COSO

- Initial work was a controls framework
- Initial ERM framework: 2004
- North American standard
- Five interrelated components
  - Governance and culture
  - Strategy and objective setting
  - Performance
  - Review and revision
  - Information, communication, reporting
- Includes 20 principles
- Last updated: 2017
  - Greater focus upon strategy
  - Designed to be scalable

ISO 31000

- Federation of national standards bodies
- Initial ERM framework: 2009
- International standard
- Three main components:
  - A set of principles
  - The framework
  - The risk management process
- Includes 8 characteristics
  - Highlights role of leadership, continuous improvement, sustainability, evolving to meet needs
- Last updated: 2018
  - Simplified, more customizable

Similarities

- Guide to analyzing and understanding risk in an organization
- Risk is uncertainty related to the achievement of objectives
- Consistent approach to managing and improving RM capabilities
- Expands scope of risk management to strategy and opportunity
- Facilitates consideration of risk at right time, and as evolving over time
- Guidelines for inclusion of risk and decision-making in governance
- Can be applied to any organization
- Tailorable to own structure, operations, culture

Key Distinctions

COSO

- Detailed, comprehensive, prescriptive
- Primary Input: USA/North America
- Authors: Audit and accounting firms
- Focused more upon mission/strategy
- Support organizational performance
  - Acknowledges opportunity
  - Corporate governance and oversight focused
  - Risk is managed, controlled, rather than pursued
- Risk appetite and tolerance concepts

ISO

- Concise, standardized, less on implementation
- Primary Input: Worldwide
- Authors: Management professionals
- More operations than control based
- Creation and protection of value
  - Opportunity vs consequence
  - Context and communication
  - Integrated decision-making