PART 2006 – MANAGEMENT

Subpart KK - RURAL DEVELOPMENT FRAUD RISK MANAGEMENT POLICY

Table of Contents

oOo

PART 2006 – MANAGEMENT

Subpart KK - RURAL DEVELOPMENT FRAUD RISK MANAGEMENT POLICY

§ 2006.1801 __Purpose__:

This document establishes Rural Development's (RD) Fraud Risk Management Policy (FRM Policy).

§ 2006.1802 __Background__:

(a) As part of the requirements outlined in the Payment Integrity Information Act of 2019 (PIIA) and Office of Management and Budget (OMB) Circular A-123, the OMB has provided fraud risk management guidance for Federal Agencies. This guidance establishes financial and administrative controls for the purpose of identifying and assessing fraud risks to prevent, detect, respond, and report frauds. Federal Agencies must:

(1) Conduct an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate identified fraud risks;

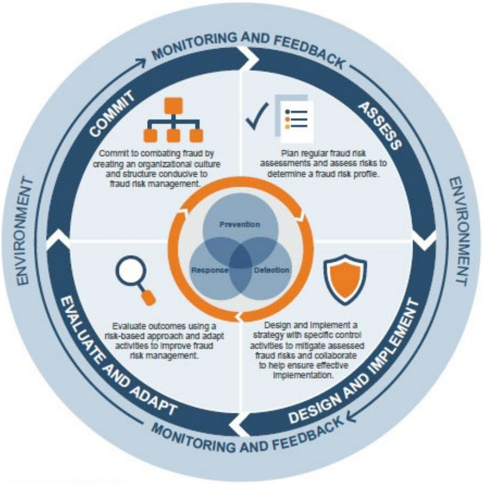
(2) Collect and analyze data on detected fraud to monitor fraud trends and use the data to continuously improve fraud controls; and

(3) Use the results of monitoring, evaluation, audits, and investigations to improve fraud prevention, detection, and response.

(b) Additionally, OMB Circular A-123 instructs Federal Agencies to implement the best practices as published in 'A Framework for Managing Fraud Risks in Federal Programs' also referred to as the U.S. Government Accountability Office (GAO) Fraud Risk Framework. The GAO Fraud Risk Framework outlines four phases in its Fraud Framework lifecycle as identified below:

(1) Commit to combating fraud at all levels of the agency by creating a culture and structure.
(2) Assess fraud risks on a regular basis to determine a fraud risk profile.
(3) Design and implement a fraud response strategy, with specific control activities to address risks that are identified as part of agency fraud risk assessments.
(4) Evaluate Fraud Risk Management (FRM) outcomes using risk-based monitoring and analysis and adapt the FRM approach to improve FRM effort.

Figure 2: The Fraud Risk Management Framework


MONITORING AND FEEDBACK
COMMIT
Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
ASSESS
Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
ENVIRONMENT
Prevention
Response
Detection
ENVIRONMENT
Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
EVALUATE AND ADAPT
DESIGN AND IMPLEMENT
MONITORING AND FEEDBACK

Source: GAO. | GAO-15-593SP

§ 2006.1803 Standards of Conduct.

This FRM Policy complements RD's Standards of Conduct and Ethics. This policy in no way supersedes, rescinds, or replaces existing procedures or processes designed to promote the highest standards of honesty, propriety, and integrity in RD standard business practices and/or compliance with laws, rules, and regulations. RD does not tolerate and will investigate any suspected fraud, waste, and abuse, activity.

§ 2006.1804 Policy.

This FRM Policy outlines the standards for preventing, detecting, responding to, and reporting of fraud and any misconduct involving RD programs and operations. The FRM Policy promotes consistent adoption of FRM practices and awareness across the organization. Fraud prevention and an anti-fraud culture are priorities at RD. Staff recognize that we are called to safeguard stakeholder interests as our public duty by maintaining the highest ethical standards to counter actions involving fraud, waste, abuse, and mismanagement. This policy applies at all levels including full time and part time employees, contractors, grantees, borrowers, beneficiaries, and external parties (vendors, consultants, etc.) that could adversely impact RD's mission. Suspected fraudulent activity, internally and/or externally, is reported to the Office of Inspector General (OIG) and will be investigated, and appropriately addressed in accordance with policies and procedures for managing fraud, waste, and abuse.

§ 2006.1805 Definitions.

RD Program(s): Refers to departments within RD which deliver grants, loans, loan guarantees, technical assistance, and related services to the public. Currently these resources are delivered through RD's three agencies of Rural Housing Service (RHS), Rural Business & Cooperative Services (RBCS), and Rural Utility Service (RUS).

RD Program Support Areas: Refers to RD departments like procurement, human resources, information technology, or others, which provide necessary support services to the RD programs, such as administrative tasks, financial management, or other support, but do not directly deliver funding.

FRM Guidance documents: Procedural or explanatory documentation and reference materials that support the FRM Policy and the continuation of FRM related systems and processes.

Fraud[1]: The theft of valuables (money, information, time, etc.) enabled by deceit.

Waste[1]: In governments, not fulfilling one's fiduciary duty to assure public monies are spent as effectively as possible.

Abuse[1]: Taking inappropriate advantage of one's position for personal gain.

[1] Fraud, Waste, & Abuse definitions cited from AGA Fraud prevention website. (2023, March 8) 'Tools & Resources, Glossary of Terms' (https://www.agacgfm.org/Resources/intergov/FraudPrevention/BestPractices/Glossary.aspx)

§ 2006.1806 Categories of Fraud.

(a) Against individuals. This is when an individual is targeted by a fraudster. Examples include identity theft, phishing scams, and "advance-fee" schemes.

(b) Internal organizational fraud. Also known as "occupational fraud," this is when an employee, manager, or executive of an organization deceives the organization itself. Examples include time sheet fraud, embezzlement, cheating on taxes, or lying to stakeholders.

(c) External organizational fraud. This includes fraud committed against an organization from the outside, such as ghost applicants, vendors or contractors who misrepresent the work they did, attempts to adversely influence employees, or cost rigging. Customers can also defraud organizations, such as when they submit bad checks or falsify grant activities. And increasingly, technology threatens organizations with theft of intellectual property or misusing customer information.

(1) First-party fraud occurs when an external party, including a RD customer, commits fraud against the agency.

(2) Victim fraud occurs when a RD customer or client is the victim of an intentional fraudulent act.

§ 2006.1807 Fraud Risk Management Program (FRM Program).

(a) In accordance with the PIIA and OMB Circular A-123 requirements, RD's leadership has the primary responsibility for prevention and detection of fraud. This can be done by establishing internal controls to manage the risk of fraud. Oversight for RD's FRM Program is provided by the Chief Risk Officer (CRO), who reports to the Undersecretary for Rural Development (USEC) on matters involving fraud risks. The FRM Program outlines governance, risk assessments, fraud prevention, detection, monitoring, and reporting for RD through this Policy.

(b) Office of the Chief Risk Officer (OCRO):

(1) Overall responsibility for the design, implementation, and leadership of the FRM Program.

(2) Maintain an enterprise fraud risk profile and departmental fraud risk strategy.

(3) Develop and maintain a repository of fraud risks and FRM activities.

(4) Oversee the fraud risk assessment process for RD programs and program support areas.

(5) Collaborate in the evaluation of RD program and program support areas' fraud risk controls and coordinate response to identified risks and vulnerabilities with appropriate leadership.

(6) Oversee the implementation of this FRM Policy within RD programs and offices and evaluate maturity against leading FRM practices.

(7) Oversee FRM communications strategy and produce FRM specific trainings and key messages.

(8) Add or revise FRM guidance documents when appropriate.

(c) Chief Financial Officer - Office of Compliance, Internal Compliance Division (CFO/OC/ICD) and Chief Financial Officer - Office of Compliance, External Compliance Division (CFO/OC/ECD):

(1) Serves as the Agency's representative on financial, accounting, and audit issues with other Federal and state agencies, utility industries and professional standard setting organizations and to ascertain FRM Policy.

(2) Provides expert financial, accounting and auditing advice to the CFO, each mission area Administrator and USEC, as well as other senior level staff of the agency on utility, cooperative, FRM practices and other accounting issues.

(3) Applies Generally Accepted Accounting Principles (GAAP), the Governmental GAAP, and Generally Accepted Auditing Standards (GAAS) to coordinate efforts with the OMB, the GAO, OIG, Agency Budget Office, and Office of General Counsel (OGC).

(4) Oversee, manage, and execute OMB Circular A-123 program in collaboration with the RD program and program support areas to assess effectiveness of RD's internal controls and PIIA implementation.

(5) Collaborate with process owners on the design, implementation, and validation of internal controls to prevent, detect and manage fraud risks.

(6) Assess and consider fraud risk assessment results when completing the annual ICR risk-based assessment

(d) RD Program and Program Support Leaders (Administrators, Deputy Administrators, Senior Executive Service (SES), etc.)

(1) Lead and advocate for the FRM Program within their program and program support areas.

(2) Designate a Fraud Risk Coordinator(s) to oversee and enforce fraud risk management activities of their programs.

(3) Review and approve assessment results. Provide appropriate feedback to Fraud Risk Coordinators.

(4) Actively foster RD's anti-fraud culture and ensure fraud risk assessments are conducted on schedule.

(e) RD Program and Program Support Fraud Risk Coordinators

(1) Coordinate and lead the implementation of RD's FRM Policy across its program or program support areas.

(2) Ensure timely completion of fraud risk assessments on each program and program support activity.

(i) Document fraud risk assessments and manage risk response plans in the RD Fraud SHIELD tool.

(ii) Deliver final assessment results to program leadership, OCRO, and Office of Compliance (OCFO/OC/ICD).

§ 2006.1808 Fraud Risk Assessments.

(a) RD Programs and Program Support Areas are responsible for performing fraud risk assessments of their respective areas to:

(1) Establish the fraud risk assessment team.

(2) Identify fraud schemes.

(3) Identify fraud risks.

(4) Identify existing controls and assess their effectiveness.

(5) Evaluate likelihood of occurrence and impact.

(6) Prioritize fraud risks and develop a risk response.

(7) Document the fraud risk assessment.

(b) The frequency and thresholds to perform fraud risk assessments vary based on the risk exposure of the program or function. Program areas and program support leadership will consider factors such as changes in programs or processes, transaction volume, level of automation, overall susceptibility to fraud, and the impact of fraud activity on RD's mission. At a minimum, a fraud risk assessment should be completed no less frequently than every 3 years and on all new programs or program support functions and whenever substantial changes have occurred. Using the results of the ranking outlined in the Fraud Risk Management Guidance, programs and functions with a high inherent risk must be prioritized for testing, preferably each year. Programs or functions undergoing significant change or corrective action may cause control testing to be deferred until the processes and controls are established.

(c) Both financial and non-financial fraud risks should be evaluated as part of these assessments to develop the fraud risk profile. RD program areas retain primary responsibility for performing these fraud risk assessments, while the CRO will provide guidance and support on training, analyzing results, and developing the fraud risk profile.

§ 2006.1809 Fraud Prevention and Detection Controls.

(a) Fraud Prevention:

(1) Fraud prevention is the processes and controls that deter fraud from initially occurring. Prevention controls can be overtly or covertly successful if they are implemented through activities such as establishing policies and procedures (overt controls) or through data analytics designed to prevent fraudulent transactions from being processed (covert controls).

(2) RD management is responsible for monitoring the effectiveness of fraud risk prevention controls. Wherever reasonable, RD will incorporate prevention controls into its business practices. These controls will include segregation of duties, physical and system access controls, approval protocols, as well as policies and procedures designed to identify suspicious activity and address any associated fraud risks.

(3) Awareness of fraud risk activities are essential components of successful fraud prevention and should be deployed through training and communication. RD Senior Leadership must foster a culture that integrates fraud risk management. Regular formal and informal training and communications should be put in place to promote an understanding of ethical principles and fraud risk concepts.

(b) Fraud Detection: Fraud detection activities and controls are designed to uncover suspicious fraudulent activities after the transaction or process has occurred. Compared to fraud prevention, detection is more reactive, involving fraud investigation and recovery activities after the incident. Detection may involve specific control activities, such as policies and procedures to identify attempted or existing suspicious activity to bypass RD's prevention controls. By engaging in fraud detection efforts and encouraging the reporting of suspicious activity, RD can reduce the cost, duration, and other impacts of fraud risks. RD performs fraud detection activities, such as monitoring, inspections and/or onsite reviews and automation, periodically across the organization. To mitigate fraud and to reveal a more accurate state of operations, compliance, and reporting, RD will limit, to the extent feasible, lengthy advance notices when conducting these activities. RD will practice a risk-based approach to demonstrate reasonable assurance of its internal controls and fraud detection activities by focusing on testing the highest risk transactions, processes, and controls.

(c) Data Analytics: Best practices include proactive data analytics as a fraud prevention, detection, and investigation tool that is integrated into a holistic FRM program. Data analysis will leverage available data and IT capabilities as available. Available data will be identified with an emphasis on relation to known fraud schemes. Combined data from across programs and databases within RD and from appropriate external sources is recommended to enable identification of fraud that may not otherwise be evident. It is anticipated that RD's methods, capabilities, and expertise in this area will evolve iteratively within the FRM program.

(d) Fraud and Misconduct Reporting:

(1) RD is committed to ensuring high ethical standards and conduct from all employees. Staff is our first line of defense against suspicious activity and misconduct. Staff must report any potential fraud, waste, abuse, and misconduct to their supervisor or, if appropriate, the OIG Hotline.

(2) Leadership should communicate reporting procedures for perceived fraudulent activity and misconduct, including information to RD OIG Hotline, personnel, and counterparties. The OIG hotline is available by phone from 8:00am to 4:00pm EST at 1-800-424-9121 via the website at https://usdaoig.oversight.gov/hotline.

(e) FRM Evaluation and Monitoring: RD program and program support areas will regularly evaluate existing fraud risk controls. To help identify early signals of fraud risk exposure, fraud risk indicators should be developed and monitored. If monitoring and evaluation efforts identify areas for improvement or emerging fraud risks and schemes, RD will adapt its methodology for the Fraud Risk Management Program. As part of this effort, the CRO will facilitate the monitoring of fraud risk mitigation strategies across the organization to determine if enhancements to fraud risk controls are necessary to reduce the risk exposure.

§ 2006.1810 Fraud Awareness Training.

To ensure that the risk of fraud and corruption is effectively mitigated, periodic training no less than annually, will be conducted to raise awareness about fraudulent acts and their prevention. RD will promote an anti-fraud/anti-corruption culture by fostering an organizational culture of integrity, transparency, and accountability, providing confidential ethics advice to all staff, including managers, on appropriate standards of conduct and including fraud and corruption awareness components in its ethics training programs.

§§ 2006.1811 – 2006.1850 [Reserved]

oOo

Exhibit A - Rural Development Fraud Policy Decision Matrix

Action Required	Investigative (OIG)	Internal/ External Audit	Finance/ Accounting	Program Support Mgmt	RD Program Mgmt	Risk Mgmt	Legal
1. Controls to Prevent Fraud		X	X	X	X	X	
2. Incident Reporting		X	X	X	X	X	
3. Investigation of Fraud	X					X	X
4. Referrals to Law Enforcement	X						X
5. Recovery of Monies due to Fraud	X						X
6. Recommendations to Prevent Fraud	X	X	X	X	X	X	X
7. Internal Control Reviews		X					
8. Handle Cases of a Sensitive Nature	X	X	X	X	X	X	X
9. Civil Litigation	X						X
10. Corrective Action/ Recommendations to Prevent Recurrences	X	X	X	X	X	X	X

Action Required	Investigative (OIG)	Internal/ External Audit	Finance/ Accounting/ Servicing	Program Support Mgmt	RD Program Mgmt	Risk Mgmt	Legal
11. Monitor Recoveries	X		X		X		X
12. Fraud Audits and Assessments		X	X	X	X	X	
13. Fraud Education/Training	X	X	X	X	X	X	
14. Risk Analysis of Areas of Vulnerability		X	X	X	X	X	
15. Fraud Case Analysis		X				X	X
16. Hotline	X					X	
17. Ethics Line				X			

oOo