

Fraud Risk Management

Developing a Fraud Risk Management Program

Discussion Questions

1. Which individual or group within your organization oversees the risk management process? How is risk management governed at the board level—through a specific committee?

Discussion Questions

2. How and where within the risk management model is fraud risk addressed within your organization?

Discussion Questions

3. How does your organization assess the effectiveness of its risk management activities overall? How about its fraud risk management activities? How do you define success for this function?

Learning Objectives

- Define the objectives of a fraud risk management program.
- Identify the steps in developing a fraud risk management program.
- Understand the components in an effective fraud risk management program.

Objectives of a Fraud Risk Management Program



- Address fraud:
 - Before it occurs—prevention
 - While it occurs—detection
 - After it occurs—response

Steps in Developing a Fraud Risk Management Program

1. Define program objectives.
2. Assess fraud risks.
3. Design program components.
4. Implement program components.
5. Communicate expectations.
6. Ensure compliance.
7. Identify and investigate violations.
8. Measure, evaluate, and report program effectiveness.

Step 1: Define Program Objectives

- Tailor objectives to the organization's specific needs and goals.
- Include a clear, explicit definition of what the organization intends to accomplish.
- Weigh:
 - Management's risk appetite
 - Investment in anti-fraud controls
 - Prevention of material frauds

Step 1: Define Program Objectives— Addressing Risk Appetite

- Every company has a different risk appetite.
- Management needs to address risk appetite in relation to fraud.
- The difference between risk appetite and risk tolerance should be understood.
 - Neither suggest acceptance of identified fraud, only undetected acts.
- Consider the non-monetary impact of fraud.

Step 1: Define Program Objectives— Establishing Context for Risk Management

- Means to identify and communicate objectives and parameters to be taken into consideration in risk management
- External context versus internal context

Step 1: Define Program Objectives— Examining Previous Fraud Incidents

- Examine previous occurrences of fraud and determine how management's ideal fraud risk management program would have prevented, detected, and responded to them.
 - Were fraud risks not fully understood?
 - Were controls insufficient in design or operation?
 - Were applicable controls overridden?
 - Were any warning signs missed?

Step 2: Assess Fraud Risks

- Identify and thoroughly understand risks faced by the organization.
- FRM initiatives developed without accurate fraud risk assessment will be:
 - Ineffective in preventing fraud
 - A waste of resources
 - Potentially counterproductive

Step 3: Design Program Components

- Considerations:
 - Organizational culture
 - Operating environment
 - Specific risks
 - Program objectives
 - Risk appetite



Step 3: Design Program Components

- Initiatives to increase the anti-fraud culture and tone of the organization
- Fraud prevention controls
- Fraud detection controls
- Policies, processes, and procedures for investigating and responding to identified fraud

Step 4: Implement Program Components

- Internal controls will only prevent or detect fraud if those responsible effectively fulfill their duties.



Step 5: Communicate Expectations



- Communicate purpose and expectations of FRM program:
 - Both formally and informally
 - To all employees at all levels of the organization

Step 6: Ensure Compliance

- Include mechanisms that monitor, identify, and address breaches in compliance.
- Designate an individual or team to monitor compliance and address noncompliance.
- Formal sanctions for intentional noncompliance must be well publicized, consistent, and firm.

Step 7: Identify and Investigate Violations

- Implement clearly defined processes for investigating suspected frauds.



Step 8: Evaluate the Program's Effectiveness

- Periodically evaluate program performance.
- Report results to upper management and the board of directors.
- Benchmark performance against internal expectations or best practices.

FRM Program Components

- Commitment
- Fraud awareness training
- Affirmation process
- Conflict disclosure
- Fraud risk assessment



FRM Program Components

- Reporting procedures and whistleblower protection
- Investigation process
- Corrective action
- Process evaluation and improvement
- Continuous monitoring

Fraud Risk Management Principle No. 5—Fraud Risk Management Monitoring

- *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.*

Fraud Risk Management Monitoring— Points of Focus

Considers a mix
of ongoing and
separate
evaluations

Considers factors
for setting the
scope and
frequency of
evaluations

Establishes
appropriate
measurement
criteria

Considers known
fraud schemes
and new cases

Evaluates,
communicates,
and remediates
deficiencies