverage

With the risk categories listed in the first column of the assurance map, additional columns are created to document assurance coverage by each provider of assurance services. Internal audit may find it helpful to organize the columns into internal providers and external providers and further group those providers using the Three Lines of Defense model, as shown in Figure 3. Visually, these groupings give a general indication of each provider's level of independence. This information may assist the CAE later in engagement planning.

Figure 3: Sample Assurance Map



The party responsible for creating the map should meet with the risk owners and assurance providers to validate the risks they cover and to fill any gaps in the risk information gathered. Ideally, each assurance provider contributes information to complete their own column on the map, describing the services they perform related to each risk category. Internal audit should avoid speculating on other assurance providers' mandate and risk coverage.

Periodically Review and Update the Assurance Map

Risks, risk management, and the assurance process are continuous and dynamic, and the assurance map should reflect this. The organization should adopt a maintenance process for regularly reviewing and updating the assurance map with input from all internal and external assurance providers. Events may change the assurance map, including:

- Mergers and acquisitions.
- Introduction of a new product line.
- Economic changes.
- Regulatory changes.
- Changes in consumer behavior.

If internal audit owns the assurance map, it should ensure that the map is updated at least annually. Internal audit may also want to request or initiate a revision of the map if significant changes are identified. This will help ensure the assurance map remains useful to the organization.

Uses for Assurance Maps

Assurance maps are useful tools for many areas of an organization, including internal audit. A complete and updated assurance map supports:

- A shared understanding of the risks faced by an organization aligned by risk categories.
- Identification of the organization's risk management and assurance roles/functions.
- Development of a holistic, comprehensive assurance framework, which can be useful during times of transition, such as mergers and acquisitions, restructuring, or assessing and changing business strategies.
- Collaboration among assurance providers to facilitate the efficient and effective use of resources.

Within the internal audit activity, the CAE may find the assurance map to be a useful tool to communicate the reasoning behind the audit plan to senior management and the board.

In conformance with Standard 2050 – Coordination and Reliance, the CAE may also establish a process and criteria for determining whether the internal audit activity can rely on the work of

another assurance provider, instead of duplicating the work. The CAE may decide to rely on the work of other internal or external assurance providers for a variety of reasons, including:

- To address areas that fall outside of the skill sets found in the internal audit activity.
- To gain knowledge from other assurance providers.
- To effectively enhance coverage of risk beyond the internal audit plan.

However, as noted in Standard 2050 – Coordination and Reliance, the CAE should carefully consider the competency, objectivity, and due professional care of the other providers, as well as clearly understanding the scope, objectives, and results of their work, because the CAE retains the responsibility for ensuring adequate support exists for the conclusions and opinions reached by the internal audit activity. An assurance map may serve as the first step in developing a plan for reliance.

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.

Standards
Standard 1000 – Purpose, Authority and Responsibility
Standard 2050 – Coordination and Reliance
Standard 2100 – Nature of Work
Guidance
Practice Guide, "Reliance by Internal Audit on Other Assurance Providers," 2011.
Practice Guide, "Internal Audit and the Second Line of Defense," 2016.
Other IIA Resources
IIA Position Paper*: The Three Lines of Defense in Effective Risk Management and Control*, 2013.

Appendix B. Glossary

Terms are taken from The IIA's International Professional Practices Framework Glossary.

Assurance Services – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

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 may 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).

Consulting Services – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Independence – The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

Objectivity – An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

Risk – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk Appetite – The level of risk that an organization is willing to accept.

Appendix C. Risk Frameworks

When developing an assurance map, internal auditors may need to refer to a risk framework to assist them in identifying and categorizing risk information. Organizations that produce risk frameworks include:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Integrated Framework.
- National Institute of Standards and Technology (NIST).
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC).
- ISACA.

Acknowledgements

Guidance Development Team

Glenn Ho, CIA, CRMA, South Africa (Chairman)

Alp Buluc, CIA, CCSA, CRMA, Turkey (Project Lead)

Global Guidance Contributors

Rune Johannessen, CIA, CCSA, CRMA, Norway

Hans Lofgren, Sweden

Sally Anne Pitt, CIA, CGAP, Australia

Bruce Turner, CGAP, CRMA, Australia

Benito Ybarra, CIA, United States

IIA Global Standards and Guidance

Anne Mercer, CIA, CFSA, Director (Project Lead)

Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President

Eva Sweet, CISA, CISM, IT and PS Director

Jeanette York, CCSA, FS Director

Debi Roth, CIA, Managing 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 are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

January 2018

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