Chapter 1
Overview of the Enterprise Risk Management Publication

I. Introduction

Every organization[1] exists for the purpose of creating value for its stakeholders. To create value, an organization sets objectives, develops strategies, and plans for pursuing them, and performs actions. However, strategies, plans, and actions alone do not guarantee a desired outcome. Events and circumstances could affect the execution of these strategies and plans. Management is faced with the challenge of dealing with the uncertainties surrounding the achievement of its objectives. Enterprise risk management (ERM) is a process that enables management to address these uncertainties in a comprehensive, integrated, and organization-wide manner in order to create value. By implementing and maintaining an effective ERM program, management teams and the governing bodies of those organizations can increase their confidence that the organization can be successful in achieving its objectives. Customers, vendors, regulators, rating agencies, and other stakeholders are increasingly interested in understanding an organization's ERM process and may base decisions regarding their interactions with the organization on the perceived sophistication and effectiveness of the ERM process.

This publication is intended to help those responsible for an ERM program, whether the program is in its early stages or is already well established, to design and operate an effective ERM program.

To begin, it is helpful to understand what an ERM program encompasses and how it is defined. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its 2017 *Enterprise Risk Management—Integrating with Strategy and Performance* publication, defines ERM as follows:

> The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

In comparison, the International Standardization Organization (ISO) 31000, *Risk Management—Guidelines*, defines risk management as ”coordinated activities to direct and control an organization with regard to risk” and further explains a risk management process as a ”systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.”

For purpose of this publication, an *ERM Program* is defined as an organization's ERM culture, capabilities, and practices, including its people, structures, governance mechanisms, documents, values and incentives, data, and supporting technologies that allow an organization to operationalize and execute its end-to-end ERM programs. Many organizations are challenged with the initial design and implementation of such an enterprise-wide risk management process and program and with maintaining and improving them over time so that they continue to operate effectively and add value.

Thus, the purpose of this publication is to leverage these two existing conceptual frameworks and provide practical guidance for designing and implementing a new ERM program along with the policies and procedures that define an entire ERM program, or for assessing and improving an existing program. This publication intends to serve as a bridge between the substantial, conceptual guidance that exists today and the practical realities of creating and sustaining a successful ERM program.

[1] **organization**. Any form of for-profit, not-for-profit, or governmental body. An organization may be publicly listed, privately owned, owned through a cooperative structure, or any other legal structure.

II. Who Should Use This Publication

This publication is intended for practitioners who are implementing a new ERM program or improving an existing program. This publication provides a summary of the concepts and components of a successful ERM program and provides a maturity matrix and self-assessment guidance that may be helpful for practitioners who are implementing or improving an ERM program. This publication may also be helpful to third parties who have been asked to provide an evaluation or assessment of an ERM program, such as auditors, compliance specialists, consultants, or other mandated parties. Internal or external auditors in particular may be called upon to independently evaluate the effectiveness of the organization's ERM program and to make meaningful recommendations for improving or enhancing the program.

The ERM concepts, components, and examples presented in this publication are intended to be industry agnostic and applicable to organizations of many sizes and types — including public, private, not-for-profit, and government organizations. An ERM program, however, may vary significantly by industry and organization, and aspects of this publication may be more useful to some organizations than others. Careful consideration should be given to the specific circumstances of each individual organization to ensure that the targeted ERM program is well-suited for the organization.

III. Conceptual Basis for This Publication

The concepts used in this publication are primarily developed based on two of the most well-known risk management frameworks, the COSO *Enterprise Risk Management—Integrating with Strategy and Performance* framework (the COSO ERM framework) and the ISO 31000 *Risk Management—Guidelines* (the ISO 31000 framework). This publication does not create a new framework but leverages the foundational concepts of these existing frameworks. To begin, this publication highlights overarching concepts of ERM, which are foundational to the ERM process and to the rest of this publication. In subsequent sections, the publication discusses in greater detail these concepts and the ERM process by leveraging COSO's framework of components and principles with comparisons to the ISO 31000 framework. A more detailed mapping of COSO ERM framework components and ISO's 31000 framework can be found in appendix A, "COSO and ISO 31000 Framework Mapping."

About the COSO and ISO Risk Management Frameworks

The June 2017 COSO *Enterprise Risk Management—Integrating with Strategy and Performance* publication provides guidance on the broader subject of enterprise risk by defining and explaining key ERM concepts, components, and principles.

The ISO 31000 *Risk Management—Guidelines of 2018* provides principles, framework, and process guidelines on managing risks faced by organizations. The document includes an approach for managing different types of risks and can be applied to any activity at all levels of an organization.