



United States Department of Agriculture

**Financial Management
Modernization Initiative (FMMI)**

***FMMI Roles and Responsibilities
for Central Security Team and
Agency Security Administrators***

Version 1.0

May 2014



Table of Contents

1	Introduction.....	4
1.1	FMMI Policy:.....	5
1.2	Roles and Responsibilities	6
1.2.1	Requestor	6
1.2.2	Agency Security Administrator	7
1.2.3	Central Security Administrator	9
	Appendix A – Job Aids for Generating SUIM Reports (Quarterly).....	11
	Appendix B – Job Aid for Generating GRC Reports of Expired Mitigations (Quarterly)	12



Previous Change History

Version	Date	Author	Comment
1.0	5/2014	Melissa Montz	Per POAM 19822 This document was created to satisfy an OIG audit recommendation (POAM 19822) which stated that one document is created that clearly identifies the Roles and Responsibilities of the FMMI Central Security Team and the FMMI Agency Security Administrators within USDA.

Document Sign-off

Date	Name	Title



1 Introduction

To address challenges and opportunities in the rapidly changing federal financial management and technology environment, the USDA Office of the Chief Financial Officer (OCFO) pursued significant modernization of its aging corporate financial and administrative payment systems and program ledgers, thus implementing Financial Management Modernization Initiative (FMMI). Through FMMI, USDA replaced its legacy mainframe systems with an advanced, web-based core financial management system that complies with Federal accounting and systems standards. FMMI has an end-to-end user access process and meets the audit requirements through the Governance, Risk and Compliance (GRC) Access Control tool.

The Associate Chief Financial Officer for Financial Systems (ACFO-FS) is the responsible organization for FMMI. FMMI is a Federal Financial System and is considered OMB reportable. The primary objective of FMMI is to improve financial management performance by providing USDA agencies with a modern, efficient core financial management system that complies with Federal accounting and systems standards and provides maximum support to the USDA Mission.

The purpose of this document is to clearly identify the Roles and Responsibilities of the FMMI Central Security Team, FMMI Requestors and the FMMI Agency Security Administrators within USDA.



1.1 FMMI Policy:

All FMMI accounts should be reviewed by Agency Security Administrators to ensure compliance with National Institute of Standards and Technology (NIST) standards ensuring identification and disabling of inactive accounts. Any FMMI account that is inactive for more than 60 days should be disabled. The FMMI Central Security Team generates Quarterly reports for each agency as a compensating control.

Any FMMI account that is inactive for more than 60 days should be reviewed and disabled, as appropriate, by the FMMI Agency Security Administrators. This task will be performed by the FMMI Agency Security Administrators for their respective agency users.

1.2 Roles and Responsibilities

This section details the roles and responsibilities of the key stakeholders namely Requestors, Agency Security Administrators and Central Security Administrators in the FMMI Access Management process.

1.2.1 Requestor

For FMMI, the user access request is submitted by the designated users (Requestors) within each Agency. Requestors will have the authorization to enter Governance Risk and Compliance (GRC) requests requesting access to FMMI. During the request submission process, it is mandatory that the Requestor ensure that the following activities are completed by the user:

1. Annual Security Awareness Training
2. Background verification
3. FMMI Training relevant to responsibilities within the FMMI system.

FMMI Requestors also assist with determining what access end users will need to perform their job tasks.

1.2.2 Agency Security Administrator

The Agency Security Administrator is primarily responsible for performing activities related to user provisioning of users within their own agency.

Agency Security Administrators:

- Approve roles for the agency users via GRC
- Perform risk analysis in GRC before approving any roles for users during the request process
- Mitigate risks at the user level and request level
- Maintain inactive users
- Perform regular risk analysis via GRC Risk Analysis Report (RAR)
- Maintain FMMI user account expiration dates for contractors
- Run audit reports to check for users to ensure least functionality
- Authorization to lock and unlock accounts

GRC Daily Tasks for FMMI Agency Security Administrators:

- **Agency Approver of GRC Requests in the Role Approval Stage**
There is a role approval stage within GRC where the administrator approves the roles that he/she owns within an Agency for all new and/or change requests for FMMI access. In cases of cross-servicing, the request is automatically routed to multiple-role approvers. The request will not enter the next stage until all the roles are approved.
- **Agency Approver of GRC Requests in the Security Administrator Approval Stage**
This is the final stage of approval in all the FMMI Access Management workflows. Risk analysis is mandatory at this stage to ensure that the user access privileges do not have any Segregation of Duty (SOD) conflicts. If there are any SOD conflicts, the Agency Security Administrator should mitigate the risk using existing mitigation controls. Provisioning through GRC will not complete without mitigation. If mitigation does not exist, the agency is responsible for requesting the establishment of one. The mitigation should identify any compensating controls to eliminate or reduce the risk. The agency is also responsible for the testing of this control as part of their A-123 testing.



The following reports should be generated by all FMMI Agency Security Administrators:

FMMI Quarterly Reports via SUIM (March, June, September and December of each year)

FMMI Reports to be generated via SUIM (See Appendix A for Job Aid) are as follows:

- Inactive Users Report (90 days) for ECC and Business Intelligence (BI)
- List of Users and Roles for ECC and BI
- Role Report by Role Name for ECC and BI

FMMI Agency Security Administrators must send an email to the FMMI Central Security Team (fmmi.security@usda.gov) every Quarter, acknowledging the Inactive Users Report, List of Users and Roles and the Role Report by Role Name Reports were all generated. That email should include what action, if any, will be taken based upon the Certification of these reports. If access is removed for a user, please provide the GRC Remove Request number in your response. If no action is required, please state that in your email response to the FMMI Central Security Team.

FMMI Quarterly Reports via GRC (January, April, July and October of each year)

FMMI SAP GRC Access Control Report (Report of expired mitigations) (See Appendix B for Job Aid):

- Risk Analysis by User Level (Under Informer Tab, Risks Analysis, User Level, Select User Group, execute, select Display Detail Report)

FMMI Agency Security Administrators must send an email to the FMMI Central Security Team (fmmi.security@usda.gov) every Quarter, acknowledging that the GRC Risk Mitigation Report was generated and action was taken to either extend the mitigations or a decision was made to remove the access from the user. If access is removed for a user, please provide the GRC Remove Request number in your response. If no action is required, please state that in your email response to the FMMI Central Security Team.

Annual Reports (January of each year)

- Agency Specific Role Review (SUIM) Reports to ensure user's have the least privilege to perform their job functions within FMMI

FMMI Agency Security Administrators must send an email to the FMMI Central Security Team (fmmi.security@usda.gov) in January of each year, acknowledging this report was generated and action was taken if required. If access is removed for a user, please provide the GRC Remove Request number in your response. If no action is required, please state that in your email response to the FMMI Central Security Team.

1.2.3 Central Security Administrators

The Central Security Administrator is part of the FMMI core team. The FMMI Central Security Administrator is responsible for managing and overseeing all access to FMMI. Some of the other responsibilities of the Central Security Administrator include periodic reporting, providing audit support, and issue resolution with respect to access related matters.

Central Security Administrators:

- Approve and assign critical roles to Agency Users
- Authorize and remove Agency Security Administrators access
- Approve SAP License requests for new users via GRC Compliance User Provisioning (CUP)
- Provides oversight for regular risk analysis in GRC RAR that is run by Agency Security Administrators
- Perform regular risk analysis via GRC RAR
- Approve GRC requests for O&M Users
- Authorization to lock and unlock accounts
- Maintain user groups for FMMI users
- Maintain GRC configuration settings
- Input approved mitigation controls into RAR
- Role Maintenance

GRC Daily Tasks for FMMI Central Security Administrator:

Agency Approver of GRC Requests in the Role Approval Stage

Apart from the license approval, the Central Security Administrator owns the entire master (department level) roles and is responsible for approving the global roles for department level users, approve O&M users, authorize Agency Security Administrators, etc. The Central Security Administrators also perform a risk analysis within RAR at the agency level and at the USDA level, as well as part of the license approval process. While roles are owned by CSA, COD has been designated as the role approval authority for department level access.

Agency Approver of GRC Requests in the Security Admin Approval Stage

This is the final stage of approval in all the FMMI Access Management workflows. Risk analysis is mandatory at this stage to ensure that the user access privileges do not have any SOD conflicts. If there are any SOD conflicts, the Agency Security Administrator should mitigate the risk using existing mitigation controls. Provisioning through GRC will not complete without mitigation.



SAP User License Approver for ALL GRC requests in the License Approval Stage

The Central Security Administrator will be performing this role through GRC CUP, under Access Control in FMMI Portal. This is the first approval stage for all ‘new account’ request type.

The following reports are generated by the Central Security Administrators for FMMI:

FMMI Quarterly Reports via SUIM (March, June, September and December of each year)

FMMI Reports to be generated via SUIM (See Appendix A for Job Aid) are as follows:

- Inactive Users Report (90 days) for ECC and BI
- List of Users and Roles for ECC and BI
- Role Report by Role Name for ECC and BI

FMMI Quarterly Reports via GRC (January, April, July and October of each year)

FMMI SAP GRC Access Control Report (Report of expired mitigations) (See Appendix B for Job Aid):

- Risk Analysis by User Level (Under Informer Tab, Risks Analysis, User Level, Select User Group, execute, select Display Detail Report)

Annual Reports (January of each year)

- FMMI Agency Security Administrators and FMMI Point of Contacts List (Review and Update)
- FMMI Role Owner Reports for entire USDA population

Semi-Annual Reports via SUIM (January, June of each year)

- FMMI Contractor Certification Reports for FMMI Production, QA, System Test, Development - Quarterly Reports
- SAP GRC-Compliant User Provisioning Reports (CUP)
 - GRC Report of all Open/Stale Requests – Semi-Annual Reports
 - GRC Report of all REMOVE Access Requests – Semi-Annual Reports

Annual Reports (July of each year)

- FMMI Expired Funds Table Report
 - Report generated in July of each year. Report is sent to all Agency CFO’s to obtain approvals/changes to this table. User’s access expires on November 1st each year unless timeframe is requested for a shorter period. Users are not allowed to have access longer than one year.



Appendix A – Job Aids for Generating SUIM Reports (Quarterly)

- [FMMI SUIM Inactive User Report](#)
- [FMMI SUIM List of Users and Roles](#)



Appendix B – Job Aid for Generating GRC Reports of Expired Mitigations (Quarterly)

- [FMMI GRC Generated Mitigations Report](#)