Enterprise Risk Management for the FCA OIG

March 2020

FCA OIG

Farm Credit Administration
Office of Inspector General

Table of Contents

Background

The Farm Credit Administration (FCA) Office of Inspector established and implemented an Enterprise Risk Management (ERM) program independent of FCA. The OIG ERM program has been designed based on our mission, regulatory environment, strategic plan, size, and tolerance for risk.

ERM is an effective approach to addressing the full spectrum of an organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos. By identifying, measuring, and monitoring a portfolio of risks separate from the Agency's risks, ERM will enable the OIG to lead by example, and improve our risk-based planning efforts; concentrate efforts towards key risk or failure potentials and thereby reduce the potential for disruptive events; protect the FCA OIG values of objectivity, integrity, relevance, and respect; and identify opportunities to create value.

We will review the ERM plan and risk profiles on a continuous basis and revise as necessary to ensure that our ERM program remains relevant and evolves to a more mature model over time. The ERM program in our office will be overseen directly by the Inspector General (IG) in consultation with the Assistant IG for Audits, Inspections, and Evaluations (AIGAIE). The IG may delegate in writing some responsibilities for the program but remains ultimately responsible for ERM within the office.

Under the ERM program, it is the duty of the IG to encourage a risk-aware culture that stresses individual accountability at all levels. It is the duty of the AIGAIE to manage risk in the audit, inspection, and evaluation programs. All OIG staff are responsible for risk awareness and understanding their roles and responsibilities within the office relating to risk. OIG staff is encouraged to be thorough, analytical and candid in discussing risk issues, raising all relevant facts and information so that the IG and AIGAIE may consider all options and make informed decisions.

Our ERM program aligns with the following guidance:

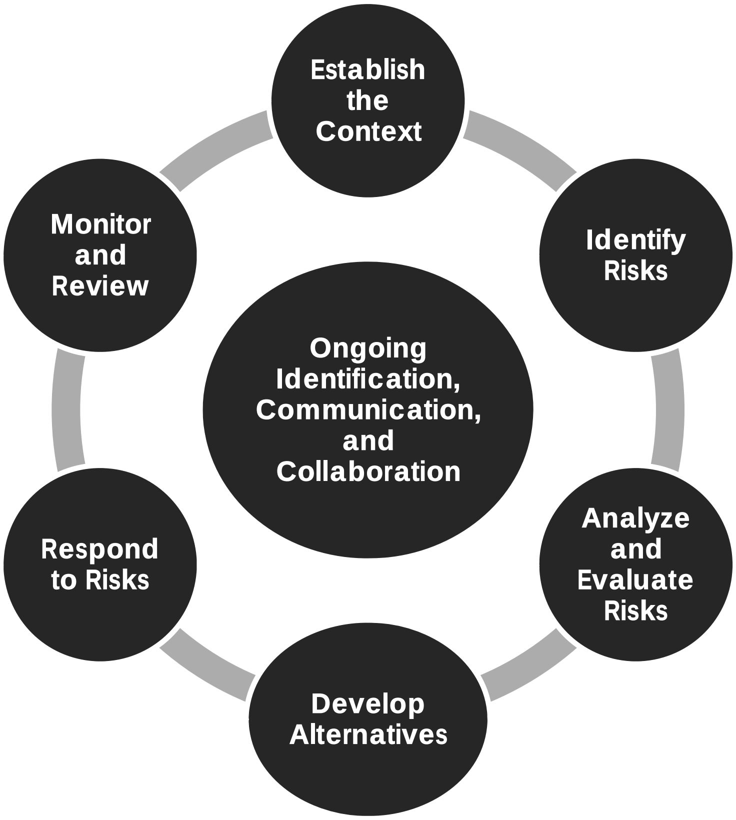
- Office of Management and Budget (OMB*) Circular A-123*, *Management's Responsibility for Enterprise Risk Management and Internal Control,*
- Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (Green Book),
- The Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Guide to Assessing Enterprise Risk Management*; and
- CIGIE's *Quality Standards for Federal Offices of Inspectors General* (Silver Book).

We will operate our ERM program with the purpose of:

- Supporting the mission and vision of the office;
- Integrating existing risk management practices across functional silos;
- Improving strategic planning and decision-making;
- Including diverse viewpoints while driving towards consensus;
- Establishing communication paths to understand early warning systems and escalation;
- Identifying, prioritizing, and proactively managing risks;
- Identifying opportunities;
- Supporting budget decisions and performance management;
- Promoting accountability and integrity of the agency's work; and
- Using a common approach to evaluating risks.

With this framework, we aim to facilitate continual improvement and build upon existing risk management processes, systems, and activities. We also aim to allow the ERM process to be systematic, structured, and timely as well as dynamic, interactive, and responsive to change.

The FCA OIG ERM framework consists of the following seven components:[1]



[1] OMB Circular A-123, p.11.

- Establish the Context – understand and articulate the internal and external environments of the FCA OIG. The environment may generate risks that cannot be controlled or constrain the way the OIG responds to a risk.
- Identify Risks – use a structured and systematic approach to recognizing where the potential for undesired outcomes or other negative consequences may arise.
- Analyze and Evaluate Risks – consider the sources, causes, probability, and potential positive or negative outcomes of risks occurring and prioritize the results of the analysis.
- Develop Alternatives – systematically identify and assess a range of risk response options guided by risk appetite.
- Respond to Risks – make decisions on the best option(s) among the alternatives and prepare and execute the selected response strategy. Risk responses will involve one or more of the following: acceptance, avoidance, reduction, sharing.
- Monitor and Review – evaluate and monitor performance to determine whether the implemented risk management options achieved the stated goals and objectives.
- Ongoing Identification, Communication, and Collaboration – identify risk throughout the year. Risk identification is an iterative process and a shared responsibility of all OIG employees.

Risk Identification Process

The IG, in consultation with OIG staff, will set the OIG risk appetite as part of each fiscal year performance planning process. The risk appetite will guide the office in establishing threshold criteria for OIG work and how best to allocate resources. Given our mission and the reliance on our work by the Agency, Congress, the IG community, and the public, we will continue to operate within an overall low risk range, when possible, and strive for continuous improvement.

On a broad level, and in accordance with OMB *Circular A-123*, the risks in the office will address the following objectives:

Strategic Objectives: strategic goals and objectives that align with and support the OIG mission to provide independent oversight to promote economy, efficiency, and effectiveness, and prevent and detect fraud, waste, and abuse in FCA programs and operations

Operations Objectives: effective and efficient use of OIG resources for administrative and major program operations, including financial and fraud objectives.

Reporting Objectives: reliability of the OIG reporting responsibilities to the FCA Board, Congress, and the public.

Compliance Objectives: OIG's compliance with the IG Act; the standards and guidance applicable to OIGs issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), U.S. Government Accountability Office, Office of Management and Budget, and Department of Homeland Security; and other applicable laws.

Key risks are those that may impact our ability to effectively execute our mission. Relevant risk categories for our office align with our strategic goals and encompass all the foregoing objectives:

1. Promoting Economy and Efficiency, which includes executing value-added audits, inspections, and evaluations; producing impactful products; and ensuring we have a diverse, professional, and highly skilled workforce.
2. Preventing and Detecting Fraud, Waste, and Abuse, which includes addressing potential matters of wrongdoing and misconduct with proficiency, independence, and due professional care; providing an independent mechanism to report fraud, waste, and abuse; and educating employees and contractors on fraud and whistleblower rights and protections.
3. Strengthening Internal and External Relationships, which includes listening to and understanding the needs, challenges, and interests of our stakeholders; reporting to and fully informing the FCA Board and Congress; and participating in and engaging with the IG community.

Risk Procedures

The OIG will maintain a risk register and risk profile to document and organize risks by objective. These items are stored on the OIG Shared Q drive. This assessment will inform our priorities, risk tolerances, and decision-making. Our risk profile will be continuously updated and communicated to staff to address emerging risks and strategic objectives. Each risk will contain the following:

1. Identification of objectives;
2. Identification of initial and new/changing risks;
3. Assessment of inherent risk, including impact and likelihood;
4. Current action taken to manage the risk;
5. Residual risk exposure from an inherent risk after action has been taken to manage it;
6. Proposed risk response to further reduce the exposure after taking risk mitigation actions; and
7. Proposed action category to identify the existing process that will be used to implement and monitor proposed actions

The OIG will use a scale to analyze and evaluate the impact and likelihood of risks. The OIG will document inherent and residual risks, and risk responses. Risk rankings will be assessed and documented on a continuous basis. However, on an annual basis, the OIG will review and adapt the risks as needed. The OIG will use the risk profile to prioritize efforts and resources, as needed. This prioritization process will ensure risks are addressed appropriately to ensure we meet our goals and objectives. The scale, and methodology, will be documented in the risk profile. We will also hold, as needed, "lessons learned" sessions on where our risk management decisions fell short and how we can improve them moving forward.

Guided by risk appetite, the OIG will systematically identify and assess a range of response options or strategies to accept, transfer, share, avoid, or mitigate major risks identified, as appropriate. Understanding priorities, the OIG will allocate resources to address risks. If needed, the OIG will set milestones for high risk items and monitor implementation.

The OIG will incorporate enterprise risk management principles in our day-to-day operations. We will regularly review, monitor, and updated risk information documents in the risk profile. The detailed risk profile shall remain on the OIG shared drive, available to all staff for viewing. Staff, at any time, may bring ideas, concern, or gaps to the attention of senior leadership.

Identifying risks is an iterative process, occurring throughout the year and a shared responsibility of all OIG employees. It includes being mindful of the leading indicators of future risk from internal and external environments. For our OIG, this means that our staff must be cognizant of current Agency challenges, the agricultural economy, and the challenges of the IG community as well as other challenges on the horizon that could affect our risk assessments.

OIG’s Current Risk Register and Scale

The OIG’s arranged its risk register by compliance, operations, reporting, and strategic objectives. In creating the risk profile, each risk from the risk register was given an inherent risk rating without factoring in control systems in place. Then, the risks are analyzed with residual risks, which is the amount of risk left over after actions and controls. The OIG uses an impact and likelihood scale as follows:

5 Point Scale - Impact

		Description	**Performance**	**Cost**	**Schedule**	**Reputation**
5	Severe	a risk event that, if it occurs, will have a severe effect on achieving desired results to the extent one or more objectives will not be achieved.	Performance unacceptable. Immediate action required.	Causing additional costs of more than $25,000	Causing delays greater than 6 months	External reputation of current leadership and organization irrevocably damaged or destroyed (e.g., congressional attention resulting in possible removal of IG)
4	Significant	a risk event that, if it occurs, will have a significant effect on achieving desired results to the extent one or more objectives will fall below acceptable levels of performance.	Performance unacceptable. Significant action required.	Causing additional costs of $25,000 to $5,000	Causing delays of 3-6 months	External reputation of current leadership and organization significantly damaged; considerable effort required to rectify (e.g., adverse national media attention, congressional oversight attention)
3	Moderate	a risk event that, if it occurs, will have a moderate effect on achieving desired results to the extent one or more objectives will fall well below goals but above acceptable levels of performance.	Performance below goal. Moderate action required.	Causing additional costs of $5,000 to $1,000	Causing delays of 30-90 days	External reputation of current leadership and organization damaged; some effort required to rectify (e.g., media attention, congressional constituent letter)
2	Minor	a risk event that, if it occurs, will have a minor effect on achieving desired results to the extent one or more objectives will fall below goals but well above minimally acceptable levels of performance.	Performance below goal but within acceptable limits. No action required.	Less than $1,000	Minor schedule slips; up to 1 month	External reputation of current leadership and organization minimally affected; little effort required to rectify (e.g., stakeholder complaint)
1	Minimal	a risk event that, if it occurs, will have little or no impact on achieving desired objectives.	Little or no impact on program success.	Little or no cost	Schedule not affected or can be adjusted within plans	External reputation of senior leadership and organization not affected.

5 Point scale - likelihood

5	Almost Certain
4	Highly Likely
3	Possible
2	Unlikely
1	Rare or Highly Unlikely

Heat Map (impact x likelihood)

Critical	18-25
High	12-18
Medium	6-11
Low	1-5

The scales and heat map allow the OIG to easily view our risks and areas needing attention.

The risk profile shows three critical areas and four high areas for inherent risks. However, for residual risks, we have no critical risks and one risk that remains high. The high risk is identified as our confidentiality risk, which is the failure to manage information technology resources to ensure confidentiality of systems and data in compliance with law.

This risk is an impact level five and likelihood as a three. These residual ratings are primarily due to the OIG documentation residing on the Agency servers. While we have certain controls in place to monitor Agency personnel accessing OIG data, we remain a user of the Agency's servers and the Office of Information Technology implements our technology. In an effort to reduce this risk, the OIG is researching options for independent servers, case management software options outside of FCA, and other best practices in the IG community.

We have also responded to two other medium rankings with mitigation efforts, and, based on sound risk management principles rate the other risks in our profile as accept. Although we rate these specific areas as accept, we remain diligent in our enterprise risk management efforts to enhance our risk models and practices and aim to move our program higher in the maturity model.

A summary of our risk profile follows on the next page.

OIG Risk Profile Summary

Risk	Definition	INHERENT RISK ASSESSMENT		AGGREGATE INHERENT	RESIDUAL RISK ASSESSMENT		AGGREGRATE RESIDUAL	RESPONSE
		Impact	Likelihood		Impact	Likelihood		
Confidentiality risk	The failure to manage information technology resources to ensure confidentiality of systems and data in compliance with law.	5	4	20	5	3	15	Mitigate
Evidentiary Support Risk	The failure to manage to ensure the accuracy and completeness of evidence necessary to accomplish program goals and objectives.	5	4	20	5	2	10	Mitigate
Systems Compliance risk	The failure to ensure major programs (IT, records management, FOIA/Privacy Act) are managed in accordance with legal requirements.	4	3	12	4	2	8	Mitigate
Work planning risk	The failure to identify and assess FCA risks and align work resources accordingly.	4	3	12	4	2	8	Accept
Leadership succession risk	The failure to prepare for leadership continuity in the event of separation or transfer.	4	3	12	4	2	8	Accept
Investigations risk	The failure to detect and address fraud, waste, abuse and misconduct in FCA programs and operations.	3	3	9	3	2	6	Accept
AIE risk	The failure to plan projects to ensure meaningful work and results and promote economy and efficiency.	3	3	9	3	2	6	Accept
Key-person dependency risk	The failure or disruption of OIG processes or products following the separation or transfer of a key person.	3	2	6	3	2	6	Accept
Financial risk	The failure to properly budget for OIG work.	3	2	6	3	2	6	Accept
Quality assurance risk	The failure to ensure work products are completed in accordance with professional standards.	5	4	20	5	1	5	Accept
Reporting risk	The failure to timely report to and fully inform the FCA Board and Congress	5	1	5	5	1	5	Accept
Illegal acts risk	The failure to prevent and detect misconduct by OIG employees.	4	2	8	4	1	4	Accept
Third party risk	The failure to provide effective oversight of OIG contractors and third party providers.	4	3	12	4	1	4	Accept
Mandate risk	The failure to meet mandated reporting requirements.	4	2	8	4	1	4	Accept
Hotline risk	The failure to provide independent mechanisms to report fraud, waste, and abuse.	3	2	6	3	1	3	Accept
Governance risk	The failure to ensure a culture of accountability and compliance.	3	2	6	3	1	3	Accept
Training and development risk	The failure to train and develop OIG personnel	3	3	9	3	1	3	Accept
Project management risk	The failure to timely manage projects to completion.	2	2	4	2	1	2	Accept
Mission support risk	The failure or disruption of timekeeping, budget, procurement, IT, HR and related mission support functions.	2	2	4	2	1	2	Accept

FCA OIG

Farm Credit Administration
Office of Inspector General

REPORT FRAUD, WASTE, ABUSE, & MISMANAGEMENT

Phone:	**(800) 437-7322 (Toll-Free)** **(703) 883-4316**
Fax:	**(703) 883-4059**
Email:	**fca-ig-hotline@rcn.com**
Mail:	**1501 Farm Credit Drive** **McLean, VA 22102-5090**

To learn more about reporting wrongdoing to the OIG, please visit our website at https://www.fca.gov/about/inspector-general.