

## Agency Risk Assessment (FMC 6.2 – January 1, 2022)

---

### **Section 1 – Definitions:**

“Risk” is the possibility that an event will occur and adversely affect the achievement of objectives.

“Risk assessment” is the process used to identify and assess internal and external risks to the achievement of objectives, and then establish risk tolerances. Each identified risk is evaluated in terms of its impact and likelihood of occurrence. Overall, risk assessment is the basis for determining how risk will be managed.

**Section 2 – General Policy:** Effective July 1, 2022, all State agencies shall conduct an annual formal risk assessment consisting of an executive management review of agency functions, activities, and processes.

The risk assessment must:

- 1) Evaluate the probability of occurrence and the likely effect of financial, managerial, compliance, and reputational risks and of risks related to the use of information technology; and
- 2) Rank risks according to the probability of occurrence and likely effect of the risks evaluated.

**Section 3 – Required Steps in Risk Assessment:** Conducting a risk assessment requires agency management to consider the impact of possible changes in the external environment and within the agency that may render the system of internal control ineffective. The required steps in a risk assessment are:

- 1) Agency management defines objectives clearly to enable the identification of risks and defines risk tolerances.
- 2) Agency management identifies, analyzes and responds to risk related to achieving the defined objectives.
- 3) Agency management considers the potential for fraud when identifying, analyzing and responding to risks.
- 4) Agency management identifies, analyzes, and responds to significant changes that could impact the internal control system.

These steps are described in more detail below.

**Section 4 – Define Agency Objectives:** Agency management should clearly define the agency’s objectives to enable the identification of risk and risks tolerances.

Objectives fall within three major categories:

- Operations - Effectiveness and efficiency of operations.
- Reporting – Reliability of reporting for internal and external use.
- Compliance – Compliance with applicable laws and regulations.

As a part of this process, agency management may consider the following:

- Defining objectives in specific measurable terms to enable the design of internal controls for related risks, to increase understanding at all levels, and to assess performance.
- Identifying what is to be achieved, who is to achieve it, how it will be achieved, and when it will be achieved.
- Incorporating external requirements, such as state statutes and Uniform Compliance Guidelines.
- Including a subset for the three categories which addresses the safeguarding of assets.

**Section 5 – Identify, Analyze, and Respond to Risks:** After defining objectives, management identifies, analyzes, and responds to risks related to achieving the agency objectives.

Identification of Risks – In the identification process, agency management recognizes the various types of risks at the agency and transaction levels for each objective. For example, risk factors may include the agency’s organizational structure; rate of change of people, processes, systems, or businesses (new technology, new or amended laws, new and/or inexperienced employees); complexity of a program or transaction; or economic instability.

Analysis of Risks – Agency management must then analyze the identified risk to estimate its effect on achieving the defined objectives at the agency and transaction level. For example,

- How likely is the risk to occur?
- How will it impact the objective?
- Is the risk based on complex or unusual transactions?
- Is the risk based on fraud?

Risks may be analyzed individually or collectively.

Response to Risks – Once risks are identified and assessed, agency management must develop appropriate control activities to minimize the risks and document the required procedures. For example, management may accept the risk and take no action in response; choose to eliminate certain processes to avoid the risk; reduce the risk by instituting controls; or transfer the risk.

Control activities detect, prevent, or reduce the identified risks that interfere with the achievement of objectives. Detection activities are designed to identify unfavorable events in a timely manner whereas prevention activities are designed to deter the occurrence of an unfavorable event. Examples of these activities include reconciliations, authorizations, approval processes, performance reviews, and verification processes. Certain responses to fraud risk are required by statute, such as the purchase of official bonds.

An integral part of the control activity component is segregation of duties. However, in very small agencies, such segregation may not be practical. In that case, compensating activities should be implemented which may include additional levels of review for key operational processes, random and/or periodic review of selected transactions. In a smaller agency, these

reviews and testing of processes might be performed by governing boards or centralized accounting.

**Section 6 – Consideration of Fraudulent Activity:** As part of the risk assessment, agency management must consider the types of fraud which can occur, such as fraudulent financial reporting, misappropriation of assets, and illegal acts. In addition to fraud, management must assess the likelihood of other types of misconduct such as waste or abuse. Various risk factors may need to be evaluated as well as allegations from internal or external parties.

The analysis and response to fraud risk is similar to the procedures set for in the analysis and response to risk in Section 5.


Agencies must report misappropriation of State funds to the Office of Management and Budget (OMB), State Board of Accounts (SBOA), and the Inspector General or Prosecuting Attorney.

Agencies must report material variances, losses, shortages, or thefts to OMB and SBOA. Agencies should reference SBOA’s Examiner Director 2015-6, or its replacement, regarding the standards for determining materiality.

**Section 7 – OMB Submission:** The State agency shall submit annual risk assessment to the Director of OMB by September 1 of each even-numbered year. The submission to OMB should also include discussion of:

- 1) The top three risks identified by the agency along with proposed plans to mitigate or eliminate each risk;
- 2) Any audit or review findings from SBOA, federal agencies, or other internal or outside auditors received during the preceding state fiscal year along with proposed plans to resolve each finding;
- 3) A progress report on the resolution of audit findings and top risks previously reported to OMB under this FMC.

In certain circumstances, such as when an agency has repeat audit findings, OMB may request that an agency also submit its annual risk assessment in odd-numbered years.

  
Zachary Q. Jackson, Director  
State Budget Agency