EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

March 10, 2026

CIRCULAR A-123
Revised

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: OMB Circular No. A-123, Management's Responsibility for Internal Control

This update to OMB Circular A-123 reflects the Administration's commitment to combatting fraud, waste, and abuse in agency operations through the identification, response to, and remediation of risks. Prior versions of Circular A-123 have overly deferred to direction and priorities of external entities whose views are not binding on the Executive Branch such as the Government Accountability Office. Doing so has failed to prioritize agency internal control processes to adequately protect American taxpayer dollars, leading to documented examples of widespread abuse.

In March the President signed Executive Order 14249 *Protecting America's Bank Account Against Fraud, Waste, and Abuse* which reinforced agencies' responsibilities under OMB Circular A-123 to identify, prevent, and reduce fraud, waste, and abuse. It is the responsibility of all Federal managers to effectively manage the internal control process to identify, prevent, reduce, and eradicate risks. This update underscores that the ultimate goal of our internal control framework is to enable effective stewardship of taxpayer resources and operational accountability.

Since 1981, the Federal Manager's Financial Integrity Act (FMFIA) has mandated Federal agencies to establish internal controls and report annually on their effectiveness. Circular A-123 ensures federal agencies are accountable for their operations and finances, foster transparency, and responsibly manage and safeguard taxpayer funds.

This Circular provides streamlined guidance for agencies to improve internal control assessment and continuous monitoring. All organizational levels and employees are responsible for internal control and identifying risks at every level of agency operation.

This revision provides agencies with guidance on adopting a comprehensive, preventative, risk-informed approach to internal control that enhances decision-making, improves program performance, ensures the integrity of Federal operations, and protects Taxpayer dollars.

The revision of Circular A-123 is effective upon issuance and supersedes all previous versions.

Russell T. Vought
Director

Attachment: OMB Circular No. A-123, Management's Responsibility for Internal Control

OMB Circular No. A-123: Management's Responsibility for Internal Control

Purpose: Office of Management and Budget (OMB) Circular A-123 provides guidance to Federal agencies regarding establishing internal control over operations, reporting, and compliance. The Circular implements the requirement that agency heads establish and maintain internal control and evaluate its effectiveness.

Authority: This Circular is authorized by the Federal Managers' Financial Integrity Act (FMFIA) of 1982 (Pub. L. 97-255), as amended and codified at 31 U.S.C. 3512(c) and (d), and the Government Performance Results Act (GPRA) Modernization Act of 2010 (Pub. L. 111-352).[1]

Policy: It is the policy of the Federal Government that agencies[2] establish and maintain effective internal control systems that establish and achieve specific internal control objectives to provide reasonable assurance that programs achieve their goals and objectives, and that agency business processes operate efficiently and effectively, comply with applicable laws and regulations, safeguard federal assets, and produce reliable financial and performance information.

Each Federal employee is responsible for implementing internal control. Federal leaders and managers are accountable for establishing internal control systems, agency strategic and performance goals, responding to risks, managing program performance and operations, and maintaining assessing controls that help their agencies operate effectively and deliver results.

Management should consistently assess and improve their agency internal control in accordance with this Circular and the requirements for internal accounting and administrative control systems set forth in 31 U.S.C. 3512.

Requirements: This Circular requires agencies to assess and report on internal control annually. Management will provide assurances on internal control effectiveness, to include information regarding identified material weaknesses and corrective action, as appropriate. These assurances must be provided annually in a single report in the Agency Financial Report (AFR), Performance and Accountability Report (PAR), or other management report labeled "Analysis of Entity's Systems, Controls and Legal Compliance."

OMB Circular No. A-123 requires agencies to establish and maintain internal control over the operation and execution of business processes and internal control systems. Management will assess its processes and systems to improve internal control over operations, reporting, and compliance, and provide reasonable, but not absolute, assurance that the objectives of an agency will be achieved.

- Management is responsible for evaluating the effectiveness of internal control annually based on these guidelines established in accordance with 31 U.S.C. 3512(c) and (d).

[1] As codified, in part, at 5 U.S.C. 306 and 31 U.S.C. 1115, 1116, and 1120 through 1125

[2] See "Applicability" section below.

- Management is responsible for establishment of a governance structure to effectively implement, direct, and oversee implementation of the Circular processes that meet internal control objectives.
- Agencies should leverage existing functions within the organization when implementing the Circular, including establishing a governance structure and evaluating agency risks and internal controls agency wide.
- Agencies should continue to develop and apply risk management practices, which include the risk assessment of internal control and the risk identification and response capabilities for new or emerging risks, or changes in existing risks, at the programmatic, agency, or organizational unit, and enterprise-wide level as applicable.

This Circular establishes minimum requirements for evaluating internal control and does not prescribe assessments of specific business functions. However, agencies may, at their discretion, conduct targeted reviews of operational areas that pose material risks (such as acquisition and cybersecurity) when these areas affect the agency's ability to provide reasonable assurance over compliance, operations, or reporting. Agencies are encouraged to use existing oversight mechanisms, performance data, and governance structures to support such reviews, where appropriate.

Effective Date: This Circular is effective on March 10, 2026. Appendices A, B, C, and D of OMB Circular No. A-123 remain in effect.

Applicability: "Agency," as that term is used in this Circular, means each "executive agency" as defined in 31 U.S.C. 102 including independent regulatory agencies.[3]

Inquiries: Information concerning this Circular can be obtained from the Office of Federal Financial Management (202) 395-3993 or the Office of Performance and Personnel Management, (202) 395-5670 Office of Management and Budget, Washington, D.C. 20503.

Copies: Copies of this Circular may be obtained from www.whitehouse.gov/omb.

[3] 31 U.S.C. §§ 102 and 3501 (defining executive agencies); 31 U.S.C. § 9106 (applying FMFIA requirements to government corporations). *See also* Executive Order 14215, "Ensuring Accountability for All Agencies," Fed. Reg. 90 FR 10447 (Feb. 18, 2025), §§ 2 and 7 (defining independent regulatory agencies).

TABLE OF CONTENTS

I. INTRODUCTION

Federal leaders and managers are responsible for establishing and achieving goals and objectives, improving operational effectiveness and efficiency, maintaining compliance with relevant laws and regulations, providing reliable reporting, and managing risks across all levels of the agency.

The Federal Managers' Financial Integrity Act of 1982 (Integrity Act or FMFIA), as amended and codified at 31 U.S.C. 3512(c) and (d), requires Federal agencies to establish internal accounting and administrative controls that reasonably ensure that: (1) obligations and costs comply with applicable law; (2) all assets are safeguarded against waste, loss, unauthorized use, and misappropriation or other misuse of agency funds or property; and (3) revenues and expenditures applicable to agency operations are recorded and accounted for properly so that accounts and reliable financial and statistical reports may be prepared and the accountability of assets may be maintained.[4] FMFIA requires the Director of the Office of Management and Budget (OMB), in consultation with the Comptroller General, to establish guidelines that the head of each agency must follow in evaluating whether such controls are consistent with the requirements of the Integrity Act.[5]

FMFIA also requires the head of each agency to evaluate such controls annually and to submit to Congress and the President either a statement that the controls are adequate or a report on any weaknesses in such controls with a plan and schedule for corrective measures.[6] In addition, the head of each agency must evaluate and report annually on whether the accounting system of the agency conforms to the principles, standards, and requirements prescribed by the Comptroller General under 31 U.S.C. 3511(a).[7]

Internal control is essential to mitigate the risks presented by an agency's operations, mission, and strategic goals. The three objectives of internal control are to reasonably ensure: (1) the effectiveness and efficiency of operations; (2) reliability of financial reporting; and (3) compliance with applicable laws and regulations. Although leadership is primarily accountable or establishing and overseeing internal control, all staff contribute to its execution and effectiveness. Federal managers must carefully consider the appropriate balance between controls and risk in their programs and operations.

Agency managers must ensure an appropriate balance between the strength of controls and the relative risk associated with particular programs and operations. As controls are designed and implemented to mitigate risk, a lack of internal control can result in unacceptable risks levels such as inaccurate data, inefficient operations, misuse of resources, or diminished public trust.

[4] 31 U.S.C. 3512(c)(1).

[5] 31 U.S.C. 3512(d)(1).

[6] 31 U.S.C. 3512(d)(2)(A) and (3).

[7] 31 U.S.C. 3512(d)(2)(B).

The U.S. Government Accountability Office (GAO), a Legislative Branch Agency whose views are not binding on the Executive Branch, is responsible for issuing the *Standards for Internal Control in the Federal Government* (commonly known as the Green Book). OMB is responsible for establishing the guidelines that the head of each Executive Branch agency must follow to implement and comply with FMFIA.[8]

This Circular implements FMFIA for the Executive Branch by providing guidance to agencies on adopting an internal control framework designed to mitigate risks and meet the requirements of FMFIA, and related to improving effectiveness and accountability. This risk-based framework adopted by agencies should be an integral part of the entire cycle of a transaction or event, which is integrated with strategic planning, budgeting, management, accounting, performance monitoring, and budget formulation processes. This integrated approach should enhance decision-making, improve program performance, support accurate auditing, and provide reasonable assurance that objectives of an entity will be achieved.

Agencies should implement an internal control framework through a governance structure defined through laws enacted by the Congress, Executive directives, and agency policies. The Federal Government's core governance processes are defined by OMB budget guidance.[9] OMB Circular No. A-123 provides guidance to Federal Managers on improving the accountability and effectiveness of Federal programs and operations by identifying and managing risks, establishing requirements to assess, correct, and report on the effectiveness of internal controls.

An effective system of internal control gives agencies the means to provide accountability for their programs, as well as the means to obtain reasonable assurance that their operations and programs meet established goals and objectives. While agency leadership and management at all levels, including program and financial managers, have a significant impact on an organization's system of internal control, all staff and personnel have a responsibility and a role in ensuring that their systems and programs are effective at achieving the organization's mission.

A. DEFINITION OF INTERNAL CONTROL

Internal control is a process effected by an entity's oversight body, management, and other personnel designed to provide reasonable assurance that the objectives will be achieved. The objectives and related risks can be broadly classified into one or more of the following three categories:

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

[8] 31 U.S.C. 3512(d).

[9] For example, OMB Circular No. A-11 defines the processes by which the Executive Branch develops and executes Strategic Plans, compiles the President's Budget request, assembles Congressional Budget Justifications, conducts performance reviews, and reports on performance.

Key characteristics of internal control include:

- Continuous, embedded, and distributed throughout organization: It is a process consisting of ongoing tasks and activities, embedded in daily operations, and effected by people at every level of the organization;
- Provides reasonable assurance: It provides reasonable assurance to the agency head and senior leadership that the organization achieved its objectives;
- Adaptable: It is adaptable to the agency's structure; and
- Flexible: It is flexible in its application across different programs and functions.

Internal control includes specific controls, which consist of documented policies and procedures that management establishes to effect relevant principles within each component of internal control. Management should establish a system of internal control that helps prevent, detect, mitigate, and respond to unacceptable risks to program objectives or agency missions.

Even the most robust internal control systems cannot guarantee absolute success as risk response should be cost-beneficial and designed to reach an acceptable level of risk. Many factors beyond an agency's control, such as natural disasters or economic shifts, can impact outcomes.

B. IMPORTANCE OF INTERNAL CONTROLS

Internal controls are the checks and balances that support the achievement of mission objectives by mitigating the likelihood and impact to risks, including fraud, waste, and abuse, while ensuring efficient use of resources. Weak internal controls can lead to a lack of accountability and a wide range of consequences, such as inaccurate or incomplete information to waste or misuse of resources. If adverse events occur, such as theft or a severe failure, it can be difficult to identify the specific cause of the problem and determine responsibility if accountability is not established.

Control activities can be either preventive or detective. Preventive controls are designed to avoid unintended events or results from occurring. Detective controls are designed to discover, and provide timely corrective actions to address, an unintended event or result after it occurs. On a broader level, a lack of accountability can result in the loss of public confidence and support, and can impede an organization's ability to serve the public effectively.

II. ORGANIZATIONAL ROLES AND REQUIREMENTS

Every member of the federal workforce has a role in the system of internal control. Depending on the structure of the agency, an individual's position may determine the extent of that individual's responsibility and involvement in internal control. Thus, the internal control activities performed by the head of the agency, senior leadership, managers (to include financial and program managers as appropriate), and staff and personnel may not have the same focus.

A. ROLES

Head of the Agency. The head of an agency's role in internal control may focus on the major objectives and strategic mission of the organization.

The head of the agency should maintain awareness of the existence of risks and opportunities in either the internal and external environment that might indicate the need for a change in the organization's plans.

In accordance with FMFIA requirements, the head of each executive branch agency must prepare an annual statement regarding whether the agency's systems of internal accounting and administrative controls comply with FMFIA.[10] If the systems do not comply, the head of the agency will prepare a report identifying any material weaknesses in the agency's system of internal accounting and administrative controls, and describing the plans and schedule for correcting any such weakness.

Senior Leadership. Senior leadership roles are generally held by agency executives holding overall responsibility for establishing the organization's system of internal control, including: (1) ensuring an efficient and effective system of internal control; (2) establishing a system of internal control review; (3) documenting the system of internal control and making policies and guidelines available to all employees; and (4) implementing education and training about the system of internal controls, related to topics including risk, internal control, and internal control evaluations. Senior leadership may assign these internal control functions to lower-level management as appropriate but should maintain an adequate level of oversight.

If senior leadership does not establish strong, clearly stated support for internal control, the organization may find it difficult to achieve an effective system of internal control. Additionally, senior leadership must set a positive "tone at the top" by conducting the organization's operations in an honest and ethical manner and by establishing accountability at all levels to establish and guide an integrated internal control framework. Finally, senior leaders should assist in identifying strategic risks that need additional cross-cutting oversight at the agency level.

Managers. Managers should monitor all activities and transactions under their purview to ensure that staff and personnel are performing their assigned responsibilities and control activities are designed and functioning properly to mitigate risk. Managers should ensure their area of responsibility has an appropriate control environment with open and sufficient communication, and risk identification. Depending on the structure of an agency, some higher-level managers may assess how well controls are functioning within an organization, and how well direct line supervisors are monitoring their respective staff and personnel. Managers should educate staff and personnel regarding control activities and encourage them to be alert to and report any irregularities. Management should also remind staff and personnel to note changes in their immediate internal and external environments, to identify any risks, and to report opportunities for improvement.

Program and Financial Managers. Depending on the structure of an agency, program and financial managers may serve as analysts and oversee a specific function, program, or area of responsibility related to the agency's mission. In some cases, they may also oversee staff and personnel. Program and financial managers may be involved in detecting any problems with existing control activities and identifying risks and opportunities.

[10] 31 U.S.C. 3512(d)(2)-(3).

Alternatively, they may hold duties more like managers as described above. In this case, their involvement and responsibilities for internal control will fall under those described under "managers."

Staff and Personnel. The primary focus of non-managerial staff and personnel should be on monitoring their own work to ensure it is being performed properly and consistently with applicable internal controls. They should correct identified errors before work is referred to higher levels for review. Because of their involvement with the details of the organization's daily operations, staff and personnel members have the best vantage point for directly implementing controls and detecting any problems with existing control activities. Staff and personnel should identify any risks or failures with control activities to the appropriate managers as previously described.

B. REQUIREMENTS FOR AN EFFECTIVE SYSTEM OF INTERNAL CONTROL IMPLEMENTATION

Agency Leadership Requirements

Related Roles: Head of the Agency and Senior Leadership

1. Control Environment: Set the "tone at the top" for the organization and provide oversight for the agency's system of internal control. Examples of related actions may include:

    a. Internal Control Policy: Establish an internal control policy that outlines the agency's commitment to maintaining effective internal controls.

    b. Internal Control Framework: Establish an internal control framework that provides a structured approach to internal control.

2. Risk Assessment: Clearly define the agency's objectives and develop risk appetite and risk tolerance levels.

3. Risk Oversight and Assessment: Identify, assess, oversee and prioritize risks to internal control at the agency level and identify or elevate strategic risks that may impact the enterprise, as appropriate.

3. Control Activities: Oversee the establishment of internal controls and ensure that the control environment is designed and operating sufficiently to mitigate risks.

4. Information and Communication: Provide external communication, as appropriate, regarding matters related to the agency's system of internal control.

5. Monitoring: Provide oversight and monitoring of the agency's system of internal control. Examples of related actions may include:

a. External Service Organization Monitoring: Review services that have been outsourced on a regular basis to ensure that the service provider has sufficiently designed and implemented controls in accordance with the established agreement.

b. Corrective Action: Take corrective action to address any internal control deficiencies or weaknesses identified at the agency level.

Agency Program / Operational Requirements

Related Roles: Managers, Program and Financial Managers, Staff and Personnel

1. Internal Control Evaluation: Assess the effectiveness of internal controls including those associated with financial reporting, performance, and operations within their program or activity.

2. Risk Assessment: Identify, assess, and prioritize risks to internal control at the program level.

3. Corrective Action: Implement control activities to mitigate identified risks within their program or activity. Take corrective action to address any internal control deficiencies or weaknesses identified at the program level.

4. Information and Communication: Ensure that relevant information is identified, documented, and communicated to stakeholders within their program or activity.

5. Monitoring: Continuously monitor controls within their program or activity to ensure their effectiveness.

6. Risk Oversight and Assessment: Identify, assess, oversee, and prioritize risks to internal control at the program level, and identify or elevate strategic risks that may impact agency objectives at the enterprise level, as appropriate.

7. Training and Awareness: Facilitate training and awareness programs to ensure that employees within their program or activity understand their roles and responsibilities in internal control.

III. COMPONENTS AND PRINCIPLES OF AN INTERNAL CONTROL FRAMEWORK

The five components of internal control must be successfully designed, implemented, and functioning sufficiently for the internal control system to be effective. Table 1 outlines five core components for internal control with 17 principles that describe the fundamental concepts associated with each component.

Table 1. Components and Principles of Internal Control

Components of Internal Control	Principles
Control Environment: The foundation for an internal control system which provides the discipline and structure to help an entity achieve its objectives.	1. The oversight body and management should demonstrate a commitment to integrity and ethical values. 2. The oversight body should oversee the entity's internal control system. 3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. 4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals. 5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.
Risk Assessment: The identification and analysis of risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.	6. Management should define objectives clearly to enable the identification of risks and define risk tolerances. 7. Management should identify, analyze, and respond to risks related to achieving the defined objectives. 8. Management should consider risks related to fraud, improper payments, and information security when identifying, analyzing, and responding to risks. 9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.
Control Activities: The actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels.	10. Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels. 11. Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels. 12. Management should implement control activities through policies and procedures.
Information and Communication: The quality information management and other personnel communicate and use to support the internal control system.	13. Management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system. 14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system. 15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.
Monitoring: Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.	16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. 17. Management should remediate identified internal control deficiencies on a timely basis.

A. CONTROL ENVIRONMENT

The **Control Environment** encompasses the set of standards, processes, and structures that are the backbone for establishing internal control across the agency. The control environment forms the foundation for effective internal control. It involves a culture of integrity, ethical behavior, and accountability at all levels of the agency, which starts from the tone set at the top of the agency, which carries throughout.

It is the product of senior leadership's governance, leadership philosophy, and management style, and includes the sense of competence, ethical values, integrity, and morale instilled throughout the organization. The control environment has a pervasive influence on the decisions and activities of an organization, and provides the foundation for the overall system of internal control.

B. RISK ASSESSMENT

Risk is the effect of uncertainty on objectives. Risk may be measured as the probability or threat of damage, injury, loss, or negative occurrence caused by external or internal factors. Risks can threaten or otherwise adversely affect the achievement of the organization's objectives. The agency's **risk appetite** may vary by the type of risk and the mission of the organization. Risk appetite articulates the level and type of risk the agency will accept while conducting its mission and carrying out its strategic plan.

Management should define objectives clearly and in alignment with the organization's mission, strategic plan, and performance goals to enable the identification of risks and also define risk tolerances. **Risk tolerance** is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. Managing the risks associated with achieving an organization's mission through its objectives requires an assessment of these risks.

A **Risk Assessment** includes the review of activities and conditions that support or prevent mission completion. A risk assessment will be based on the impact and likelihood of an event to prevent achieving the defined objectives. The risk tolerance, or variation in performance, should be relative to the importance of achieving the objectives. For each risk that is identified, management may develop a risk registry to document the different types of risks, as a list, to inform decisions regarding the appropriate risk response, such as: accept the risk, reduce the risk to an acceptable level, share the risk, or avoid the risk.

Risk assessments should specifically include consideration of the impact to the mission and objectives of the agency. They should also include consideration of vulnerabilities to fraud, improper payments, and information security risk. Fraud risk should be evaluated in conjunction with other risks that may impact the program or agency's ability to achieve its objectives. This includes assessing the likelihood and significance of potential fraud scenarios including monetary and non-monetary fraud. Agencies should identify where fraud risk is most likely to occur and incorporate those risks into the broader risk assessment process. Management should ensure that fraud risk is considered when setting risk tolerances and determining appropriate responses to identified risks.

Since the risk environment and posture are always changing, agencies are encouraged to utilize a change assessment process to identify, analyze, and respond to risks resulting from significant external or internal changes. A change assessment process and other recurring risk assessment processes assure agencies that the internal control system is ready to identify, analyze and respond to changing conditions.

Risk assessments include identifying the risks from stakeholders, learning more about the risk relative to objectives, and determining what can be done about it. A risk evaluation includes development of the risk appetite as the amount of risk that an organization is willing to accept to achieve its objectives, given conditions. Additional details of the risk assessment process can be found in Attachment 1 of this Circular (The Risk Assessment Process).

Risk Management is discussed further in Section VI.

C. CONTROL ACTIVITIES

Control activities are the actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels. They are designed to ensure proper execution of agency actions to achieve objectives and prevent or mitigate identified risks. When designing and implementing control activities, management should consider the following:

- The control activity's cost should not exceed the costs incurred (as defined by management) if the undesirable event occurred.
- Control activities should be built into business processes and systems as they are being designed. Adding control activities after the development of a process or system, while sometimes necessary, is generally more costly.
- The allocation of resources among control activities should be based on the impact and likelihood of the risk they are intended to reduce.

Control activities may include several ways to mitigate risks and can be preventive or detective, depending on when the control activity occurs within the process cycle.

- Preventive controls aim to avoid unintended events before they happen (for example, employee background checks, data encryption, segregation of duties, equipment maintenance, safety training, etc.).
- Detective controls identify and correct issues or events that do occur, and alert managers so they can take corrective action (for example, audits, performance reviews, inventory counts, log monitoring, accounting reconciliation, etc.).

Management is responsible for prioritizing preventive controls for cost-efficiency and effectiveness, when possible, and employing detective controls to identify undesired outcomes in a timely manner.

In situations where preventive controls are not feasible, strengthening detective controls and monitoring activities becomes critical. Each control type is necessary to manage risk.

Steps to Designing Control Activities Include:

- Review the goals and objectives for each of the major processes in your agency, program, or entity (or all of these, as applicable).
- Identify potential risks that may impact the agency's ability to satisfy those goals and objectives and determine a risk appetite and tolerance, as appropriate.

- Assess vulnerabilities in the steps of each process to identify weaknesses in control based on your risk assessment.
- Diagnose a clear picture of "what works" and "what could go wrong" in the control environment.
- Design control activities to respond to the risks identified in the previous steps. If the agency decides to mitigate an inherent risk, control activities should be designed and implemented until the residual risk remaining is at or below the tolerable level.
- Do the work to implement the controls, communicate the change, and monitor results.

The following are some of the more commonly used control activities:

- Documentation: preserving evidence to support a decision, or record an event, transaction, or system.
- Demonstration: a dynamic, observable validation method where capabilities are actively shown to function as intended under realistic conditions
- Approval and Authorization: higher level endorsement or validation of decisions, events, or transactions
- Verification: determination of the completeness, accuracy, authenticity and/or validity of transactions, events, or information
- Supervision: ongoing oversight, management, and guidance of an activity to ensure the results of the activity achieve the established objectives.
- Separation of Duties: the division of key tasks and responsibilities among various employees and units of an organization
- Safeguarding Assets: restricting access to resources and information to help reduce the risk of unauthorized use or loss.
- Reporting: conveying information to promote accountability for actions and decisions

D. INFORMATION AND COMMUNICATION

Information and communication are critical to maintaining internal control. Agencies should have established channels to share processes, systems, procedures, relevant risk, and control information across the organization. Information must come from reliable internal and external sources in a timely manner based on the identified information requirements. Quality information must be appropriate, current, complete, accurate, accessible, and provided on a timely basis. Reporting systems should ensure timely identification of success and resolution of issues.

1. INTERNAL COMMUNICATION

Information should travel in all directions (across, and up and down within an organization) to ensure that all appropriate members of the organization are informed and that decisions and actions of different units are communicated and coordinated. Agencies should establish communication channels that:

- provide timely information;
- inform employees of their duties and responsibilities;

- enable the reporting of sensitive matters;
- enable employees to provide suggestions for improvement;
- provide information necessary for all employees to carry out their responsibilities; and
- convey leadership’s message that internal control responsibilities are important and should be taken seriously.

2. EXTERNAL COMMUNICATION

External communication with customers, regulators, auditors, contractors, service providers, and other outside organizations is also essential to effective internal control. Information should be communicated externally through appropriate reporting lines so that external parties can help the agency or program achieve its objectives and address related risks.

E. MONITORING

Monitoring is the ongoing evaluation of internal control components, either individually or as a whole system, to determine if they are present and functioning, as well as to evaluate if desired outcomes are achieved within the risk tolerance, or if residual risk remains and adjustments are needed. Agencies should focus monitoring efforts on internal control and achievement of the organization’s mission.

All personnel within the agency have some responsibility for monitoring, with the position a person holds in the organization determining the focus and extent of their responsibilities. Thus, the monitoring performed by staff, managers, and senior leadership generally will not have the same focus.

The monitoring performed by staff, managers, and senior leadership should regularly evaluate the system of internal control and focus on the following areas:

- Control Environment: Senior leadership and managers should monitor the control environment to ensure that staff at all levels maintain established standards of behavior, staff is competent, and training is sufficient to accomplish the agency’s mission.
- Risk Assessment: Managers should also monitor the organization’s internal and external environment to identify any changes in risks and the development of opportunities for improvement. If changes are identified, managers should take appropriate action to address these new or changed risks and opportunities.
- Control Activities: Effective monitoring provides the opportunity to correct any control activity problems and to control the risk before an unfavorable event occurs.
- Information and Communication: Staff at all levels must evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior leadership, as appropriate.

For monitoring to be most effective, all employees need to understand the agency or program mission, objectives, and risk tolerance levels, as well as their own responsibilities.

In addition, if deficiencies or gaps are identified as part of the monitoring efforts, management must also monitor the corrective actions to resolve such deficiencies.

IV. MANAGING AND ASSESSING THE INTERNAL CONTROL SYSTEM

An agency's senior leadership is responsible for ensuring that the right controls are in place, and that they are performing as intended. While senior leadership is responsible for the organization's control framework, the managers are responsible for implementing and monitoring internal controls. All levels of management must work together to create an integrated internal control system that lowers risk to an acceptable level and assists the program or agency in meeting its goals and objectives.

Managers and staff are generally responsible for identifying potential risks, designing and implementing controls for their areas of responsibility, and keeping current with events and changes that may affect the controls implemented.

In addition to establishing internal controls, agency managers must continuously monitor, assess, and improve the effectiveness of controls associated with their internal control objectives. This continuous monitoring, and other periodic evaluations, provide the basis for the agency head's annual assessment and report on internal control as required by FMFIA.

A. DOCUMENTATION REQUIREMENTS FOR INTERNAL CONTROL ASSESSMENT

Agency managers must determine the appropriate level of documentation needed to support assessments. Proper documentation is a necessary part of an effective internal control system. The level and nature of documentation may vary based on the size of the entity and the complexity of the operational processes the entity performs. Documentation to fulfill the FMFIA requirements may include:

- The results of risk assessments, including the analysis of risk, identification of risks, and the associated controls. Risk assessments should annotate whether the risk is related to fraud, improper payments, information security, significant internal and external changes, or some combination of these.
- Documents detailing the design, implementation, and operating effectiveness of the internal control system.
- Support for decisions that a principle is not relevant, including rationale for how the associated component is designed, implemented, and operated effectively.
- Policies that define internal control responsibilities.
- Results from ongoing monitoring and change assessments, and separate evaluations to identify control issues.
- Corrective action plans and results for mitigating control deficiencies in a timely manner.

Sources of Information: Agency assessments may draw from multiple information sources, including:

- Management documentation of its control systems, policies, procedures, and daily operational insights.
- Reviews specifically conducted for control assessment or those where internal control is assessed as part of another review.
- Assessments and reviews conducted to reduce improper payments, fraud, waste, and abuse in accordance with the Payment Integrity Information Act of 2019[11] and OMB Circular No. A-123, Appendix C (Requirements for Payment Integrity Improvement).
- Annual organizational performance plans, reports, data-driven performance and strategic reviews, and program evaluations in accordance with the GPRA Modernization Act of 2010 and OMB Circular No. A-11.
- Information security and technology governance reports pursuant to the Federal Information Security Modernization Act (FISMA) of 2014[12] and OMB Circular No. A-130 (Managing Information as a Strategic Resource).
- Program reviews under OMB Circular No. A-129 (Policies for Federal Credit Programs and Non-Tax Receivables).
- Single Audit Act reports, related recipient compliance with OMB Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.[13]
- Reviews under the Antideficiency Act.[14]
- Independent audit reports, including Office of Inspector General (OIG) Management Challenges.
- Congressional reports.
- Other reviews relevant to agency operations or management controls.

Use of information should take into consideration the completeness of the assessment and whether the process included an evaluation of internal control. Agency management should avoid duplicating reviews that assess internal controls, and should coordinate their efforts with other evaluations to the extent practical. Agencies should internally retain sufficient documentation to support their assurance statements under FMFIA.

B. INTERNAL CONTROL ASSESSMENT

Internal control assessment is the process used to determine whether the agency or program will achieve its goals and objectives, whether the elements of the internal control system are functioning effectively, and whether risks to the organization and opportunities for improvement are being identified.

While monitoring involves performing daily or routine procedures—such as supervision, transaction review, and problem resolution—evaluation involves conducting periodic assessments of performance compared against established expectations or standards.

[11] Pub. L. 116-117, codified at 31 U.S.C. §§ 3351-3358.
[12] Pub. L. 113-283, codified at 44 U.S.C. §§ 3551-3558.
[13] 2 CFR part 200.
[14] Codified at 31 U.S.C. §§ 1341, 1342, 1349-1351, and 1511-1519.

When assessing whether a system of internal control reduces the risk of not achieving objectives related to operations, reporting, or compliance to an acceptable level, management should follow a risk-based assessment approach, described in the following example:

- Conduct an Assessment of Internal Control: Management conducts an evaluation of internal controls for each of the internal control principles for each of the entity objectives.
- Prepare a Summary of Internal Control Deficiencies: Management creates an aggregated or summary log of all identified internal control deficiencies and the results of their assessment process. The log may support the evaluation of the internal control components and principles.
- Conclude an Internal Control Principle Evaluation: Management summarizes its determination of whether each principle is designed, implemented, and operating effectively. That determination is a function of management judgment based on:
    - the applicability of the principle to the agency's circumstances;
    - whether the agency has been able to implement, perform, and apply the principle;
    - any internal control deficiency that may result from not adequately implementing the principle; and
    - the extent of compensating internal controls within the principle, and the extent to which the remaining risk impacts the agency's ability to achieve its objectives and meet its mission and goals.
- Internal Control Component Evaluation: Management summarizes its determination of whether each of the five components is designed, implemented, and operating effectively. Evaluation of internal control components is a function of management judgment and qualitative determinations. If an internal control component or associated principle is not designed, implemented, and operating effectively, management is unable to conclude that the internal control component is operating effectively.
- Overall Assessment of a System of Internal Control: Management summarizes its determination of whether each of the five components and associated principles are designed, implemented, and operating effectively within the agency, and whether components are operating together in an integrated manner.
- In addition, management must determine the severity of internal control deficiencies or a combination of deficiencies when aggregated across the components.

Attachment 2 of this Circular (Internal Control Assessment Exhibits) provides tables that demonstrate internal control assessment examples.

C. IDENTIFICATION OF INTERNAL CONTROL DEFICIENCIES

An effective internal control assessment will evaluate for and identify potential deficiencies in internal control. When deficiencies are identified they must, at a minimum, be reported to the next supervisory level for consideration of importance. Reporting of deficiencies should also include the agency's Inspector General.

Agency managers and employees are encouraged to identify control deficiencies at every level of an agency’s processes. Definitions of control deficiencies, significant deficiencies, and material weaknesses are provided in Table 2, Section V of this Circular. If one or more internal control components are not operating effectively, a material weakness must be reported in the AFR or PAR, or applicable management reports.

D. INTERNAL AND EXTERNAL AUDITS

Agencies should conduct regular audits to evaluate effectiveness of their control systems. These audits provide an objective perspective on the robustness and compliance of the agency's controls. Audits should focus on the adequacy of the control environment, reliability of reporting, compliance with applicable laws and regulations, and effectiveness of risk management. Audits are critical for identifying potential weaknesses that may not be self-identified and validating the integrity of the agency’s controls.

Audit findings that identify deficiencies—whether internal or external— should be analyzed and used to improve internal control activities and risk management processes. Agencies should systematically review and prioritize audit recommendations, focusing on control deficiencies or high-risk areas that may have the most significant impact on operations, financial reporting, or compliance. Agencies must develop a detailed corrective action plan based on audit findings, ensuring that the plan addresses both the root causes and the symptoms of identified deficiencies. The implementation of corrective actions should be tracked to ensure timely completion.

E. CORRECTIVE ACTION PLANS

When internal control deficiencies are identified, including those identified through external audits and evaluations, agency management is responsible for developing appropriate corrective action. Corrective action should be implemented without delay to minimize any potential adverse effects on the agency operations or mission.

Agencies must document the steps taken to resolve identified issues, the timeline for completing corrective actions, and the responsible parties. Management should determine the necessary resources for addressing control deficiencies, which may include personnel, operational support, training, and senior leadership support.

Senior leadership should receive timely updates on the status of ongoing corrective actions and any emerging risks that may require management attention. Reports should be timely and detailed enough to allow leadership to make informed decisions regarding resource allocation, policy adjustments, and risk mitigation strategies.

Corrective actions will be tracked, tested, and verified to ensure their effectiveness in resolving the identified issues in alignment with a management decision. In cases where corrective action takes longer than anticipated, agencies should provide regular updates to senior management and relevant oversight bodies on the progress of remediation efforts.

A summary of corrective actions for any material weaknesses that remain unresolved at the time of reporting, including those identified through external audits and evaluations, must be included in the AFR or PAR, or applicable management reports. This summary should include a description of the weakness, the status of corrective actions, and the timeline for resolution. Detailed corrective action plans must be maintained internally and made available for OMB and audit review.

The performance appraisals of relevant officials may reflect their effectiveness in resolving or implementing corrective actions for identified material weaknesses. Agencies must fully disclose any uncorrected internal control weaknesses, particularly those that are material.

A determination that a control deficiency has been corrected should only be made after sufficient corrective actions have been taken and validated. This determination should be documented in writing, supported by appropriate evidence, and made available for review.

Agencies should perform a root-cause analysis for each deficiency to ensure that corrective actions address the underlying causes, not just the symptoms. Identifying the root cause is management's responsibility and should include considerations from audit findings, if applicable. However, auditors are not responsible for identifying the root causes, so relying solely on audit recommendations may result in incomplete or ineffective corrective actions.

Corrective action plans must be consistent with applicable laws, regulations, and agency policies. Corrective action plans may include the root cause analysis, milestones, planned actions, measurable indicators of remediation associated with planned actions, the agency official reasonable for remediation, and the completion date.

V. REPORTING ON INTERNAL CONTROLS

Agencies should establish a clear and transparent reporting system to communicate the results of internal control activities to senior leadership and relevant oversight bodies, such as OMB and the agency Inspector General. The reporting system should ensure that information is presented in a timely, consistent, and understandable format, highlighting key internal control findings, performance metrics, and risk areas requiring attention or improvement.

Assurance Statement

The assurance statement and summary information related to Section 2 (31 U.S.C. 3512(d)(2)-(3)) and Section 4 (31 U.S.C. 3512(d)(2)(B)) of FMFIA must be provided within the annual AFR, PAR, or other management report. Agencies must clearly address the effectiveness of internal control and, separately, whether the agency's financial management systems conform to the principles, standards, and requirements established under 31 U.S.C. 3511(a). The assurance statement is an accountability statement so only essential information must be included. Attachment 3 of this Circular (Illustrative Assurance Statements) provides examples of assurance statements.

Reporting Requirements for Deficiencies and Corrective Actions

The effectiveness of an agency's internal control environment is reflected in its ability to address and correct deficiencies. Correcting deficiencies is critical to achieving the objectives of FMFIA. Unresolved or longstanding deficiencies should be considered when assessing the overall effectiveness of controls. The corrective action process provides a structured approach for management to mitigate the risks associated with control deficiencies. Table 2 below outlines how deficiencies are reported.

Table 2. Deficiency Reporting Requirements

Category	Definition	Reporting
Control Deficiency	A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve the entity's objectives. A deficiency in design exists when: (1) a control necessary to meet a control objective is missing; or (2) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.	Internal to the organization and not reported externally. Progress against corrective action plans must be periodically assessed and reported to agency management.

Category	Definition	Reporting
Significant Deficiency	A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less significant or severe than a material weakness yet important enough to merit attention by those charged with governance.[15]	Internal to the organization and not reported externally. Progress against corrective action plans must be periodically assessed and reported to agency management.
Material Weakness	A material weakness is a deficiency, or a combination of deficiencies, in internal control that that the agency head determines to be significant or severe enough to report outside of the agency. Non-achievement of a relevant principle and related component results in a material weakness. A material weakness in internal control over operations may include, but is not limited to, a condition that: • impacts the operating effectiveness of Entity-Level Controls; • impairs fulfillment of essential operations or mission; • deprives the public of needed services; or • significantly weakens established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest.	Material weaknesses and a summary of corrective actions must be reported to OMB and Congress through the AFR, PAR, or other management reports. Progress against corrective action plans must be periodically assessed and reported to agency management.

[15] Consistent with AU-C 260, The Auditor's Communication With Those Charged With Governance, the 2011 revision of Government Auditing Standards defines those charged with governance as the person(s) or organization(s) with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit, including related internal controls

Category	Definition	Reporting
Material Weakness (continued)	A material weakness in internal control over reporting is a deficiency, or a combination of deficiencies, in internal control that the agency head determines significant enough to impact internal or external decision-making and reports outside of the agency as a material weakness. A material weakness in internal control over external financial reporting is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A material weakness in internal control over compliance is a condition where management lacks a process that reasonably ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving agency objectives.	Material weaknesses and a summary of corrective actions must be reported to OMB and Congress through the AFR, PAR, or other management reports. Progress against corrective action plans must be periodically assessed and reported to agency management.

To promote transparency and accountability, agencies should provide regular updates on the status of their internal control efforts. These updates should include performance summaries, an assessment of control effectiveness, any identified deficiencies, and progress on corrective actions.

Some agencies utilize Cooperative Audit Resolution and Oversight (CAROI)[16] or similar mechanisms to enhance audit follow-up and control resolution efforts. CAROI can improve communication, foster collaboration, build trust, and create a shared understanding of audit findings, ultimately promoting better Federal program outcomes. While the establishment of a CAROI is not mandatory, its use is encouraged to complement audit follow-up efforts and enhance corrective actions.

VI. THE ROLE OF RISK MANAGEMENT IN INTERNAL CONTROL

Risk management is a systematic process including risk assessment, risk response designed to mitigate or reduce risks, and risk monitoring to achieve agency objectives, which is ongoing and iterative to manage the ever-changing likelihood and impact of adverse events that may occur across an agency's operations. This process helps address risks proactively and may be preventative or encourage opportunity-taking when successful.

Risk management's desired outcomes include increased likelihood of successfully delivering on agency goals and objectives; fewer unanticipated outcomes encountered; and better assessment of risks associated with changes in the environment.

Risk management is an integral part of internal control. Through successful risk management tools like risk assessments and continuous monitoring, necessary controls may be identified to mitigate risks. Risk assessments and continuous risk management can help ensure effective internal control and identify necessary controls. Management is responsible for implementing practices that identify, assess, respond to, and report on risk. This entails not only performing risk assessments as discussed in Section III.B, but also:

- Identifying risk tolerance (for example, margin of error, materiality), which is the acceptable level of variance in performance relative to the achievement of objectives, and what is deemed an unacceptable event;
- Monitoring legislation, mission changes, funding changes, or program changes and their resulting potential impact on the organization;
- Performing internal assessments of organization-wide risks, known risks that may occur and require mitigation strategies, and potential emerging risks that may be preventable or require mitigation; and
- Designing risk management and control practices to be forward-looking and preventative, help leaders make better risk-based decisions and reduce threats, and help identify opportunities to be implemented that improve the efficiency and effectiveness of government operations.

Through risk management and employment of adequate controls, agencies assure effective and efficient operations, resource allocation, and accountability across Federal programs.

[16] AGA, Guide to Improving Program Performance and Accountability Through Cooperative Audit Resolution and Oversight (May 2010).

VII. OTHER CONSIDERATIONS AND BEST PRACTICES

Benchmark Internal Control Systems: Agencies are encouraged to establish clear benchmarks to assess effectiveness of their internal control systems. These benchmarks should:

- Include quantifiable and qualitative indicators tailored to the agency's mission and operational context;
- Facilitate comparative analysis over time to track improvements or identify areas requiring further attention; and
- Align with applicable Federal law, such as the Federal Information Security Modernization Act (FISMA), and applicable standards, such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), or others), and include best practices for risk management.

Performance Metrics for Executives: Agencies may incorporate specific performance metrics into the evaluation criteria for executives and senior leadership. Such measures may:

- Measure the effectiveness of risk identification and mitigation efforts;
- Reflect progress toward achieving risk management objectives; and
- Incentivize proactive engagement in strengthening controls.

Integration of Risk Management in Control Development: Control activities should routinely integrate risk management. Risk assessments should serve as a foundational tool for the design, implementation, and refinement of controls. These assessments identify emerging risks, evaluate existing control weaknesses, and align controls with organizational priorities and regulatory requirements. By using risk assessments, agencies can tailor their internal control frameworks to address both current and emerging risks.

Control Activities Targeting Identified Risks: Control activities may be specifically designed to mitigate identified risks as part of a risk response. Controls should seek to address root causes and likely consequences of risks. Control activities, when prioritized by most significant risks, help allocate resources efficiently.

Automated Systems for Risk Assessments and Control Testing: When possible, agencies should consider automated systems and technologies to streamline the process of conducting risk assessments, testing controls, and monitoring control performance. Automated solutions can provide real-time data, improve timeliness and accuracy of risk identification and control adjustments, and enhance the agility of control frameworks.

Develop a Risk Management Council (RMC) to oversee the establishment of an agency risk profile, regular assessment of risk, and development of appropriate risk response. An effective RMC may include senior officials for program operations and mission-support functions to help ensure those risks are identified which have the most significant impact on the mission outcomes of the agency.

Implement or Continue Risk Management Practices: Risk management practices such as Enterprise Risk Management (ERM) can be a valuable tool for designing, assessing, and improving controls. ERM is a process applied across an organization to identify potential risk events that may affect organization's objectives, and determine how to mitigate and reduce risks and manage risks that may fall within the agency's risk appetite.

Create a Risk Profile to provide a thoughtful analysis of the risks an agency faces toward achieving its objectives and arising from its activities and operations, and to identify appropriate options for addressing those significant risks. The risk profile may consider risks from a portfolio perspective and identify sources of uncertainty, both positive (opportunities) and negative (threats), providing transparency into which risks the agency is willing to take or treat.

The profile may include components such as identification of objectives, risks, inherent and residual risk assessments, current and proposed risk responses, and action categories. An agency may have multiple types of risk profiles: an enterprise-level risk profile encompassing significant risks across the agency, and focused risk profiles concentrating on specific areas or activities, such as fraud, cybersecurity, sub-agency, or program.

Implement Data Analytics for Performance Monitoring: Agencies are encouraged to implement advanced data analytics tools to track and assess the performance of controls and their effectiveness in mitigating identified risks. Data analytics can monitor key performance indicators (KPIs) in real-time, enabling management to identify trends, uncover inefficiencies, and assess performance across various functions.

Regular Training on Controls and Risk Management: Employee education is critical to understanding how to employ controls and manage risk. Employees should be equipped with the knowledge necessary to recognize risks and understand the mechanisms in place to address them. Continuous employee education reinforces an effective control environment. Training should be routinely reviewed for updates to reflect changes in policies, procedures, and technology.

Collaboration Across Functions: Effective internal control includes collaboration across organizational function. Communication across departments responsible for risk assessment, control implementation, strategic planning, and performance monitoring is essential to ensure that strategies are coordinated, and risks are managed comprehensively. Agencies should establish cross-functional teams to review risk management initiatives, share best practices, and ensure that controls are applied consistently throughout the organization.

Oversight of Service Organizations: Service organizations can be helpful partners, such as shared service providers or third-party contractors, who share risk when an agency does not have a capability. Agencies may develop agreements with service organizations and begin to rely on the service organization to perform critical functions.

The use of a third-party provider should be considered for management's oversight and assessment of internal control based on risk and when the activity is significant to an agency's achievement of internal control objectives.

Service Organizations are responsible for providing assurances to their customers and assisting customers in understanding the relationship between the service provider's controls and the customer's user controls. However, it is important to understand that, while the service organization may do some of the work function, the agency is not relieved of its responsibilities to manage risk when outsourcing functions.

Agencies are ultimate responsibility for internal control over operations, reporting, and compliance. When agencies chose to use a service organization, agencies should:

- establish and evaluate controls that complement the service organization's controls;
- review the defined service-level agreements to ensure they meet entity risk tolerance and monitor the third-party performance metrics; and
- maintain oversight of processes performed by third parties to ensure they support agency objectives.

VIII. CONCLUSION

Effective internal control sets conditions that promote successful achievement of Federal program missions and objectives. Through deliberate assessment, design, and implementation of controls, communication, and continuous monitoring, agencies can safeguard public resources, protect sensitive information, and ensure compliance with Federal laws and regulations. In an increasingly complex environment, Federal agencies should advance systems and frameworks that will achieve mission objectives, manage a broad range of risks, and evolve to meet and overcome challenges.

The success of internal control systems is strengthened when aligned with a robust risk management framework. By embedding risk management into the culture and strategic fabric of the agency, leaders can make more informed decisions, anticipate disruptions, and ultimately improve mission outcomes and accountability to the public.

Attachment 1: The Agency Risk Assessment Process

Step 1: Define Objectives and Risk Tolerances

- Identify the agency, program or process objective to focus the assessment.
- Obtain and understand the tone at the top for risk tolerance relative to mission, time, and resources.

Step 2: Risk Identification

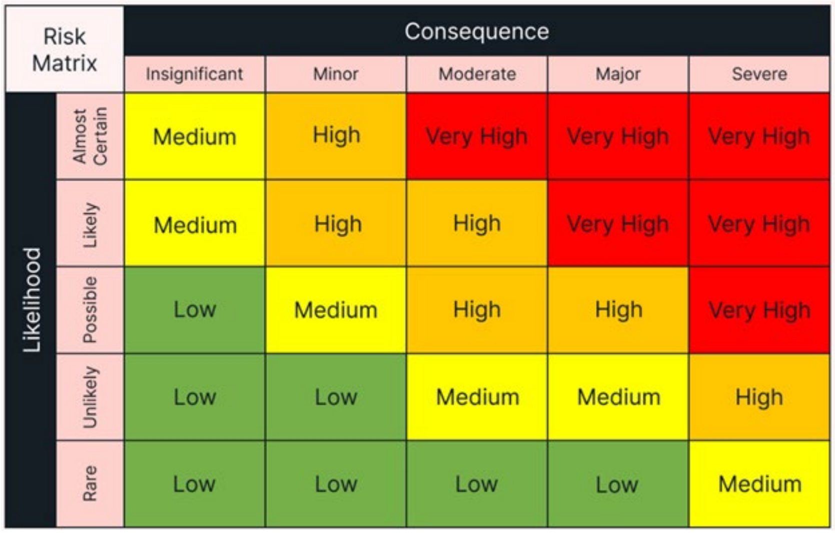
- Interview, brainstorm, and document potential risks with stakeholders from across the aspects of your operations; considering both internal and external factors.
- Use techniques and tools like interviews, surveys, checklists, lessons learned, past incidents, and audit reports of similar entities to identify potential risks.

Step 3a: Risk Analysis

- Assess the likelihood or probability of the risk occurrence (for example, low, medium, high).
- Assess the severity of impact and extent of potential harm in the event of risk occurrence (for example, minor injury, major damage, financial loss).
- Document the risk level based on likelihood and impact/ severity.

Step 3b: Risk Evaluation

- Align the risks on a risk matrix
- Use a risk matrix, chart, or similar tool like the one below to evaluate the risk against the agency's risk tolerance.



Risk Matrix		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	Very High	Very High	Very High
	Likely	Medium	High	High	Very High	Very High
	Possible	Low	Medium	High	High	Very High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

- Consider the type of risk assessment and conditions, as there may be greater risk tolerance in emergency responses.

- Determine or revalidate the risk appetite relative to the program objectives.
- Evaluate the risks and their placement against the risk appetite.
- Develop recommendations for a risk response: avoid, share, mitigate, or accept. (See below for more information.)

Step 4: Risk Response

Risk Response is the choice an entity makes on what to do about identified risk. Management should decide on a course of action to respond to the risk, most often through one of the options outlined below, then plan, develop, and implement the action.

Risk response options include:

- **Avoid**: the entity will discontinue, stop, or not conduct the process.
- **Share / Transfer**: the entity partners with another entity, or outsources all or portions of activities that result in risk. While this does not relieve the entity of the responsibility, it can reduce the likelihood or impact (for example, insurance, or shared services).
- **Mitigate / Reduce**: the entity develops or modifies controls to reduce the risk likelihood, impact, or both. (*See control development below*.)
- **Accept**: the entity determines the residual risk is acceptable and proceeds.

Responding to risk can be preventative or reactive. Most risk assessments will help inform and develop a preventative response so that in the event a risk occurs, the entity has sufficiently anticipated the risk event, the risk response is effective, and the program accomplished its objective without unnecessary costs.

When appropriate to mitigate or reduce the risk by developing or modifying controls, the earlier discussion above on preventative and detective control activities may apply. Actions may include:

  - Developing risk response for identified risk;
  - Developing mitigation strategies for identified risk;
  - Considering ability to eliminate potential emerging risks, and examining methods to reduce risks such as substituting materials, engineering controls, administrative controls, or personal protective equipment;
  - Assigning responsibility for implementing controls and set deadlines;
  - Identifying how to measure control effectiveness; and
  - Implementing the controls.

Step 5: Risk Monitoring is an ongoing review of an entity’s risks, and determination of whether performance is within the appropriate risk tolerance and current risk appetite. Actions may include:

- Reviewing the process execution to assess if the desired outcome is achieved, and if risk likelihood or impact has been lowered;
- Reviewing the risk assessment to identify changes in circumstances;
- Adjusting the risk response or controls to achieve an acceptable level of risk;

- Using the updated data to inform adjustments to the risk profile, as appropriate;
- Tracking the effectiveness of implemented controls and adjust, as necessary; and
- Documenting changes and updates to the risk assessment.

Types of Risk to Consider

There are various types of risk to consider when agencies are conducting risk assessments. These risks can be significant to Federal programs by diverting resources, undermining missions, and damaging public trust. In all cases, it is helpful to consider the review of risks against the following objectives to help guide the risk management process towards effective controls:

- Operational Objectives Pertain to effectiveness and efficiency of the agency's operations, including operational and financial performance goals, and safeguarding assets against loss.
- Reporting Objectives: Pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms set forth by regulations, standards, or policy.
- Compliance Objectives: Pertain to adherence to laws and regulations for the agency.
- Fraud is a risk all agencies must consider. Management should consider and assess the following when evaluating potential risks for fraud:
    - Types of Fraud: fraudulent reporting, possible loss of assets, and corruption resulting from the many ways that fraud and misconduct can occur
    - Incentives and Pressures for Fraud: internal and external motives and demands
    - Opportunities for Fraud: vulnerabilities to unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or other inappropriate acts. Also consider the opportunities for fraud and abuse afforded certain positions or scopes of authority over operations
- Management should identify and analyze improper payment risks, considering factors such as program complexity, volume of payments, and reliance on self-certification by recipients. Agencies should continuously review all programs for risk of improper payments.
- Information technology and security risks threaten an entity's operations, assets, and personnel. Protecting Federal information systems from security threats is a critical component of the risk management process. Risks to confidentiality, integrity, and availability can arise from unauthorized access, malicious software, or physical threats. Agencies should prioritize strategies to secure their systems and protect sensitive information. Among the questions management should consider are:
    - How does the new technology contribute to achieving the organization's mission?
    - Does the new technology increase risks that may hinder the accomplishment of objectives? (for example, reduced data security, frequent or prolonged service interruptions, steep learning curves)
    - What changes to internal controls (for example, control activities) are necessary to manage these risks?
- The Federal Government's collection, use, and management of Personally Identifiable Information (PII) requires careful consideration of privacy risks and protective measures. Agencies should assess the risk that PII could be exposed or misused and take appropriate actions to protect the privacy of individuals.

- Agencies should consider risks resulting from significant changes to the internal and external environment that can create new vulnerabilities and alter existing risk exposure.
- Agencies should assess acquisition activities and programs as part of their control processes. Agencies should consider the potential for fraud at all stages of the acquisition lifecycle, including planning, procurement, contract management, and post-award monitoring.
- Agencies should adopt a risk-based approach to managing Federal grants and other forms of financial assistance, as outlined in the requirements set forth at 2 CFR part 200.
- The Antideficiency Act (ADA) imposes strict limitations on the amounts of obligations or expenditures that agencies can make without proper appropriations. Agencies must establish funds controls that ensure compliance with the ADA, including monitoring fund usage and preventing violations.

Attachment 2: Internal Control Assessment Exhibits

The tables in this Attachment provide hypothetical examples of agency evaluations of internal controls. Table 1 illustrates how principles within the control environment can help inform if the control is well-designed, in place, and working.

Table 1: Example of Internal Control Evaluation Control Environment

Principle	Control Deficiency Summary
Principle 1: Demonstrate Commitment to Integrity and Ethical Values	The Agency's ethics training program is not sufficient to make all employees aware of the importance of adhering to the executive branch employee standards of conduct.
	The Agency does not have processes in place to detect and mitigate potential employee conflicts of interest.
	Management concludes the principle is not designed, implemented, and operating effectively.
Principle 2: Exercise Oversight Responsibility	Internal control deficiency noted because the Senior Management Council's review of risk assessments and remediation plans are not documented.
	Management concludes that the principle is designed, implemented, and operating effectively despite internal control deficiencies based on an evaluation of the severity of deficiencies and that compensating controls are in place.
Principle 3: Establish Structure, Responsibility and Authority	Internal control deficiency noted because oversight and control structures have not evolved to keep up with changes in operations.
	Management concludes that the principle is designed, implemented, and operating effectively as the deficiency noted only affect a small portion of the Agency.
Principle 4: Demonstrate Commitment to Competence	No internal control deficiencies noted.
	Management concludes that the principle is designed, implemented, and operating effectively.
Principle 5: Enforce Accountability	Internal control deficiencies noted because management, with oversight from the Senior Management Council, does not take necessary corrective actions.
	Management concludes that the principle is not designed, implemented, and operating effectively.

The following Table 2 is an illustrative example of the results of management's assessment of the control environment component:

Table 2: Example of Principle Evaluation

Principle	Designed & Implemented (Yes/No)	Operating Effectively
(1) Demonstrate Commitment to Integrity and Ethical Values	No	Ineffective
(2) Exercise Oversight Responsibility	Yes	Effective with internal control deficiencies and compensating controls noted
(3) Establish Structure, Responsibility and Authority	Yes	Effective with internal control deficiencies and compensating controls noted
(4) Demonstrate Commitment to Competence	Yes	Effective
(5) Enforce Accountability	No	Ineffective

In Table 3 and Table 4, management found the Control Environment is not working well. As a result, the overall internal control system is not effective.

Table 3: Example of Overall Assessment of a System of Internal Control

System Evaluation	Designed & Implemented (Yes/No)	Operating Effectively
Control Environment	No	Ineffective
Risk Assessment	Yes	Effective
Control Activities	Yes	Effective
Information and Communication	Yes	Effective
Monitoring	Yes	Effective
Are all Components operating together in an integrated manner?	No	Ineffective

Table 4: Example of Overall Evaluation of a System of Internal Control

Overall Evaluation	Operating Effectively
Is the overall system of internal control effective?	No

Attachment 3: Illustrative Assurance Statements

Exhibit 1: Example of Unmodified Assurance Statement

The [agency] management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act (Act). The [agency] conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*. Based on the results of the assessment, the [agency] can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 20XX. The accounting system of the [agency] conforms to applicable principles, standards, and requirements consistent with the Act.

Agency Head Signature

Exhibit 2: Example of Modified Assurance Statement

The [agency] management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act (Act). The [agency] conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*. Based on the results of the assessment, the agency can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 20XX, except for the following material weaknesses reported: *[Insert brief description of each control material weakness;]*

The accounting system of the [agency] conforms to applicable principles, standards, and requirements consistent with the Act, except as follows: *[If applicable, insert brief description]*.

Agency Head Signature

Exhibit 3: Example of Statement of No Assurance

- The [agency] management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the Federal Managers' Financial Integrity Act (Act). The [agency] conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*. Based on the results of the assessment, the agency is unable to provide assurance that internal control over operations, reporting, and compliance was operating effectively due to the following material weaknesses: *[Insert brief description of each control material weakness;]*

The accounting system of the [agency] conforms to applicable principles, standards, and requirements consistent with the Act, except as follows: *[If applicable, insert brief description]*.

Agency Head Signature