U.S. Office of Personnel Management

FRAUD RISK MANAGEMENT POLICIES AND PROCEDURES

March 2026

Version	Date	Revision
1.0	March 2026	Initial Release

Contents

U.S. Office of Personnel Management
Fraud Risk Management Policies and Procedures

Purpose

This document sets forth the U.S. Office of Personnel Management's (OPM's) Fraud Risk Management (FRM) policies and procedures. The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and impact of fraud. Effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded. These FRM policies and procedures establishes a framework for fraud risk management across the agency that is integrated into OPM's culture and operations.

Scope

These policies and procedures form part of OPM's governance framework.

Authorities

These policies and procedures are issued under the authority of the Payment Integrity Information Act of 2019 (PIIA), Pub. L. No. 116-117, as codified in 31 U.S.C. 3351. It is also issued pursuant to Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, which directs executive agencies to adhere to the leading practices set forth in the U.S. Government Accountability Office's (GAO's) *A Framework for Managing Fraud Risks in Federal Programs* (the Fraud Risk Framework) as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risk.

Additional References and Resources

GAO-25-107721, *Standards for Internal Control in the Federal Government*, May 2025

OMB Memorandum M-21-19, *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement*, March 5, 2021

OPM's Financial Management Manual, Chapter 24 – Fraud Risk Policy, August 2024

OPM's Risk Management Council (RMC) Charter, Version 8.0, December 2025

Policies and Procedures

1. **Policy: OPM is committed to combatting fraud by creating an organizational culture and structure conducive to fraud risk management.**

    1.1. **Procedure**: OPM's fraud risk management structure demonstrates a senior-level commitment to integrity and combatting fraud and the involvement of all levels of the agency in OPM's antifraud culture by vesting oversight of the fraud risk management program in the RMC, which is comprised of senior-level executives from across OPM, and day-to-day management in OPM's Chief Risk Officer (CRO).[1] The RMC will:

        - Review and approve these policies and any changes or amendments thereto

---

[1] The CRO will be supported by the Privacy and Risk Management Office in the Office of the Director (PRMO).

recommended by the CRO.

- On an annual basis, review the effectiveness of OPM's FRM program (see Procedure 4.1 for additional information).

1.2. **Procedure**: The CRO shall monitor these FRM policies and procedures and their implementation and effectiveness and may from time to time in its discretion, amend, supplement, delete, or otherwise modify the FRM procedures as it deems appropriate to improve OPM's fraud risk management program.[2]

1.3. **Procedure**: The CRO is designated as the "antifraud entity" (as such term is defined in the Fraud Risk Framework) with the responsibility and authority to:

- Serve as the repository of knowledge on fraud risk and controls within OPM. Accordingly, the CRO will be responsible for:

  o Drafting and revising as necessary written policies and procedures governing the FRM program (which policies and procedures shall be subject to the review and approval of the RMC).

  o Maintaining OPM's fraud risk profile in the form attached as Exhibit A, as the same may be modified from time to time by the CRO (the FRP Template).

  o Keeping and maintaining the FRM program files in readily accessible formats in compliance with OPM's record retention policies.

- Manage the annual fraud risk assessment process (see Policy 2 for more information).

- Lead or assist with employee training and other fraud-awareness activities. The CRO will review OPM's training program at least annually as part of its annual review of the FRM program same (see Procedure 4.1) to assess the quantity and quality of fraud awareness training and, if necessary, supplement the same.

- Coordinate antifraud initiatives across OPM by meeting with internal stakeholders of each program having one or more Frauds Risks with a Residual Risk Assessment– Combined Risk of "High" on the then-current Fraud Risk Profile quarterly and internal stakeholders of each other program annually to obtain updates on the status of antifraud initiatives and to share best practices.

1.4. **Procedure**: Each member of the RMC is responsible for ensuring the full cooperation of their office with the CRO in its implementation of the FRM program. Further, each member of the

---

[2] Please note, however, that changes to FRM policies require the approval of the RMC (see Procedure 1.1).

RMC is expected to model OPM's culture of integrity and to combat fraud within the agency.

1.5. **Procedure**: OPM's Designated Agency Ethics Official will provide or arrange for initial ethics awareness training pursuant to 5 CFR 2638.304 for all new OPM employees within 90 days of appointment, and annual ethics training for financial disclosure filers and other certain employees described in 5 CFR 2638.307 and 308, as required by Federal regulations.

1.6. **Procedure**: OPM's Office of the Chief Human Capital Officer will be responsible for ensuring that all new hires are informed of how to access OIG's whistleblower resources, including the whistleblower hotline.

1.7. **Procedure**: The CRO will ensure that the current FRM policies and procedures are available to all OPM employees (including by posting on a shared webpage accessible to all OPM employees) and each office will be responsible for ensuring that its employees are aware of and compliant with its antifraud policies and procedures, including applicable controls.

2. **Policy: OPM shall conduct regular fraud risk assessments to develop and maintain an up-to-date fraud risk profile.**

2.1. **Procedure**: Commencing Q3 FY2026, and annually in Q1 thereafter, the CRO shall select the programs to be assessed during that fiscal year with the goal of reviewing each program having one or more Frauds Risks with a Residual Risk Assessment–Combined Risk of "High" on the then-current Fraud Risk Profile annually, each program having one or more Fraud Risks with a Residual Risk Assessment–Combined Risk of "Medium" on the then-current Fraud Risk Profile at least every two years, and each other program at least every three years. In determining that year's assessment plan, the CRO shall also consider whether there have been changes in the program or operating environment since the last fraud assessment.

2.2. **Procedure**: The CRO shall conduct its fraud assessments during Q2 and Q3 using such tools, methods, and sources as it deems appropriate, taking care to implement best practices as developed in the Fraud Risk Framework, including input from internal and external stakeholders (such as OIG and external contractors).

2.3. **Procedure**: The CRO shall document the results of its fraud risk assessment in a fraud risk profile using the FRP Template, which shall include, for each specific fraud risk: identifying OPM's fraud risk tolerance, assessing the inherent fraud risk, identifying current risk responses, assessing residual risk, and identifying proposed risk responses. An updated fraud risk profile incorporating the results of that year's fraud risk assessment shall be presented to the RMC during Q4 of each fiscal year.

3. **Policy: OPM shall design and implement a fraud risk strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.**

3.1. **Procedure**: The CRO shall use the fraud risk profile to assess and manage OPM's FRM program, including the effectiveness of current fraud risk responses, the allocation of antifraud

resources, and the need for additional fraud risk responses, including controls.

3.2. **Procedure**: As necessary, based on the fraud risk profile, the CRO shall work with internal stakeholders to design and implement written control activities to reduce fraud risk.

3.3. **Procedure**: Each office will be responsible for maintaining written documentation of its antifraud controls and ensuring that employees are aware of and compliant with the same (See Procedure 1.6).

3.4. **Procedure**: As part of its fraud risk assessment, the CRO will review written controls, written fraud response plans, and the actual implementation thereof.

3.5. **Procedure**: On an ongoing basis (including as part of its regular quarterly or annual meetings with internal stakeholders (see Procedure 1.2)), the CRO will work with internal and external stakeholders to implement the FRM program, including providing guidance and support on specific antifraud activities and sharing information regarding fraud risks and schemes and best practices.

3.6. **Procedure**: the CRO shall work with internal stakeholders to develop performance metrics to measure, and incentives to reward, fraud risk management efforts.

3.7. **Procedure**: the CRO shall identify relevant open recommendations associated with the fraud risk management program and coordinate successful closure of these with the appropriate offices.

4. **Policy: OPM shall evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.**

4.1. **Procedure**: The CRO will conduct an annual assessment of the FRM program and present the same to the RMC during each Q4. Such assessment shall include the following elements:

- An updated fraud risk profile incorporating the results of that year's risk assessments (see Procedure 2.3).

- A review of fraud activity during the past year, as reported by internal and external stakeholders.

- The results of periodic testing of controls.

- A review and assessment of OPM's fraud risk training program.

- An assessment of internal or external factors that could influence the FRM environment (including controls) for the next year.

- An annual testing plan for fraud risk controls for the next year.

- Changes to the FRM program, including:

    o Revisions to the allocation of antifraud program resources.

    o Changes to antifraud education and training.

    o Changes to these policies and procedures, including the roles and responsibilities of the CRO and RMC and timelines.

    o Changes to the roles and responsibilities of other stakeholders (including external stakeholders) or the monitoring and evaluation thereof.

    o New or changed fraud responses, including fraud controls.

    o Changes to performance metrics to measure, and incentives to reward, fraud risk management efforts.

4.2. **Procedure**: The RMC will review the aforementioned FRM program assessment and recommendations and respond to the same no later than the end of Q4.

Calendar of Action Items/Deliverables

Time	Action Item/Deliverable
Q1	• CRO prepares its fraud assessment plan for the current fiscal year (Procedure 2.1)
Q2 & Q3	• CRO conducts risk assessments (Procedure 2.2) • CRO tests internal controls (Procedure 4.1)
Q4	• CRO submits updated risk profile to the RMC (Procedure 2.3) • CRO submits its annual FRM program assessment and any recommendations for changes thereto to the RMC (Procedure 4.1) • RMC responds to the FRM program assessment and recommendations (Procedure 4.2).
Quarterly	• CRO meets with internal stakeholders of each program having one or more Frauds Risks with a Residual Risk Assessment–Combined Risk of "High" on the then-current Fraud Risk Profile to obtain updates on the status of antifraud initiatives and to share best practices (Procedure 1.2)
Annually	• CRO meets with internal stakeholders of each other program to obtain updates on the status of antifraud initiatives and to share best practices (Procedure 1.2)

Roles and Responsibilities

Associate Directors and Office Heads	Implement the FRM policies and procedures within their offices, including establishing effective fraud controls, ensuring staff comply with the FRM policies and procedures, and fostering a fraud risk aware culture where fraud risks can be identified and escalated.
Chief Financial Officer	Design, implement, and lead financial fraud risk management strategies and activities in accordance with the FRM policies and procedures.
Chief Risk Officer	Act as the designated antifraud entity with primary responsibility for designing and overseeing OPM's FRM activities, including: • serving as the repository of knowledge on fraud risks and controls, • managing the fraud risk assessment process, • coordinating antifraud initiatives across OPM; and • leading or assisting with trainings and other fraud-awareness activities. The CRO is authorized to, from time to time in its discretion, amend, supplement, delete, or otherwise modify the FRM procedures as it deems appropriate to improve OPM's fraud risk management program. The CRO will be supported by the Privacy and Risk Management Office in the Office of the Director (PRMO).
Managers	Ensure staff comply with the FRM policies and procedures and fraud controls and foster a culture where fraud risks can be identified and escalated.
OPM Director	Set a tone at the top for the rest of the organization and drives the culture of Integrity and combatting fraud.
Risk Management Council	Oversee the FRM program to ensure that an appropriate fraud risk management framework is established and maintained, including reviewing and approving FRM policies.

Definitions

Fraud	Obtaining something of value through willful misrepresentation. Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond OPM's professional responsibility for assessing risk. For the purposes of these policies and procedures, unless noted otherwise, the term "fraud" includes potential fraud for which a determination has not been made through the judicial or other adjudicative system.
Risk	The effect of uncertainty on the achievement of objectives. An effect is a deviation from the desired outcome, which may present positive or negative results.
Risk Assessment	Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.
Risk Management	A process that helps agency managers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty to mitigate risks.

Risk Profile	A prioritized inventory of an organization's most significant risks.
Risk Response	Management's strategy for managing (or responding to) a given risk. Risk response strategies include accept, reduce, avoid, or share (or transfer).
Risk Tolerance	The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level, identifies the tolerance band for a specific risk, and is stated in measurable terms. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

Exhibit A
Fraud Risk Profile Template

[See accompanying Excel spreadsheet]