State Accounting Office

Statewide Internal Control Guidance

Section: Risk Assessment	**Issued Date:** 08/01/2016 **Revision Date:**

Index

Overview

Every organization faces a variety of risks from external and internal sources that impact the achievement of the organization's objectives, and risk assessment is the identification and analysis of these risks. The nature and extent of management's risk assessment activities should be proportionate to the size of the organization and complexity of their operations. For example, the risk assessment process is likely to be less formal and less structured in smaller entities. Additionally, management recognizes that not all risks are equal and drives the allocation of more resources to the areas of highest risk, while considering cost factors in relation to expected benefits. However, while allocating resources, management also considers that fraud can occur in organizations of any size or type, and that almost any employee may be capable of committing fraud given the right set of circumstances. Additionally, management establishes mechanisms to identify, analyze, and respond to changes potentially impacting the internal control system. This is necessary because conditions impacting the organization and the environment it operates in are continually changing. Ultimately, the risk and change responses become internal controls that management places in to operation.

Component	Principles	Attributes
Risk Assessment	6. Management defines objectives clearly in order to identify risks and define risk tolerances.	6.1 Definitions of Objectives 6.2 Definitions of Risk Tolerances
	7. Management identifies, analyzes, and responds to risks related to achieving the defined objectives.	7.1 Identification of Risks 7.2 Analysis of Risks 7.3 Response to Risks
	8. Management considers the potential for fraud when identifying, analyzing, and responding to risks.	8.1 Types of Fraud 8.2 Fraud Risk Factors 8.3 Response to Fraud Risks
	9. Management identifies, analyzes, and responds to significant changes that could impact the internal control system.	9.1 Identification of Change 9.2 Analysis of and Response to Change

6. Management defines objectives clearly in order to identify risks and define risk tolerances.

6.1. Definitions of Objectives

Concept

Objectives, which are initially set as part of the objective-setting process, guide the organization's design of internal controls for related risks and are refined as they are incorporated in to the internal control system. Objectives are broadly classified into one or more of three categories:

- Reporting – reliability of internal and external reports. This would include any type of financial report such as the Budgetary Compliance Report (BCR), and year-end forms which are used to create the Comprehensive Annual Financial Report (CAFR). Reporting objectives can also be defined for nonfinancial data
- Operational – effectiveness and efficiency of operations. This would include making sure the organizational mission is accomplished at the least possible cost and also includes the safeguarding of assets
- Compliance – operating in accordance with applicable laws and regulations

Management Responsibilities

- Management defines objectives that are in alignment with the organization's mission, strategic plan, and performance goals, while considering:
  - External requirements the organization is required to follow that are established by laws, regulations, and standards
  - Internal expectations established by the principles and attributes of the organization's control environment
  - The need for objectives to be defined in specific and measurable terms:
    - Specific – fully and clearly defined so they can be easily understood at all levels (specifying what, who, how, and a time frame for achievement)
    - Measurable – stated quantitatively or qualitatively, in terms that are free of bias and subjective judgments, to allow for consistent measurement and for the assessment of performance
- Management evaluates and revises these objectives, as needed, to keep the objectives consistent with the organization's requirements and expectations. This consistency enables management to identify and analyze risks associated with achieving the defined objectives.
- Management establishes, and revises as necessary, performance measures for evaluating the achievement of objectives, by considering:
  - Targeted percentages or numerical values for quantitative objectives
  - Level or degree of performance, such as milestones, for qualitative objectives

Key Importance to Internal Control

Properly defined objectives allow for the identification of risks that could impact the overall achievement of the organization's objectives.

Examples[1]

- Management ensures proper reporting objectives are defined. Some possible objectives could include ensuring the internal and external reports:
  - Comply with accounting standards (items are recorded at the proper basis)
  - Are complete
  - Contain accurate amounts
  - Are available on a timely basis
- Management ensures proper operational objectives are defined. Some possible considerations could include:
  - Organization's mission
  - Organization's strategic plan
- Management ensures proper regulatory objectives are defined. Some possible considerations could include requirements contained in:
  - Federal Laws, including grant requirements contained in the Uniform Grant Guidance (Title 2 of the U.S. Code of Federal Regulations (CFR) Part 200)
  - State Laws

6.2. Definitions of Risk Tolerances

Concept

Risk tolerance is essentially how much risk an organization is willing to accept. More specifically, what is the acceptable level of variation in performance compared to the achievement of objectives. Depending on the category of objectives, risk tolerances are expressed as follows:

- Financial reporting objectives – judgments about materiality, involve both quantitative and qualitative considerations, and are impacted by the needs of the financial report users and size or nature of a misstatement
- Nonfinancial reporting objectives – level of precision and accuracy suitable for user needs, involving both quantitative and qualitative considerations to meet the needs of the nonfinancial report user
- Operations objectives – level of variation in performance in relation to risk
- Compliance objectives – concept of risk tolerance does not apply, as an organization is either compliant or not compliant

Management Responsibilities

- Management defines risk tolerances in specific and measurable terms[2], so they are clearly stated and can be measured, for the defined objectives.
- Management ensures that the acceptable levels of risk tolerance are appropriate for the design of the internal control system, and as necessary, revises them to be consistent with the external requirements and internal expectations.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.
[2] Risk tolerance is often defined in the same terms as the performance measures for the defined objectives.

Key Importance to Internal Control

Operating within risk tolerances enables the appropriate design of internal controls, and provides management with greater assurance that the organization will achieve their objectives.

Example[1]

Management ensures proper risk tolerances are defined. Some possible examples could include:

- Establishing a low risk tolerance relating to the quality, timing, and availability of financial data
- Establishing an acceptable error rate
- Establishing a very low risk tolerance relating to material deficiencies in internal control
- Establishing a low risk tolerance relating to financial reporting for such things as: timeliness, transparency, GAAP, etc.
- Establishing a zero tolerance for violating standards of conduct
- Requiring backup on computer systems so that the likelihood of computer failure is less than a certain percentage

7. Management identifies, analyzes, and responds to risks related to achieving the defined objectives.

7.1. Identification of Risks

Concept

The identification of risks detects risks impacting the organization's achievement of their defined objectives, and allows for the risks to be analyzed and risk responses to be designed. This identification is the start of the risk assessment process.

Management Responsibilities

Management identifies risks by considering various factors:

- The types of risks that impact the organization:
  - Inherent risk – risk to the organization in the absence of management's response to the risk
  - Residual risk – risk that remains after management's response to inherent risk.
- All significant interactions within the organization and with external parties
- Quantitative and qualitative ranking activities, forecasting and strategic planning, and consideration of deficiencies identified through audit and other assessments
- Changes within the organization's internal and external environment and other internal and external factors, at both the entity and transaction levels:
  - Internal factors may include the complex nature of an organization's programs (level of judgment or special skills needed to come up with

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list, and relate mainly to the financial reporting objective. Also, see the more detailed sample template document for more specific examples.

financial numbers, number of transactions, etc.), its structure (extent of reliance on other areas or other systems, level of manual intervention, etc.), or the use of new technology in operational processes

- External factors may include new or amended laws, regulations, or professional standards (including new Reporting requirements), economic instability, or potential natural disasters

Key Importance to Internal Control

Management's lack of identification of the appropriate risks could cause deficiencies in the internal control system because the analysis and response of the risks would not be appropriate.

Examples[1]

- Management ensures proper risks are identified for the defined objectives. Some possible examples based on external financial reporting objectives could include:
  - The financial reports and/or year-end forms do not comply with accounting standards (items are not recorded at the proper basis) because staff was not knowledgeable of current accounting guidance
  - The financial reports and/or year-end forms are not prepared and/or reviewed by the appropriate personnel
  - The financial reports and/or year-end forms are not complete because all items were not recorded
  - The financial reports and/or year-end forms do not contain accurate amounts because the amounts provided were at the wrong period end (such as May 31 and not June 30)
  - The financial reports and/or year-end forms are not available on a timely basis because it is after the respective due date, however, the accounting records are still not closed
- Management maintains awareness of ways to identify the various risk factors. Some possible ways this could be done include considering elements, such as:
  - Reading SAO guidance about accounting updates
  - Referring to SAO published guidance (Accounting Policies, Business Process Policies, etc.)
  - Automatically receiving notifications relating to technical updates from applicable trade organizations (such as GASB)
  - Using pre-established accounting software (such as Teamworks)
  - Using a pre-defined chart of accounts
  - Using common accounting services (such as SAO' s TeamWorks Travel and Expense)
  - Correcting previous audit findings

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list, and relate mainly to the financial reporting objective. Also, see the more detailed sample template document for more specific examples.

7.2. Analysis of Risks

Concept

The analysis of risks estimates the significance of their impact on achieving defined objectives. The specific risk analysis methodology used can vary because of differences in the organization's mission and difficulty in qualitatively and quantitatively defining risk tolerances.

Management Responsibilities

- Management analyzes risks, including fraud risks[3], on an individual basis or collectively by grouping related risks, and considers the correlation among different risks or groups of risks when estimating their significance.
- Management estimates the significance of the identified risk's impact on the achievement of objectives, at both the organization and transaction levels, by considering:
    - Magnitude of impact – likely scale of the deficiency that could result from the risk and is impacted by factors such as the size, pace, and duration of the risk's impact
    - Likelihood of occurrence – level of possibility that a risk will occur
    - Nature of risk – factors such as the degree of subjectivity and whether the risk arises from fraud or from complex or unusual transactions
- The oversight body oversees management's estimates of significance relating to identified risks, ensuring risk tolerances have been properly defined.

Key Importance to Internal Control

Management's lack of proper risk analysis could result in inappropriate risk responses being identified, ultimately impacting the internal control system and the organization's achievement of their defined objectives.

Examples[1]

- Management analyzes risks impacting the achievement of financial reporting objectives, some possible ways this could be done include:
    - Establishing a materiality threshold (such as any expense account that is x% of total expenses)
    - Establishing a higher priority to accounts that would always be included since they are inherently risky (such as cash)
    - Establishing a higher priority to accounts that would always be included since they had previous trends in audit findings (this could be internal or external audits)
    - Establishing a higher priority to accounts that would always be included since they include the use of significant judgment
- Some possible ways the oversight body oversees management could include:
    - Having periodic meetings and other communications with management
    - Reviewing management's analysis

[3] Fraud includes the intentional material misstatement in the financial statements or intentional loss or misuse of assets. Also, fraud concepts are discussed more in depth in Principle 8.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list, and relate mainly to the financial reporting objective. Also, see the more detailed sample template document for more specific examples.

7.3. Response to Risks

Concept

The risk response effectively mitigates the identified risk or reduces the identified risk to be within the defined risk tolerance. Risk responses are generally the control activities placed in to operation within the organization.

Management Responsibilities

- Management designs risk responses, to respond to the analyzed risks, based on the significance of the identified risk and the defined risk tolerance. These risk responses include:
  - Acceptance – no action is taken based on the insignificance of the risk
  - Avoidance – action is taken to stop the operational process or the part of the operational process causing the risk
  - Reduction – action is taken to reduce the likelihood or magnitude of the risk
  - Sharing – action is taken to transfer or share risks across the organization or with external parties (such as insuring against losses)
- Management conducts periodic risk assessments and uses performance measures to evaluate whether the risk response actions enable the organization to operate within the defined risk tolerances. As needed, management revises risk responses and controls or reconsiders defined risk tolerances.

Key Importance to Internal Control

By appropriately responding to risks, and allowing the organization to operate within the defined risk tolerance, the organization has greater assurance that they will achieve their objectives.

Example[1]

Management establishes appropriate responses to identified risks, some possible ways this could be done include:

- Establishing appropriate control activities
- Implementing mitigating controls (such as a secondary review)
- Rearranging job responsibilities
- Segregating Duties
- Having pertinent staff attend training and/or read applicable guidance

8. Management considers the potential for fraud when identifying, analyzing, and responding to risks.

8.1. Types of Fraud

Concept

- The types of fraud include:
  - Fraudulent financial reporting – intentional misstatements or omissions of amounts or disclosures in financial statements. This could include:
    - Intentional alteration of accounting records

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.

        - Misrepresentation of transactions
        - Intentional misapplication of accounting principles
    - Misappropriation of Assets – theft of an organization's assets, which could include theft of property, embezzlement of receipts, or fraudulent payments
    - Corruption – bribery and other illegal acts
- Types of misconduct include:
    - Waste – use or expense of resources carelessly, extravagantly, or to no purpose
    - Abuse – behavior that is lacking or improper when compared with the behavior of a prudent person given the facts and circumstances, which could include misuse of authority for personal gain or for the benefit of another

Management Responsibilities

Management considers the types of fraud and misconduct[4] that can occur within the organization in order to identify fraud risks.

Key Importance to Internal Control

These fraud types provide a basis for identifying risks relating to fraud or misconduct that may impact the organization's achievement of their defined objectives.

Example[1]

Management considers which fraud types may apply. Some possible ways to do this could include:

- Brainstorming with others what type of fraud or misconduct could occur
- Reviewing audit findings relating to potential fraud areas
- Attending training relating to fraud
- Reviewing information about actual fraud cases to determine how they occur and analyze if that could occur in the organization

8.2. Fraud Risk Factors

Concept

Fraud risk factors do not necessarily indicate that a fraud exists but are often present when fraud occurs.

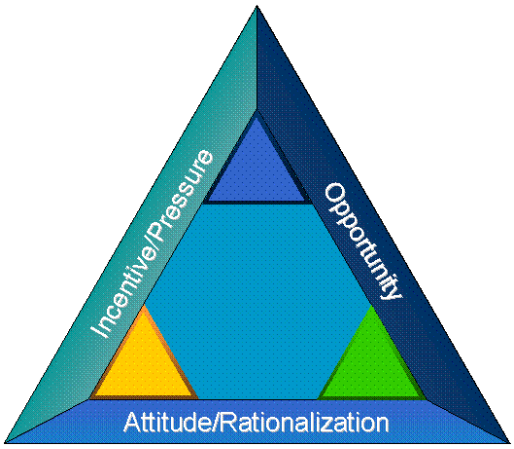
Management Responsibilities

- Management identifies fraud risks by considering the following fraud risk factors:
    - Incentive/pressure – management or other personnel have a motivation or are under a burden, which provides a motive to commit fraud
    - Opportunity – circumstances exist such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud
    - Attitude/rationalization – individuals involved are able to rationalize committing fraud

[4] Even though, waste and abuse do not necessarily involve fraud or illegal acts, they may be an indication of potential fraud or illegal acts and may still impact the achievement of the defined objectives.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.

- These three factors are often presented as a fraud triangle. Fraud risk may be greatest when all three factors are present, however one or more of these factors may indicate a fraud risk.



The Fraud Triangle

- Management should also consider other possible identifiers of fraud risk, such as allegations of fraud or suspected fraud provided by internal and external parties, including personnel or auditors.

Key Importance to Internal Control

Management's lack of identification of the appropriate fraud risks could cause deficiencies in the internal control system which could allow a fraud to occur because the analysis and response of the fraud risks was not be appropriate.

Example[1]

Management considers how fraud could occur in the organization. Some possible ways to do this could include:

- Brainstorming with others as to how fraud or misconduct could occur
- Reviewing the internal control system looking for weaknesses where fraud or misconduct could occur
- Considering areas more susceptible to fraud such as travel or purchasing, including pcards or fuel cards
- Performing data analytics and following up on anomalies in data (such as a large number of the payments to an employee, or a large number of payments at an even dollar amount, etc.)
- Observing employee behaviors (such as living beyond their means, never taking vacations, etc.)
- Having hotlines or other methods that allow for suspected fraud or misconduct to be reported

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.

8.3. Response to Fraud Risks

Concept

The response to fraud risks is the process of analyzing and responding to the identified fraud risks so that they are effectively mitigated.

Management Responsibilities

- Management analyzes identified fraud risks, by using the same analysis process performed for other identified risks, and:
  - Estimates their significance, both individually and in the aggregate, of impact on achieving the defined objectives
  - Assesses the risk of management override of controls
- Management responds to identified fraud risks so they are effectively mitigated, by using the same analysis process performed for other identified risks, and:
  - Designs an overall risk response including specific actions for responding to fraud risks
  - Considers if changes to the organization's activities and processes would reduce or eliminate certain fraud risks. These changes may include:
    - Stopping or reorganizing certain operations
    - Reallocating roles among personnel to enhance segregation of duties
  - Develops further responses to address the risk of management override of controls
- Management revises the risk responses, and when appropriate the risk assessment process, when fraud has been detected.
- The oversight body oversees management's assessments of fraud risk and the risk of management override of controls so that they are appropriate.

Key Importance to Internal Control

Mitigating fraud risks lessens the risk that an organization will incur a loss and also provides greater assurance that the organization will achieve their objectives.

Examples[1]

- Management responds to fraud risks that could occur in the organization. Some possible ways to do this could include:
  - Establishing appropriate control activities
  - Implementing mitigating controls (such as a secondary review)
  - Rearranging job responsibilities
  - Segregating Duties
- Some possible ways the oversight body oversees could include:
  - Having periodic meetings and other communications with management
  - Reviewing management's action taken

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.

9. Management identifies, analyzes, and responds to significant changes that could impact the internal control system.

9.1. Identification of Change[5]

Concept

Changes that could significantly impact the organization's internal control system are detected through risk assessment or a similar process.

Management Responsibilities

- Management identifies, on a timely basis, significant changes to internal and external conditions that have already occurred:
  - Internal conditions – changes to the organization's programs or activities, oversight structure, organizational structure, personnel, or technology
  - External conditions – changes in the governmental, economic, technological, legal, regulatory, or physical environments.
- Management uses a forward-looking process to anticipate and plan for significant changes that are expected to occur to internal and external conditions.
- Management communicates the identified significant changes to the appropriate personnel across the organization by using established reporting lines.

Key Importance to Internal Control

Management's lack of identification of the appropriate changes could cause deficiencies in the internal control system because the analysis and response of the changes would not be appropriate.

Example[1]

Management maintains awareness of the applicable changes impacting their internal control system. Some possible ways this could be done include:

- Having routine meetings with division/program heads to discuss changes to key personnel, key systems, etc
- Having routine meetings with legal staff to discuss changes to Laws, Regulations, etc.
- Attending trainings on applicable upcoming technical issues
- Automatically receive notifications relating to technical updates from applicable trade organizations (such as GASB, etc.)

[5] Change is discussed separately because it is critical to an effective internal control system and can often be overlooked or inadequately addressed in the normal course of operations.

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.

9.2. Analysis of and Response to Change

Concept

The analysis and response to identified changes, as existing controls may not be effective for meeting objectives or addressing risks under changed conditions.

Management Responsibilities

- Management, as part of the risk assessment process, identifies changes along with the related risks, and any new risks prompted by the changes, in order to maintain an effective internal control system.
- Management also considers whether existing risks require further assessment to determine whether the defined risk tolerances and risk responses need to be revised.
- Management analyzes the impact of the identified changes and risks on the internal control system and, when necessary, revises the internal control system to maintain effectiveness.

Key Importance to Internal Control

Management's lack of proper change analysis could result in inappropriate change and risk responses being identified, ultimately impacting the internal control system, and the organization's achievement of their defined objectives.

Example[1]

Management responds to changes that could occur in the organization. Some possible ways to do this could include:

- Establishing appropriate control activities
- Implementing mitigating controls (such as a secondary review)
- Rearranging job responsibilities
- Segregating Duties

[1] The examples provided throughout this framework are intended to be a minimum starting point and not an all-inclusive list. Also, see the more detailed sample template document for more specific examples.