APPENDIX 2.1

ERM FRAMEWORKS

There are various frameworks that can be considered when determining the appropriate approach for your organization, including three that are among the most widely recognized frameworks in use: The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management: Integrating Strategy and Performance (June 2017); ISO 31000:2018; and the United Kingdom's (UK) Orange Book – Principles and Concepts, (August 2021).

COSO Framework

The COSO framework defines ERM as the "culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value." COSO starts the risk process by reviewing the organization's business strategies and aligning risks to those objectives.

The COSO framework presents a risk management approach centered around five interrelated components:

1. Governance and culture
2. Strategy and objective setting
3. Performance
4. Review and revision
5. Information, communication, and reporting

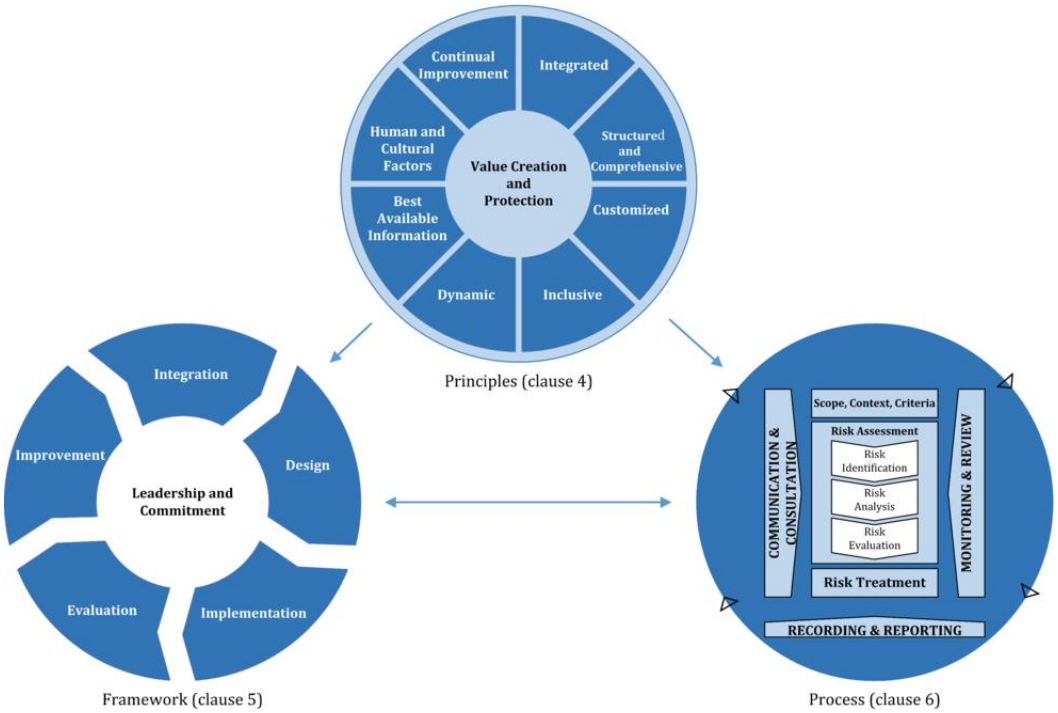
These five components contain a series of 20 total principles that provide much more specific guidance for everything from governance to monitoring. They describe specific actions and practices that can be applied in a scalable manner to organizations of all kinds but emphasize an overall correlation between the effectiveness of these risk-related activities and the successful achievement of the organizations' strategy and business objectives.

COSO ERM Model (www.coso.org)

ISO 31000 ERM Framework

The ISO 31000 ERM framework is a cyclical risk management process that incorporates integrating, designing, implementing, evaluating, and improving the ERM process. The ISO 31000 framework covers various risks and is customizable for organizations, regardless of size, industry, or sector. With ISO, the risk process begins by defining the purpose and scope of risk management activities. The principles define the purpose of risk management as existing to create and protect value, and correlates eight different characteristics that must either be factored in or aligned with that central purpose.

The ISO framework highlights the essential role of leadership support and commitment with effective risk management and illustrates the continuous improvement cycle required to ensure that risk management activities are sustainable and continually evolve to meet the organization's needs. The framework is the infrastructure/governance structure used to support risk management activities in a sustainable fashion.



*ISO 31000 Model (*https://www.iso.org/iso-31000-risk-management.html)

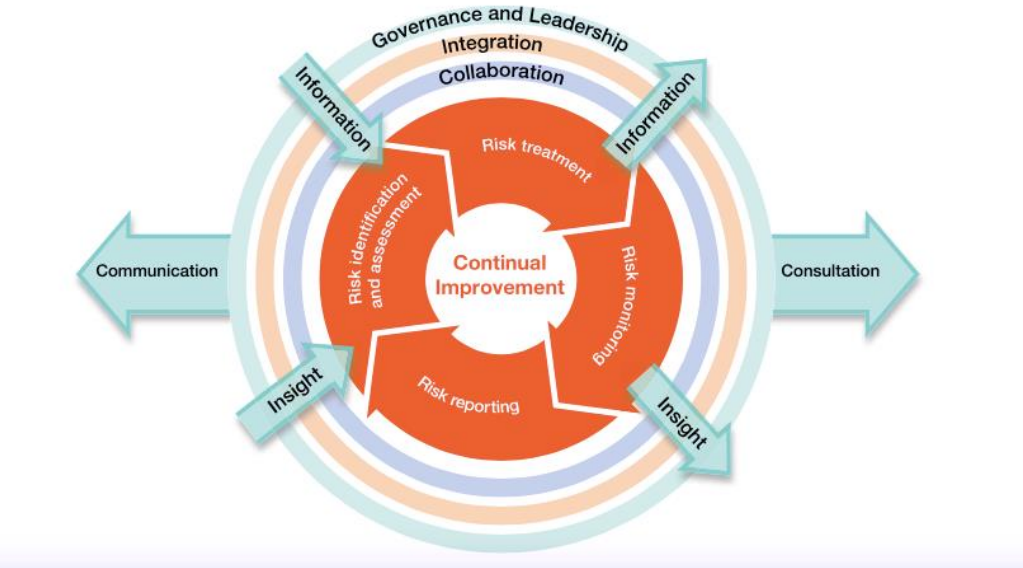
Orange Book Risk Management Framework

The UK Orange Book risk management framework supports the consistent and robust identification and management of opportunities and risks within desired levels across an organization, supporting openness, challenge, innovation, and excellence in the achievement of objectives.

Per the Orange Book, “for the risk management framework to be considered effective, the following principles shall be applied:

- Risk management shall be an essential part of **governance and leadership**, and fundamental to how the organization is directed, managed and controlled at all levels.
- Risk management shall be an **integral** part of all organizational activities to support decision-making in achieving objectives.
- Risk management shall be **collaborative and informed** by the best available information and expertise.
- Risk management processes shall be **structured** to include:
  - **Risk identification and assessment** to determine and prioritize how the risks should be managed;
  - The selection, design and implementation of **risk treatment** options that support achievement of intended outcomes and manage risks to an acceptable level;
  - The design and operation of integrated, insightful and informative **risk monitoring**; and
  - Timely, accurate and useful **risk reporting** to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

- Risk management shall be **continually improved** through learning and experience."



Orange Book Model
*(*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF)

Three Lines Model

When settling on and articulating an ERM framework, it can also be helpful to reference the Three Lines Model. This model provides structure around risk management and internal controls within an organization by defining roles and responsibilities in different areas and the relationship among those different areas.

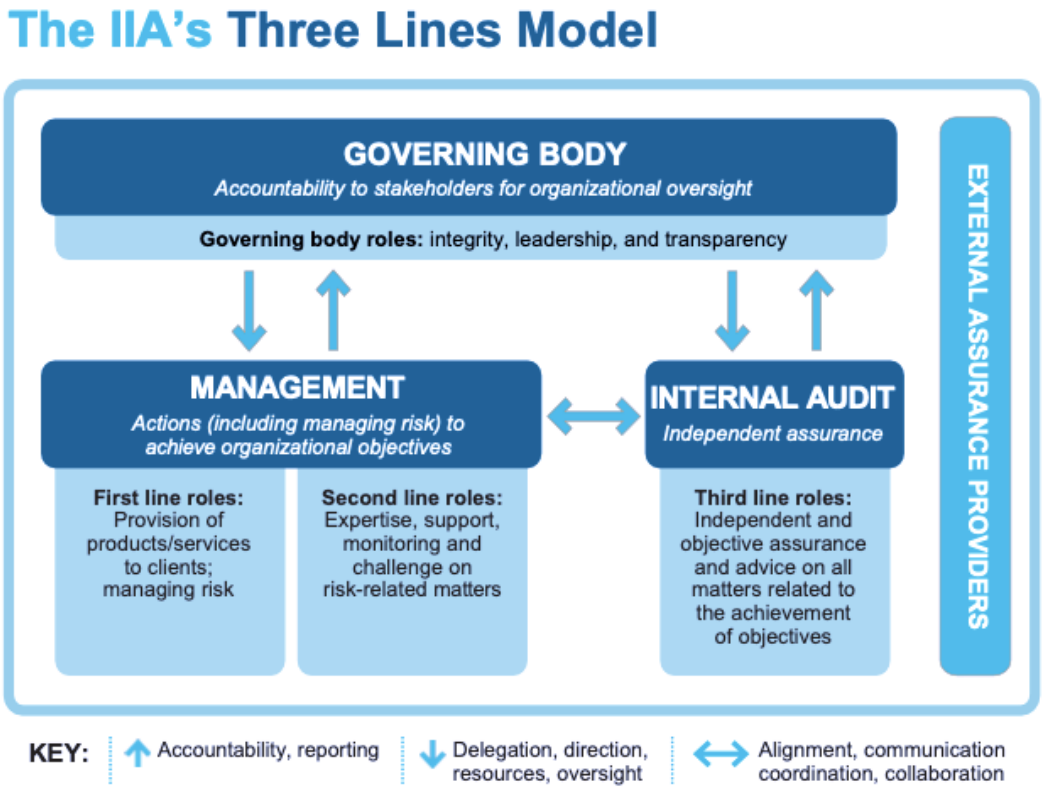
The first line comprises business units and support departments/units which take on risks and are expected to manage and mitigate them. The first line **owns and manages risks**. Contrary to how risk management is perceived, individual risks and the controls that mitigate them are not owned by risk or compliance staff. Rather, operational management and senior leadership are responsible for ongoing activities that include:

- Owning and managing risks.
- Identifying, assessing, and treating risks.
- Implementing corrective actions.
- Implementing and maintaining internal controls.
- Conducting evaluations of internal controls.
- Executing risk and control procedures on a daily basis.

The second line **oversees risks**. It is at this line where functions associated with risk are found, including Enterprise Risk Management. Functions of the second line include:

- Ensuring that operational management and senior leadership are implementing effective risk management practices.
- Assisting risk owners with risk evaluation by taking into account the institution's risk appetite and tolerance levels.
- Helping risk owners report risk-related information throughout the institution.
- Providing updates on the status of risk and resiliency to senior leadership.

The third line **provides independent assurance**. Internal Audit forms the third line, and provides assurance on the effectiveness of governance, risk management, and internal controls. It assesses the effectiveness of the first and second lines in achieving risk management objectives, and the effectiveness of the risk management and internal control framework.



The Three lines model from the Institute of Internal Auditors (www.theiia.org). The IIA is an international professional association headquartered in the U.S. It has more than 230,000 members globally.