# Fraud Risk Management

*Fraud Risk Management—Overview*

# Discussion Questions

1. Does your organization follow a specific risk management model? If so, which one? Do you think this model adequately addresses the risks your organization faces? Why or why not?

# Discussion Questions

2. What are some of the risks your organization faces? Where does the risk of fraud fit into your organization's risk hierarchy?

# Discussion Questions

3. Does your organization have a formal risk management function? If so, are anti-fraud initiatives integrated into the risk management initiatives?

# Discussion Questions

4. How does your organization categorize the risks that are identified in the risk management process?

# Learning Objectives

- Analyze the current state of the risk management landscape.
- Compare different risk management frameworks.
- Recognize what fraud risk is and the factors that influence it.
- Understand the reasons for effectively managing fraud risk.
- Determine who is responsible for managing fraud risk within an organization.

# Introduction to Risk Management

- Risk management involves:
  - Identification of risks
  - Prioritization of risks
  - Treatment of risks
  - Monitoring of risks

# Introduction to Risk Management

- Balances risk appetite with the ability to meet strategic, operational, reporting, and compliance objectives
- Requires a proactive, rather than reactive, approach

# 2019 the Current State of Risk Management Initiatives

- Risk management initiatives appear relatively immature:
  - 23% describe their risk management as “mature” or “robust.”
  - 38% described their risk management as “very immature” or “developing.”

# 2019 the Current State of Risk Management Initiatives

- 41% are “minimally” or “not at all” satisfied with the nature and extent of reporting of key risk indicators to senior executives.
- 39% do not have risk oversight activities formally assigned to a board subcommittee.
- External parties, such as regulators and investors, are placing greater expectations on management to strengthen risk oversight.

# Risk Management Frameworks

- An entity's risk management program should be specifically tailored to its unique needs.
- However, the use of a framework can provide guidance and structure in developing the program.

# COSO *Enterprise Risk Management—Integrating Strategy and Performance*

| Governance and culture | Strategy and objective setting | Performance | Review and revision | Information, communication, and reporting |
|---|---|---|---|---|
| • Exercises board risk oversight<br>• Establishes operating structures<br>• Defines desired culture<br>• Demonstrates commitment to core values<br>• Attracts, develops, and retains capable individuals | • Analyzes business context<br>• Defines risk appetite<br>• Evaluates alternative strategies<br>• Formulates business objectives | • Identifies risk<br>• Assesses severity of risk<br>• Prioritizes risk<br>• Implements risk responses<br>• Develops portfolio view | • Assesses substantial changes<br>• Reviews risk and performance<br>• Pursues improvement in enterprise risk management | • Leverages information and technology<br>• Communicates risk information<br>• Reports on risk, culture, and performance |

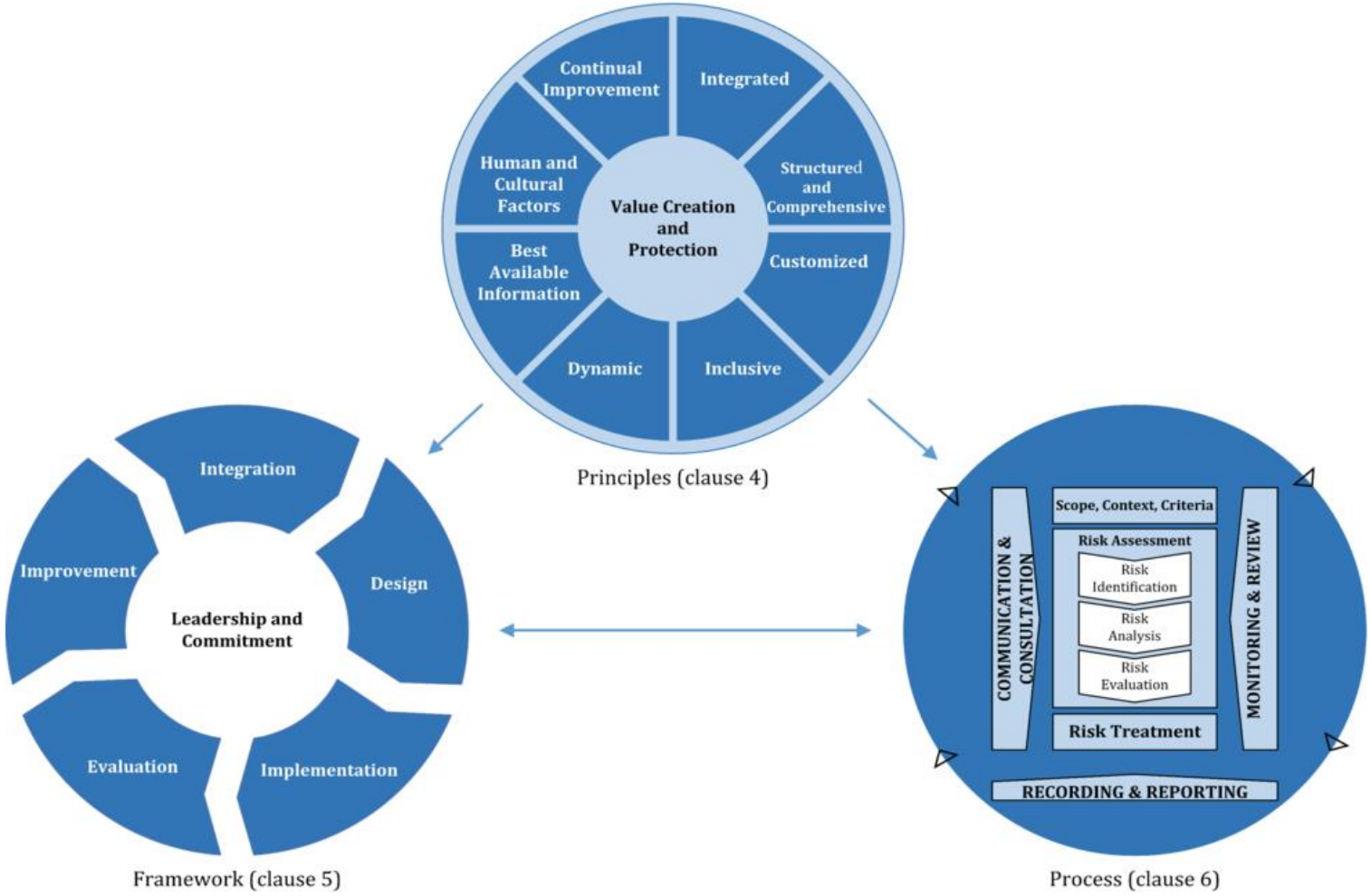
# ISO 31000

- Lays out eight principles of effective risk management
- Provides guidance on developing both a framework and a process for managing risk that is based on those principles

# ISO 31000: 2018
# Risk Management Principles

| | | | |
|---|---|---|---|
| Integrated into organization | Structured and comprehensive | Customized and proportionate | Inclusive |
| Dynamic | Based on the best available information | Takes human and cultural factors into account | Facilitates continuous improvement |

# ISO 31000:2018




(Source: ISO 31000:2018, *Risk Management—Guidelines*)

# Choosing a Risk Management Framework

- Might start with COSO or ISO framework as is
- But should customize to the organization and its needs based on:
  - Organizational structure
  - Nature of operations
  - Environment(s)
  - Size
  - Nature of risks

# *Fraud Risk Management Guide* 2016

- Published by COSO in collaboration with the ACFE
- Five principles of FRM:
  - One aligned with each of the five components of internal control
- Supported by individual points of focus for each principle
- Not formally linked to COSO ERM 2017, but there are several connections

# IC ↔ FRM ↔ ERM

| IC 2013 Component | FRM 2016 Principle | ERM 2017 Component |
|---|---|---|
| Control environment | The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk. | Governance and culture |
| Risk assessment | The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks. | Strategy and objective-setting |

# IC ↔ FRM ↔ ERM

| IC 2013 Component | FRM 2016 Principle | ERM 2017 Component |
|---|---|---|
| Control activities | The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner. | Performance |
| Information and communication | The organization establishes a communication process to obtain information about potential fraud and deploys a coordinate approach to investigation and corrective action to address fraud appropriately and in a timely manner. | Information, communication, and reporting |

# IC ↔ FRM ↔ ERM

| IC 2013 Component | FRM 2016 Principle | ERM 2017 Component |
|---|---|---|
| Monitoring activities | The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors. | Review and revision |

# IC ↔ FRM ↔ ISO 31000

| IC 2013 Component | FRM 2016 Principle | ISO 31000 Framework | ISO 31000 Process |
|---|---|---|---|
| Control environment | The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk. | Leadership and commitment<br><br>Design | Establish the scope, context, and criteria |
| Risk assessment | The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks. | Design<br><br>Implementation | Risk assessment:<br>– Identification<br>– Analysis<br>– Evaluation |

# IC ↔ FRM ↔ ISO 31000

| IC 2013 Component | FRM 2016 Principle | ISO 31000 Framework | ISO 31000 Process |
|---|---|---|---|
| Control activities | The organization selects, develops, and deploys preventive and detective fraud controls activities to mitigate the risk of fraud events occurring or not being detected in a timely manner. | Integration<br><br>Implementation | Risk treatment |
| Information and communication | The organization establishes a communication process to obtain information about potential fraud and deploys a coordinate approach to investigation and corrective action to address fraud appropriately and in a timely manner. | Implementation<br><br>Evaluation | Communication and consultation |

# IC ↔ FRM ↔ ISO 31000

| IC 2013 Component | FRM 2016 Principle | ISO 31000 Framework | ISO 31000 Process |
|---|---|---|---|
| Monitoring activities | The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors. | Evaluation<br><br>Improvement | Monitoring and review |

# The Fraud Risk Management Process

# What Is *Fraud Risk*?

- The vulnerability that an organization has to those capable of overcoming the three elements of the Fraud Triangle
- Comes from both internal and external sources
- Differs from other risks because fraud, by definition, entails intentional misconduct designed to evade detection

# Types of Fraud Risk

- Inherent risk—risk present before management takes action
- Residual risk—risk that remains after management takes action

# Factors Influencing Fraud Risk

- The nature of the business
- Economic conditions
- The operating environment
- The ethics and values of the company and its people
- Technology
- The legal environment
- The effectiveness of internal controls

# Who Is Responsible for Managing Fraud Risk?

- Team responsible for executing, monitoring, and ensuring success:
  - Executive management
  - Audit committee
  - Investigations group
  - Compliance
  - Controller's group
  - Internal audit
  - IT
  - Security
  - Legal department
  - Human resources

# Who Is Responsible for Managing Fraud Risk?

- The team should have a designated leader.
- Synergy and communication are keys to success.