20.22 Risk Assessment

20.22.10 Risk assessment overview

July 1, 2017

Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Therefore, a precondition to risk assessment is establishing objectives. Risk assessment involves a dynamic and iterative process for identifying risks to achieving agency objectives, analyzing the risks, and using that information to decide how to respond to risks.

In risk assessment, management considers the mix of potential events relevant to the agency and its activities in the context of the agency's public visibility, size, operational complexity, regulatory restraints, and other factors. Because of these variables, the same activity could have very different levels of risk for two different agencies.

20.22.20 Risk assessment principles

July 1, 2025

There are four principles relating to risk assessment.

6. Management specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to its objectives.
7. Management identifies and analyzes risks to the achievement of its objectives and uses that as a basis for determining how the risks should be managed.
8. Management considers the potential for fraud, improper payments, and information security in assessing risks to the achievement of its objectives.

9. Management identifies, analyzes, and responds to changes that could significantly impact its system of internal control.

20.22.30 Principle 6 – Specifies objectives

July 1, 2017

Management specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to its objectives. The following points of focus highlight important characteristics relating to this principle.

- **Defines specific and measurable objectives** - Management defines objectives at the agency and unit level in alignment with the agency's mission and strategic plan. Objectives:
  - Are fully and clearly set forth so they can be easily understood at all levels of the agency.
  - Can be broadly classified into one or more of three categories: operations, reporting, or compliance
  - Are stated in a quantitative or qualitative form that permits reasonably consistent measurement.
- **Considers external and internal factors** - Management considers external requirements and internal expectations when defining objectives to enable the design of internal control. Legislators, regulators, and standard-setting bodies set external requirements by establishing the laws, regulations, and standards with which the agency is required to comply. Management sets internal expectations and requirements by establishing standards of conduct, assigning responsibility, and delegating authority.
- **Considers risk tolerance** - Management considers risk tolerances for the defined objectives. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives.

20.22.40 Principle 7 – Identifies and analyzes risks

July 1, 2017

Management identifies and analyzes risks to the achievement of its objectives and uses that as a basis for determining how the risks should be managed. The following points of focus highlight important characteristics relating to this principle.

- **Identifies risk** - Management identifies risks throughout the agency relevant to the achievement of its objectives, considering both internal and external factors. Management considers the types of risks that impact the agency which may include both inherent and residual risk. Management's lack of response to risk could cause deficiencies in the internal control system.

  Management considers significant interactions within the agency and with external parties, changes within the agency's internal and external environment, and other internal and external factors to identify risks. Internal risk factors may include the complex nature of an agency's

programs, its organizational structure, or the use of new technology in operational processes. External risk factors may include new or amended laws, regulations, or professional standards; economic instability; or potential natural disasters.

- **Analyzes risks** - Management analyzes identified risks to estimate their significance, which provides a basis for responding to the risks. Management estimates the significance of a risk by considering the magnitude of impact and likelihood of occurrence.

  Magnitude of impact refers to the likely magnitude of deficiency that could result from the risk and is affected by factors such as the size, pace, and duration of the risk's impact. Likelihood of occurrence refers to the level of possibility that a risk will occur.

- **Manages risk** - Management considers how the risk should be managed. Management designs overall risk responses based on the significance of the risk and defined risk tolerance. Risk responses may include the following:

  - **Acceptance** - No action is taken to respond to the risk based on the magnitude of impact, likelihood of occurrence, and nature 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 agency or with external parties, such as insuring against losses.

Typically, no control activities are needed for acceptance and avoidance responses. When risk response actions do not enable the agency to operate within its risk tolerances, management may need to revise risk responses or reconsider risk tolerances. Periodic risk assessments allow management to evaluate the effectiveness of the risk response actions.

20.22.50 Principle 8 – Assesses fraud, improper payments, and information security risks

July 1, 2025

Management considers the potential for fraud, improper payments, and information security in assessing risks to the achievement of its objectives. The following points of focus highlight important characteristics relating to this principle.

- **Considers various types of fraud** - Management considers the types of fraud, improper payments, and information security risks that can occur within the agency to provide a basis for identifying potential risks, such as:

  - **Fraudulent financial reporting** - Intentional misstatements or omissions of amounts or disclosures in financial reporting to deceive users of the financial information. This could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles.

- **Misappropriation of assets** - Theft or misuse of an agency's assets. This could include theft of property, misuse of data, embezzlement of receipts, or fraudulent payments.
- **Other illegal acts** - Intentional violations of laws or regulations through willful misrepresentation that may be related to financial or nonfinancial activities including but not limited to corruption, bribery, extortion, and cybercrimes.

- **Considers fraud risk factors** - Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs. Management considers fraud risk factors which include the following:

  - **Incentive/pressure** - Management or other personnel have an incentive or are under pressure, 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. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

  While fraud risk may be greatest when all three risk factors are present, one or more of these factors may indicate a fraud risk. Other information provided by internal and external parties can also be used to identify fraud risks. This may include allegations of fraud or suspected fraud reported by an internal auditor, employees, or external parties that interact with the agency.

- **Considers improper payments risks -** Improper payment risk factors that could impact the agency can result from lack of oversight, mismanagement, errors, deficiencies in internal control, abuse, or fraud. While all payments that result from fraud are considered improper, not all improper payments are the result of fraud. Types of improper payments may include the following:

  - **Overpayments -** Payments in excess of the amount due to be paid to the recipient. They include payments to ineligible recipients, any payments for ineligible goods and services, payments for goods and services not received, and duplicate payments.
  - **Underpayments -** Payments to recipients that were not received but to which they were entitled.

- **Considers information security risks -** Information security risk is the risk to an agency's operations, assets, and personnel, as well as external parties, due to unauthorized access, use, disruption, modification, or destruction of information or information technology. These risks may impact the information security objectives of confidentiality, integrity, and availability. Types of information security risk may include the following:

  - **Unauthorized access** - Controls may be overridden by unauthorized users gaining access to the agency's information technology platform or software system. Failure to appropriately limit physical access to information or an information technology system may also allow a malicious attacker to access or modify information.

- **Exploitation of personnel** - Attacks that coerce users into revealing information or giving an unauthorized user access to a platform or software system.
- **Installation of malicious software** - Installation of a program or file that intentionally attacks an agency's information technology by corrupting or stealing data or locking the entity out.
- **Automated attacks** - Attacks on information technology may be automated through mechanisms may include bots, artificial intelligence, and machine learning software.
- **Undetected errors** - An agency's information technology may be improperly altered by unauthorized users without visible evidence and therefore may not be readily detectable by users.
- **Threats to physical environment** - Threats to the physical environment can result in the loss of information or information technology system damage or disruption. This may include events such as a fire, loss of electricity, or a natural disaster.

- **Responds to fraud risk** - Management analyzes and responds to fraud, improper payments, and information security risks using the same process performed for all risks so they are effectively mitigated. Refer to Principle 7 in Subsection 20.22.40.

20.22.60 Principle 9 – Identifies, analyzes, and responds to changes

July 1, 2025

Management identifies, analyzes, and responds to changes that could significantly impact its system of internal control. The following points of focus highlight important characteristics relating to this principle.

- **Identifies significant changes** - The risk identification process considers significant changes in:
  - **The external environment** which includes the regulatory, economic, technological, legal, and physical environment in which the agency operates.
  - **The business model** due to new technologies, rapid growth, legislation, and other factors.
  - **Leadership** which could lead to changes in management attitudes and philosophies on the system of internal control.
- **Establishes a change assessment process -** Management develops and documents a change process assessment for identifying, analyzing, and responding to risks related to significant changes. Establishing a change process assessment before changes occur is essential to maintaining an effective internal control system.
- **Analyzes and responds to changes** - Because changing conditions may prompt new risks or changes to existing risks, management analyzes and responds to identified changes that could significantly impact its system of internal control in order to maintain its effectiveness. Management analyzes and responds to changes using the same process performed for all risks so they are effectively mitigated. Refer to Principle 7 in Subsection 20.22.40.