U.S. DEPARTMENT OF ENERGY
FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT
(FMFIA)

Internal Control Evaluations

Fiscal Year 2022 Guidance

Key Dates	Deliverables
December 2	AMERICA open for documenting FY 2022 internal control testing and evaluation results.
February 3	Headquarters Offices and Power Marketing Administrations (PMA) upload Risk Profile excel and signed PDF versions, updated and revised only **if there are substantive changes to risks**, with consideration of reporting from Field Offices, Site Offices, M&O and non-M&O Contractors as applicable, **or a signed memorandum from the organization's management indicating there are no changes from the FY 2021 Risk Profile** to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov. Reporting organizations should check with their cognizant organization to determine substantive changes for Risk Profiles and follow cognizant organizations subsequent timelines to assure Risk Profiles are provided to DOE on time.
March 3	Under Secretaries provide Risk Profile excel and signed PDF versions,updated and revised only **if there are substantive changes to risks or a signed memorandum indicating there are no changes from the FY 2021 Risk Profile**, to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov based on the input of the reporting offices.
March 17	Reporting organizations (M&O Contractors, Site Offices, Field Offices, & HQ Offices) provide Interim Internal Control Status using the AMERICA Application. Reporting organizations should follow subsequent timelines published by cognizant organizations to assure IICS Modules are provided to DOE on time.
	Reporting organizations provide Risk POC names to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.
April 6	OCFO publishes the FY 2022 Assurance Memoranda Template to reporting organizations.
April 14	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review and the FY 2024 Budget Formulation process.
May 26	OCFO provides the lead responsible offices with Management Priorities in required templates for FY 2022 update. **Note:** Applicable to Management Priority Owners Only.
June 23	Lead responsible offices provide OCFO with mid-year updates on Management Priorities using provided templates based on FY 2022 enterprise activities performed and planned. **Note:** Applicable to Management Priority Owners Only.
July 7	M&O Contractors, PMAs, and Field Offices provide FMA Module and EA Module using the AMERICA Application. Reporting organizations should follow subsequent timelines published by cognizant organizations to assure FMA and EA Modules are provided to DOE on time.
July 21	Headquarters Offices provide FMA Module and EA Module using the AMERICA Application.
August 4	PMAs and Field Offices provide draft Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov, considering and incorporating Site Offices and M&O Contractors.
August 18	Headquarters Offices provide draft Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.
August 22	OCFO provides eDOCS information to Headquarters Offices.
August 25	PMAs and Field Offices provide signed Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.
August 31	AMERICA close-out performed for FY 2022.
September 8	Headquarters Offices provide signed Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov and eDOCs.
	Lead responsible offices provide OCFO with Management Priorities year-end updates. **Note:** Applicable to Management Priority Owners Only.
September 22	Under Secretaries provide signed Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov and eDOCs.
October 3	Organizations that resolve or identify a significant deficiency or material weakness, after June 30, 2022, and no later than September 30, 2022 that is not included in a signed Assurance Memoranda, must notify the OCFO and update the Assurance Memoranda.
October - TBD	OCFO will provide Management Priorities updates to the DICARC in early October for review. **Note:** Applicable to Management Priority Owners; Per DICARC recommendation, the final Management Priorities are incorporated into the AFR and proceed through Exec Sec Concurrence Process.

Department of Energy
Washington, DC 20585

December 13, 2021

MEMORANDUM FOR DISTRIBUTION

FROM: KARIN DASUKI
DIRECTOR, OFFICE OF FINANCE AND ACCOUNTING

Karin Dasuki Digitally signed by Karin Dasuki Date: 2021.12.22 17:01:55 -05'00'

SUBJECT: Federal Managers' Financial Integrity Act of 1982 Requirements and DOE FY 2022 Internal Control Evaluations Guidance

Per the *Federal Managers' Financial Integrity Act of 1982* (FMFIA), federal agencies are required to establish and annually evaluate internal controls systems. The attached Department of Energy (DOE) FY 2022 Internal Control Evaluations Guidance provides the departmental process for meeting FMFIA requirements in accordance with the Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (Green Book) and Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

DOE's Internal Control Program continues to execute initiatives to reduce burdens on reporting organizations while maintaining effective internal controls for the Department. The initiatives are:

- Conducting a pilot program with four laboratories to evaluate alternative control test cycle approaches, analytical and business process approaches;
- Continued implementation of a Departmental Fraud Risk Framework to mitigate and reduce potential fraud activities; and,
- Further synchronization of the Department's Risk Profile to Budget Formulation processes to better align funding to needed resources.

Heads of Departmental Elements (Field and Headquarters) and Under Secretaries are responsible for maintaining and evaluating internal controls, and evaluating financial management systems compliance with federal requirements, and reporting FMFIA evaluation results to the Secretary in an annual Assurance Memorandum. Assurance Memoranda report on the overall adequacy and effectiveness of internal controls, identify any material weaknesses or significant deficiencies and assert financial management systems compliance with government-wide requirements. These individual assurances are compiled to support the Secretary's annual assurances in DOE's Agency Financial Report.

Assurance Memoranda are due from Field Elements on **August 25, 2022,** Headquarters Offices on **September 8, 2022,** and each Under Secretary on **September 22, 2022**. If there is an issue preventing a timely Assurance Memorandum, organizations must provide the reason(s) for the delay and advance notice of any potential significant deficiencies or material weaknesses to the Director, Internal Controls and Fraud Risk Management Division. A summary of all key dates and deliverables is provided on the front inside cover of the guidance.

If you have any questions about this guidance, please contact Lynn Harshman, Division Director, Internal Controls and Fraud Risk Management, at 301-903-2556.

DISTRIBUTION LIST:

S-1 Chief of Staff
S-2 Chief of Staff
Under Secretary for Science and Energy
Under Secretary
Under Secretary for Nuclear Security/ Administrator for National Nuclear Security Administration
Assistant Secretary for Congressional and Intergovernmental Affairs
Assistant Secretary, Cybersecurity, Energy Security & Emergency Response
Assistant Secretary for Electricity
Assistant Secretary for Energy Efficiency and Renewable Energy
Assistant Secretary for Environmental Management
Assistant Secretary for Fossil Energy
Assistant Secretary for Nuclear Energy
Assistant Secretary, International Affairs
Associate Under Secretary, Environment, Health, Safety and Security
Deputy Under Secretary for Artificial Intelligence and Technology
Administrator, Energy Information Administration
Office of Policy
Chief Human Capital Officer
Chief Information Officer
General Counsel
Inspector General
Executive Director, Loan Programs Office
Director, Advanced Research Projects Agency-Energy
Director, Arctic Energy
Director, Office of Artificial Intelligence and Technology
Director, Office of Clean Energy Demonstrations
Director, Office of Economic Impact and Diversity
Director, Office of Enterprise Assessments
Director, Office of Hearings and Appeals
Director, Office of Indian Energy Policy and Programs
Director, Office of Intelligence and Counterintelligence
Director, Office of Legacy Management
Director, Office of Management
Director, Office of Project Management Oversight & Assessment
Director, Office of Public Affairs
Director, Office of Science
Director, Office of Small and Disadvantaged Business Utilization
Director, Office of Technology Transitions
Power Marketing Administration Liaison Office

Summary of Changes in FY 2022 Internal Controls Guidance

Infrastructure Investment and Jobs Act (*Infrastructure Bill*): Reporting organizations and their downstream organizations that receive funding from the Infrastructure Bill must ensure properly working controls are in place to mitigate risks that are associated with providing financial assistance awards. Risks associated with this bill should be properly evaluated for potential inclusion in the FY 2022 Risk Profile. For more information, see Section IV: Financial Management Assessment (FMA) Evaluation.

Risk Profile: Under Secretaries, Headquarters Offices and Power Marketing Administrations will submit Risk Profiles **only if there are substantive changes to risks**, with consideration of risks reported by Field Offices, Site Offices, M&O and non-M&O Contractors. If Under Secretaries, Headquarters Offices and Power Marketing Administrations do not have substantive changes to their FY 2022 Risk Profile, **the organization's management will provide a signed memorandum** indicating there were no changes in the previous year's Risk Profile. While DOE does not require every organization to provide Internal Control and Risk Profile deliverables, organizations **should check** with respective Headquarter Offices.

Documentation Requirements: Organizations are responsible for **uploading requested documentation** in AMERICA for the ***Cost Monitoring*** **sub-process risk statement CR1405**. Documentation may include business process narratives or flowcharts, risk analyses, test plans, and other applicable documents that support the entity's assessment and evaluation. Organizations will upload documentation sufficient to demonstrate the scope and type of testing performed and notable findings or exceptions. For more information on the business sub-processes which require supporting documentation to be uploaded, refer to Section IV: Financial Management Assessment (FMA) Evaluation.

Corporate Risks Update: Entities will reassess the applicability of corporate risks (CR) 2109, 2112, 2116, and 2120 in the *Acquisition Management* business process and CR6408 and CR6409 in the *Contractor Oversight* business process. Risk statements have been updated to include risks that are associated with having sub-contractors. CR6408 and CR6411 were combined into one risk statement. In FY 2022, reporting organizations should reassign the controls mitigating CR6411 to mitigate CR6408. In FY 2023, CR6411 will be deleted from the AMERICA FMA Module. Reporting organizations should also reassess the applicability of CR2405 in the Travel Administration business process.

Fraud/ Improper Payments: *Fraud/ Improper Payments* dropdown options have been removed from the *Type of Risk* field. Therefore, entities **must** identify in the FMA Module **local risks** that are subject to fraud, improper payment, or both by selecting the appropriate designation from the dropdown menu of the *Fraud/ Improper Payments* field. In FY 2022, local risks with designations of *Fraud, Improper Payments,* or *Both Fraud and IP* designations have been changed to *Business*. A list of risks will be sent in December to the affected organizations for review to either confirm or change the *Business* designation. **Corporate risks** with designations of *Fraud, Improper Payments,* or *Both Fraud and IP* at the end of FY 2021 have been changed to their pre-AMERICA designations. No further actions on **corporate risks** are required by users.

If a control is designed to mitigate a fraud and/ or improper payment risk and the control fails testing, or fails related to the detection of potential fraud, the organization will notify the organization's assigned OCFO Analyst on the control failure and the remediation plan to confirm a control is designed and operating effectively to mitigate the risk. For further information on managing fraud risks and the fraud related internal controls requirements, refer to Appendix E, Fraud Risk Management Guidance.

Internal Controls and Financial Management Oversight: DOE Order 520.1B was approved January 2021 directing the head of each Departmental Element to designate an Internal Control Action Officer that will coordinate the organization's Internal Control Program that is consistent with the DOE Internal Control Evaluations Guidance. When an organization changes the designated Internal Control Action Officer, the updated name and contact information should be provided to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.

Table of Contents

List of Figures

List of Tables

Appendices

I. Introduction

A. Purpose and Background

Internal control requirements are codified in the *Federal Managers' Financial Integrity Act of 1982* (FMFIA). The Act requires the Comptroller General of the Government Accountability Office (GAO) to establish internal control standards and the Director of the Office of Management and Budget (OMB), to establish guidelines for agency evaluation of systems of internal control to determine such systems' compliance with the requirements. The GAO established formal standards in the *Standards for Internal Control in the Federal Government* (Green Book), and OMB established guidelines for evaluation in OMB Circular A-123 (A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control*.

This guidance establishes the Department of Energy's (DOE) Internal Control Program requirements for evaluating and reporting on internal controls and preparation of a DOE Risk Profile in accordance with A-123. Each reporting organization is responsible for establishing, maintaining, and evaluating systems of internal controls in compliance with this guidance.

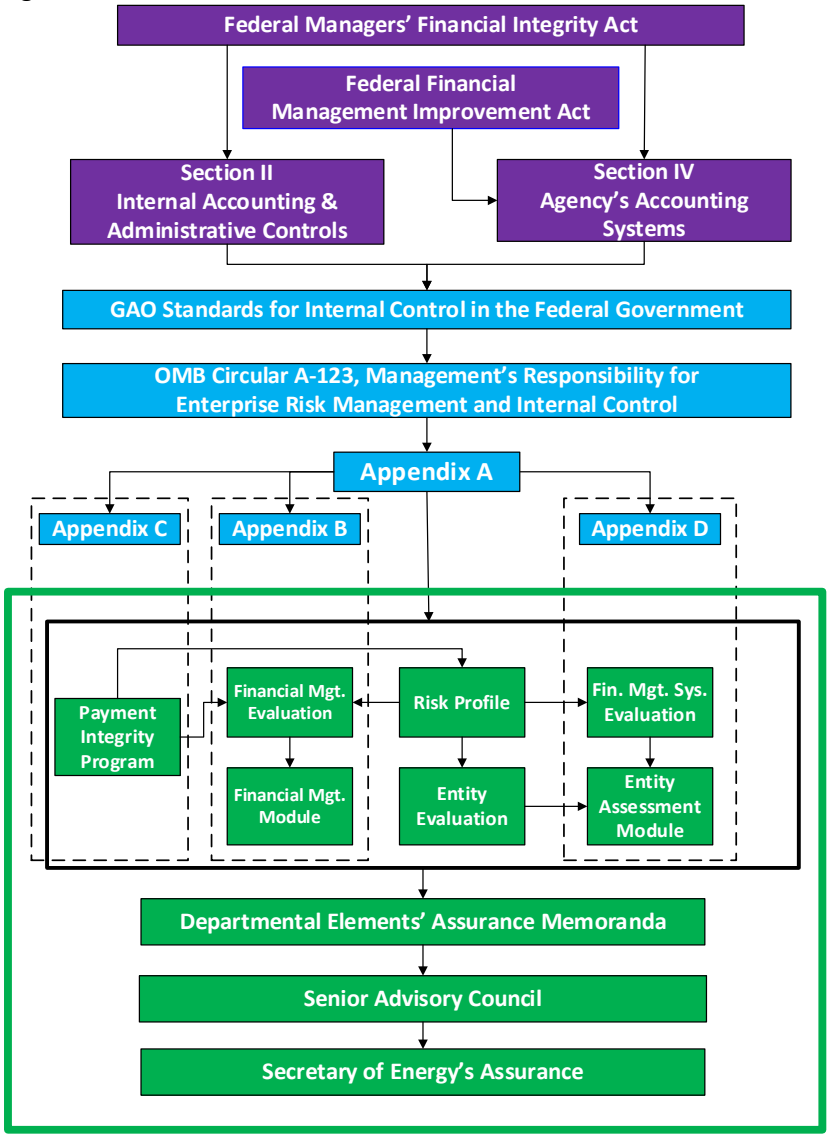
FMFIA requires each agency to:

- Establish and maintain an internal control system, and report on the overall adequacy and effectiveness of internal control systems. Internal control systems should provide: 1) obligations and costs to be recorded in compliance with applicable laws; 2) funds, property, and other assets to be safeguarded; and 3) revenues and expenditures applicable to agency operations to be properly recorded and accounted for to provide reliable financial reporting and to maintain accountability over the assets;
- Evaluate financial management systems to determine compliance with government-wide requirements mandated by Section 803(a) of the *Federal Financial Management Improvement Act* (FFMIA), and to take corrective actions if systems are non-compliant; and,
- Provide an annual assurance statement signed by the head of the agency reporting on the overall adequacy and effectiveness of internal controls related to operations, reporting, and compliance; identified material weaknesses; and whether the agency's financial management systems are in compliance with FFMIA.[1]

[1] Agency requirements mandated by Federal Managers' Financial Integrity Act of 1982

Figure 1 presents the DOE framework for internal control evaluations. The DOE activities (in green) meet statutory requirements (in purple) and Federal Government guidance (in blue).

Figure 1 DOE Internal Controls Evaluation Framework



Legislation

Federal Standards & Guidelines

DOE Requirements

B. OMB Circular A-123

In FY 2022, DOE continues to comply with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* which provides guidance for internal control and risk management requirements. OMB Circular A-123 also establishes the requirement to produce an agency Risk Profile as part of the implementation of an Enterprise Risk Management (ERM) capability coordinated with strategic planning, strategic review, and internal control processes.

OMB Circular A-123 requires:

- Integration of risk management and internal control functions;
- Implementation of an ERM capability in coordination with the strategic planning and strategic review process required by the *Government Performance and Results Act Modernization Act* (GPRAMA) and the internal control processes required by FMFIA;

- Incorporation of risk identification capabilities into the framework to identify new/ emerging risks or changes in existing risks;
- Development of a Risk Profile, including fraud risk evaluation, coordinated with annual strategic reviews;
- Establishment and maintenance of internal controls to achieve objectives related to operations, reporting and compliance;
- Evaluation of the effectiveness of DOE internal controls in accordance with the GAO Green Book; and,
- Annual reporting of overall adequacy and effectiveness of DOE internal controls related to operations, reporting, and compliance, and compliance of financial management systems with government-wide requirements.

On June 6, 2018, OMB released a revised Appendix A, *Management of Reporting and Data Integrity Risk*, to OMB Circular A-123. The objectives of Appendix A are to effectively manage taxpayer assets, including government data, improve data quality, and streamline efforts for agencies by shifting away from compliance activities and moving toward actions that will support the reporting of quality data. Prior to the update, Appendix A was prescriptive in the activities agencies needed to implement to provide reasonable assurance over internal controls over financial reporting which organizations may still use as a best practice. The revised Appendix A balances prior requirements with flexibility for agencies to determine which control activities are necessary to achieve reasonable assurance for internal control over reporting (ICOR). The updated Appendix A also further aligns ICOR with existing OMB Circular A-123 efforts.

On August 27, 2019, OMB released a revised Appendix B, *A Risk Management Framework for Government Charge Card Programs*, to A-123. The purpose of Appendix B is to consolidate current government-wide charge card program management requirements and guidance issued by various Federal agencies as well as provide a single document that incorporates new guidance or amendments to existing guidance. Appendix B also establishes standard minimum requirements and best practices for government charge card programs that may be supplemented by individual organization policies and procedures. Reporting organizations will continue providing assurance there are appropriate controls established to mitigate the risk of inappropriate charge card practices.

On June 26, 2018, OMB released a revised Appendix C, *Requirements for Payment Integrity Improvement*, to A-123. The primary goal of Appendix C is to transform the improper payment compliance framework to a unified and comprehensive set of requirements. Improper payments consist of intentional fraud and abuse, unintentional payment errors, and instances where the documentation for a payment is insufficient for the reviewer to determine whether a payment is proper. Organizations that provide an improper payment report to the Office of the Chief Financial Officer (OCFO) will receive separate and detailed guidance for DOE's Improper Payment Program by the start of Q4 in FY 2022. For further details on improper payments, Internal Controls Points-of-Contact (POC) may reference DOE's FY 2021 Improper Payment Program guidance and should coordinate with the organization's Improper Payment POC.

In March 2020, the President signed into law the *Payment Integrity Information Act of 2019* (PIIA) that incorporated select provisions from Fraud Reduction and Data Analytics Act of 2015 (FRDAA), the *Improper Payments Information Act of 2002*, and the *Improper Payments Elimination and Recovery Act of 2010* (IPERA) into a single subchapter in the US Code. PIIA of 2019 consolidates the previous published laws.

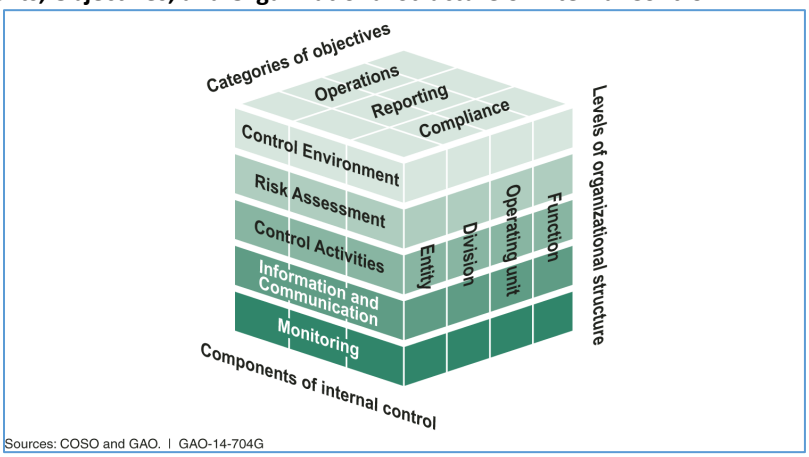
C. GAO Standards for Internal Control

The GAO's *Standards for Internal Control in the Federal Government* (Green Book) provides criteria for designing, implementing, and operating an effective internal control system, and through the use of components and principles, establishes standards for internal control. Internal control in an organization provides reasonable, not absolute, assurance that the organization will achieve objectives related to operations, reporting, and compliance.

Using the standards and guidance provided in the Green Book, an organization can design, implement and operate internal controls to achieve objectives related to operations, reporting, and compliance.

The five components of internal control are: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. There are 17 principles which support the effective design, implementation, and operation of the five components and represent requirements necessary to establish an effective internal control system.

Figure 2 The Components, Objectives, and Organizational Structure of Internal Control



D. Managing Fraud Risks

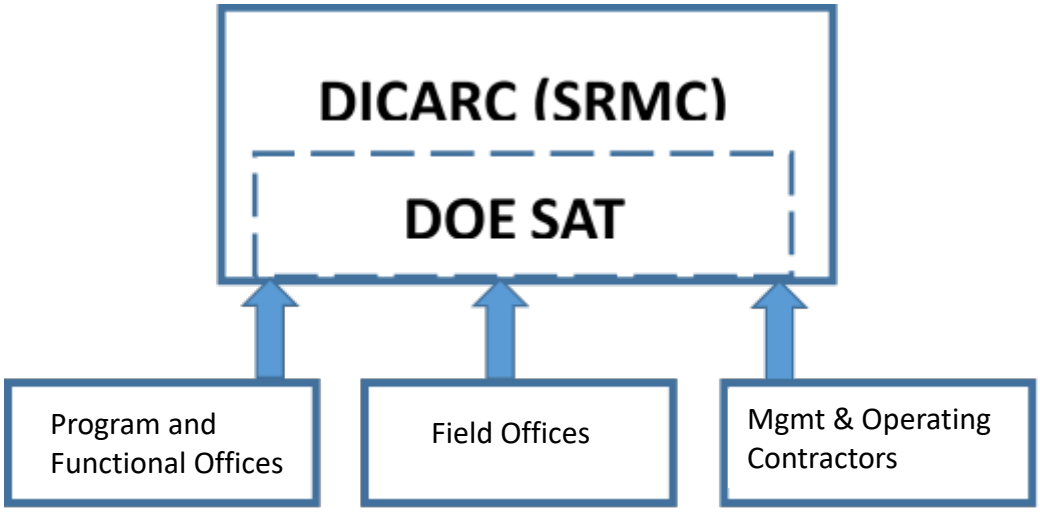
OMB Circular A-123 establishes that managers are responsible for determining the extent to which the leading practices in GAO-15-593SP, GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Framework) are relevant to the program and for tailoring the practices, as appropriate, to align with program operations. To help combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks in the Fraud Framework. Managers should adhere to these leading practices as part of the efforts to effectively design, implement, and operate an internal control system that addresses fraud risks.

In FY 2022, DOE will continue implementing a fraud risk framework over the next several years using a three-phased approach. Phase I adjusts the roles and responsibilities of the Departmental Internal Control and Assessment Review Council (DICARC) to perform additional duties as the Senior Risk Management Council (SRMC). The DICARC and SRMC will lead the effort for implementing DOE's Fraud Risk Framework based on recommendations from working groups (Figure 3). Phase II focuses on evaluating fraud risk occurrences across DOE along with preparing and providing direction on DOE's anti-fraud strategy. Phase III will continue to mature and monitor DOE's fraud risk framework. **Reporting organizations will identify and provide the name of their Risk POC to the OCFO** in accordance with

NEW in FY 2022

Table 2 *DOE Internal Controls and Risk Profile Important FY 2022 Dates*. For more details, refer to the Risk Profile Guidance (Appendix A) and Fraud Risk Management Appendix (Appendix E).

Figure 3 DICARC and SRMC Organization and Reporting Structure; SAT stands for Senior Assessment Team



E. Shifting From Low-Value to High-Value Work

DOE continues to streamline operations and incorporate flexibility for the components, complementing broader Government-wide efforts to shift resources to high-value work. Consistent with this effort, the Department will continue convening the Internal Controls Evaluation Approach Working Group to evaluate alternative control test cycle approaches. Four labs are piloting alternative control test cycle approaches – including both analytical and business process approaches – as part of the DOE Financial Management Assessment.

To continue streamlining efforts in FY 2022, select reporting organizations **will not be required to** evaluate the environmental liabilities focus area risks. The environmental liabilities focus area risks (CR6101 – CR6117) will only be required for the Office of the Assistant Secretary for Environmental Management (EM) direct reporting organizations and other reporting organizations that have a combined risk rating of moderate or high for specific risks. POC's should refer to Table 6 in Section C, Focus Area Guidance for a complete listing of reporting organizations exempt from the environmental liabilities focus areas in FY 2022.

NEW in FY 2022

Other streamlined efforts for FY 2022 will allow Under Secretaries, Headquarters Offices, and Power Marketing Administrations to submit Risk Profiles **only if there are substantive changes to risks**, with consideration of risks reported by Field Offices, Site Offices, M&O and non-M&O Contractors. If Under Secretaries, Headquarters Offices, and Power Marketing Administrations do not have substantive changes to their FY 2022 Risk Profile, **the organization's management will provide a signed memorandum** indicating there were no changes in the previous year's Risk Profile. For more details, refer to the Risk Profile Guidance (Appendix A).

F. Key Internal Control and Risk Profile Requirements

This guidance provides the FY 2022 Internal Control and Risk Profile requirements for:

- Risk Profiles (Excel Workbook);
- Financial Management Assessment Evaluations (FMA Module);
- Entity Assessment Evaluations (EA Module);
- Financial Management Systems Evaluations (FMS Tab within the EA Module);
- Interim Internal Controls Status (IICS Module); and,
- Assurance Memoranda.

Table 1 provides the DOE Internal Control and Risk Profile requirements for each entity. While DOE does not require every organization to provide Internal Control and Risk Profile deliverables, organizations **should check** with respective Headquarter Offices to determine if a deliverable is needed by the cognizant organization. A brief synopsis for organizations at each level within a reporting hierarchy are:

- Departmental Elements (Headquarters and Field Offices) are responsible for considering internal control evaluation results of Major/ Integrated Contractors, **including both Management and Operating (M&O) and integrated non-M&O Contractors**;[2]
- Small Departmental Elements are not required to perform FMA evaluations. These Elements must complete the five peripheral entity objectives in the EA Module. (Small Departmental Elements are identified in Table 1);
- Site Offices[3] are not required to provide an EA deliverable to the OCFO and should check with the cognizant Field and Headquarters Offices to determine if an EA deliverable is required to either cognizant organization; and,
- Major/ Integrated Contractors, **including both M&O and integrated non-M&O Contractors**, are required to provide a Risk Profile to the cognizant Field Office and are not required to provide the Risk Profile to the OCFO.

[2] Major/ Integrated Contractors are DOE contractors with responsibility for the management and/or operation of a Department-owned or leased facility.

[3] The site offices are Kansas City, Livermore, Los Alamos, Nevada, NNSA Production, Sandia, Ames, Argonne, Brookhaven, Fermi, Bay Area, Princeton, Oak Ridge, Pacific Northwest, and Thomas Jefferson.

Table 1 Listing of Required Internal Control and Risk Profile Evaluations due to OCFO by Organization

Departmental Elements & Reporting Organizations		FMA Evaluation	Entity Evaluation	FMS	Risk Profile	Interim Internal Control Status	Assurance Memorandum
Under Secretary Offices	Office of the Under Secretary (S3)				✓		✓
	Office of the Under Secretary for Science and Energy (S4)				✓		✓
	Office of the Under Secretary for Nuclear Security and National Nuclear Security Administration (S5)				✓		✓
Independent Agency	Federal Energy Regulatory Commission						✓
Headquarters Offices	Advanced Research Projects Agency-Energy	✓	✓	✓	✓	✓	✓
	Office of Clean Energy Demonstrations *	✓	✓	✓	✓	✓	✓
	Office of the Chief Financial Officer	✓	✓	✓	✓	✓	✓
	Office of the Chief Information Officer	✓	✓	✓	✓	✓	✓
	Cybersecurity, Energy Security & Emergency Response	✓	✓	✓	✓	✓	✓
	Office of Electricity	✓	✓	✓	✓	✓	✓
	Energy Efficiency and Renewable Energy	✓	✓	✓	✓	✓	✓
	Environment, Health,Safety and Security	✓	✓	✓	✓	✓	✓
	Environmental Management	✓	✓	✓	✓	✓	✓
	Fossil Energy	✓	✓	✓	✓	✓	✓
	Human Capital Officer	✓	✓	✓	✓	✓	✓
	Inspector General		✓			✓	✓
	Legacy Management	✓	✓	✓	✓	✓	✓
	Loan Programs Office	✓	✓	✓	✓	✓	✓
	Management	✓	✓	✓	✓	✓	✓
	National Nuclear Security Administration	✓	✓	✓	✓	✓	✓
	Nuclear Energy	✓	✓	✓	✓	✓	✓
	Project Management Oversight and Assessment	✓	✓	✓	✓	✓	✓
	Science	✓	✓	✓	✓	✓	✓
Small Headquarters Offices	Arctic Energy		✓		✓	✓	✓
	Artificial Intelligence & Technology		✓		✓	✓	✓
	Congressional and Intergovernmental Affairs		✓		✓	✓	✓
	Economic Impact and Diversity		✓		✓	✓	✓
	Energy Information Administration		✓		✓	✓	✓
	Office of Policy		✓		✓	✓	✓
	Enterprise Assessments		✓		✓	✓	✓
	General Counsel		✓		✓	✓	✓
	Hearing and Appeals		✓		✓	✓	✓
	Indian Energy Policy & Programs		✓		✓	✓	✓
	Intelligence and Counterintelligence		✓		✓	✓	✓
	International Affairs		✓		✓	✓	✓
	Public Affairs		✓		✓	✓	✓
	Small and Disadvantaged Business Utilization		✓		✓	✓	✓
	Technology Transitions		✓		✓	✓	✓
Power Marketing Administrations	Bonneville Power Administration	✓	✓	✓	✓	✓	✓
	Southeastern Power Administration	✓	✓	✓	✓	✓	✓
	Southwestern Power Administration	✓	✓	✓	✓	✓	✓
	Western Area Power Administration	✓	✓	✓	✓	✓	✓
Field/Operation Offices	EM Consolidated Business Center	✓	✓	✓		✓	✓
	Golden Field Office	✓	✓	✓		✓	✓
	Idaho Operations Office	✓	✓	✓		✓	✓
	National Energy Technology Laboratory	✓	✓	✓		✓	✓
	NNSA Albuquerque Complex	✓	✓	✓		✓	✓
	Naval Reactors Laboratory Field Office	✓	✓	✓		✓	✓
	Oak Ridge Environmental Management	✓	✓	✓		✓	✓
	Richland Operations Office	✓	✓	✓		✓	✓
	Savannah River Operations Office	✓	✓	✓		✓	✓
	Science Consolidated Service Center	✓	✓	✓		✓	✓
	Strategic Petroleum Reserve Project Management Office	✓	✓	✓		✓	✓
Major/ Integrated Contractors	Kansas City National Security	✓	✓	✓		✓	
	Lawrence Livermore National Laboratory	✓	✓	✓		✓	
	Los Alamos National Laboratory	✓	✓	✓		✓	
	Nevada National Security Site	✓	✓	✓		✓	
	Pantex Plant/ Y-12 National Security Complex	✓	✓	✓		✓	
	Sandia National Laboratory	✓	✓	✓		✓	
	Naval Nuclear Laboratory	✓	✓	✓		✓	
	Ames Laboratory	✓	✓	✓		✓	
	Argonne National Laboratory	✓	✓	✓		✓	
	Brookhaven National Laboratory	✓	✓	✓		✓	
	Fermi National Accelerator Lab	✓	✓	✓		✓	
	Lawrence Berkeley National Laboratory	✓	✓	✓		✓	
	Princeton Plasma Physics Laboratory	✓	✓	✓		✓	
	Oak Ridge National Laboratory	✓	✓	✓		✓	
	Oak Ridge Institute for Science & Education	✓	✓	✓		✓	
	Pacific Northwest National Laboratory	✓	✓	✓		✓	
	Thomas Jefferson National Accelerator Facility	✓	✓	✓		✓	
	SLAC National Accelerator Laboratory	✓	✓	✓		✓	
	National Renewable Energy Laboratory	✓	✓	✓		✓	
	Strategic Petroleum Reserve	✓	✓	✓		✓	
	Idaho National Laboratory	✓	✓	✓		✓	
	Waste Isolation Pilot Plant	✓	✓	✓		✓	
	East Tennessee Technology Park	✓	✓	✓		✓	
	Savannah River Site	✓	✓	✓		✓	

* This office will be established in FY 2022.

G. Important Dates and Transmittal Methods

Table 2 DOE Internal Controls and Risk Profile Important FY 2022 Dates

Key Dates	Deliverables
December 2	AMERICA open for documenting FY 2022 internal control testing and evaluation results.
February 3	Headquarters Offices and Power Marketing Administrations (PMA) upload Risk Profile excel and signed PDF versions, updated and revised only **if there are substantive changes to risks**, with consideration of reporting from Field Offices, Site Offices, M&O and non-M&O Contractors as applicable, **or a signed memorandum from the organization's management indicating there are no changes from the FY 2021 Risk Profile** to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov. Reporting organizations should check with their cognizant organization to determine substantive changes for Risk Profiles and follow cognizant organizations subsequent timelines to assure Risk Profiles are provided to DOE on time.
March 3	Under Secretaries provide Risk Profile excel and signed PDF versions,updated and revised only **if there are substantive changes to risks or a signed memorandum indicating there are no changes from the FY 2021 Risk Profile**, to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov based on the input of the reporting offices.
March 17	Reporting organizations (M&O Contractors, Site Offices, Field Offices, & HQ Offices) provide Interim Internal Control Status using the AMERICA Application. Reporting organizations should follow subsequent timelines published by cognizant organizations to assure IICS Modules are provided to DOE on time.
	Reporting organizations provide Risk POC names to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.
April 6	OCFO publishes the FY 2022 Assurance Memoranda Template to reporting organizations.
April 14	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review and the FY 2024 Budget Formulation process.
May 26	OCFO provides the lead responsible offices with Management Priorities in required templates for FY 2022 update. **Note:** Applicable to Management Priority Owners Only.
June 23	Lead responsible offices provide OCFO with mid-year updates on Management Priorities using provided templates based on FY 2022 enterprise activities performed and planned. **Note:** Applicable to Management Priority Owners Only.
July 7	M&O Contractors, PMAs, and Field Offices provide FMA Module and EA Module using the AMERICA Application. Reporting organizations should follow subsequent timelines published by cognizant organizations to assure FMA and EA Modules are provided to DOE on time.
July 21	Headquarters Offices provide FMA Module and EA Module using the AMERICA Application.
August 4	PMAs and Field Offices provide draft Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov, considering and incorporating Site Offices and M&O Contractors.
August 18	Headquarters Offices provide draft Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.
August 22	OCFO provides eDOCS information to Headquarters Offices.
August 25	PMAs and Field Offices provide signed Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov.
August 31	AMERICA close-out performed for FY 2022.
September 8	Headquarters Offices provide signed Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov and eDOCs.
	Lead responsible offices provide OCFO with Management Priorities year-end updates. **Note:** Applicable to Management Priority Owners Only.
September 22	Under Secretaries provide signed Assurance Memoranda to the Internal Controls and Fraud Risk Management Division's shared mailbox at cfo-icfrmd@hq.doe.gov and eDOCs.
October 3	Organizations that resolve or identify a significant deficiency or material weakness, after June 30, 2022, and no later than September 30, 2022 that is not included in a signed Assurance Memoranda, must notify the OCFO and update the Assurance Memoranda.
October - TBD	OCFO will provide Management Priorities updates to the DICARC in early October for review. **Note:** Applicable to Management Priority Owners; Per DICARC recommendation, the final Management Priorities are incorporated into the AFR and proceed through Exec Sec Concurrence Process.

Table 2: *DOE Internal Controls and Risk Profile Important Dates* provides Internal Control Evaluation deadlines. Organizations must provide the Internal Control deliverables on time. If there is an emerging issue preventing an organization from providing a deliverable on time, the organization will provide the specific reason(s) for the delay to include any potential significant deficiency or material weakness to the assigned OCFO analyst for the organization. Management quality assurance reviews will take place at every level prior to providing Internal Control deliverables and Risk Profiles.

Entities (Federal and contracting organizations) should provide the Internal Control Deliverables that are listed in Table 2 *DOE Internal Controls and Risk Profile Important FY 2022 Dates* in accordance with Table 3 *Reporting Documentation Transmittal Methods*.

Table 3 Reporting Documentation Transmittal Methods

Deliverable	Format	Method	Recipient(s)
Risk Profile	Excel File & Signed PDF -or- Signed memo if there are no substantive changes	E-mail to ICFRMD's shared mailbox at cfo-icfrmd@hq.doe.gov	Major/ Integrated Contractors to: Field Office Field Office to: Lead Program Secretarial Office Headquarters to: Appropriate Under Secretary and OCFO Under Secretary to: OCFO
EA, FMA, FMS Evaluations and IICS	AMERICA	A-123 Application	Major/ Integrated Contractors to: Field Office Field Office to: Lead Program Secretarial Office Headquarters to: OCFO
Assurance Memorandum (Including Corrective Action Plan Summary)	Signed PDF	E-mail to ICFRMD's shared mailbox at cfo-icfrmd@hq.doe.gov	Field Office and PMA Assurance Memorandum addressed To: Lead Program Secretarial Office with copies to the Cognizant Secretarial Office(s).
	Signed PDF	E-mail to ICFRMD's shared mailbox at cfo-icfrmd@hq.doe.gov and upload to eDOCS	Headquarters Assurance Memorandum addressed To: The Secretary Through: Appropriate Under Secretary Under Secretary to: The Secretary

II. Documentation Requirements

All organizations are required to maintain written policies and procedures for implementing the internal controls evaluation process described in this guidance. 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. Management uses professional judgment in determining the extent of the documentation that is developed. Documentation is required to demonstrate the design, implementation, and operating effectiveness of an entity's internal control system. These policies and procedures must include a quality assurance (QA) program conducted by Departmental Elements on inputs from the reporting organizations to provide quality and accuracy. Documentation supporting internal control evaluations and results will remain on file with the organization and upon request, provided to the OCFO, respective Field or Headquarters Office, senior managers, or auditors.

Examples include:

- Internal and external assessments;
- Results of external audits, including financial statement audits and findings along with appropriate work papers;
- Internal audits to include working papers and/ or management reviews;
- Process flows and descriptions;
- Biennial pricing reviews;
- Test documentation more detailed than what is included in the FMA and EA Modules; and,
- Evidence collected during testing.

Organizations must have appropriate and verified procedures to test the effectiveness of the controls using re-performance, observation, inquiry, and inspection. These key procedures as referenced by A-123, Appendix A, *Implementation Guide,* should be cited in the FMA and EA Modules where applicable:

- **Re-performance** is an objective execution of procedures or controls performed as part of a test of the effectiveness of the entity's internal control (e.g., recalculating an estimate or re-performing a reconciliation).
- **Observation** is the viewing of a specific business process in action, and in particular the control activities associated with the process, to test the effectiveness of an internal control (e.g., observing a physical inventory or watching a reconciliation occur).
- **Inquiry** is a detailed discussion with knowledgeable personnel to determine if controls are in place and functioning (e.g., do you reconcile your activity or do you review a certain report each month).
- **Inspection/ Examination** is scrutiny of specific business processes and documents through consideration and analysis for approval authorities that indicate the effectiveness of controls (e.g., looking for signatures of a reviewing official or reviewing past reconciliations).

Controls testing must be sufficient and well documented. Examples of **insufficient test** result descriptions or narratives that **should be avoided** include:

- **Walkthroughs;**
- **Limited Discussions;**
- **Reviews of organization charts**; and,
- **Talking to a limited number of people, performing inadequate testing**.

These test procedures result descriptions are not adequate and detailed enough to reveal the effectiveness or weakness of internal controls. Testing procedures and results should be adequately written and have enough detail that will provide an understanding of the test and results.

When determining test procedures, complexity and frequency of controls including whether the controls are automated or manual are key considerations. For example, complex controls that are manual and used on a regular basis should be tested more in-depth than less complex controls that are automated and used on a periodic basis. Sampling is used to select the appropriate number of transactions to test for each control. Sampling methods for consideration are:

- **Random** – A method of selecting a sample whereby each item in the population[4] of transactions is given an equal chance of selection regardless of the population size. Typically, sampling software or a random number generator is used to identify the items comprising the sample. Random selection is generally considered the most likely method to result in a sample that is representative of the population.
- **Judgmental** – A method of sample selection whereby the sampled items are selected based on a deliberate choice based on the profile of the population of transactions (i.e., there may be unusual patterns or higher-risk items that exist). This method provides validation that high-risk or other items of interest are included in the selected sample and reviewed as part of testing the control.
- **Systematic** – A method of sample selection whereby a uniform interval (i.e., every *n*th item) is selected throughout the population. The appropriate interval is determined by dividing the number of items in the population by the sample size.

Sample sizes for consideration are listed in Table 4 *Suggested Sample Sizes*.

[4] A population includes every transaction that occurred within a given time period.

Table 4 Suggested Sample Sizes

Minimum Sample Size for Testing Manual Controls		
Assumed Population of Control Occurrences	Approximate Frequency of Control	Sample Size
1 – 3	Annual / Semi-Annual / Bi-Annual	1
4 – 11	Quarterly	2
12 – 23	Monthly	2 – 4
24 – 52	Weekly / Bi-Weekly	3 – 8
53 – 250	Daily	22
Over 250	Multiple Times Per Day	22
Note: In certain instances, sample sizes may need to be adjusted. There are times when the sample sizes should be increased and determined based on the population of occurrences instead of relying on the control frequency to provide reasonable assurance over the operating effectiveness of the control.		
Minimum Sample Size for Testing Automated Controls		
Description		Sample Size
For an automated control, the number of items required to be tested is minimal.		1

III. Risk Profile

OMB Circular A-123 requires each agency to prepare an annual prioritized and ranked Risk Profile, for use as part of the annual Strategic Review and proposed future years budgets. In FY 2022, DOE will continue synchronizing risk profile and budget formulation processes. Risk consideration is a key element during budget formulation and is vital in an organization's planning process. As such, risk management professionals should be part of every organization's leadership efforts for planning future years budgets. At the DOE enterprise level, resource planning is an organizational effort that is guided by the OCFO. This approach provides oversight that the agency's risk posture is reflected in the Department's budget, addresses budget needs for key controls to mitigate the most important risks, and reflects the priorities and risk appetite of the Department's leadership. The Department's risk profile is used to shape discussions between DOE and OMB in supporting budget justifications. Leadership should consider risks during budget execution with discussions on funding to improve performance while responding to emerging risks.

The Risk Profile must identify the risks to achieving agency strategic objectives and the appropriate options for addressing the risks. Organizations should perform analysis on the risks in relation to the achievement of DOE Strategic Plan goals and objectives as well as internal control objectives related to operations, compliance, and reporting. The Risk Profile requires both identification and analysis of risks. Risk identification offers a structured and systematic approach to recognizing where the potential for undesired outcomes can arise. Risk analysis and evaluation considers the causes, sources, probability of risk occurring, potential outcomes, and prioritizes the results of the analysis.

Major/ Integrated Contractors, **including both M&O and integrated non-M&O Contractors**, must identify the risks and provide a Risk Profile in accordance with the guidance in Appendix A, *Risk Profile Guidance*, to the cognizant Field Office. Field Offices, taking into consideration the Major/ Integrated Contractors **including both M&O and integrated non-M&O Contractors** must identify the risks and provide a Risk Profile to the cognizant Headquarters Office in accordance with the due dates in Table 2.

Each Headquarters Office, PMA, and Under Secretary must prepare a Risk Profile identifying the top risks or a **memorandum indicating there are no significant changes** to the organization's FY 2022 Risk

NEW in FY 2022

Profile. Each lower-level organizational element will produce a Risk Profile to provide to the higher-level organization for consideration and consolidation. The Risk Profiles from each Under Secretary, and each Headquarters Office not reporting to an Under Secretary, will be consolidated into a prioritized DOE Risk Profile and used during the Department's FY 2024 budget formulation process and discussed as part of the annual Strategic Review with OMB in May.

Risk Profiles are updated and prepared on an annual basis. Appendix A, *Risk Profile Guidance*, provides the Risk Profile template and detailed instructions for developing the Risk Profile. The Risk Profile deliverable must be reviewed and approved by the reporting organization's management. Approval of an entity's Risk Profile should be indicated by a signature of the Head of the organization on the Risk Profile using the provided template. **Organizations will provide both the completed Risk Profile in Excel as well as PDF versions with signature. Reporting organizations will also identify and provide the name of their Risk POC to the OCFO** in accordance with Table 2 *DOE Internal Controls and Risk Profile Important FY 2022 Dates*. For more details, refer to the Risk Profile Guidance (Appendix A) and Fraud Risk Management Appendix (Appendix E).

NEW in FY 2022

Risk Profile, FMA and EA Module Reporting

To the extent internal controls are necessary to manage or mitigate risks identified in Risk Profiles, the controls must be established and evaluated as part of FY 2022 internal control testing and attested in the FY 2022 assurance statement. If a control existed in last year's Risk Profile deliverable, the Departmental Element may apply the focus area exemption to the existing control and treat it similar to the focus area exemption.

Reporting organizations should indicate where each reported risk is evaluated using the Current Evaluation Category column (Column M) in the Risk Profile template. Risk Profile financial risks must be documented and evaluated, including the establishment and testing of controls when applicable, in the **FMA Module** in AMERICA. Risk Profile non-financial risks are evaluated, including the establishment and testing of controls when applicable, as part of the EA process and reported in the appropriate section of the **EA module** in AMERICA (e.g., internal control risks assessed and reported in the **Internal Control Evaluation** tab; entity objective risks assessed and reported in the **Entity Objective Evaluation** tab). Entities should provide supplementary detail on where a risk is being evaluated within the EA or FMA Modules using the Current Evaluation Details column (Column N) in the Risk Profile template.

Fraud Considerations in the Risk Profile

In FY 2022, reporting organizations must continue to identify the top financial and non-financial fraud risks in the Risk Profile. These ongoing fraud risk statements must be included in each entity's Risk Profile deliverable along with other identified risks. **Organizations must identify each risk with financial or nonfinancial fraud impact by completing the *Fraud Impact* column (Column E) in the Risk Profile template.** Organizations will select from a drop-down menu identifying whether a risk is a **financial fraud, non-financial fraud, top financial fraud, or top non-financial fraud**. If a risk does not have a financial or nonfinancial fraud implication, organizations will select *N/A*, from the drop-down menu selection. Refer to the Fraud Risk Management Appendix (Appendix E) for more details.

IV. Financial Management Assessment (FMA) Evaluation

A. FMA Supporting Documentation

The FMA Module is the central location for documenting the evaluation of the relevant financial business processes, sub-processes, and risks facing each reporting entity, as well as the key controls and testing information for each process that are relied upon to mitigate the risks. Reporting entities should reference within the **Documentation Location** section of the **Assessment** tab in AMERICA the physical or

electronic location of the documents that support the identification of the controls and verification of the applicability of the business process, sub-process, corporate and local risks to the entity.

This year reporting organizations which complete the FMA Module will upload supporting documentation for corporate risk CR1405, which is associated with the ***Cost Monitoring*** **sub-process** into AMERICA. **Reporting organizations will provide documentation that demonstrates sufficient testing was performed on CR1405.** With the exception of Pilot Program labs, **there are no exemptions for testing the controls mitigating CR1405**.

Such documentation may include business process narratives or flowcharts, risk analyses, test plans, and other applicable documents that support the entity's assessment and evaluation. Entities are not expected to provide evidence documentation for individual sample items tested. Rather, entities should upload supporting documentation sufficient to demonstrate the scope and type of testing performed and notable findings or exceptions. Organizations that have assessed risks as **Not Relevant** do not need to provide further documentation.

B. Requirements for FY 2022

In FY 2022, entities must perform, at a minimum, these actions:

1. *Re-assess risks and adjust Risk Exposure Ratings in the FMA Module* - Each entity should consider whether risk factors, such as organizational restructurings, system changes or upgrades, process changes, audit findings, external events, or other changes that occurred over the past year affect the risk assessment ratings. If so, entities can adjust their risk exposure rating or mark the appropriate area in the **Assessment** tab in the **Other Factors to Consider** section, and the *In Scope Now* column may change to **yes** due to the updated risk assessment. If the controls in the *In Scope Now* column change to **yes** due to a change in the risk assessment, entities should include the testing for those controls related to the respective risks into the testing schedule. It is important to note that the annual risk re-evaluation could result in a determination that certain risk exposure ratings may be reduced because of program changes, including a decreased amount of transactions or lower dollar amounts.
2. *Consider applicabiilty of corporate risk statements that uses Federal language and/ or identifies DOE specific systems* – **Major/ Integrated Contractors should reconsider corporate risk statements that have previously been marked as not relevant due to the language or naming of a system**. When reassessing the corporate risk statements, reporting organizations should determine whether the corporate risk has been previously identified as not relevant due to the language that is used or the naming of a system. For example, a corporate risk statement may identify a risk using a term such as "Contracting Officer Representative". A Major/ Integrated Contractor may use the term "Technical Project Officer". Another example may be the naming of a system such as the "Strategic Integrated Procurement Enterprise System (STRIPES)", which is the Department's procurement system for contract requisitions. A Major/ Integrated Contractor's procurement system has a different name. Regardless of the term or name that is used, the intent of the risk remains the same. In each situation, Major/ Integrated Contractors should:
    a. Identify the corporate risks to remain not relevant and prepare local risks using the language that is specific to the reporting organization, then perform risk assessments on the local risks; or,
    b. Identify the corporate risks as relevant and perform risk assessments on the corporate risks with an understanding the language may be different. However, the intent of the risk is the same.

3. *Corporate risk update* – **Each entity should reassess the applicability of corporate risks (CR) 2109, 2112, 2116, and 2120 in the *Acquisition Management* business process and CR6408 and CR6409 in the *Contractor Oversight* business process.** These risk statements have been updated to include risks that are associated with having sub-contractors. In addition, CR6408 and CR6411 were combined into one risk statement. **In FY 2022, reporting organizations should reassign the controls mitigating CR6411 to mitigate CR6408.** In FY 2023, CR 6411 will be deleted from the AMERICA FMA Module. **Reporting organizations should also reassess the applicability of CR2405 in the Travel Administration business process**.

NEW in FY 2022

4. *Consider if multiple controls are needed for risks rated as high* - For entities that have risks which are rated high **and only** have one control to mitigate the risk from occurring, the entity should carefully re-evaluate the risk to determine if the one control is sufficient to mitigate the risk(s) from occurring or if more controls should be developed to mitigate high rated risk(s) from occurring.
5. *Evaluate risks and test controls in cycle for the processes/ sub-processes identified in Table 5 Sub-Processes for FMA Review and Testing*. The processes/ sub-processes listed in Table 5 are the **minimum required business sub-processes** that will continue to be included in each reporting organization's FMA Module in the **Assessment** tab. If the corporate risks for these required business sub-processes do not apply, reporting organizations must provide a brief, but sufficient rationale that explains the reason for the *Not Relevant* risk rating in the **Assessment** tab. Rationales that state a risk is "DOE's responsibility", "HQ responsibility", or it is "not the organization's responsibility" are not acceptable rationales and will require updating in FY 2022. Before concluding a corporate risk is not relevant to an entity, the organization should consider whether the risk is applicable at the local or organizational level. If needed, create a local risk for the organization and complete the evaluation and testing of controls associated with the local risk. Organizations are responsible for the risks, and the controls to manage these risks, related to the activities within these required business sub-processes.

Table 5 Sub-Processes for FMA Review and Testing

Process	Sub-process	Applicability		
		HQ	Field	IC
Funds Management	Budget Formulation	✓	✓	
	Budget Generation	✓	✓	✓ (CR1204)
	Funds Distribution	✓	✓	
	Budget Execution	✓	✓	✓
Acquisition Management	Requisitioning	✓	✓	✓
	Receipt of Goods and Services	✓	✓	✓
	Contract Solicitation, Award and Adjustment	✓	✓	✓
	Contract Closeout	✓	✓	✓
	Purchase Card Program Management	✓	✓	✓
Payables Management	Invoice Approval	✓	✓	✓
Travel Administration	Travel Authorization	✓	✓	✓
	Voucher Processing	✓	✓	✓
	Travel Closeout	✓	✓	✓
	Travel Card Program Management	✓	✓	✓
Payroll Administration	Time and Attendance Processing	✓	✓	✓
	Leave Processing	✓	✓	✓

6. *Fraud and Improper Payments Consideration* - Effective fraud risk management determines whether taxpayer dollars and government services serve the intended purposes. Entities are

NEW in FY 2022

responsible for reviewing the controls to determine if the controls are mitigating a fraud and/ or improper payments risk. Controls that mitigate a fraud and/ or improper payments risk should be designated as such in the **Assessment** tab by **selecting the appropriate designation from the *Fraud/ Improper Payments* dropdown option for controls**. Entities should also continue to improve data integrity by removing all Fraud/ Improper Payment selections from the *Control Category* field. If a control is designed to mitigate a fraud and/ or improper payment risk and the control fails testing, or fails related to the detection of potential fraud, the organization will notify their assigned OCFO Analyst on the control failure and the remediation plan to confirm a control is designed and operating effectively to mitigate the risk.

In FY 2022, the *Fraud/Improper Payments/Both Fraud & IP* dropdown options have been removed from the *Type of Risk* field. **Local risks** which were reported as *Fraud, Improper Payments,* or *Both Fraud & IP* in the *Type of Risk* field at the end of FY 2021 have been changed to *Business*. Organizations affected by this change will need to review and update these **local risks,** if needed. Affected organizations will be notified in December of the local risks affected by this change and **must** identify in the FMA Module **local risks** that are subject to fraud, improper payment, or both by **selecting from the dropdown menu of the *Fraud/Improper Payments* field**.

7. *New Risks and Controls Added to the FMA Module and Control Set Execution* – AMERICA will provide a one year grace period for reporting organizations to test the controls that are mitigating new risks that are added to the FMA module. **However, if there is sufficient data to conduct control testing, reporting organizations must test the controls that are mitigating risks with a high exposure risk rating in the same year the risks are added to the FMA Module or if the added risk is a corporate risk that has been identified as a focus area regardless of the risk rating.** If there is no sufficient data to conduct the controls testing in the same year when a reporting organization adds a risk with a high exposure risk rating or is a focus area risk, then the reporting organization will test the controls the following year. Instances when a reporting organization does not have sufficient data to test the controls for a newly added risk, **there will not be a *Control Execution* rating**. As a result, the *Control Set Execution* rating should remain blank. Some scenarios may exist that will allow reporting organizations to receive a two year grace period for a newly added risk and control. **However, reporting organizations are required to test newly added risks and controls within one year of the risk being added to AMERICA.** Also, the reasons for controls that are due or overdue for testing, but are not tested, should be entered into *Control User Field 1.* For more details, refer to the AMERICA FMA, EA, and IICS Module User Guide (Appendix C).

8. *Complete Current Year Test Requirements* – Using the ***Assessment Tab*** of the FMA Module in AMERICA, entities must test applicable controls identified as **yes** or **overdue** in the *In Scope At Rollover* column and **yes** or **overdue** in the *In Scope Now* column no later than June 30. Entities should remain cognizant that the *In Scope Now* is a dynamic column that will update when **risk assessments** and control tests are updated. When the controls in the *In Scope Now* column change to **yes** due to an updated risk assessment, entities should factor the testing for those controls into the testing schedule.
9. *Complete Focus Area Testing and Actions* – Organizations must complete testing and other required actions to address the FY 2022 focus area risks and document the actions taken in the **Assessment** tab of the FMA Module. **Controls testing is required by reporting organizations along with providing documentation that demonstrates sufficient testing was performed on CR1405, which focuses on the risk of costs not being maintained at an appropriate level of detail.** Supporting documentation should be uploaded to the FMA Module using the **Attachments** tab in AMERICA. **Documentation for risk statement CR1405 located within the *Cost Monitoring* sub-process is required due to concerns linked to the termination of the**

Cooperative Audit Strategy, the potential effect of contractor oversight across the Department, management concerns identified in FY 2021, and continued interest from Congress, GAO, and Office of the Inspector General (OIG). With the exception of pilot labs, there are no exemptions for testing the controls mitigating CR1405.

The environmental liabilities focus area risks (CR6101-CR6117) will only be required for the EM direct reporting organizations and reporting organizations that do not report to EM, but have a combined risk rating of moderate or high, for specific risks. Therefore, the environmental liabilities focus area risks will not be required for select organizations. Organizations piloting an alternative control test cycle approach as part of the Internal Controls Evaluation Approach Working Group are exempt from each focus area contained in Table 7 FY 2022 Focus Areas. Section C, Focus Area Guidance provides more details on focus areas and assessment requirements.

10. *Develop Corrective Action Plans As Applicable* - A Corrective Action Plan (CAP) is required for each risk with a risk occurrence rating of 3 or a control set execution rating of 3. Organizations also have the option of developing formal CAPs for control tests that **pass with some failures**. During these instances, the organization may opt to select a control set execution rating of **2 with CAP** (rather than a **2 without CAP** rating), which will automatically initiate the CAP process similar to a rating of **3** within the FMA Module. In AMERICA, risks with a risk occurrence rating of **3** or control sets identified as a **2 with CAP** or **3** rating will automatically initiate a CAP. The CAP is a detailed, step-by-step plan with associated milestones and contains the signatures of the authorized individual approving the plan and the individual confirming completion of the plan. OMB Circular A-123 emphasizes the need to identify the root cause when developing a CAP, prompt resolution, and internal control testing to validate the correction of the control deficiency. Entities must report the root cause, along with other necessary CAP information, in the *Internal Control CAPS Details* section in the **Assessment** tab of the FMA Module.

    At a minimum, a CAP will contain these key elements:
    - Issue description;
    - General Description;
    - Source/ Type;
    - CAP Title;
    - Root Cause;
    - Remediation Strategy/ Criteria for Closure (e.g., training, system, organization);
    - Remediation Actions Taken;
    - Current status and planned completion date or actual completion date; and,
    - Approving Official – The first line supervisor or higher may be considered the approving official.

    Entities are responsible for maintaining the CAPs and are not required to provide CAP documentation unless requested by the OCFO.

11. *Upload Relevant and Appropriate Supporting Documentation* – Organizations are responsible for **uploading requested documentation in AMERICA for risk statement CR1405 located within the *Cost Monitoring* sub-process**. Documentation may include business process narratives or flowcharts, risk analyses, test plans, and other applicable documents that support the entity's assessment and evaluation. Organizations will upload documentation sufficient to demonstrate the scope and type of testing performed and notable findings or exceptions. For further information, refer to Section A, FMA Supporting Documentation.

12. ***Infrastructure Investment and Jobs Act (Infrastructure Bill)*** – In FY 2022, reporting organizations and their downstream organizations that receive funding from the Infrastructure

Bill must ensure business process documentation is current and properly working controls are in place for financial assistance awards that will ensure:

a. DOE officials that are involved in the review of financial assistance applications do not have conflicts of interest;
b. Financial assistance applications are reviewed, selected, and awarded according to the planned schedule;
c. Financial assistance awards are approved by contracting officers that are certified for financial assistance;
d. Financial assistance awards are issued with sufficient funding;
e. Advance notification is provided to the House and Senate appropriations committee for financial assistance awards that are in excess of $1 million;
f. Non-competitive financial assistance awards have the appropriate level of authority and the approval is documented;
g. Monitoring of the financial assistance award is consistent with the award terms and conditions;
h. Recipients submit its single audit reporting package to the Federal Audit Clearinghouse in a timely manner;
i. Recipients are aware of required reporting;
j. Financial assistance awards are closed out properly and in a timely manner; and,
k. Performance metrics are established as part of the financial assistance or program plan, and the plans are approved prior to the transfer of funds.

C. Focus Area Guidance

Focus area risks represents areas of emphasis for the Department and are determined by senior management concerns, GAO and OIG repeat audit findings, or areas of high risks throughout the Department. Focus are risks require additional assessment by reporting organizations regardless of the risk rating or test cycle. Reporting organizations piloting an alternative control test cycle approach as part of the Internal Controls Evaluation Approach Working Group are exempt from each FY 2022 Focus Area and are identified in Pilot Programs in Table 6.

To continue streamlining efforts in FY 2022, select reporting organizations (identified in

Table 6) **will not be required to** evaluate the environmental liabilities focus area risks. The environmental liabilities focus area risks (CR6101 – CR6117) will only be required EM direct reporting organizations and reporting organizations that do not report to EM, but have a combined risk rating of moderate or high for specific risks. **Reporting organizations, except EM direct reporting organizations, that had a low combined risk rating for environmental liabilities focus area risks are fully exempt from testing the controls mitigating environmental liabilities focus area risks.** Organizations, except EM direct reporting organizations, that reported environmental liabilities focus area risks with a combination of low and moderate/ high combined risk ratings are partially exempt. **The partially exempt organizations are required in FY 2022 to address the environmental liabilities focus areas with a moderate or high combined risk rating.**

The reporting organizations exempt, or partially exempt, from testing the environmental liabilities focus area risks are identified in
Table 6**.** Organizations not listed in

Table 6 are EM direct reporting organizations, did not have any environmental liabilities risks with a low combined risk rating, or did not identify at least one of the environmental liabilities focus area risks as relevant in FY 2021 and are not responsible for addressing these risks as focus areas in FY 2022.

Table 6 Environmental Liabilities Focus Area Exemptions

Entities Fully Exempt from Testing Environmental Liabilities Focus Area Risks	Entities Partially Exempted from Testing Environmental Liabilities Focus Area Risks
Ames National Lab (AMESL)	Argonne National Lab (ANL)
Brookhaven National Lab (BNL)	Idaho National Lab (INL)
Fermi National Accelerator Lab (FNAL)	Nevada National Security Site (NNSS)
Kansas City National Security Campus (KC)	NNSA Albuquerque Complex
Idaho Operations Office (ID)	Oak Ridge National Laboratory (ORNL)
National Energy Technology Lab (NETL)	Pantex Plant & Y-12 National Security Complex (PX/Y12)
Naval Reactors Laboratory Field Office (NRLFO)	
Oak Ridge Institute for Science and Education (ORISE)	
Office of the Chief Financial Officer (CF)	
Office of Legacy Management (LM)	
Pacific Northwest National Lab (PNNL)	**Pilot Program Entities Fully Exempt from Testing Environmental Liabilities Focus Area Risks**
Princeton Plasma Physics Lab (PPPL)	SLAC National Accelerator Laboratory (SLAC)
Science Consolidated Service Center (SC-CSC)	Lawrence Livermore National Lab (LLNL)
Thomas Jefferson National Accelerator Facility (TJNAF)	Lawrence Berkley National Lab (LBNL)
Western Area Power Administration (WAPA)	Sandia National Lab (SNL)

The environmental liabilities focus areas that are exempted from testing in FY 2022 will be appropriately flagged and addressed in AMERICA by OCFO and no further action will be required by the corresponding entities.

Table 7 FY 2022 Focus Areas

FY 2022 Focus Areas
Acquisition Management
• Contract Solicitation, Award, and Adjustment-Competitive process not followed (CR2115)
• Receipt of Good and Services-Inadequate costs and price analyses (CR2116)
• Contract Closeout-Improper/untimely closeout (CR2118)
• Contract Closeout- Improper/untimely De-obligations (CR2121)
Project Cost Management
• Project Monitoring-Cost/timeline issues (CR4106)
• Project Monitoring-Improper transfer of assets (CR4110)
Cost Management
• Cost Monitoring-Costs not maintained at an appropriate level of detail (CR1405)
• Cost Monitoring-Unallowable or unreasonable costs are incurred (CR1406)
• Cost Monitoring-Improper or untimely capitalization of costs (CR1407)
• Cost Monitoring-Incurred cost overruns (CR1408)
Environmental Liabilities
• Liability Validation-Insufficient documentation (CR6101)
• Liability Validation-Subsequent events not considered (CR6102)
• EM Liability-IPABS out of date (CR6103)
• EM Liability-Unapproved baselines in IPABS (CR6104)
• Non-EM Liabilities-Improper accounting for contaminated media/oil & ground water remediation. (CR6105)
• Non-EM Liabilities-Untimely updates to Long-term stewardship (CR6106)
• Non-EM Liabilities-Improper accounting of surplus materials. (CR6107)
• Non-EM Liabilities-Improper accounting of non-EM Environmental Liabilities (CR6108)
• Policy Execution-Environmental policies and procedures not up to date (CR6109)
• Policy Execution-Environmental policies/procedures not communicated (CR6110)
• Policy Execution-Roles and responsibilities not known (CR6111)
• Policy Execution –Staff has inadequate skills/knowledge (CR6112)
• Active Facilities-Incorrect Active Facility Data Collection Systems (AFDCS) data (CR6113)
• Active Facilities-Best estimates for AFDCS not used (CR6114)
• Active Facilities-Omitted or duplicate facilities (CR6115)
• Active Facilities- Facility surveys/contamination swipes/etc. not considered (CR6116)
• Active Facilities-Leased facilities inappropriately considered (CR6117)
Contractor Oversight
• Performance- Contractor/Subcontractor progress improperly assessed (CR6404)
• Performance-Contractor/Subcontractor performance and billing not monitored (CR6405)
Improper Payments
• SPC: Payment Disbursing-Incorrect implementation of OMB requirements (CR6601)
Payroll Administration
• Time and Attendance-Unauthorized or invalid time and attendance is reported (CR5103)
• Time and Attendance-Time is not tracked and reported against an appropriate cost unit (CR5104)

The Focus Area processes and risks are identified in Table 7. For the 32 FMA Focus Area risks**,** with the notable exception of the environmental liabilities' exemptions, the controls require evaluation and testing by each reporting entity in FY 2022 unless the organization has tested the controls within the **past 15-month period**, which is July 1, 2020 – September 30, 2021. For risks that have a low or moderate combined risk rating, and the entity has tested the controls within the last 15-month period, then the focus area assessment may verify that:

1. The business process has not changed, and
2. There were no audit findings and there were no deficiencies found during the controls testing.

If these requirements are met, the organization will check the focus area exemption box and enter this verbiage into the Action Taken dialogue box in the **Focus Area** tab: "***The controls have been tested within the past 15-month period, the business process has remained the same, and zero deficiencies were noted during testing. The organization performed the assessment on MM/DD/YYYY***." If the organization has not tested the controls within the last 15-month period, then the controls mitigating the focus areas risk will require testing **regardless of the risk rating or test cycle**.

D. FMA IT Corporate Controls

For FY 2022, the Information Technology (IT) controls will remain corporate controls within the FMA Module. The IT corporate controls are security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. IT corporate controls are updated each year to keep DOE compliant with the National Institute of Standards and Technology (NIST) SP 800-53, Revision 5 cyber and privacy requirements. Table 8 identifies the latest updates to the IT corporate controls for FY 2022.

Table 8 FY 2022 IT Corporate Controls Update

CNO	RNO	Control Description	Status
CC0242 (Deleted)	CR6509	SA-12 Supply Chain Protection	The corporate control was deleted in AMERICA and is no longer a separate control. Per NIST SP 800-53, Rev 5, (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) this baseline control has moved to the Supply Chain Risk Management (SR) Family. The four new controls displayed below replaced CC0242.
Per NIST SP 800-53, Rev 5, CC0273 – CC0276 were added in FY 2021. (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)			

Corporate Control (CC) 0242 was deleted from the FMA Module within AMERICA. Reporting organizations that did not replace CC0242 with CC0273, CC0274, CC0275, or CC0276 in FY 2021 will be required to identify and replace CC0242 in FY 2022. If CC0242 was tested in FY 2021 or is due for testing in FY 2022, then reporting organizations are required to test the newly identified replacement control in FY 2022. Affected organizations will be notified in December.

Entities with IT systems will **select the IT sub-processes** applicable to the site, evaluate the appropriate risks, and test controls. Risks rated as **not relevant** must include an accompanying explanation. Controls mitigating the selected risks will receive testing based on the risk rating coupled with the last control test date.

V. Entity Assessment Evaluation

A. Purpose

The purpose of the Entity Assessment (EA) Evaluation is to conduct structured self-evaluations to provide reasonable assurance that internal control systems are designed and implemented as well as operating effectively. Self-structured evaluations are performed to verify that risks are mitigated and to validate that mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulations.

There are two major goals in the EA Evaluation. The first is to assess the status of an entity's internal controls. The second is to evaluate each entity's objectives (functions, missions, activities) to determine if there are issues that require attention.

B. Internal Controls Evaluation

Section II of FMFIA requires an assessment of non-financial controls to verify the effectiveness and efficiency and compliance with laws and regulations. The Green Book has five components, 17 principles and 48 attributes to guide the EA Evaluation. As with last year, each reporting organization, as shown in Table 1, is required to perform an EA evaluation of the internal controls for entity functions (administrative, operational, and programmatic).

Organizations will report the results of the evaluations in the EA Module. The **Internal Control Evaluation** tab requires an evaluation of each entity's internal controls against the Green Book's five components and 17 principles. Issues found in the evaluation must be identified and rated as to the seriousness on a scale of 1 (least serious) to 3 (most serious). Issues rated **2** or **3** require a CAP, and these issues automatically populate in the **Action Tracking** tab and require further information. There is also an **IC Summary Evaluation** tab which summarizes the results of the evaluation reported in the **Internal Control Evaluation** tab. As a result, there are **only two lines on the IC Summary Evaluation tab that require user input:**

- **Are all components operating together in an integrated manner?**
- **Is the overall system of internal control effective?**

C. Entity Objectives Evaluation

The second aspect of the EA Evaluation is an evaluation of each entity objective (e.g., functions, missions) to determine if there are issues that need to be addressed to help meet the objective. There are nine entity objective categories identified in the EA Module that need evaluation by reporting organizations:

- Fraud Prevention
- Establishment of Entity-Wide Objectives (Entity Missions)
- Infrastructure Status
- Systems & IT Posture
- Safety & Health (S&H) Posture
- Security Posture
- Continuity of Operations
- Contractor/ Subcontractor Oversight
- Environmental

Small Headquarters Offices in Table 1, *Listing of Required Internal Control and Risk Profile Evaluations due to OCFO by Organization* must complete five accompanying entity objectives:

- Funds Management
- Acquisition Management
- Payables Management
- Travel Administration
- Payroll Administration

The results of the evaluation for the nine (or 14 for the Departmental Elements indicated in Table 1) entity objective categories are reported in the **Entity Objectives Evaluation** tab. As with the evaluation of internal controls, issues identified in the entity objectives evaluation will be reported and given a rating of 1 (least serious) - 3 (most serious) depending on the seriousness of the issue. Issues identified with a rating of **2** or **3** require a CAP.

D. Fraud Considerations in the Entity Review

The GAO *Standards for Internal Control* (Green Book) principle 8 addresses fraud as an aspect of internal control. Specifically, entities must consider the potential for fraud when identifying, analyzing, and responding to risks. Reporting organizations must also evaluate the Fraud Prevention entity objective. For more information on fraud related internal controls requirements in the EA Module, refer to Appendix E.

VI. Financial Management Systems (FMS) Evaluation

OMB Circular A-123, Appendix D, defines a financial management system as including an agency's overall financial operation, **reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions**. Financial management systems include hardware, applications and system software, personnel, procedures, data, and reporting functions. The financial management system may fully integrate with other management information systems (i.e., mixed systems) where transactions automatically flow into an accounting general ledger. The financial management system could also include manual processes to post transactions from other management systems into the accounting general ledger. OMB Circular A-123, Appendix D provides a risk-based evaluation model that leverages the results of existing audits, evaluations, and reviews which auditors, agency management, and others already perform. This evaluation model also includes:

1. Financial management goals common to all Federal agencies;
2. Compliance indicators associated with each financial management goal; and,
3. Recommended risk or performance level that entities should consider when assessing whether financial management goals have been met.

Organizations identified in Table 1 as responsible for an FMS Evaluation must evaluate the design and efficacy of system controls to determine to what degree their system meets the eight financial management goals. As indicated in Table 1, most entities are required to complete an FMS Evaluation. The FMS Evaluation is a risk assessment that should be conducted toward the end of the assessment year and it relies on the results of internal control evaluations and other assessment activities already performed. Organizations may use A-123 Internal Review evaluations, management's knowledge of operations, Federal Information Security Management Act (FISMA) review results, and external financial statement/ IG/ GAO audits, as applicable, to determine the entity's risk of non-compliance with the eight goals. No further evaluations or testing should be necessary to perform this FMS Evaluation. If the entity's internal control evaluations and other assessments do not provide an adequate basis for the FMS evaluation, then the entity should raise the risk levels of non-compliance with the eight goals.

The **FMS** tab within the EA Module provides a uniform Department-wide mechanism for documenting the FMS Evaluation. For each of the eight Financial Management System Goals listed in the **FMS** tab, entities will record:

- Level of risk of being non-compliant with that goal;
- Sources used in determining that risk level; and
- An evaluation summary that briefly describes any relevant assessments, evaluations, and testing performed during the assessment year – both internal and external – and the outcomes.

Designated Departmental Elements and Major/ Integrated Contractors should use the *FMS Evaluation Worksheet* found in Appendix F, to assist with the evaluation in the EA Module. The *FMS Evaluation Worksheet* will guide organizations with the evaluation of the organization's achievement of the eight financial management goals by using compliance indicators to assess the risk of non-compliance with the FFMIA on a rating assessment of Low, Moderate, or High. Guidance to assist with this determination is co-located with each rating. For each goal, entities are required to document the risk level rating and the sources used along with a summary of the evaluation results for each financial management goal in the FMS Tab in the EA Module. After entities have determined the risk level rating for each goal, the sum of the risk level ratings will automatically calculate to determine the overall FMS risk of non-compliance with FFMIA, which should support the FMS assurance in the Assurance Memorandum. Similar to the evaluation of internal controls, entities should report identified deficiencies or issues found in the FMS Evaluation and provide a rating of 1-3 depending on the seriousness of the issue. A rating of 1 being the least serious and 3 being the most serious. Issues identified in the **FMS** tab will create a line in the **Action Tracking** tab. Then, the user will need to input information required for each issue. Issues identified with a rating of **2** or **3** will require a CAP. If there is an **existing CAP** for an FMS issue, reporting organizations must indicate and identify the existing CAP name and number in the EA Module.

Managers must use professional judgment in assessment of the FMS Goals. For example, a rating of 3 on one goal does not necessarily indicate non-conformance for the entire FMS Evaluation.

Additionally, organizations identified as owners of an FMS included in Table 9 *DOE Financial Management Systems*, must perform an FMS Evaluation to support core requirements of Section IV of FMFIA and FFMIA. If an entity's system (including Major/ Integrated Contractor systems) feed into a DOE financial management system, then those systems are subject to an FMS Evaluation for FY 2022.

Table 9 DOE Financial Management Systems

Financial Management System and Mixed Systems	System Owner(s)
Power Marketing Administration Systems	BPA, WAPA, SWPA, & SEPA
Standard Accounting and Reporting System (STARS)	CFO
Federal Energy Regulatory Commission Systems	FERC
Budget Formulation and Distribution System (BFADS-formerly FDS 2.0)	CFO
Electronic Work for Others	ORNL
Active Facilities Database	CFO
ABC Financials	NNSA-NA-532
Integrated Planning, Accountability and Budgeting System (IPABS)	EM-62
Facilities Information Management System (FIMS)	MA-50
Strategic Integrated Procurement Enterprise System (STRIPES)	CFO
Vendor Inquiry Payment Electronic Reporting System (VIPERS)	CFO
Financial Accounting Support System (FAST)	CFO
iBenefits	CFO
Budget and Reporting Codes System (BARC)	CFO

In accordance with the FFMIA and OMB Circular A-123, Appendix D, system owners and users should determine whether the financial and mixed systems conform to federal financial management systems requirements. As a result, entities are required to have financial management systems that substantially comply with the requirements of FFMIA Section 803(a), which includes Federal Financial Management System Requirements, federal accounting standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the requirements of the United States Standard General Ledger (USSGL) at the transaction level.

VII. Classifying Deficiencies

In accordance with OMB Circular A-123, DOE adopted a three-level rating system for reporting deficiencies to internal control principles and to issues identified in entity objective reviews. The severity of the deficiencies determines if the entity should report it in the organizational Assurance Memorandum. An entity control deficiency requires qualitative judgment that a significant deficiency exists that could adversely affect the organization's ability to meet internal control objectives, and an entity material weakness is a significant deficiency which the head of the organization determines is significant enough to report outside of the organization. The entity should document the information gathered and the decisions made related to the considerations.

Organizations must report control deficiencies that meet certain criteria in the Assurance Memorandum. Table 10, Deficiency Classifications provides a description of the issues that organizations should report for each section of the Assurance Memorandum, a definition for each issue, and an indication of which issues requires a corrective action plan in the Assurance Memorandum.

NOTE: Organizations must distinguish control deficiencies (including significant deficiencies and material weaknesses) from funding and resource issues. Funding levels are not control deficiencies, and organizations should not report funding and budgetary limitations as a significant deficiency or material weakness in the Assurance Memorandum.

Table 10 Deficiency Classifications

Deficiency Title	Definition	Applicable to	Reported in Assurance Memorandum
Control Deficiency (Non-Significant Issue)	A control deficiency exists when the design, implementation, or operation of a control does not provide management or personnel, in the normal course of performing the assigned functions, to achieve control objectives and address related risks. 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.	FMA, EA	No
Significant Deficiency	A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.	FMA, EA	Yes
Material Weakness	A significant deficiency that the Entity Head determines to be significant enough to report outside of the Entity as a material weakness. In the context of the Green Book, non-achievement of a relevant Principle and related Component results in a material weakness. A material weakness in internal control over operations might include, and is not limited to, conditions 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. A material weakness in internal control over reporting is a significant deficiency, in which the Entity Head determines significant enough to impact internal or external decision-making and reports outside of the Entity 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 assures 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 Entity objectives. A **No** response on either Line 46 or 47 in the **EAT IC Summary Evaluation** tab requires a Material Weakness to be reported: • Are all components operating together in an integrated manner? or • Is the overall system of internal control effective?	FMA, EA	Yes
Non-Conformance	Exists when financial systems do not substantially comply with federal financial management system requirements OR where local control deficiencies impact financial systems ability to comply. The EA Module defines the criteria against which conformance is evaluated and captures identified non-conformances.	FMS (in the EA Module)	Yes
Scope Limitation	Exists when the Entity has identified potentially significant deficiencies in the scope of the internal controls evaluations conducted, which would warrant disclosure to assure limitations are understood. Scope limitations may be determined by the entity or may be required by the CFO in certain circumstances.	FMA and EA	Yes

VIII. Annual Assurance Memorandum

Each entity is required to provide an annual Assurance Memorandum that documents the results of the annual FMA Evaluation if applicable, EA Evaluation, and FMS Evaluation, if applicable, along with other reviews conducted. The Assurance Memorandum provides a status of the overall adequacy, effectiveness, and efficiency of the organization's internal controls. The Assurance Memorandum must identify significant deficiencies or material weaknesses which might qualify that assurance, as defined in Table 10, Deficiency Classifications, and a summary of the corrective action plans developed to address such issues will accompany the Assurance Memorandum. Organizations will also report instances of non-compliance with Federal FMS requirements or control deficiencies that affect an organization's ability to comply with the eight financial management goals.

Headquarters Offices with Field organizations must consider the results of the Field organization FMA and EA evaluations. Likewise, Field organizations with Major/ Integrated Contractors, must consider the results of the contractor FMA and EA evaluations. When considering the results of various cognizant organizations, the Departmental Element should consider multiple instances of similar control deficiencies and similar significant deficiencies across the entity to determine if a significant deficiency or material weakness exists at the Departmental Element's level.

To align and comply with OMB Circular A-123, Appendix B, *A Risk Management Framework for Government Charge Card Programs*, assurances are in the Assurance Memorandum in reference to the implementation of safeguards and internal controls for inappropriate charge card practices as well as assurances that organizations have processes in place to identify risks, controls, and that the controls are operating effectively.

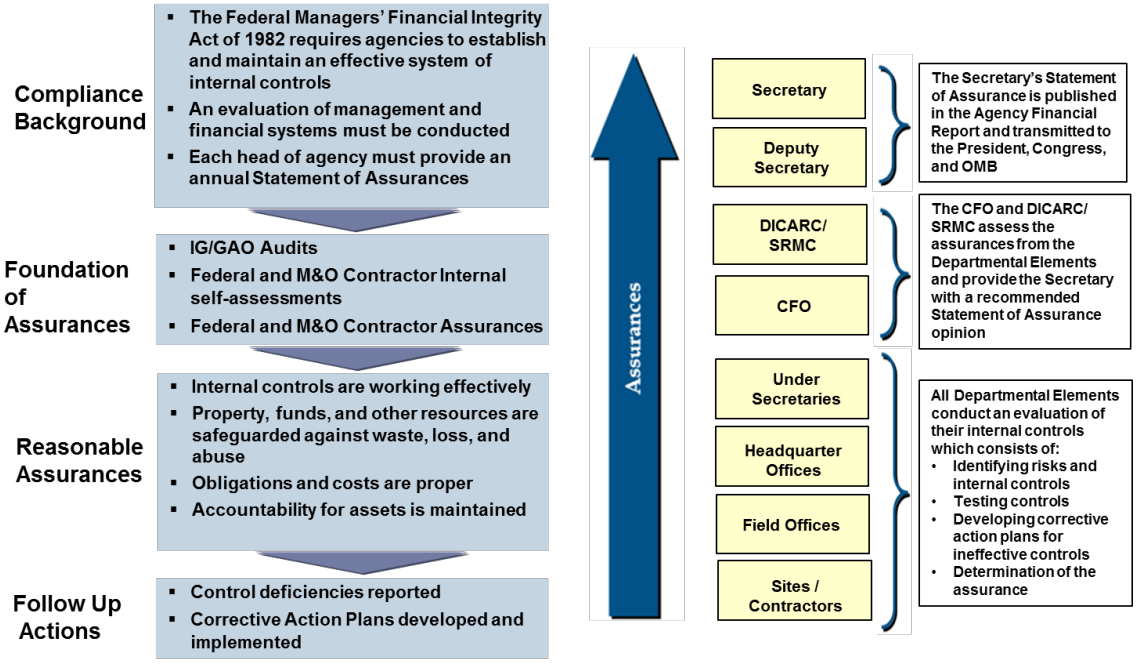
Organizational assurance statements include an evaluation of the effectiveness of internal control over operations, reporting and compliance as of June 30. Organizations remain responsible to provide an update to the assurance statements when a significant deficiency or material weakness is resolved or identified after June 30:

- If an organization discovers a significant deficiency or material weakness by June 30, and implements corrective actions by September 30, the organization will update the statement identifying the significant deficiency or material weakness, the corrective action taken, and the resolution occurred by September 30.
- If an organization discovers a significant deficiency or material weakness after June 30, and before September 30, the organization will update the statement identifying the significant deficiency or material weaknesses to include the subsequently identified significant deficiency or material weakness.

Organizations will notify the OCFO immediately of any resolved or new significant deficiencies or material weaknesses no later than October 1, 2022, per Table 2, DOE Internal Controls and Risk Profile Process Important Dates.

Figure 4 presents the DOE annual assurance process. Assurance flows from each major/ integrated contractors to the respective Departmental element, and from the Departmental element (Field and Headquarters Offices) to the Under Secretaries. The CFO and DICARC assess the assurances from the Under Secretaries and provide the Secretary with the recommendation to sign the DOE Management Assurances.

Figure 4 DOE Assurance Process



Appendix D provides separate templates for Field Offices, PMAs, large Headquarters Offices, smaller Headquarters Offices, and Under Secretaries to use in preparation of the Assurance Memorandum. PMAs should continue to use the Field Office template.

The Assurance Memorandum consists of two portions:

1. Main Body – Contains the actual assurance statements and executive summaries of identified significant deficiencies or material weakness.

2. Corrective Action Plan Summary – Lists CAPs for each significant deficiency, material weakness, or non-conformance reported in the Assurance Memorandum. The CAP Summary briefly describes the remediation activities that have occurred or the remediation activities the organization will implement in the next fiscal year.

   CAP Summary includes:
   (a) New Issues and CAPs; and,
   (b) Action Plans from prior-year reporting (may be open or closed). For CAPS that remediate deficiencies reported in previous years and now closed in FY 2022, the CAP Summary must include a statement noting the closure of the CAP.

Final responsibility for making assurances that financial, entity, and financial management systems internal controls are effective and efficient, produce reliable reports, and are compliant with all applicable laws and regulations lies with the head of each entity. The **head of the Departmental Element must sign the Assurance Memorandum**. During instances when the head of the Departmental Element is not available, the organization's Assurance Memorandum may be signed by the designated representative that has a Delegation of Authority Memorandum signed by the head of the Departmental Element. Headquarters-level entities that report to an Under Secretary will provide the Assurance Memorandum to the respective Under Secretary for signature.

NEW in FY 2022

DOE Order 520.1B was approved January 2021 directing the head of each Departmental Element to designate an Internal Control Action Officer that will coordinate the organization's Internal Control

Program that is consistent with the DOE Internal Control Evaluations Guidance. **When an organization changes the designated Internal Control Action Officer, the updated name and contact information should be provided to the Internal Controls and Fraud Risk Management Division's shared mailbox** at cfo-icfrmd@hq.doe.gov.

Listing of Appendices

Title	Description
Appendix A, *Risk Profile Guidance*	The appendix focuses on completing the Risk Profile template and provides the purpose and definition for each column in the Risk Profile template.
Appendix B, *AMERICA Overview, Workflow, and Reports*	The appendix provides an overview of AMERICA and describes the workflow and types of reports that are offered.
Appendix C, *AMERICA EA, IICS, and FMA Modules*	The appendix describes the purposes and use of the IICS, EA and FMA Modules in AMERICA.
Appendix D, *Assurance Memorandum Templates*	The appendix provides the templates that Under Secretary Offices, Headquarter Offices and Field Offices must use to provide assurances on the effectiveness of the reporting organization's System of Internal Controls. **Note: To be published by April 6, 2022.**
Appendix E, *Fraud Risk Management Guidance*	The appendix provides information on how to identify and combat fraud through DOE's Internal Controls Program.
Appendix F, *Financial Management Systems Evaluation Guidance*	The appendix informs Internal Control POCs how to perform and document FMS Evaluations.
Appendix G, *Glossary*	The appendix provides a listing of common terms and definitions as they pertain to DOE Internal Controls Program.
Appendix H, *Management Priorities Guidance*	The appendix is applicable to select organizations that are responsible for DOE's Management Priorities and describes the process for updating the management priorities.

The information contained herein is valid at the time of distribution and is subject to change. Any official updates occuring during the fiscal year will be announced by the ICFRMD Division Director and addressed via supplemental guidance and/ or webinars.

Please contact CFO-ICFRMD@hq.doe.gov for any recommendations or concern.

Appendix A – Risk Profile Guidance

The Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, requires each agency to perform risk assessments to develop a prioritized and ranked Risk Profile. The Risk Profile identifies the most significant risks faced by an agency in meeting strategic objectives and communicates the strategy for addressing those significant risks. Significant risks are captured from detailed financial and non-financial risks reported through AMERICA to provide an entity wide view of all risks.

This guidance provides the Risk Profile template and instructions to produce a Risk Profile compliant with OMB and Department of Energy (DOE or Department) requirements. OMB Circular A-123 requires that risks be analyzed in relation to the achievement of objectives in the following areas:

- **Strategic**: DOE strategic goals and objectives
- **Operations**: effective and efficient use of DOE resources in administrative and major program operations, including financial and fraud objectives covered in annual internal control testing
- **Compliance**: DOE compliance with applicable laws and regulations
- **Reporting**: reliability of DOE internal and external financial or non-financial reporting

Consideration of Risks During Budget Formulation

Risk consideration is a key element during budget formulation and vital to an organization's planning process. As such, risk management professionals should be part of every organization's leadership efforts for planning future years' budget. At the Department level, resource planning is a joint effort that is guided by the Chief Financial Officer (CFO) and Chief Risk Officer (CRO). Using this approach, the agency's risk posture is reflected in the Department's budget, addresses budget needs for key controls to mitigate the most important risks, and reflects the priorities and risk appetite of the Department's leadership. The Department's risk profile is also used to shape discussions between DOE and OMB in supporting budget justifications. Leadership should also consider risks during budget execution with discussions on funding to improve performance while responding to emerging risks.

Fraud Considerations in the Risk Profile

For fiscal year (FY) 2022, reporting organizations will continue to evaluate each risk on the risk profile to determine if it is also a fraud risk. All entities must identify whether each risk has a financial fraud impact, non-financial fraud impact, or neither. Departmental elements must also identify the top financial and non-financial fraud risks for the organization. Each Risk Profile must include **at least one financial fraud risk and one non-financial fraud risk**. See Appendix E: Fraud Risk Management Guidance for additional information on fraud risk considerations.

Deliverable Requirements

The Risk Profile deliverable must be reviewed and approved by the reporting organization's management. The Risk Profile template includes a signature box at the top where the entity's management should document approver name, title, and sign-off. Reporting organizations with substative changes to risks in their FY 2022 Risk Profile will provide both the completed Risk Profile excel template as well as a PDF version of the template with management's signature. Both the PDF and excel Risk Profile documents will be sent to the Internal Controls and Fraud Risk Management Division's e-mail address at CFO-ICFRMD@hq.doe.gov, **not through the A-123 Application, AMERICA**. Reporting organizations that **do not have substantive changes** to risks in their FY 2022 Risk Profile will provide a

signed memorandum[1] from the organization's management indicating there are no substantive changes from the organization's FY 2021 Risk Profile. The signed memorandum will be sent to the Internal Controls and Fraud Risk Management Division's shared mailbox at CFO-ICFRMD@hq.doe.gov. **Reporting organizations will also identify and provide the name of their Risk POC to the Office of the Chief Financial Officer.**

Each lower-level reporting organization with substantive changes to risks in FY 2022 will produce a Risk Profile and provide it to the higher-level organization for consideration and consolidation. Major/ Integrated contractors, including Management and Operating (M&O) and integrated non-M&O Contractors, with substantive changes to risks, should provide a Risk Profile to each responsible Field Office. Field Offices should take into consideration the Risk Profiles from the Major/Integrated contractors, including M&O and integrated non-M&O Contractors, under their purview when providing the Field Office Risk Profiles to each responsible Headquarters (HQ) Office. Each HQ Office with substantive changes to risks, taking into consideration the Field Offices under their purview, must provide a Risk Profile identifying the most significant risks (including fraud risks) to the Office of the Chief Financial Officer and to each responsible Under Secretary Office, if applicable. The Under Secretary Offices review provided risk profiles and prepare an approved Risk Profile representing the top top risks of reporting organizations and send both the PDF and excel Risk Profile documents to the Internal Controls and Fraud Risk Management Division's shared mailbox at CFO-ICFRMDd@hq.doe.gov. Under Secretary Offices that do not have substantive changes to risks in their FY 2022 Risk Profile will provide a signed memorandum from the Under Secretary or designated representative indicating there are no substantive changes from the organization's FY 2021 Risk Profile.

The Risk Profiles from each Under Secretary, and each Headquarters element not reporting to an Under Secretary, will be consolidated into a prioritized DOE Risk Profile and used during the Department's FY 2024 budget formulation process and as part of the annual Strategic Review with OMB in May. The risks identified as fraud related in the Risk Profile will also be considered for DOE's Fraud Risk Profile.

Table 1 Important Dates for Risk Profile Deliverable

FY 2022 Key Dates	Deliverables
February 3	Headquarters Offices and Power Marketing Administrations (PMA) provide the Risk Profile excel and signed PDF versions, updated and revised only **if there are substantive changes to risks**, with consideration of reporting from Field Offices, Site Offices, M&O and non-M&O Contractors as applicable, **or a signed memorandum from the organization's management indicating there are no changes from the FY 2021 Risk Profile** to the Internal Controls and Fraud Risk Management Division's shared mailbox at CFO-ICFRMD@hq.doe.gov. Reporting organizations should check with their cognizant organization to determine substantive changes for Risk Profiles and follow cognizant organizations subsequent timelines to assure Risk Profiles are provided to DOE on time.
March 3	Under Secretaries provide Risk Profile excel and signed PDF versions, updated and revised only **if there are substantive changes to risks or a signed memorandum indicating there are no changes from the FY 2021 Risk Profile**, to the Internal Controls and Fraud Risk Management Division's shared mailbox at CFO-ICFRMD@hq.doe.gov based on the input of the reporting offices.
April 14	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review and the FY 2024 Budget Formulation process.

[1] Use the prescribed Risk Profile Memorandum Template provided in this Appendix.

Risk Profile FMA and EA Module Reporting

To the extent additional internal controls are necessary to manage or mitigate risks identified in Risk Profiles, the controls must be established and evaluated as part of annual internal control testing and attested in the annual assurance statement. If a control existed in last year's Risk Profile deliverable, the Departmental Element may treat it in the same manner as a focus area exemption.

Reporting organizations should indicate where each reported risk is evaluated using the Current Evaluation Category column (Column M). Risk Profile financial risks must be documented and evaluated, including the establishment and testing of controls when applicable, in the **FMA Module** in AMERICA. Risk Profile non-financial risks are evaluated, including the establishment and testing of controls when applicable, as part of the Entity Assessment (EA) process and reported in the appropriate section of the **EA Module** in AMERICA. Internal control risks are assessed and reported in the **Internal Control Evaluation** tab and the entity objective risks assessed and reported in the **Entity Objective Evaluation** tab.

Entities should continue to provide further detail of where risks are being evaluated within the EA or FMA Modules using the Current Evaluation Details column (Column N). For example, if the current evaluation category is "Internal Control Evaluation," indicate which of the 17 Principles the risk is evaluated. If the current evaluation category selected is "Entity Objectives Evaluation," identify the specific entity objective. For the FMA Module, if the current evaluation category is "FMA Evaluation," identify the sub-process where the controls are located that mitigate the risk.

Instructions for Risk Profile Template

The Risk Profile Template involves the identification and analysis of risk. Risk identification offers a structured and systematic approach to recognizing where the potential for undesired outcomes can arise. Risk analysis and evaluation considers the causes, sources, probability of risk occurring, the potential outcomes, and prioritizes the results of the analysis.

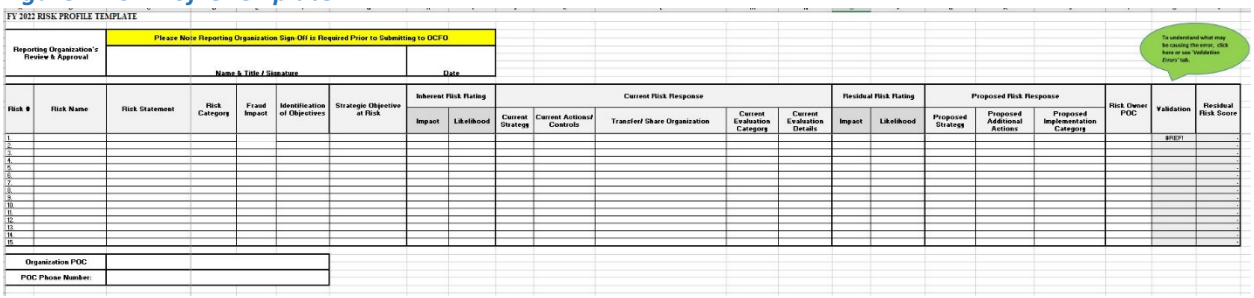
When identifying and analyzing your organization's risks, consider these questions:

- What are my organization's goals and objectives that support the DOE Strategic Plan?
- What events could happen that would prevent my organization from achieving its goals and objectives aligned with the DOE Strategic Plan?
- What events could impede effective or efficient use of resources for Departmental operations?
- What events could affect reliability, accuracy, or timeliness of reporting?
- What events could prevent us from achieving compliance with statutory, Congressional, OMB, or other requirements?
- What are the corresponding impacts of these risks and what is the severity of this impact? (according to the criteria presented)
- What is the likelihood that this event will occur? (according to the criteria presented)
- What are the most significant risks?
- What are the fraud risks?
- Which risks require a response?
- What actions will you take to address these risks? What actions could you take in the future to address these risks?
- Did the actions taken to address a risk have an effect? Is there any remaining residual risk? If so, what is the severity of impact and likelihood of occurrence of this risk?
- Who is accountable for the actions to address the risk?

After risks are identified, management must determine a risk response. In determining a risk response, management should consider risk tolerance, placement of controls, and other mitigating actions. Risk tolerance is particularly important as management has significant discretion in setting risk tolerance levels. The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book) defines risk tolerance as the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerance levels will significantly impact management's risk response decisions and should always be considered.

The Risk Profile template is presented in *Figure 1 Risk Profile Template* followed by instructions explaining how to complete each column in the FY 2021 Risk Profile. The template and instructions will be provided in Excel for your organization's use in completing the Risk Profile.

Figure 1 Risk Profile Template


FY 2021 RISK PROFILE TEMPLATE

Please Note Reporting Organization Sign-Off is Required Prior to Submitting to OCFO

Reporting Organization's Review & Approval — Name & Title / Signature — Date

To understand what may be causing the error, click here or see 'Validation Errors' tab.

Risk #	Risk Name	Risk Statement	Risk Category	Fraud Impact	Identification of Objectives	Strategic Objective at Risk	Inherent Risk Rating		Current Risk Response					Residual Risk Rating		Proposed Risk Response			Risk Owner POC	Validation	Residual Risk Score
							Impact	Likelihood	Current Strategy	Current Actions/ Controls	Transfer/ Share Organization	Current Evaluation Category	Current Evaluation Details	Impact	Likelihood	Proposed Strategy	Proposed Additional Actions	Proposed Implementation Category			
1																				#REF!	
2																					
3																					
4																					
5																					
6																					
7																					
8																					
9																					
10																					
11																					
12																					
13																					
14																					
15																					

Organization POC	
POC Phone Number:	

NOTE: Verify that the file is "Enabled" by clicking on "File," "Enable Content," "Enable All Content" before entering data into the template. Provide Name and Title of the Department Head approving the Risk Profile and the date when the Risk Profile was completed. Provide the POC Name and POC phone number at the bottom of the Risk Profile. After completion, the Risk Profile must be produced in PDF format with signature as well.

Risk # (Column A): This column is pre-populated with a unique number and used to assign a numerical ID to each identified risk.

Risk Name (Column B): Use this column to name the identified risk statement. This risk name can be used for easy identification of a specific risk statement across an entity.

Risk Statement (Column C): Use this column to identify risks and the impacts/ effects. Use the "if, then" sentence construction to describe the event ("if") and the impacts ("then"). List all possible impacts in the statement and do not limit the statement to a single impact to avoid understatement of the risk. For example:

- If the roof collapses at Building X, then workers may be injured, water infiltration can damage equipment, and the protected area adjacent to Building X will be more vulnerable to additional damage that could render the storage of nuclear material unsafe.
- If we lose technical capabilities in the program's workforce, then we will not be able to complete the work on schedule and at cost.

Risk Statements are not meant to be descriptions of issues, meaning risks that have already occurred, but are potential events that could occur. Some risks may be unavoidable and beyond an organization's ability to reduce to a tolerable level. Nevertheless, the organization should identify these risks, make contingency plans, and manage risks against those plans to the best of abilities. For example, many organizations have to accept risks that arise due to natural disasters that cannot be controlled, but may have emergency response mechanisms in place to mitigate against these risks.

Risk Category (Column D): Use this column to select a risk category to describe the identified risk. The drop-down menu lists the 10 management priorities identified in the FY 2021 Agency Financial Report (Contract & Major Project Management; Safety & Security; Environmental Cleanup; Nuclear Waste Disposal; Nuclear Stockpile Stewardship; Cybersecurity; Infrastructure; Human Capital Management & Diversity and Inclusion; Energy Justice; and Climate Change) along with seven other common risk categories (Political, Reputational, IT, Grants/Loans, COOP, and Financial Management). These management priorities along with the other listed categories serve as proxies for risk categories and will be used to aggregate risks. Select one risk category only. For instances where multiple risk categories may seem to apply, use best judgement to select the most relevant category. In addition, if the identified risk does not align with one of the listed risk categories, choose "Other" from the drop down menu.

Dropdown Options:

- Contract & Major Project Management
- Safety & Security
- Environmental Cleanup
- Nuclear Waste Disposal
- Nuclear Stockpile Stewardship (NEW)
- Cybersecurity
- Infrastructure
- Human Capital Management & Diversity and Inclusion (UPDATED)
- Energy Justice (NEW)
- Climate Change (NEW)
- Political
- Reputational
- Information Technology
- Grants/Loans
- COOP
- Financial Management
- Other

Fraud Impact (Column E): Use this column to identify if the risk is a Financial, Non-financial, Top Financial, or Top Non-financial fraud related risks. If a risk does not have a fraud impact, then organizations should select "N/A" from the drop-down menu. Note that if a fraud sub-category is not identified for each risk, an error will occur in the validation column (Column U).

Dropdown Options:

- Financial Fraud
- Non-Financial Fraud
- Top Financial Fraud
- Top Non-Financial Fraud
- N/A

Identification of Objectives (Column F): Risks must be linked to achievement of one of the four objectives identified by OMB: strategic objectives (objectives established in the DOE Strategic Plan), operational objectives (administrative and major program operations), reporting objectives (reliability of internal and external financial and non-financial reporting objectives), and compliance objectives (compliance with applicable laws and regulations). Only select one objective, and for instances where multiple objectives may seem to apply, use best judgement to select the most relevant objective.

Strategic Objective at Risk- Primary (Column G): This column has a drop-down menu that will allow only one choice. Use this column to select the strategic objective from the drop-down menu that the risk affects only if the "Strategic Objectives" option was selected in the Identification of Objectives column (Column F). The drop-down menu contains the strategic objectives from the Draft DOE Strategic Plan Framework. Select one primary strategic objective only, and for instances where multiple strategic objectives may seem to apply, use best judgement to select the most relevant strategic objective. If the objective identified is anything but Strategic in the previous field, then select 'N/A - Strategic Objective was not selected as an objective in the previous field" for this column. Note that a validation error will occur if the requirement stated here is not fulfilled.

Dropdown Options:

- **Objective 1:** Develop energy technologies that increase the affordability of domestic energy resources
- **Objective 2:** Reduce regulatory burdens on domestic energy resources
- **Objective 3:** Revitalize U.S. nuclear energy sector
- **Objective 4**: Improve electric grid reliability and resilience
- **Objective 5:** Increase domestic and international accessibility to American energy resources
- **Objective 6:** Protect the U.S. economy from severe petroleum supply disruptions
- **Objective 7:** Conduct discovery-focused research to increase our understanding of matter, materials, and their properties
- **Objective 8:** Provide the Nation's researchers with world-class scientific user facilities that enable research and advance scientific discovery
- **Objective 9:** Advance high-performance and future computing technologies and the potential of artificial intelligence technologies to ensure American primacy in computing and to meet national research, security, and economic objectives
- **Objective 10:** Enable commercialization of national laboratory innovation
- **Objective 11:** Maintain the safety, security, and effectiveness of the Nation's nuclear deterrent
- **Objective 12:** Strengthen key science, technology, and engineering capabilities and modernize the national security infrastructure
- **Objective 13:** Reduce global nuclear and radiological security threats and strengthen the nuclear enterprise
- **Objective 14:** Provide safe and effective integrated nuclear propulsion systems for the U.S. Navy
- **Objective 15:** Develop and implement a robust interim storage program
- **Objective 16:** Continue environmental remediation of DOE legacy and active nuclear waste sites
- **Objective 17:** Enhance energy infrastructure situational awareness, strengthen cyber incident response capabilities, and leverage the national laboratories to drive cybersecurity innovation
- **Objective 18:** Modernize DOE IT infrastructure to deliver effective services supporting smart, efficient cybersecurity and enhance DOE's cybersecurity risk management structure to create transparency across the enterprise
- **N/A –** Strategic Objective was not selected as an objective in the previous field.

Inherent Risk Rating: Inherent risk is the exposure arising from a risk before any action is taken to manage it. Because the Inherent Risk Rating is the assessment of a risk before any action to manage or mitigate the risk through the use of controls, the Inherent Risk Rating will **never be lower** than the Residual Risk Rating. Inherent risk is measured using the impact and likelihood metrics described below.

Inherent Impact (Column H): Inherent Impact refers to the measurements of the effect of an event that could result from the occurrence of the identified risk. The impact is assessed to gauge how severe the effect will be on the ability to achieve an organization's goals and objectives. Assess this by estimating the level of impact, using a scale of 1 to 5, which will happen if the risk occurs. Use informed judgment

and the experience of knowledgeable individuals and groups to assist in determining the level of impact. In this assessment, consider these questions:

- Is there a threat to human life?
- Is there a threat of fraud, waste, and abuse?

Use the scale with defined parameters in *Table 2 Impact Assessment,* to rate the impact of the risk.

Table 2 Impact Assessment

Measured Impact	Reduced Quality and Performance
1 – Very Low	The **impact is insignificant** and localized and does not affect the entity's ability to achieve one or more of its objectives or performance goals. Impact on single non-critical task/objective resulting in minor plan/work adjustment with no impact on achieving project/organizational goals/deliverables, e.g., data for a report provided late but ultimate deadline met.
2 – Low	The **impact will not significantly affect** the entity's ability to achieve one or more of its objectives or performance goals. Impact on multiple non-critical plan tasks/objectives resulting in several minor plan/work adjustments with no significant impact on achieving project/organizational goals/deliverables, e.g., data provided fails data checks and data accumulations system/process must be corrected and rerun resulting in delays.
3 – Moderate	The **impact could significantly affect** the entity's ability to achieve one or more of its objectives or performance goals. Impact on one or more critical plan tasks/objectives resulting in major plan/work adjustments with significant impact resulting in reduced achievement of project/organizational goals/deliverables, e.g., expected data unavailable and final report/product lacks expected, information/analysis or results in significant delivery delay.
4 – High	The **impact could preclude or highly impair** the entity's ability to achieve one or more of its objectives or performance goals. Impact on one or more critical plan tasks/objectives resulting in major plan/work adjustments with major impact resulting in only partial achievement of project/organizational goals/deliverables, e.g., expected data unavailable and final report/product lacks critical information/analysis and/or results in significant delays.
5 – Very High	The **impact will likely preclude** the entity's ability to achieve one or more of its objectives or performance goals. Impact on one or more critical plan tasks/objectives resulting in major plan/work adjustments with severe impact resulting in failure to achieve project/organizational goals/deliverables, e.g., expected data unavailable and final report/product not issued.

Inherent Likelihood (Column I): This is the probability that a given event will occur. Assess the likelihood (using a scale of 1 to 5) based on data (when available) or use the knowledge and experience of an expert or group. Use the scale with defined parameters in *Table 3 Likelihood*, to rate the likelihood of the identified risk:

Table 3 Likelihood

Likelihood	Definition
1 – Very Low	Risk event **rarely** to occur. Less than a 5% chance of occurrence.
2 – Low	Risk event **unlikely** to occur. Between a 5% - 25% chance of occurrence.
3 – Moderate	Risk event **possible** to occur. Between a 26% - 49% chance of occurrence.
4 – High	Risk event **highly likely** to occur. Between a 50% - 74% chance of occurrence.
5 – Very High	Risk event **almost certain** to occur. Greater than a 75% chance of occurrence.

Current Strategy (Column J): Use this column to indicate the action currently taken to manage the identified risk. Consider these questions when preparing a risk response:

- What action or multiple actions will be taken to address this risk?
- How are these actions managing the risk?
- How long will these actions continue?

Select a current risk response from the options in the drop-down menu. (See *Table 4 Risk Responses)*

Table 4 Risk Responses

Response Type	Definition	Example
Accept	Take no action to respond to the risk based on insignificance of risk, requirement to complete the work, or benefits and opportunities exceed the risk.	Continue an environmental cleanup project, despite identified risks, because taking no action has unacceptable public safety and environmental impacts.
Avoid	Action is taken to stop the operational process, or the part of the operational process, causing the risk.	Supplier of a specialty part may no longer be in business when part is needed, so action is taken to modify the design specifications to use generic, widely available part.
Reduce	Take action to reduce the likelihood or impact of the risk.	Past end-of-life infrastructure needs replacement, but increased inspection and extraordinary maintenance reduces risk of catastrophic failure.
Transfer	Take action to transfer the responsibility for ownership and handling the risk to an organization other than the current entity that owns the risk.	Scope of work on a project is transferred to another organization with more expertise or experience.
Share	Take action to share the risk with another entity within the organization or with one or more external parties.	Strategic partnership formed to share high risk work with an outside organization with expertise and special facilities.

In developing the Risk Profile, management must determine those risks for which the appropriate response includes implementation of formal internal controls activities according to defined criteria, as described in Section III of OMB Circular A-123 and which conforms to the standards published by GAO in the Green Book. Note that to the extent internal controls are necessary to manage or mitigate risks identified in Risk Profiles, the controls must be established and tested as part of annual internal control testing and included in the annual assurance memorandum.

Current Actions/Controls (Column K): This column provides a narrative explanation of how to currently apply the risk response identified in the prior column. Include any formal internal control activities that are currently in place to manage the risk. The brief narrative should also summarize the **action** taken, and as applicable, may include an explanation of the action. For example, the action to address a safety risk might involve repair of faulty equipment, so the selection "reduce" from the risk response strategy drop-down menu is appropriate and then explain in this text box how the faulty equipment was repaired to reduce the risk. Also, the narrative should explain the **controls** put in place to reduce the risk. Using the same example above, explain how regular safety inspections were implemented.

Transfer/Share Organization (Column L): If the Current Strategy is to "Transfer" or "Share," then this field should be used to identify the organization to which the risk is transferred or shared. Organizations will need to coordinate with the identified organization to which the risk ownership is transferred to or

shared with to ensure that the risk is included on the identified organization's risk profile as well. The inclusion of the risk on the identified organization's risk profile will not only indicate that they accept the transfer or sharing of risk ownership but will also close the gap on the actions taken to respond to the risk. If the Current Strategy is other than "Transfer" or "Share," then "N/A" should be selected in this field. However, if the Current Strategy in column J is "Transfer" or "Share", then select the organization the risk is being transferred to or the risk is being shared with. Note that if an organization does not identify the Transfer/Share Organization in this column (only for risks with a transfer or share risk response) or select "N/A" when applicable, an error will occur in the validation column (Column U).

Current Evaluation Category (Column M): Use this column to indicate where the internal control activities to manage the risk have been evaluated. If the risk is a financial risk, and the appropriate internal controls are tested and documented in the entities' FMA Module in AMERICA, select "FMA Evaluation" from the drop-down menu. If the risk is a non-financial risk, and the controls to manage this risk are evaluated in the Entity Assessment's Entity Objective Evaluation, select this option from the drop-down menu. If the internal control activities to address the risk are evaluated in the Entity Assessment's Internal Control Evaluation, then select this choice from the available options. If formal internal control activities were not implemented to manage the risk (i.e., the current strategy is to "Accept"), then this column should be left blank.

Current Evaluation Details (Column N): This column provides text space to provide further detail of where the risk is currently evaluated. For example, if the current evaluation category is "Internal Control Evaluation", indicate which of the 17 Principles the risk is evaluated. If the current evaluation category is "Entity Objectives Evaluation", identify which entity objective. If the current evaluation category is "FMA Evaluation", identify the sub-process where the controls are located that mitigate the risk.

Residual Risk Rating: Residual risk is the amount of risk that remains after action has been taken to manage it. In the earlier example about safety, after implementation of safety inspections, residual risk from the limitations of testing equipment may remain. Use the same assessment standards provided in the prior section to assess residual risk impact and likelihood on a scale of 1 to 5 (*Table 2 Impact Assessment* and *Table 3 Likelihood*, respectively). Because the Residual Risk Rating is the assessment of a risk after actions have been implemented to manage or mitigate the risk, the Residual Risk Rating will **never be higher** than the Inherent Risk Rating. However, if no actions were taken to address the inherent risk or if the Current Risk Response strategy is "Accept", then the residual risk field will be the same as the inherent risk.

Residual Impact (Column O): This column refers to the measurement of the effect of an event that could result from the occurrence of the identified residual risk. The impact is assessed to gauge how severe the effect will be. Assess this by estimating the level of impact that will happen if the event occurs based on informed judgment and experience of knowledgeable individuals and groups on a scale of 1 to 5 (using the scale in *Table 2 Impact Assessment*). For risks where no actions were taken to address the inherent risk, then the residual risk impact field will be the same.

Residual Likelihood (Column P): This is the probability that a given event will occur. This assessment is used to gauge how likely an event is to occur. For example, events that may happen every day have a far greater likelihood than events that may only happen once in 10 years. Assess the likelihood (using a scale of 1 to 5) based on data available or use the knowledge and experience of an expert or group using the scale in *Table 3 Likelihood*. For risks where no actions were taken to address the inherent risk, then the residual risk likelihood field will be the same.

Proposed Risk Response Strategy (Column Q): This column indicates proposals on how to treat the residual risk similar to the consideration of the inherent risk discussed above. Consider these questions when preparing a proposed risk response:

- What additional actions would address this risk in addition to the initial risk mitigation actions already taken?
- Would these actions actually manage the risk?
- How long will the actions continue?

Select a proposed residual risk strategy from the options found in *Table 4 Risk Responses*. For risks where no actions were taken to address the inherent or residual risk, the proposed risk response may be blank.

Proposed Additional Actions (Column R): Use this column to provide a narrative explanation of how to employ the proposed risk response to the residual risk identified in the prior column. These additional actions could further reduce the exposure remaining after the initial risk mitigation actions have been taken. The amount and type of description in this column is subjective, but a brief summary is recommended. Proposed risk responses should use the same standards applied to the current risk response, as described above, including the identification of risks for which implementation of formal internal control activities is appropriate. This column is also to be used to explain why it is appropriate to accept the residual risk, if that is the decision.

Proposed Implementation Category (Column S): Identify the management process that will be used to implement, test, and monitor proposed actions. Select one of the following three options as the relevant management process: (1) Strategic Review; (2) Budget Formulation Process; or (3) Internal Control Assessment.

Risk Owner POC (Column T): In this column, provide the name of the person accountable for implementing risk response(s) and ensuring that risk mitigation plans are developed and implemented. For cross-cutting risks involving multiple programs across organizations, use the lead coordinator of the risk response. This person also will identify or monitor mitigating controls, if applicable.

Validation (Column U): This is an automatically calculated column and requires no input. This column will identify if a selection was not made where it is required or a wrong combination of selection was made. Review this column prior to submission and getting approval to ensure the accuracy of the Risk Profile.

Table 5 Possible Validation Errors

Possible Validation Errors
▪ If a selection was not made in the *Fraud Impact* column (Column E) from the dropdown menu.
▪ If a *Strategic Objective at Risk* (Column G) is applicable and missing.
▪ If *Operations Objectives*, *Reporting Objectives*, or *Compliance Objectives* is selected for Identification of Objectives (Column F) and "*N/A - Strategic Objective was not selected as an objective in the previous field*" is not selected for *Strategic Objective at Risk* (Column G).
▪ If a *Transfer/ Share Organization* (Column L) is applicable and missing.
▪ If *Accept*, *Avoid*, or *Reduce* is selected for *Current Strategy* (Column J) and "N/A" is not selected for *Transfer/ Share Organization* (Column L).
▪ If *Inherent Risk Rating* for *Impact* and *Likelihood* (Column H & I) are blank.
▪ If the *Residual Risk Impact* and/or *Likelihood* values are greater than the *Inherent Risk Impact* and/or *Likelihood* values. For example, if the *Inherent Risk Rating* is 4 for *Impact* and 4 for *Likelihood*, and the current strategy is to reduce the risk, then selecting a *Residual Risk Impact* or *Likelihood* rating of 5 should not occur.

Residual Risk Score (Column V): This column automatically calculates the residual risk score for each identified risk by multiplying the risk's residual impact (Column O) by the residual likelihood (Column P). A score of 25 reflects the highest possible residual risk rating (5 x 5) and a score of 1 reflects the lowest possible residual risk rating (1 x 1).

U.S. Department of Energy

Office of the Chief Financial Officer

Appendix B

Risk & Internal Controls Application

Overview and Workflow & Reports

User Guide

Version 1.8

November 2021

DOCUMENT REVISION PAGE

Document source: This document is maintained as an online document. Contact the author for the latest version.

Revision history

Version number	Date	Summary of changes	Revised By
1.0	01/30/2019	Document Creation	IDW Team (CF-40)
1.1	03/01/2019	Document Edits	Scott Anderson
1.2	03/24/2020	FY 2020 Update	Bonnie Giampietro
1.3	05/08/2020	FY 2020 Revisions	Stephen Roberts
1.4	06/03/2020	Revisions	Joshua Leutz
1.5	11/13/2020	FY 2021 Update	Stephen Roberts
1.6	10/5/2021	FY 2022 Revisions	Stephen Roberts
1.7	11/15/21	FY 22 Helpdesk Revisions	Wilbert Walker
1.8	11/16/21	FY 22 Helpdesk Final Revisions	Wilbert Walker

Contents

Application Overview

AMERICA is the acronym for **A**-123 **M**anagement of **E**ntity **R**isk and **I**nternal **C**ontrols **A**pplication. It is an application that automates and streamlines the Department's management, reporting, and analysis of risks and controls in compliance with OMB Circular A-123. Reporting Organizations are required to report Entity Assessment (EA), Financial Management Assessment (FMA), Interim Internal Control Status (IICS), or Risk Profiles (upcoming FY 23) under the annual Internal Control Evaluations Guidance. AMERICA Reporting Organizations includes: major contractors and DOE entities such as site offices, field offices, headquarters program offices, and the PMAs (Power Marketing Administration).

Application Modules

AMERICA users (including DOE employees and contractors) will enter information directly into the application. Data can be entered for the current year at any time after the Office of Chief Financial Officer (CF) opens the AMERICA application. This will normally coincide with the issuance of the annual Internal Control Evaluations Guidance. Reporting Organizations will submit and approve assessments within the application. AMERICA will document and track the Reporting Organizations assessment through workflow.

The process of obtaining access to the AMERICA application is provided below.

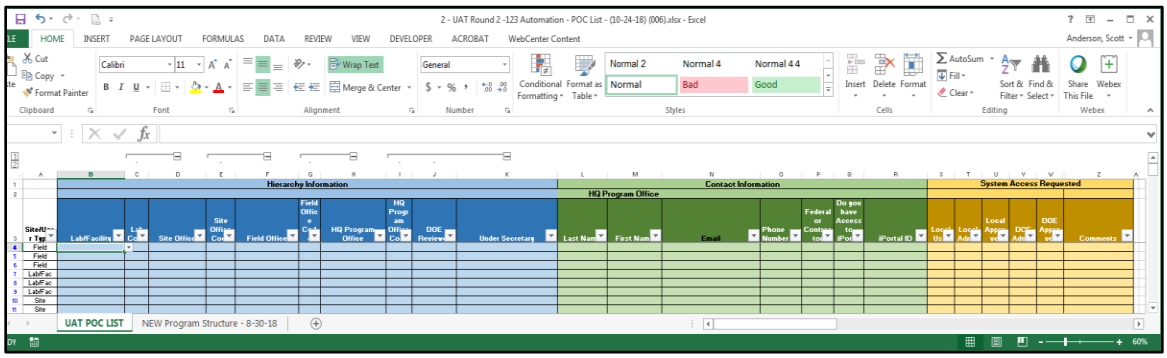
User Access Request

To request an AMERICA user account:

1. To request an AMERICA account, the user contacts the AMERICA Administration (AMERICA Helpdesk) by sending an email to the Internal Controls Support mailbox at:

   AMERICA_A-123_Helpdesk@hq.doe.gov

2. The user will receive an Excel form to complete request of an AMERICA user account, including the entity name and required role(s). Please see the Workflow & Reporting User Guide for definitions of application roles.



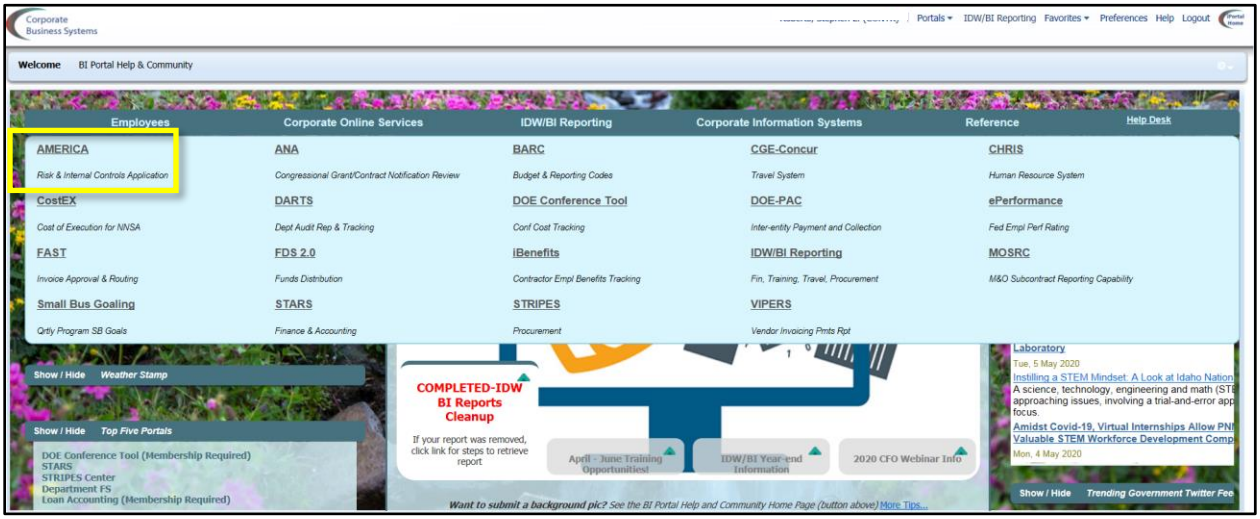
3. Once the completed Excel form is received, the AMERICA Helpdesk will review the user's request and will approve/disapprove the request for access to the application. They will then confirm the user's iPortal account prior to the approval of the request.
4. If the user does not have an existing iPortal account the AMERICA Helpdesk will provide the user-specific instructions on how to obtain an iPortal account, depending on whether that individual is a Federal employee or a contractor. If the individual is a Federal employee, they will receive instructions on how to request an iPortal account through ESS. If the individual is a contractor, then the CF-10 Admin team will work the streamlined two-step contractor process to obtain an iPortal account.
5. The CBS Help Desk will create the user account within the AMERICA application, update the user profile with the associated entity and role(s), and close the ticket.
6. AMERICA Helpdesk will get an email stating the ticket has been closed and that the user account has been created in the AMERICA application.
7. AMERICA Helpdesk will email the user that the request/access has been granted in the AMERICA Corporate Business Application along with:
    a. A description of the User's AMERICA role
    b. Instructions on accessing the application
    c. User Guide
    d. Contact Information if there are questions

Accessing the AMERICA Application

AMERICA is a DOE online application for the process of official U.S. government information only. Users can access AMERICA application through a secure gateway via iPortal or at https://iportalwc.doe.gov/a123

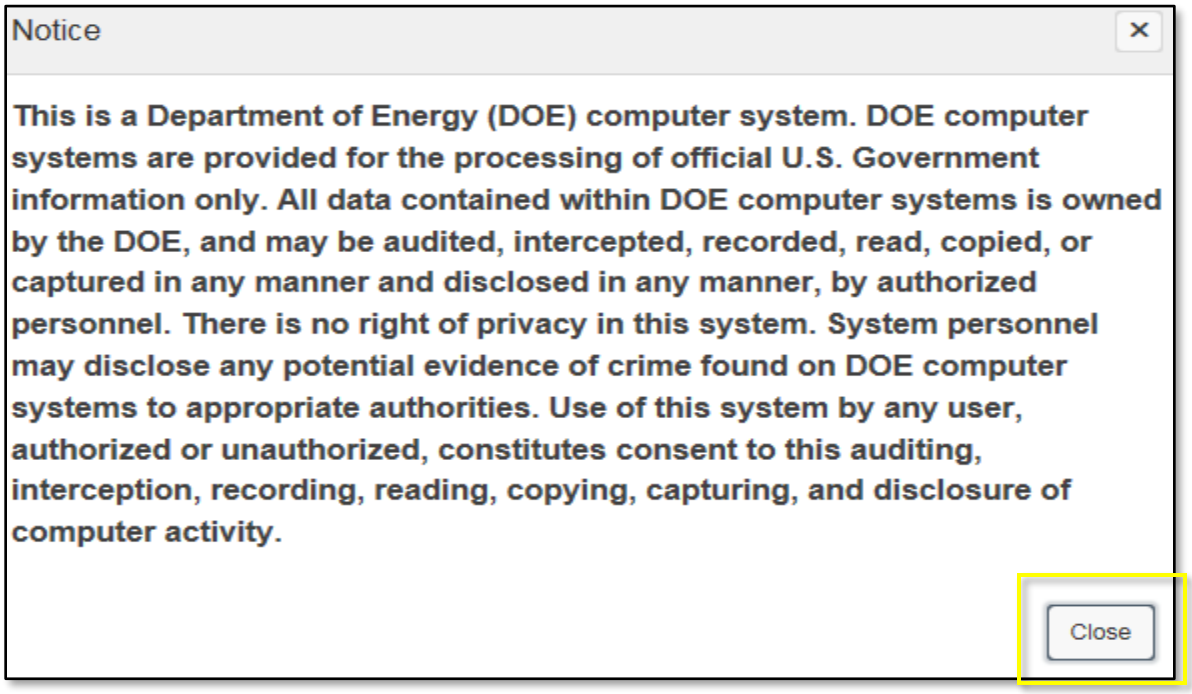
How to Access AMERICA via the iPortal:

1. Using a preferred web browser, enter the web address iPortal.doe.gov
2. iPortal landing page will display; locate and select the login link
3. iPortal credentials may be required
4. iPortal homepage will display. Within the iPortal global menu, select 'Corporate Online Services'
5. A shortcut link to the AMERICA application will display
6. Select the 'AMERICA' shortcut link

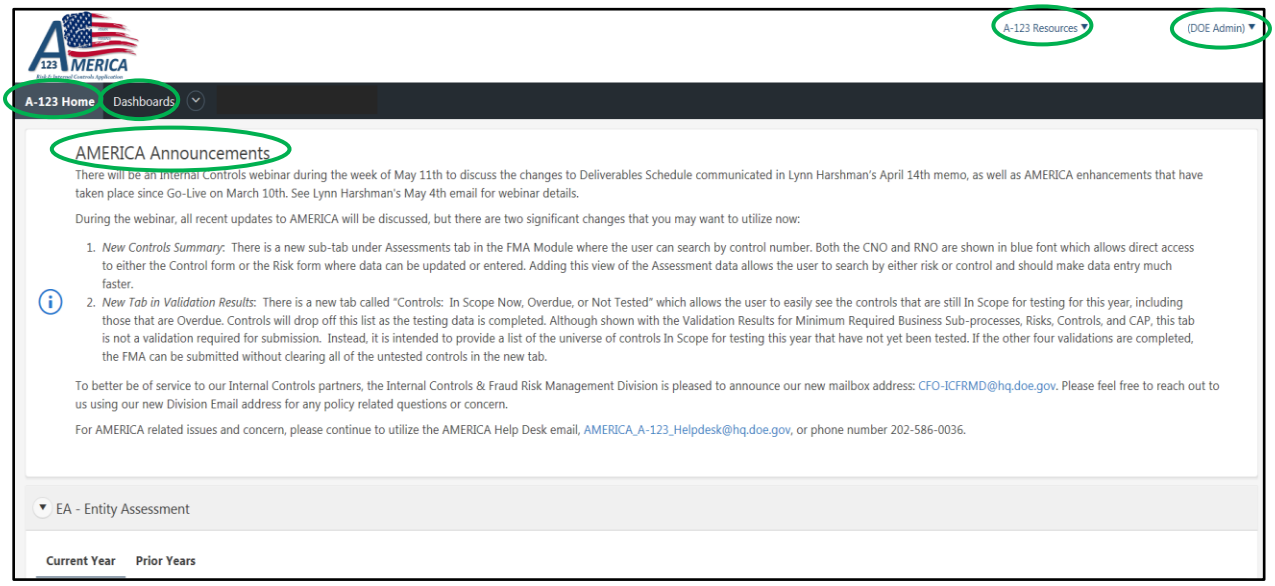


AMERICA Homepage

Once logged in, a security warning is displayed. Review the security message and select 'Close.'



The user's AMERICA homepage is displayed.



Homepage Design and Navigation

The AMERICA homepage is designed to be intuitive and informational. The following resources are displayed on the top global menu:

- **A-123 Home:** Indication of the current page
- **Dashboards:** Menu option for dashboard reports by entity
- **A-123 Resources:** Menu option for System & IC Documentation, including FAQs, User Guide, and guidance is located here along with Help Desk contact information
- **Username (Role):** Displays the user's name and selected role
- **AMERICA Announcements:** Displays information about Internal Controls news, AMERICA updates, and any upcoming due dates

The AMERICA homepage workspace is broken down into sections for each module:

1. EA - Entity Assessment
2. FMA - Financial Management Assurance
3. IICS - Interim Internal Control Status
4. Risk Profile – *Planned for FY23*

The homepage will display the assessments available for an entity and downstream entities within the review hierarchy. Downstream entities' assessments will be read-only.

Each summary table shown presents the following information:

- **Name:** The assigned entity. The entity name will be displayed in blue text, indicating the user has the ability to open and view the assessment
- **Code:** The entity office code
- **Fiscal Year**: This field will automatically populate with the current fiscal year

- **Status:** The current status of the assessment
    - **Working** – Users are currently working on tasks within the assessment
    - **Pending Approval** – Assessment is waiting for approval from the responsible entity
    - **Submission Accepted** – DOE has accepted the Entities assessment
- **Current Office:** The office currently accountable for the assessment
- L**ast Updated Date:** The date and time the assessment was last updated

To view an individual assessment, click on the blue text in the name column, and the assessment will open.

The intention of this user guide is to provide general information regarding the application and access the home page and related features. See Appendix C for details regarding the application modules.

AMERICA Workflow

The AMERICA Workflow: 1) Allows the EA, FMA, and IICS submissions to be reviewed and approved through the Program Hierarchy, and 2) formally documents the review and approval process.

For each EA, FMA, and IICS, a successful validation is required to proceed into workflow. Once all validations have been completed for the EA, FMA, or IICS, Workflow will be available via the Validation and Approval tab on the global menu at the top of the screen.

To begin the Workflow, the Local Admin submits the EA, FMA, or IICS for approval. Upon submission, the document is locked, and no edits/changes can be made to the EA, FMA, or IICS. After the Local Admin has submitted the assessment, the Local Approver will get an email notification that an assessment is ready for review. The Local Approver can either approve the assessment to the next higher level or return the assessment for edits. After the assessment progresses throughout all required levels of the approval hierarchy, the module is submitted to the DOE Reviewer for acceptance or return.

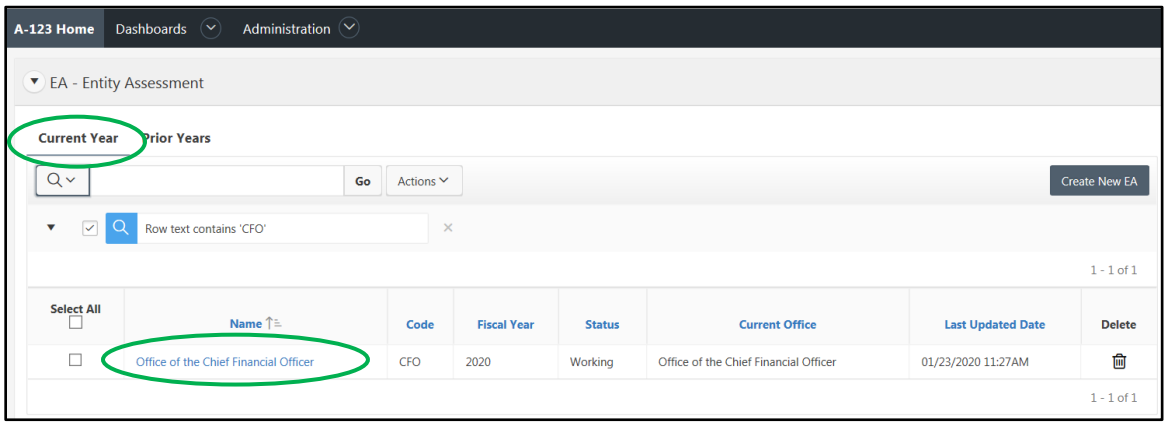
Workflow includes the following:

- Workflow Comments – Add/view an annotation for a workflow status
- Submission Buttons – Submit, approve, or return a submission
- Report Buttons – Select Summary and Detail reports for the submission
- Workflow History – View the current status of the submission, including all workflow actions to date

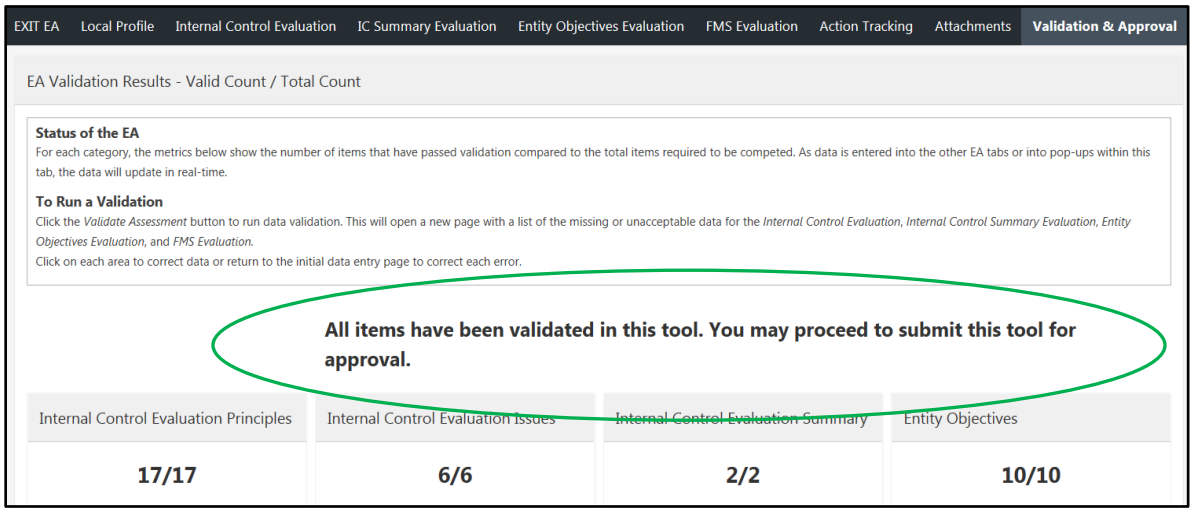
EA/FMA/IICS Workflow

On the AMERICA homepage, locate and navigate to either the EA, FMA, or IICS section. The entity name(s) will be displayed in the blue text within each section, indicating the ability to open and view.

To access the desired EA, FMA, or IICS, click on the entity name under the Current Year sub-tab.



The selected entity EA, FMA, or IICS will be displayed. Locate and select Validation and Approval from the global menu at the top of the screen. If the EA, FMA, or IICS has passed all validations, the statement, *"All items have been validated in this tool. You may proceed to submit this tool for approval."* will appear.



Note: If the EA, FMA, or IICS has NOT passed all validations, the above statement will NOT appear. The entity will need to make corrections until the EA, FMA, or IICS passes all validations before submitting it into Workflow.

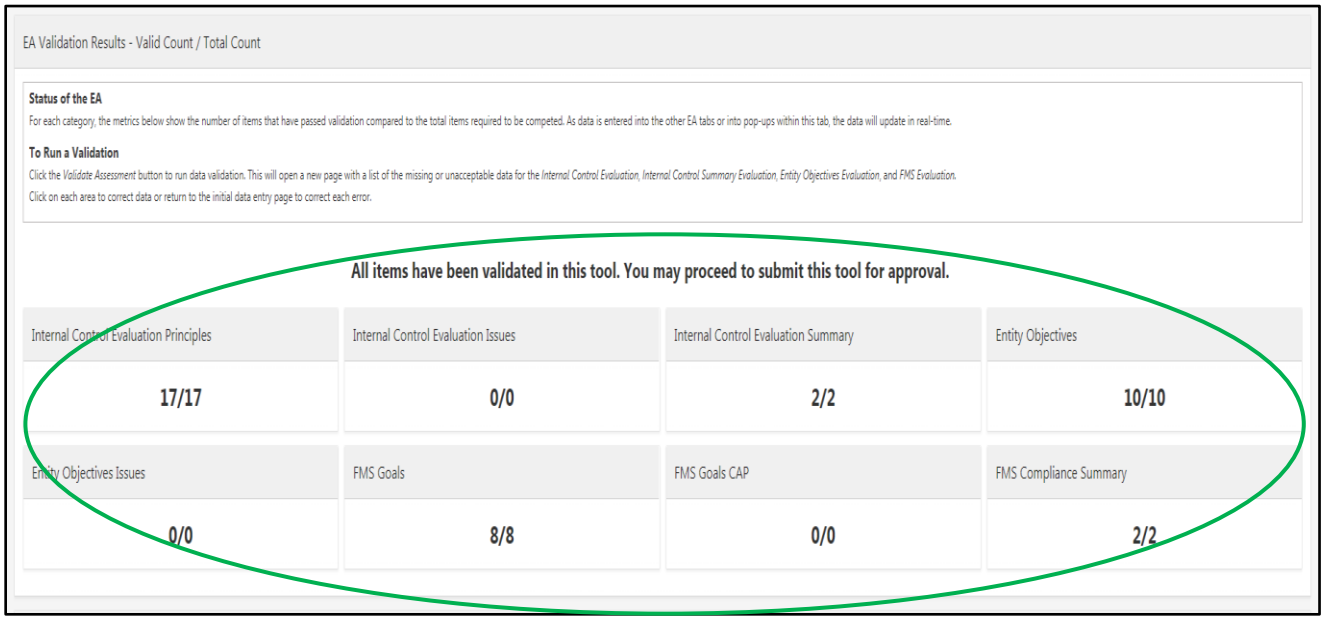
After a successful Validation, the 'Submit for Approval' button will appear.

Note: The "Submit for Approval" button will not appear until all validations have been completed.

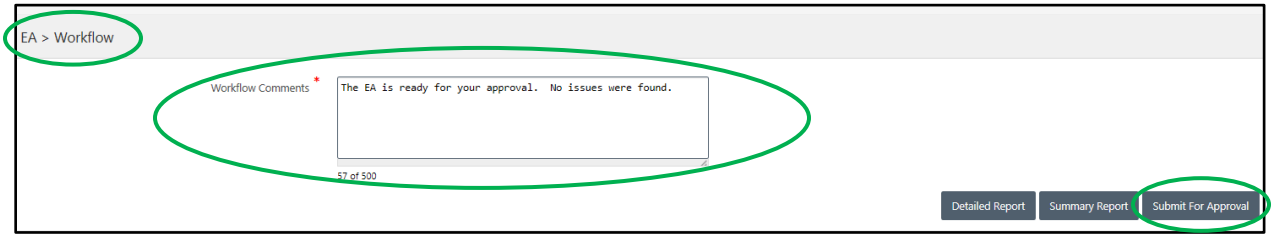
Validation and Approval Tab Overview

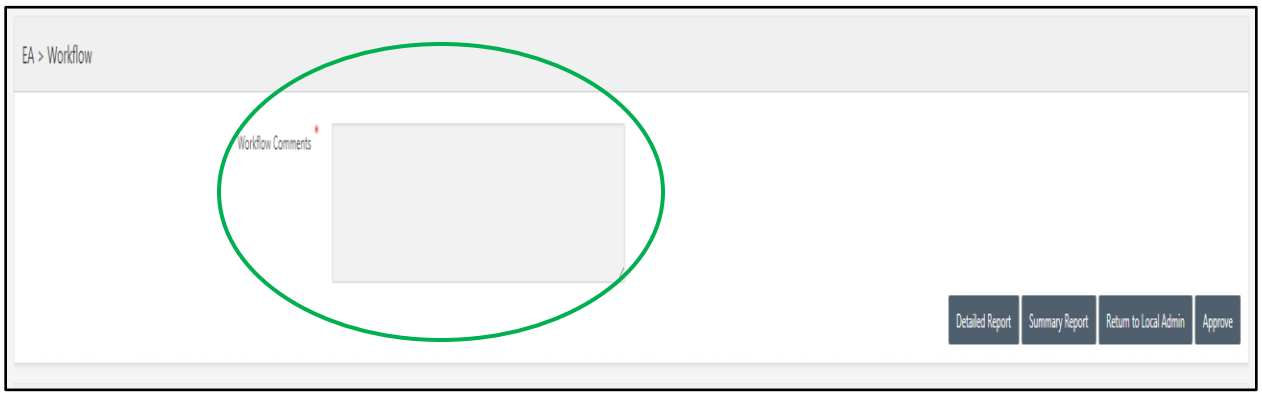
Upon the selection of the Validation and Approval tab, the following will display:

Validation Results – For each category, the metrics display the number of items that have passed validation compared to the total items required to be completed.



Workflow Section: Admins, Approvers, and DOE Reviewers take action (Submit for Approval, Approve, Return to Local Admin, Submit for Acceptance, Accept, etc.) in this section.





- **Workflow Comments**: Workflow comments are required prior to selecting the workflow action of 'Return to Local Admin' or 'Approve.'
- **Report Buttons**

  EA

  - EA Detailed Report: Provides detailed data for Internal Controls, Entity Objectives and, if applicable, Financial Management Systems (FMS)
  - EA Summary Report: Provides an overview of the data from the EA through pie charts and summary tables

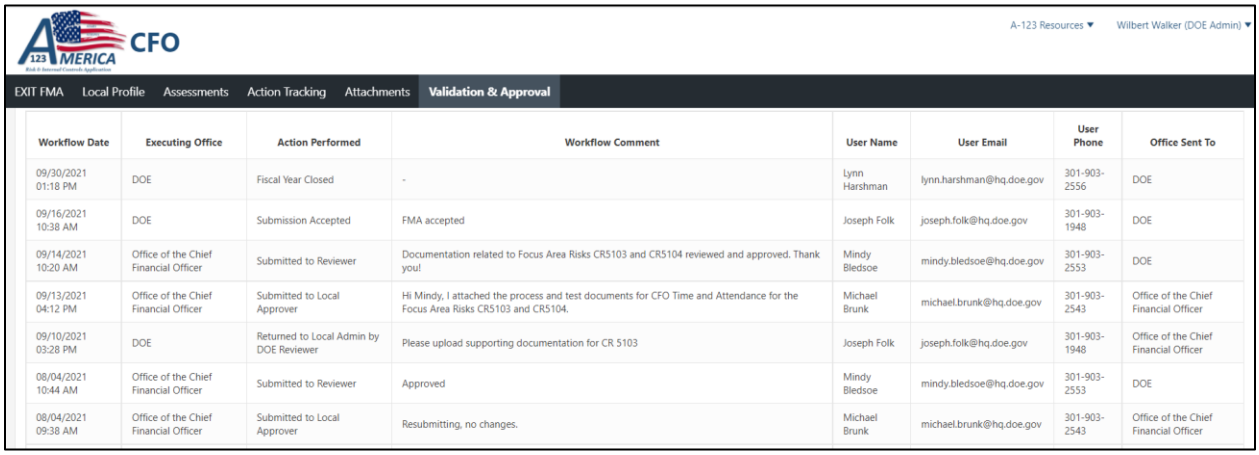
  FMA

  - FMA Detailed Report: Provides detailed data of all Risk and Control data as well as the entity's scope for the current year
  - FMA Summary Report: Provides an overview of the FMA Risks and Control sets as well as the entity's ratings and testing information
- **Action Buttons**
  - **Submit for Approval**: This button is only visible to the selected entity's Local Admin. Upon the selection of the 'Submit for Approval' button, the assessment will be in a read-only state and added to the Local Approver's queue for review and approval
  - **Return to Local Admin**: This button is only visible to Local/Next Level Approvers and DOE Reviewers. Upon the selection of the 'Return to Local Admin' button, the assessment will be opened for modifications and added to the Local User/Admin's queue for review, update, and resubmission
  - **Approve:** This button is only visible to the Local/Next Level Approvers. Upon the selection of the 'Approve' button, the assessment will move upstream within the workflow hierarchy to the Next Level Approver for approval
  - **Submit to DOE Reviewer:** This button is only visible to the Program Office Local Approver. Upon the selection of the 'Submit to DOE Reviewer' button, the DOE Reviewer will be notified (via email) that the assessment is ready to be reviewed for acceptance or return
  - **Accept:** This button is only visible to the DOE Reviewers. Upon selection of the 'Accept' button, the submission is accepted. Local Admins and Approvers and the Next Level Approvers will receive an email notifying of the acceptance

Workflow History Section: Shows the path the EA, FMA, or IICS module has taken through the workflow process. Fields in the table are as follows:

- **Workflow Date:** The date and time the workflow action was taken
- **Executing Office:** The office that took action
- **Action Performed**: The workflow action performed
- **Workflow Comment:** The user adds remarks/information for explanation or reference purposes
- **User Name:** The name of the user who took action
- **User Email:** The email of the user who took action
- **User Phone:** The phone number of the user who took action
- **Office Sent To:** The office currently responsible for the next workflow action

Workflow History



Workflow Date	Executing Office	Action Performed	Workflow Comment	User Name	User Email	User Phone	Office Sent To
09/30/2021 01:18 PM	DOE	Fiscal Year Closed	-	Lynn Harshman	lynn.harshman@hq.doe.gov	301-903-2556	DOE
09/16/2021 10:38 AM	DOE	Submission Accepted	FMA accepted	Joseph Folk	joseph.folk@hq.doe.gov	301-903-1948	DOE
09/14/2021 10:20 AM	Office of the Chief Financial Officer	Submitted to Reviewer	Documentation related to Focus Area Risks CR5103 and CR5104 reviewed and approved. Thank you!	Mindy Bledsoe	mindy.bledsoe@hq.doe.gov	301-903-2553	DOE
09/13/2021 04:12 PM	Office of the Chief Financial Officer	Submitted to Local Approver	Hi Mindy, I attached the process and test documents for CFO Time and Attendance for the Focus Area Risks CR5103 and CR5104.	Michael Brunk	michael.brunk@hq.doe.gov	301-903-2543	Office of the Chief Financial Officer
09/10/2021 03:28 PM	DOE	Returned to Local Admin by DOE Reviewer	Please upload supporting documentation for CR 5103	Joseph Folk	joseph.folk@hq.doe.gov	301-903-1948	Office of the Chief Financial Officer
08/04/2021 10:44 AM	Office of the Chief Financial Officer	Submitted to Reviewer	Approved	Mindy Bledsoe	mindy.bledsoe@hq.doe.gov	301-903-2553	DOE
08/04/2021 09:38 AM	Office of the Chief Financial Officer	Submitted to Local Approver	Resubmitting, no changes.	Michael Brunk	michael.brunk@hq.doe.gov	301-903-2543	Office of the Chief Financial Officer

How to Submit an EA, FMA, or IICS for Approval – Local Admin

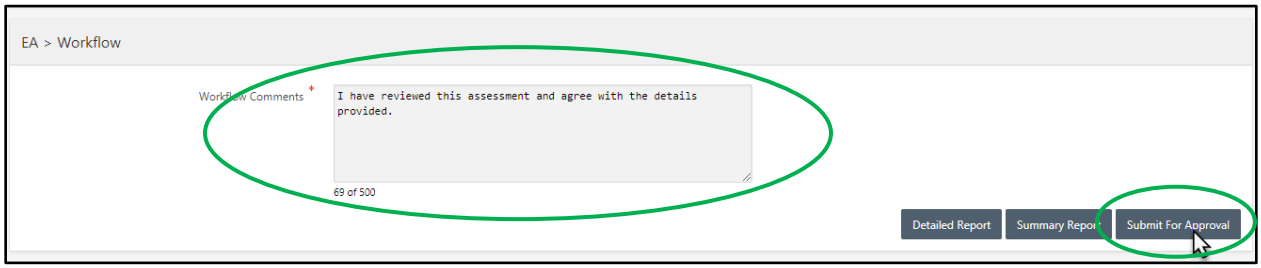
This option is only available to the entity's Local Admin when the EA, FMA, or IICS has passed all validations. To submit to the Local Approver, the Local Admin will:

1. Within the EA, FMA, or IICS, select the Validation & Approval tab
2. The Validation and Workflow page will display. Note the confirmation statement appears in the Validation Results section: "All items have been validated in this tool. You may proceed to submit this tool for approval."
3. Within the Workflow section, enter a comment into the Workflow Comments text box
4. Select the 'Submit for Approval' button. (For the EA/FMA two Report buttons, 'Detailed Report' and 'Summary Report' are available if the Local Admin wants to view these reports prior to submission.)
5. The Submission Confirmation dialog box will display. Review and select 'OK'

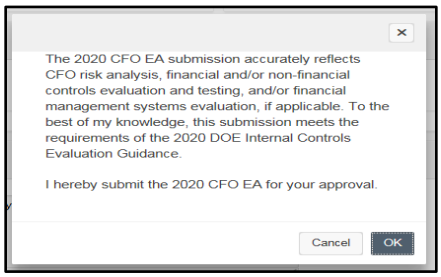
Note: The Workflow History section updates with the submission information. An email notification will be sent to the entity's Local Approver(s) requesting a review and approval. Workflow comments are shown within the notification. The EA, FMA, or IICS is in a 'read-only' state, and no further changes can

be entered unless a Local Approver (at any level) or DOE Reviewer returns the EA, FMA, or IICS for modification.

Workflow - Submit for Approval



Workflow - Submission Confirmation



Workflow – Request for Approval Notification to Local Approver

To: Originating Local Approver(s),

The **FY 2018 EA** – has been submitted by for *your review and approval*.

Individuals listed as To: in this e-mail are required to take action. Those listed as Cc: are being copied for situational awareness only.

To complete your action, please access the FY 2018 EA – at the following URL: A-123 Homepage.

Comments: approve

Thank you,

A-123 Team

If you believe you have received this email in error or do not believe you are the appropriate user to complete the above referenced form, please contact the Help desk for Internal Controls Support at AMERICA_A-123_Helpdesk@hq.doe.gov.

How to Approve an EA, FMA, or IICS – Local Approver

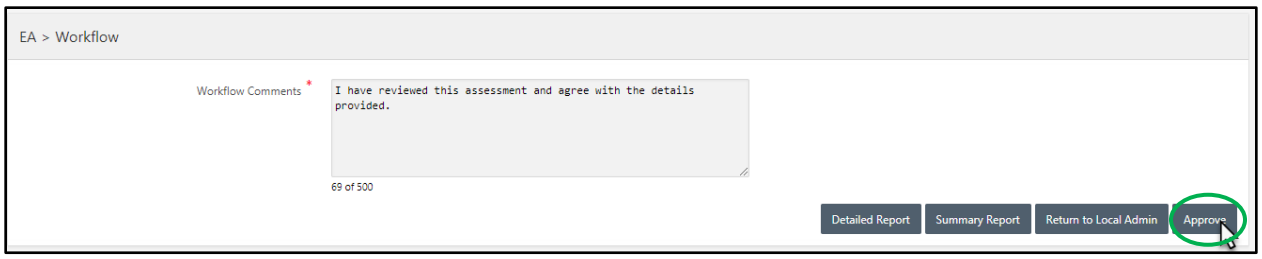
This option is only available to the Local Approver when the EA, FMA, or IICS has been submitted for approval. To approve an EA, FMA, or IICS and submit it to the Next Level Approver, the Local Approver will:

1. Within the EA, FMA, or IICS, select the Validation & Approval tab

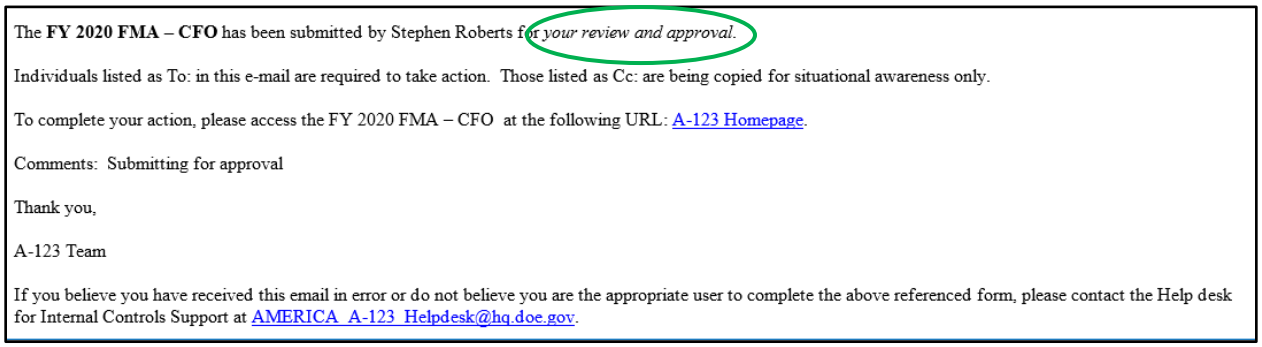
2. The Validation and Workflow page will display. Note the confirmation statement appears in the Validation Results section: “All items have been validated in this tool. You may proceed to submit this tool for approval.”
3. Within the workflow section, enter a comment into the Workflow Comments text box
4. Select the ‘Approve’ button. (For the EA/FMA two Report buttons, ‘Detailed Report’ and ‘Summary Report’ are available if the Local Approver wants to view these reports prior to submission.)
5. The Submission Confirmation dialog box will display. Review and select ‘OK’

Note: The Workflow History section updates with the Approval information. An email notification has been sent to the Next Level Approver(s) requesting to review and approve. Copies sent to the Local Admins. Workflow comments are shown within the notification.

Workflow - Approve



Workflow – Request for Approval Notification



The **FY 2020 FMA – CFO** has been submitted by Stephen Roberts for *your review and approval.*

Individuals listed as To: in this e-mail are required to take action. Those listed as Cc: are being copied for situational awareness only.

To complete your action, please access the FY 2020 FMA – CFO at the following URL: A-123 Homepage.

Comments: Submitting for approval

Thank you,

A-123 Team

If you believe you have received this email in error or do not believe you are the appropriate user to complete the above referenced form, please contact the Help desk for Internal Controls Support at AMERICA_A-123_Helpdesk@hq.doe.gov.

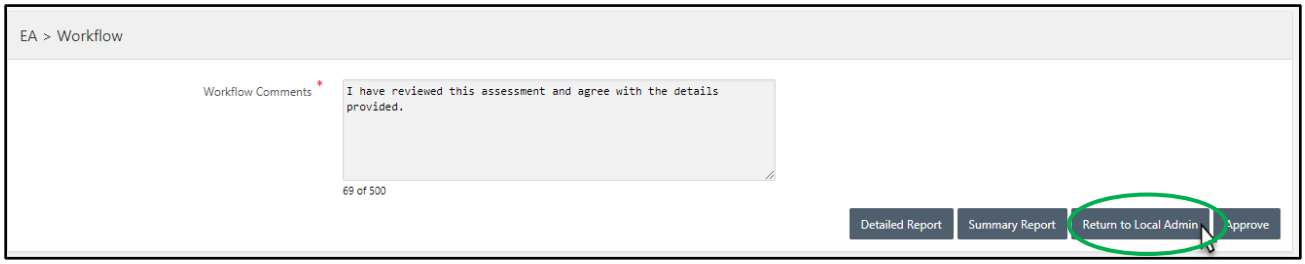
How to Return an EA, FMA, or IICS to Local Admin – Local Approver

This option is only available to Local Approver when the EA, FMA, or IICS has been submitted for approval. The Local Approver will:

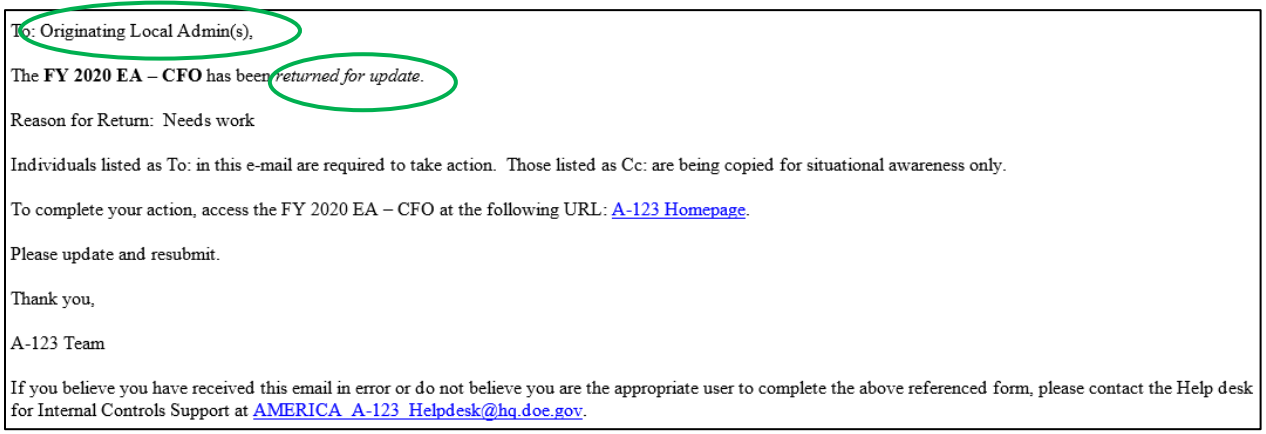
1. Within the EA, FMA, or IICS, select the Validation & Approval tab
2. The Validation and Workflow page will display. Note the confirmation statement appears in the Validation Results section: *“All items have been validated in this tool. You may proceed to submit this tool for approval.”*
3. Within the workflow section, enter a comment into the Workflow Comments text box
4. Select the ‘Return to Local Admin’ button
5. The Submission Confirmation dialog box will display. Review and select ‘OK’

Note: The Workflow History section updates with the Return information. An email notification has been sent to the Local Admin(s) requesting updates and resubmission, with copies to applicable Users. Workflow comments are shown within the notification.

Workflow - Return to Local Admin



Workflow – Return for Update



To: Originating Local Admin(s),

The **FY 2020 EA – CFO** has been *returned for update*.

Reason for Return: Needs work

Individuals listed as To: in this e-mail are required to take action. Those listed as Cc: are being copied for situational awareness only.

To complete your action, access the FY 2020 EA – CFO at the following URL: A-123 Homepage.

Please update and resubmit.

Thank you,

A-123 Team

If you believe you have received this email in error or do not believe you are the appropriate user to complete the above referenced form, please contact the Help desk for Internal Controls Support at AMERICA_A-123_Helpdesk@hq.doe.gov.

NOTE: For the EA, FMA, or IICS, the approval process continues through all program hierarchy levels. The Next Level Approvers' action to Approve or Return to Local Admin is similar to the Local Approver shown above.

How to Submit an EA, FMA, or IICS to DOE Reviewer – Program Office Local Approver

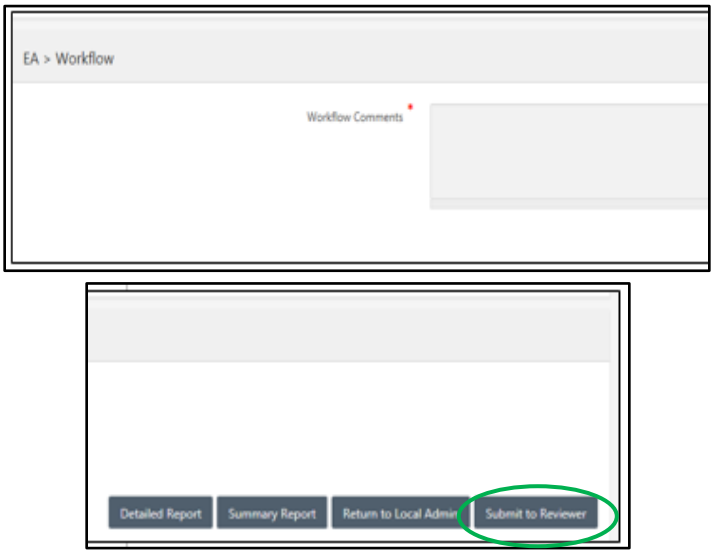
This option is only available to the Local Approver at the Program Office level when the assessment has been submitted for approval. To submit an assessment to the DOE Reviewer, the Program Office level Local Approver will:

1. Within the EA, FMA, or IICS assessment, select the Validation & Approval tab
2. The Validation and Workflow page will display. Note the confirmation statement appears in the Validation Results section: a message appears in the Validation Results section: "All items have been validated in this tool. You may proceed to submit this tool for approval."
3. Within the workflow section, enter a comment into the Workflow Comments text box
4. Select the 'Submit to DOE Reviewer' button
5. The Submission Confirmation dialog box will display. Review and select 'OK'

Note: The Workflow History section updates with the Approval and Submission to DOE Reviewer information. An email notification has been sent to the DOE Reviewer(s) requesting review and

acceptance, with copies to all lower-level Admins and Approvers. Workflow comments are shown within the notification.

Workflow – Submit to DOE Reviewer



Workflow – Request for Acceptance

To: DOE Reviewer(s),

The **FY 2020 EA – CFO** has been submitted for *your review and acceptance.*

Individuals listed as To: in this e-mail are required to take action. Those listed as Cc: are being copied for situational awareness only.

To complete your action, access the FY 2020 EA – CFO at the following URL: A-123 Homepage.

Comments: EA Approved

Please contact Bonnie Giampietro at 301-903-4666 if you have questions about this submission.

Thank you,

A-123 Team

If you believe you have received this email in error or do not believe you are the appropriate user to complete the above referenced form, please contact the Help desk for Internal Controls Support at AMERICA_A-123_Helpdesk@hq.doe.gov.

Final Submissions

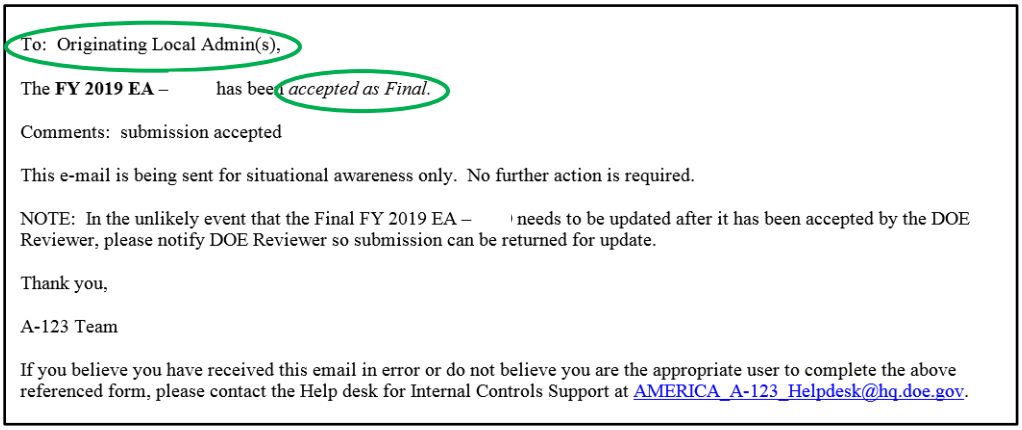
Once all Approvers have approved the assessment within the entity's hierarchy, it will be placed in the DOE Reviewer queue. The DOE Reviewer will review and either accept the submission if it meets acceptance criteria or returns for modification.

If not accepted, the DOE Reviewer will return the assessment for revisions. A system notification will be sent to the submitting lower level Local Administrator(s), with copies to the all applicable lower level Local Approvers, as notification that the submission was not accepted and needs to be modified. Notification will include Workflow Comments and the Summary Report. The DOE Reviewer must include a reason for the return.

If the assessment was accepted and approved, the submission is considered final, and the EA, FMA, or IICS remains in a 'read-only' state. If accepted, a notification is sent to the submitting Local Administrator with a copy to all lower-level Approvers within the hierarchy.

NOTE: At any time, even after the submission was accepted, the DOE Reviewer will have the ability to return an assessment for additional modifications before the fiscal year closeout.

Workflow – DOE Reviewer Acceptance Email Notification



To: Originating Local Admin(s),

The **FY 2019 EA** – has been *accepted as Final.*

Comments: submission accepted

This e-mail is being sent for situational awareness only. No further action is required.

NOTE: In the unlikely event that the Final FY 2019 EA – needs to be updated after it has been accepted by the DOE Reviewer, please notify DOE Reviewer so submission can be returned for update.

Thank you,

A-123 Team

If you believe you have received this email in error or do not believe you are the appropriate user to complete the above referenced form, please contact the Help desk for Internal Controls Support at AMERICA_A-123_Helpdesk@hq.doe.gov.

AMERICA Reporting

AMERICA's standard reports are referred to as Dashboard reports and can be accessed through the Dashboards tab on the AMERICA Homepage. Dashboard reports provide a summary overview of all data input or details of specific items of interest such as issues, CAPs, ratings, and/or status of progress through the workflow. End users will have access to all Dashboard reports for the user's assigned entity and any downstream entities.

Dashboard Reports

The Dashboards tab will have dropdown menus available with reports for each module. Below are the reports with descriptions:

EA

- Progress Reports: Illustrate the workflow status and progression for active EA tools
- Workflow History Reports: Illustrates the flow of actions from one entity to the next, including details on the approvals and returns throughout the process. This is the same report that displays in the EA in the Validation and Approval section.
- Summary Reports - Workflow: This report illustrates an overview of the data input from the EA utilizing pie charts and summary tables
- Detailed Reports - Workflow: This report displays information about the EA (Principles, Objectives, and Goals) at a high level. The report also contains information about any Issues or CAPs that were created.

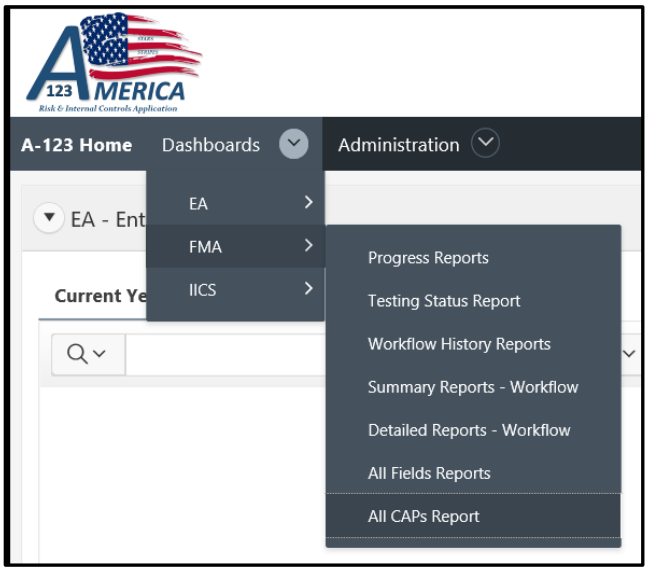
- All Fields Reports: This report provides all fields and input from the EA for a given entity or multiple entities

Dashboard Reports - EA

FMA

- Progress Reports: Illustrates the workflow status and progression for active FMA tools
- Testing Status Report: The FMA Testing Status report displays: test status at rollover, the current test status, and the percentages and counts for Control testing of each entity
- Workflow History Reports: Illustrates the flow of actions from one entity to the next, including details on the approvals and returns throughout the process. This is the same report that displays in the FMA in the Validation and Approval section.
- Summary Reports – Workflow: This report illustrates an overview of the FMA Risks and Control Sets as well as ratings and testing information through pie charts and summary tables
- Detailed Reports – Workflow: This report provides a detailed analysis of all risk, control data, and scope status for the current year
- All Fields Reports: This report provides all fields and input from the FMA Assessments tab for a given entity or multiple entities
- All CAPs Report: This report provides all fields and inputs from the FMA module's Corrective Action Plans

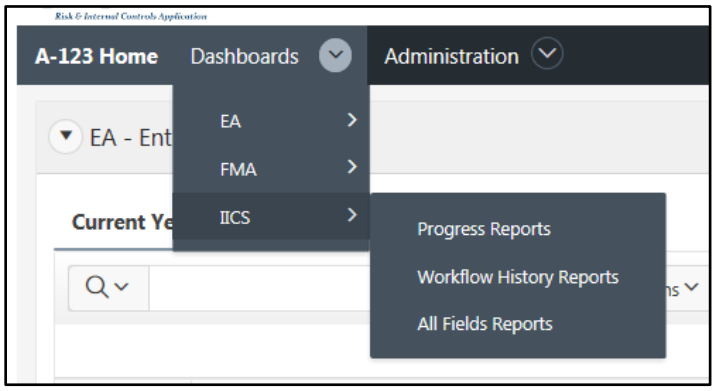
Dashboard Reports - FMA



IICS

- Progress Reports: Illustrates the workflow status and progression for active IICS tools
- Workflow History Reports: The table report illustrates the flow of actions from one entity to the next, including details on the approvals and returns throughout the process. This is the same report that displays in the assessment in the Validation and Approval section.
- All Fields Reports: This report provides all fields and input from the IICS for a given entity or multiple entities

Dashboard Reports - IICS



Dashboard Report Functionality

Dashboard Reports in AMERICA are formatted in 3 different types of layouts. They are:

- Reports with filter/query selection
- Reports with filter and the ability to select multiple entities
- Reports without filter/query selections

Please note you must select the fiscal year first before a report can be generated!

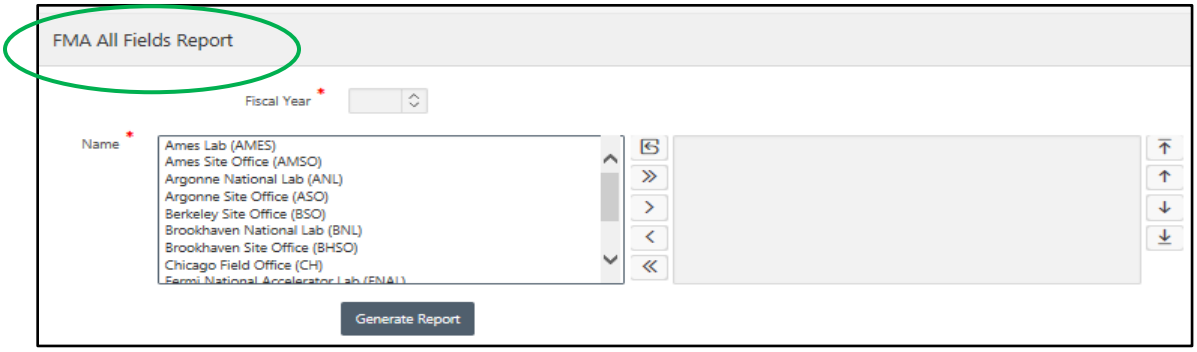
Reports with filter/query selections

Reports with filter/query selections will have the following layout:

- Dashboard Report Name
- Fiscal Year: (Required) Make a selection from the dropdown
- Name: (Required) The dropdown list will be based on the user assigned entity and any potential downstream entities
- Generate Report button: The Fiscal Year and Name must be populated to generate a report when this button is selected

Reports with filter and the ability to select multiple entities

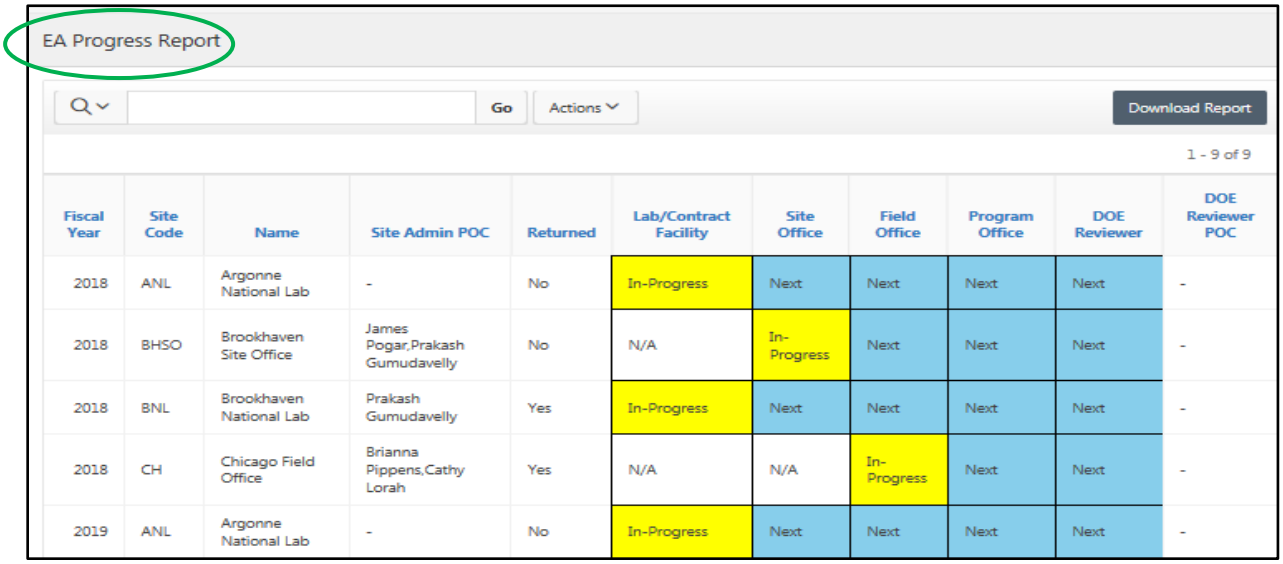
The All Fields Report and FMA All CAPs Reports has a slightly different layout that allows for selecting multiple entities. The Name selection box is limited based on the user's assigned entity and any potential downstream entities.



Reports without filter/query selections

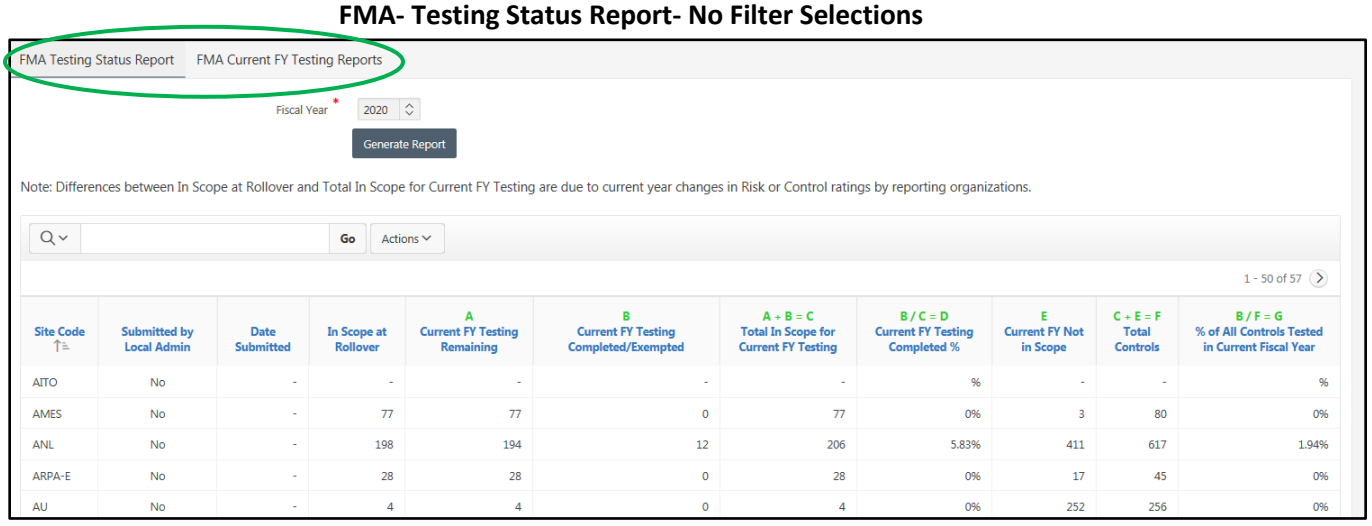
Reports with no filter/query selection will automatically display results based on the user's assigned entity and potential downstream entities. These reports are the EA, FMA, and IICS Progress Reports and the FMA Testing Status Report.

EA- Progress Report – No Filter Selections



Fiscal Year	Site Code	Name	Site Admin POC	Returned	Lab/Contract Facility	Site Office	Field Office	Program Office	DOE Reviewer	DOE Reviewer POC
2018	ANL	Argonne National Lab	-	No	In-Progress	Next	Next	Next	Next	-
2018	BHSO	Brookhaven Site Office	James Pogar,Prakash Gumudavelly	No	N/A	In-Progress	Next	Next	Next	-
2018	BNL	Brookhaven National Lab	Prakash Gumudavelly	Yes	In-Progress	Next	Next	Next	Next	-
2018	CH	Chicago Field Office	Brianna Pippens,Cathy Lorah	Yes	N/A	N/A	In-Progress	Next	Next	-
2019	ANL	Argonne National Lab	-	No	In-Progress	Next	Next	Next	Next	-

FMA- Testing Status Report- No Filter Selections



Site Code	Submitted by Local Admin	Date Submitted	In Scope at Rollover	A Current FY Testing Remaining	B Current FY Testing Completed/Exempted	A + B = C Total In Scope for Current FY Testing	B / C = D Current FY Testing Completed %	E Current FY Not in Scope	C + E = F Total Controls	B / F = G % of All Controls Tested in Current Fiscal Year
AITO	No	-	-	-	-	-	%	-	-	%
AMES	No	-	77	77	0	77	0%	3	80	0%
ANL	No	-	198	194	12	206	5.83%	411	617	1.94%
ARPA-E	No	-	28	28	0	28	0%	17	45	0%
AU	No	-	4	4	0	4	0%	252	256	0%

Downloading a Report

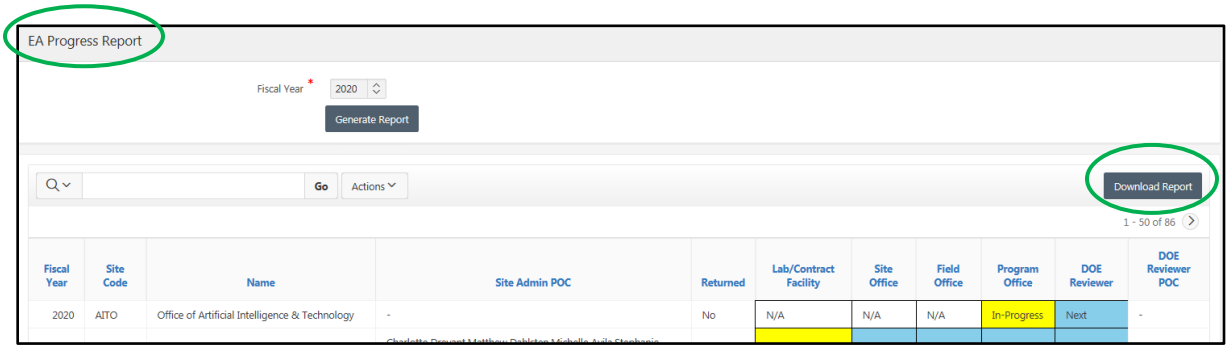
Reports can be downloaded in two different ways: "Download Report" button or through the "Actions" menu.

Download Report

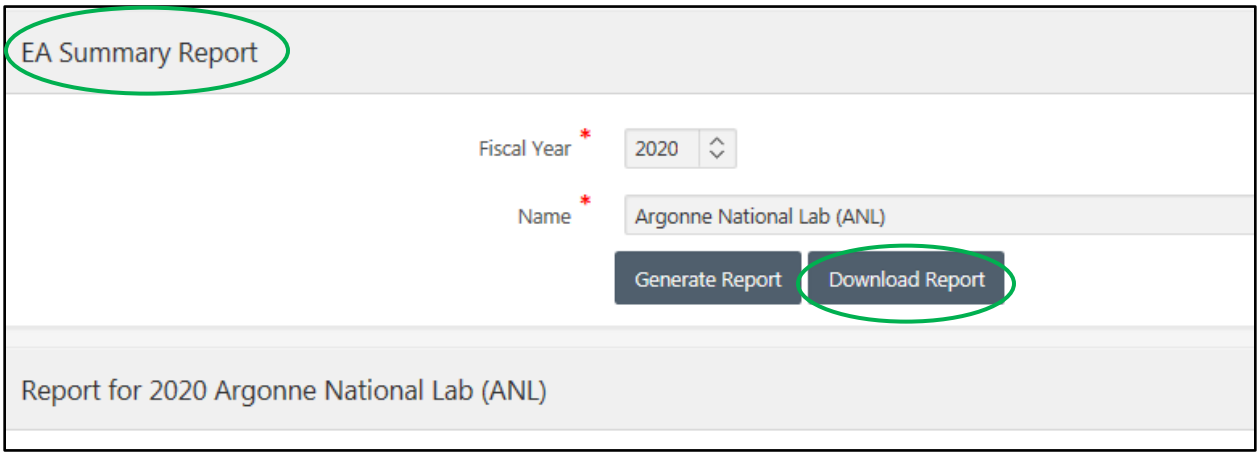
Once you are finished generating a report, the "Download Report" button will display. Using this option, the export will maintain the color coding and formatting shown in the Dashboard report.

- EA Progress Reports
- EA Summary Report – Workflow
- EA Detailed Report – Workflow
- FMA Progress Reports
- FMA Summary Report – Workflow
- FMA Detailed Report – Workflow
- IICS Progress Reports

"Download Report" Button – EA Progress Report



Download using "Download Report" Button



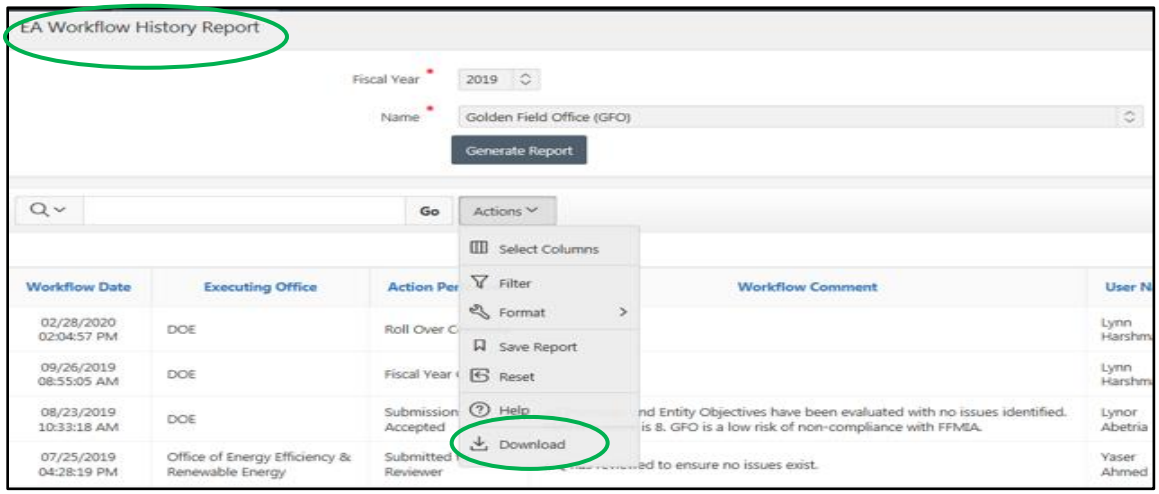
Actions Menu

Once the menu dropdown is open select the last option, "Download". A pop-up window will appear in which the user can select the desired format for the information to be displayed.

The following reports can be downloaded by using the Actions menu.

- EA Workflow History Report
- EA All Fields Reports
- FMA Testing Status Report
- FMA Workflow History Report
- FMA All Fields Reports
- FMA All CAPs Report
- IICS All Fields Reports

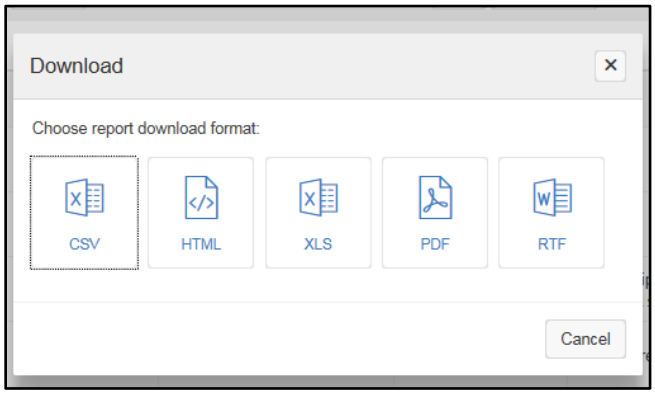
Download using "Download" from Actions Menu



The report can be downloaded in the following formats:

- CSV
- HTML
- XLS
- PDF
- RTF

Download Formats



Role Descriptions

The AMERICA application has the following User Roles:

DOE Entities	DOE CF-TEAM
Local User	DOE Admin (Administrator)
Local Admin (Administrator)	DOE Reviewer
Local Approver	DOE Approver
CBS Helpdesk	

Role *	**Functionality**
Local User	Has the ability to: • Read and perform data entry in all Modules within the organization the user is listed is assigned to. • Run both standard and ad-hoc reports and export them to Excel or PDF • Access historical data on a read-only basis • Upload documents to the application
Local Admin (Administrator)	Has all the capabilities of Local Users, plus the ability to: • Add information to a local profile • Add/delete sub-processes in FMA • Submit into workflow to the Local Approver for review/approval
Local Approver	Is responsible for: • Reviewing and approving or returning the site's submission • Reviewing and approving or returning any lower-level hierarchical organization
DOE Admin (Administrator)	The DOE Admin abilities are: • Permissions to all entities. • Access to administrative functions in each module, such as adding/deleting entity objectives and issue categories. • DOE Admin has read-only access to the User list. • Access to the A-123 Trace Log. • Update the AMERICA Announcements section
DOE Reviewer	Has access to review data (read-only) and accepts submissions from all entities.
DOE Approver	Has access to review data (read-only) from all entities.
CBS Help Desk	Has access to add users, update assigned entity and role(s), and delete users. Also has read only access to data from all entities.

* Most users will only have one role at any given time. Users can have multiple roles in certain limited situations if approved by the entity's Local Admin and the DOE Admin.

Information Security

The AMERICA application may contain Sensitive Unclassified Information (SUI). However, AMERICA should, under no circumstance, include any Personally Identifiable Information.

Sensitive Unclassified Information (SUI)

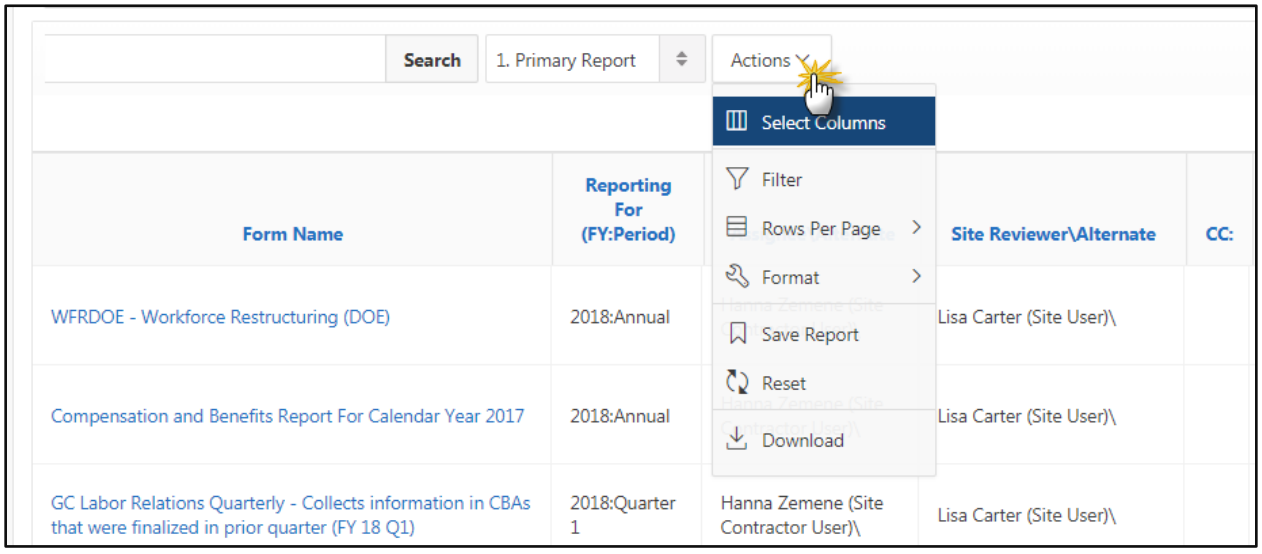
- **Transport:** Any SUI which is transported on portable devices (laptops, CDs, thumb drives, etc.) must be encrypted according to FIPS 140-2 standards
- **Electronic Transport:** Transport as defined above includes email or data as well as access from a location other than a DOE facility work location
- **Physical Transport:** Sensitive documents in hard copy are transported in an opaque, sealed envelope
- **Destruction:** Any SUI stored on removable media must be reviewed every 90 days and deleted if not needed
- **Theft:** Suspected theft of device with SUI must be reported within 45 minutes

Personally Identifiable Information (PII)

- **No PII in AMERICA:** Absolutely NO personally identifiable information is to be uploaded or stored on the AMERICA application.
- **Census Data:** Any census data that is uploaded must be cleansed of all PII prior to upload.
- **Removal of PII Identified:** If PII is discovered on the application,
  - It must be deleted immediately
  - The System Owner and AMERICA Admin must be notified immediately
  - If the user cannot delete the PII data, the AMERICA Admin will remove it

Search Bar and Actions Menu

AMERICA – Search Bar and "Actions" Menu



The majority of pages contain data shown via Interactive Report. The Search Option and Action Menu are the primary tools to locate the information needed within an Interactive Report.

The layout can be altered by selecting columns, applying filters, highlighting, sorting, and have the ability to define breaks based on a value. Multiple variations of a report can be created and saved as named reports for a private viewing.

The following summarizes ways to customize an interactive report.

Search Bar

At the top of each report is a search region. This region (or Search bar) provides the following features:

- **Text area** enter (case insensitive) search criteria (wild card characters are implied)
- **Search button** executes the search. Hitting the enter key will also execute the search when the cursor is in the search text area.
- To the immediately to the right of the 'Search' button will be a dropdown list that includes any saved reports and the primary report.

Actions Menu

The Actions Menu appears to the right of the search bar. Use this menu to customize an interactive report.

Select Columns

The columns listed on the right will be displayed on the report. The columns on the left are hidden. Use the arrows in the center to move the columns. Displayed columns can be reordered by using the arrows on the far right.

Filter

Set conditions so that only certain data is displayed; it is done to make it easier to focus on specific information in a large dataset.

Format

Format enables the user to customize the display of the report. Format contains the following options:

Sort

Used to change the columns to sort on and determines whether to sort in ascending or descending order. The user can also specify how to handle Null values. The resulting sorting displays to the right of column headings in the report.

Control Break

Used to create a break group on one or several columns. This pulls the columns out of the interactive report and displays them as a section heading.

Highlight

This enables a condition to be highlighted. The rows that meet the criteria display as highlighted using the characteristics associated with the filter. Options include:

- **Name** is used only for display.
- **Sequence** identifies the sequence in which the rules are evaluated.
- **Enabled** identifies if a rule is enabled or disabled.
- **Highlight Type** identifies whether the row or cell should be highlighted.
- **Background Color** is the new color for the background of the highlighted area.
- **Text Color** is the new color for the text in the highlighted area.
- **Highlight Condition** defines the user's criteria by column.

Save Report

To save a customized report for the future, provide a name and an optional description. The report is saved as a private report. Only the end-user that created the report can view, save, rename, or delete the report.

If customized reports is created then a search bar will be displayed in the Reports selector.

Reset

Resets the report back to the default settings, removing any customizations made.

Download

Enables the current result set to be downloaded. The downloadable formats are CSV, HTML, Email, XLS, PDF, and RTF.

Column Heading Options

Clicking on any column heading exposes a column heading menu. Not all options are available for every column, as some options do not apply and will not be shown.

- **Sort Ascending** icon sorts the report by the column in ascending order
- **Sort Descending** icon sorts the report by the column in descending order
- **Hide Column** hides the column. Not all columns can be hidden. If a column cannot be hidden, there will be no Hide Column icon.
- **Control Break** creates a break group on the column. This pulls the column out of the report as a master record.
- **Highlight** used to define a filter. The rows that meet the filter criteria display as highlighted using the characteristics associated with the filter. Options include:
    - **Name** is used only for display
    - **Sequence** identifies the sequence in which the rules are evaluated
    - **Enabled** identifies if a rule is enabled or disabled
    - **Highlight Type** identifies whether the row or cell should be highlighted. If Cell is selected, the column referenced in the Highlight Condition is highlighted.
    - **Background Color** is the new color for the background of the highlighted area
    - **Text Color** is the new color for the text in the highlighted area
    - **Highlight Condition** defines the user's filter condition

EA/FMA/IICS Workflow Process and Procedures

Below illustrates the step-by-step process and procedures of the workflow model.

Step	Role	Step Description	Step Details	Automatic Notification
1	Local User	Enter Data for own organization.	The system will have automatic data input edit checks. It will alert the user if the entry does not meet input criteria, with a brief explanation for why the entry was not accepted.	None
2	Local User	Notify Local Administrator that data entry is complete.	The user notifies the Local Administrator that submission is ready for review/consolidation outside of the system.	None
3	Local Administrator	Consolidate, edit, and validate data.	The Local Administrator consolidates and/or edits input data, ensures data is complete and accurate, and completes validation.	None
4	Local Administrator	Run Summary Report.	The EA and FMA Summary Reports are available directly on the Workflow tab or from the Dashboards tab. The Local Administrator can review and save the report.	None
5	Local Administrator	Submit data to the Local Approver.	The Local Administrator submits the assessment to the Local Approver. If the submission is a 'returned' submission that has been updated, the Local Administrator must provide an explanation of changes made in response to the Approver's returned Notification. Note: Data is automatically locked upon submission to prevent further changes.	Local Approver for own level
6	Local Approver	Approve or return submission to Local Administrator.	Local Approver will review submission (received from Local Administrator) and either approve or return submission. If returned, send back to the Local Administrator. If approved, send it to the Next Level Approver.	If approved - Local Administrator and Next Level Approver If returned - Local Administrator, with a copy to the applicable users

Step	Role	Step Description	Step Details	Automatic Notification
7	Next Level Approver	Approve or Return to Submitting Local Administrator.	Next Level Approver reviews the submission and either approves or returns to the Local Administrator for revision. Next Level Approvals are based on the Originating Office and the Program Structure. The submission works through the approver levels (i.e., Site Office, Field Office, and/or HQ Office) as needed. If approved, notification of approval will be sent to the Next Level Approver. It will also be sent with copies to the lower-level Approver(s), Administrators, and the submitting Local Administrator, including the Summary Report and Workflow comments. Upon HQ Office approval, the submission is forwarded to the DOE Reviewer. The Notification will include Workflow Comments and the Summary Report.	If approved - Next Level Approver(s) until it reaches HQ Office Approver, with a copy to submitting Local Administrator, lower-level Approvers and Administrators If returned - Submitting Local Administrator, with a copy to Submitting Approver, lower-level Approvers and Administrators
8	Next Level Approver	Return to Local Administrator	If the assessment is returned by any Next Level Approver, notification of the return will be sent to the Local Administrator for update, with copies to submitting Approver and any lower level Approvers and Administrators. Notification will include Workflow Comments, and the Approver must provide a reason for the return in the Comment box. The Next Level Approver can also give direction to the Local Administrator (via Comment box) for the re-Approval process.	If approved - Next Level Administrator(s) until it reaches HQ Office Administrator; copy to submitting Local Administrator, lower level Approvers and Administrators If returned - Submitting Local Administrator; copy to Submitting Approver, lower level Approvers and Administrators
9	Local Administrator	Update submission and resubmits the assessment to the Local Approver.	The Local Administrator updates the submission.	None

Step	Role	Step Description	Step Details	Automatic Notification
10	Local Approver	Approve or return submission to Local Administrator.	Local Approver will review submission (received from Local Administrator) and either approve or return submission. If returned, send back to the Local Administrator. If approved, send to Next Level Approver.	If approved - Local Administrator and Next Level Approver If returned - Local Administrator, with copy to applicable Users
11	Next Level Approver	Approve or Return?	If approved by the HQ Office Approver, the submission goes to the DOE Reviewer. If not approved, the submission goes back to the submitting Local Administrator.	If approved by HQ Office Approver level, DOE Reviewer with copy to the lower level Administrators and Approvers. If not approved, submitting Local Administrator with copy to all lower level Approvers
12	DOE Reviewer	Accept submission or return to Submitting Local Administrator.	The DOE Reviewer will review and either accept the submission if it meets acceptance criteria or return for correction. If not accepted, a notification will be sent to the submitting Local Administrator, with copies to all applicable Approvers, to notify that the submission was not accepted and needs to be corrected. Notification will include Workflow comments and the Summary Report. The DOE Reviewer must include a reason for the return. If the submission is accepted, the submission is considered Final.	In either case, submitting Local Administrator with copy to all lower level Approvers and Administrators within hierarchy
13	DOE Reviewer	When accepted, submission is Final.	When accepted, the submission is considered final and input remains locked. NOTE: If User/Local Administrator needs to update after a submission is accepted by the DOE Reviewer, they must notify DOE Reviewer so submission can be returned for update.	When accepted, submitting Administrator with copy to all lower level Approvers within hierarchy

U.S. Department of Energy

Office of the Chief Financial Officer

Appendix C

Entity Assessment, Interim Internal Control Status, and Financial Management Assessment Modules

User Guide

Version 2.5

October 2021

DOCUMENT REVISION PAGE

Document source: This document is maintained as an online document. Contact the author for the latest version.

Revision history

Version number	Date	Summary of changes	Revised By
1.0	01/30/2019	Document Creation	IDW Team (CF-40)
1.1	02/19/2019	Document Edits	Kearney & Company
1.2	02/28/2019	Document Edits	Scott Anderson
1.3	03/15/2020	2020 Update	Lyn Henderson
1.4	04/07/2020	Document Edits	Joshua Leutz
1.5	04/21/2020	Document Edits	Lyn Henderson
2.0	05/07/2020	Document Edits	Lyn Henderson
2.1	05/07/2020	Revisions	Stephen Roberts
2.2	06/04/2020	Revisions	Joshua Leutz/Stephen Roberts
2.3	11/16/2020	Document Edits	Lyn Henderson
2.4	11/30/2020	2021 Updates	Stephen Roberts
2.5	10/27/2021	2022 Updates	Wilbert Walker
2.6	11/15/2021	FY 22 Helpdesk Revisions	Wilbert Walker
2.7	11/16/2021	FY 22 Helpdesk Final Revisions	Wilbert Walker

Contents

Entity Assessment (EA) Module

The Entity Assessment (EA) module is used to conduct structured self-evaluations to provide reasonable assurance that internal control systems are designed and implemented and operating effectively to mitigate risk and validate mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulations.

The EA module will capture the most critical supporting information of these evaluations, including:

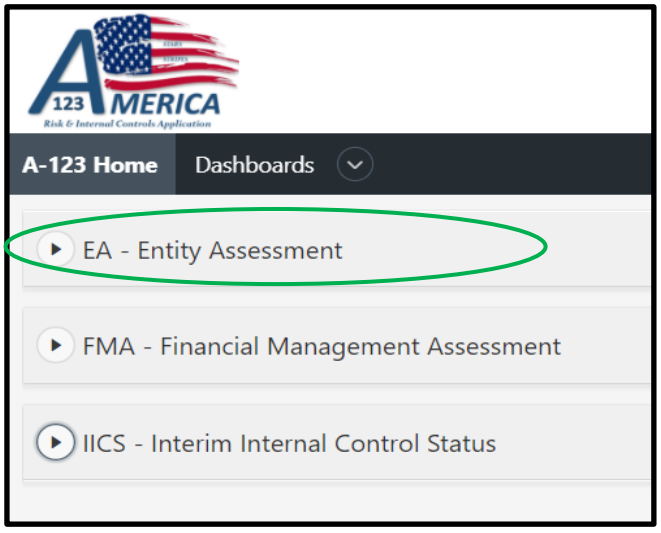
- Five components of Internal Control and 17 principles
- Evaluation of entity objectives
- Eight Financial Management System Goals (*If applicable*)
- Reporting and tracking of issues along with corresponding Corrective Action Plans (CAPs)
- Other critical information

This EA User Guide provides detailed instructions for completing the EA in the AMERICA application.

EA Homepage

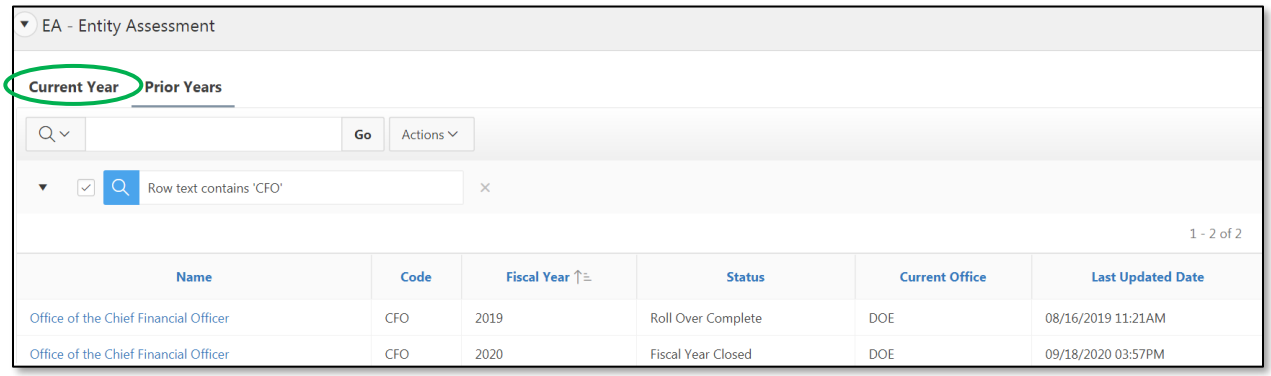
First, to access the EA homepage, log into the AMERICA system either through the secure gateway via iPortal or the direct link https://iportalwc.doe.gov/a123

Within the AMERICA homepage, navigate to the EA - Entity Assessment section, located under the A-123 Home Tab.



Accessing the EA Module

Upon opening the EA Module, a list of your EA entity and all associated downstream entities will appear along with a table of summary information regarding those assessments. In addition, Current Year and Prior Year sub-tabs will appear at the top of the page.

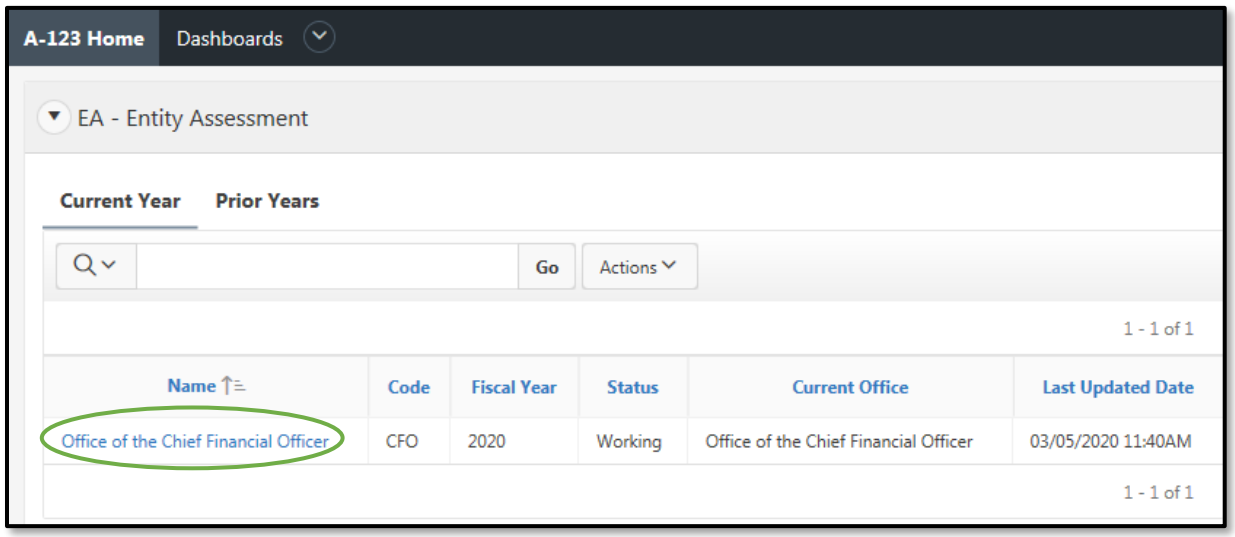


EA Module

The summary of the information in the table is described as follows:

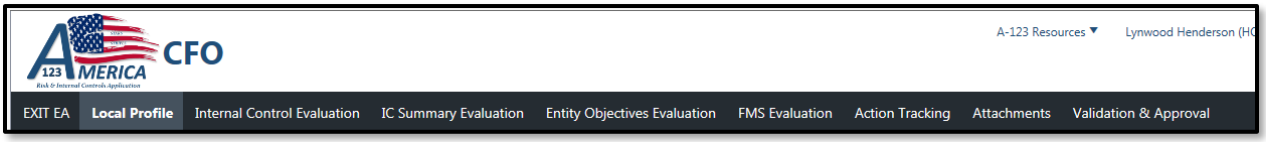
- **Name:** The entity name is displayed in blue text, indicating the user can open/view the assessment
- **Code:** The entity office code, which is populated from the Program Hierarchy provided by Office of Chief Financial Officer (CF)
- **Fiscal Year:** This field is automatically populated with the current fiscal year
- **Status:** Current status of the assessment – Working, Pending Approval, or Submission Accepted by Office of Chief Financial Officer (CF)
- **Current Office:** The office where the next action is pending in the workflow
- **Last Updated Date:** The date and time the assessment was last updated

The entity name will be displayed in blue text, indicating the ability to open and view. To access the desired EA evaluation, click on the entity name.



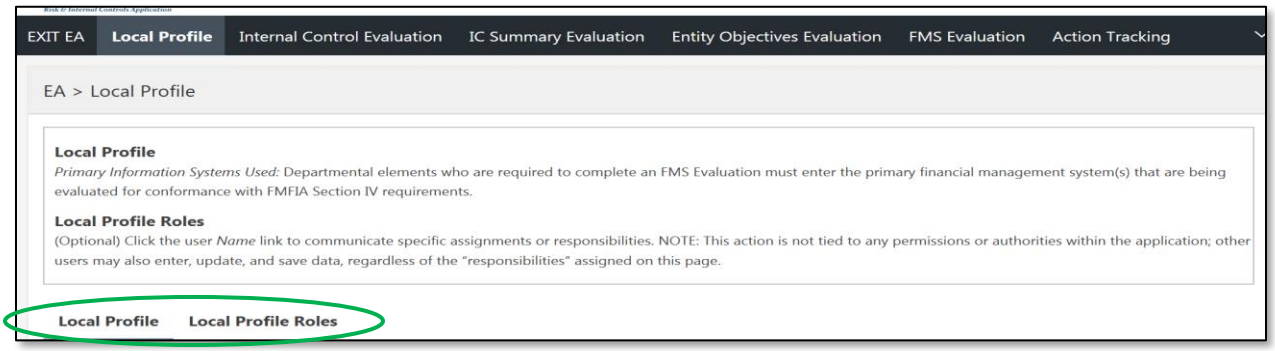
EA Global Menu

Upon selecting the entity name, the following tabs will appear along the top global menu.



Navigating the EA: Local Profile

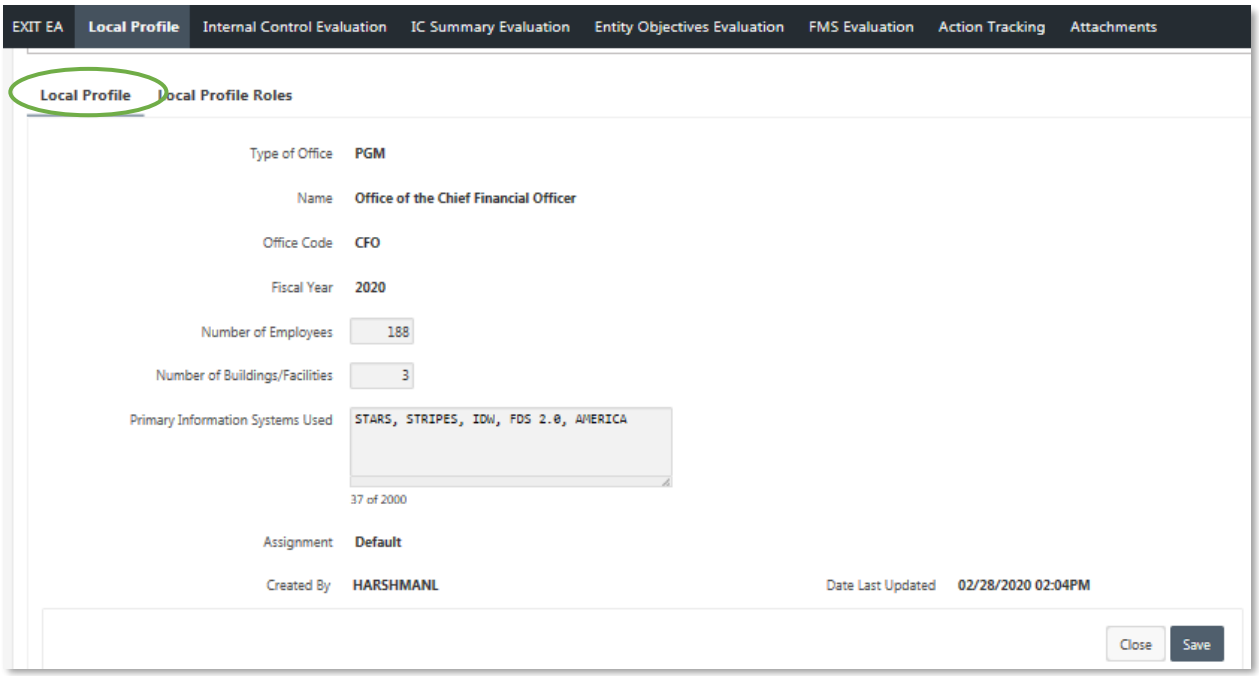
The Local Profile tab within the EA Global Menu contains the sub-tabs Local Profile and Local Profile Roles.



Local Profile

The Local Profile sub-tab is used to record and display high-level information for the entity conducting the EA including, the following fields:

- **Type of Office:** This field will automatically populate from the entity name selected during the EA setup
- **Name:** The entity name is selected from a drop-down menu during assessment setup
- **Office Code:** This field will automatically populate from the entity name selected during the EA setup
- **Fiscal Year:** This field will automatically populate with the current fiscal year during the assessment set up
- **Number of Employees:** Enter the number of Full Time Employees, or Full-Time Equivalents, located at the selected entity
- **Number of Buildings/Facilities:** Enter the number of buildings/facilities at the entity
- **Primary Information Systems Used:** For entities required to complete a Financial Management Systems (FMS) Evaluation, enter the primary financial management system(s) that are being evaluated for conformance with Federal Managers Financial Integrity Act Section IV requirements
- **Assignment:** The two options are Default and Extended, which are selected by CF during the setup of the EA and are based on the current FY Internal Control Guidance. Default entities are required to assess 9 Entity Objectives and complete the FMS evaluation. Extended entities have 14 Entity Objectives to evaluate but no FMS evaluation to complete.
- **Created By:** The CF creator of the specific EA evaluation
- **Date Last Updated:** The date and time the assessment was last updated



EA Local Profile

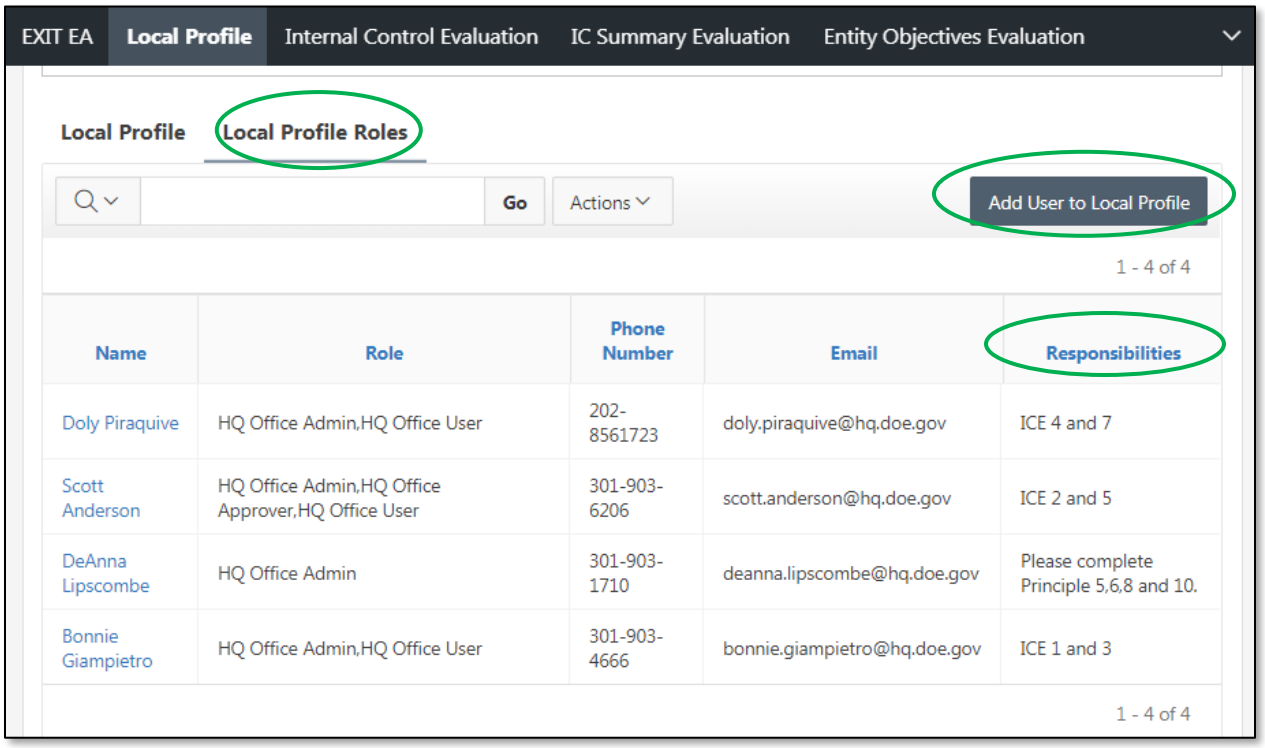
Local Profile Roles

The Local Profile Roles tab is a space that can be used by the entity's Local Administrator to communicate who within the entity is assigned to complete what roles. This input is similar to a note pad or table of contents and is strictly informational. It does not restrict who can complete items on the EA.

The Local Profile Roles summary table will provide the following information:

- **Name:** The user is assigned responsibilities within the EA module
- **Role:** The user's role(s) assigned in the system
- **Phone Number:** The user's contact number
- **Email:** The user's email address
- **Responsibilities:** The user's responsibilities is a free form text field that can be used by the Local Administrator to clarify and communicate who is responsible for updating what sections of the EA

  Note: Personnel phone number and email address are provided from iPortal.

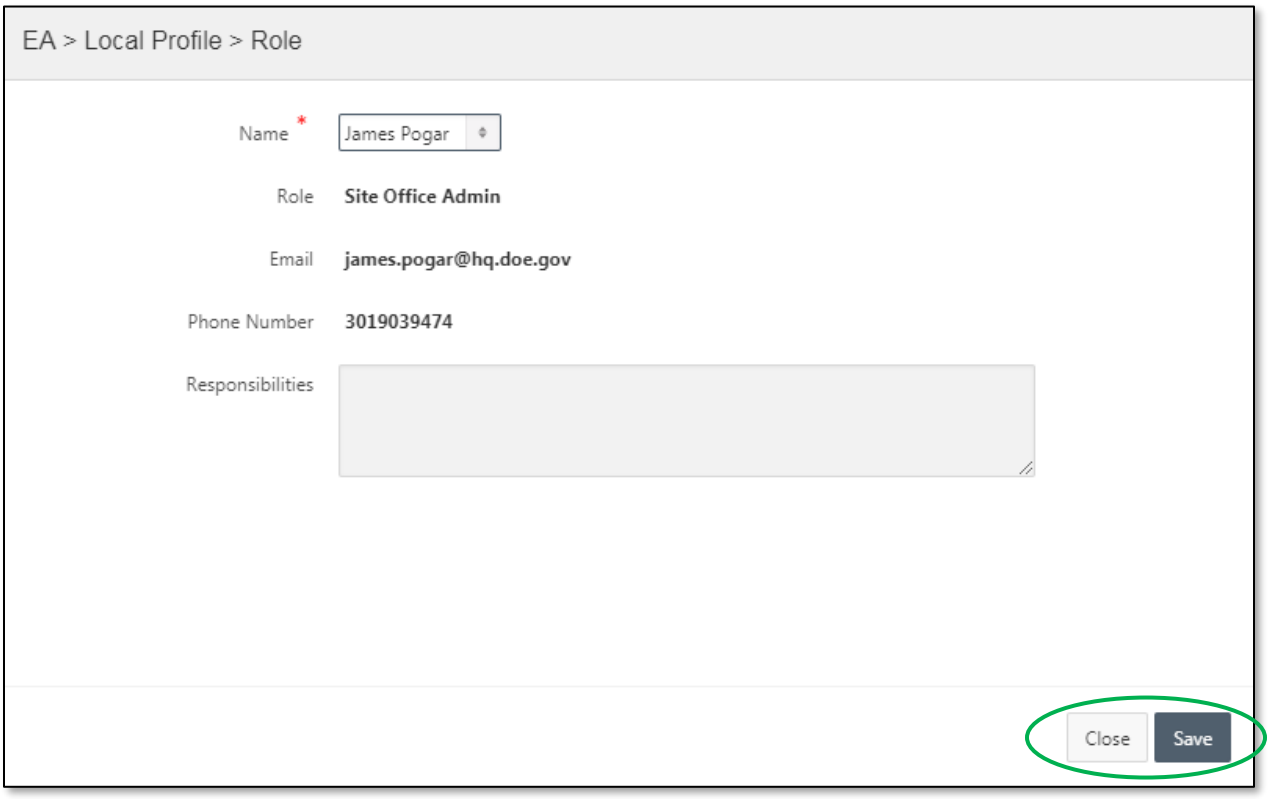


How to Add User to Local Profile

Adding Users to the Local Profile

Only the Local Admin will have the ability to specify user responsibilities on the Local Profile Roles.

1. Within the Local Profile>Local Profile Roles tab, locate and select the 'Add User to Local Profile' button
2. The EA>Local Profile>Role form will display with the following fields:
   Name: (Required) Selection from drop-down list
   Role: System generated per the Name selection
   Email: System generated per the Name selection
   Phone Number: System generated per the Name selection
   Responsibilities: Administrator input
3. Locate the 'Name' field. Select the drop-down next to the field. The value list shown will display users that have been assigned to the entity
4. Locate and select the desired user. The user's role(s), email, and phone number will populate based on the user selection.
5. Enter the user's responsibilities within the text box
6. Select the 'Save' button



Local User Profile

Navigating the EA: Internal Control Evaluation

The Internal Control Evaluation (ICE) tab captures the entity's assessment of the seventeen principles contained in the Government Accountability Office's *Green Book*, which support the effective design, implementation, and operation of the five internal control components. This tab is where the user records Evaluation Summary data for each principle and identifies whether or not the assessment of each principle's controls has revealed any substantive control deficiencies or issues.

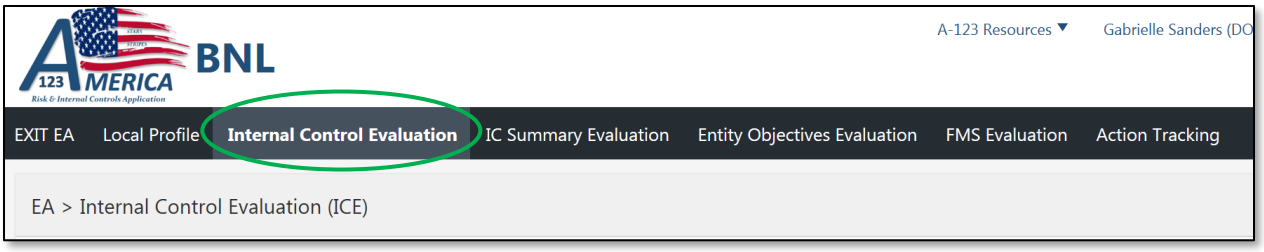
The user will determine:

- What documentation exists to support the entity evaluation and FMS evaluation
- Whether issues have been identified
- The appropriate rating for any issues identified

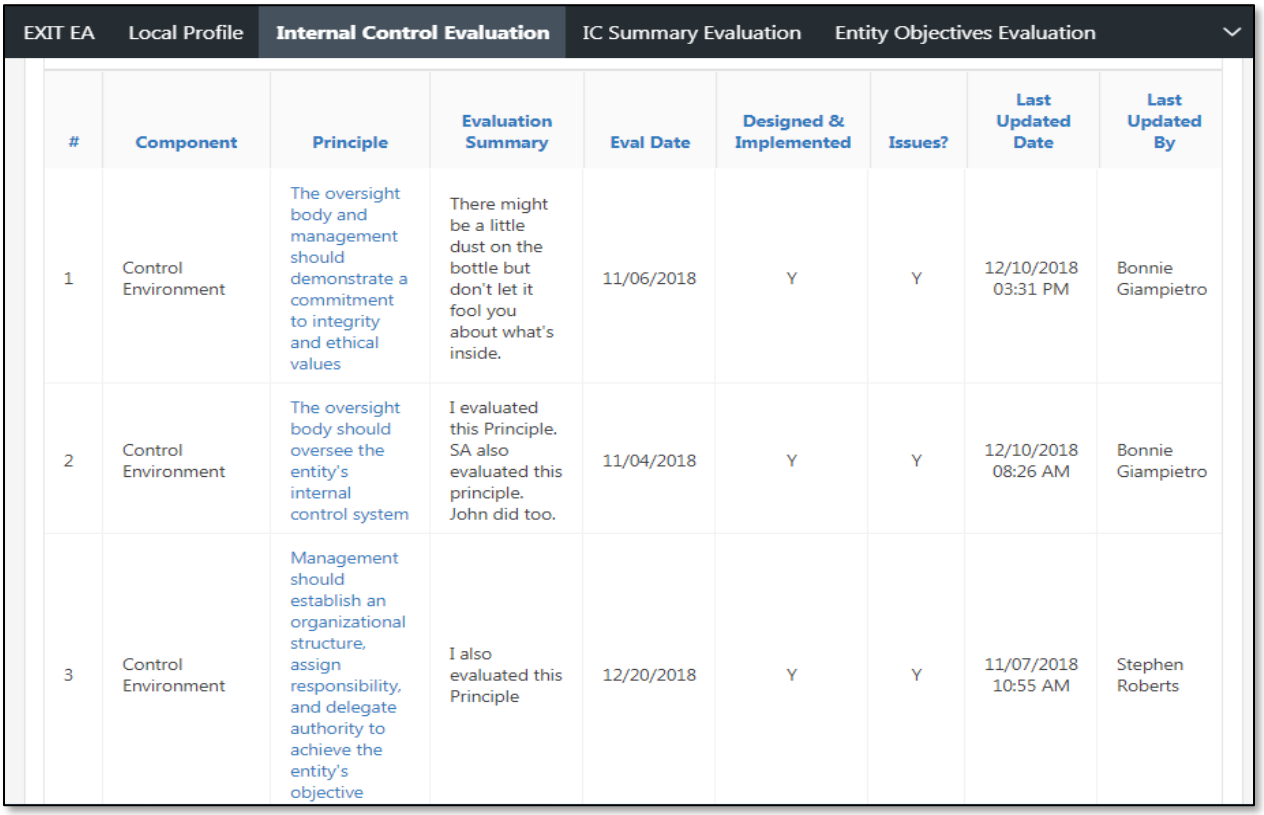
This tab is also used to record supporting documentation for the evaluation, date of the evaluation, issue reference, description, and Corrective Action Plan (CAP) reference.

Accessing the Internal Control Evaluation Tab

1. Within EA - Entity Assessment, locate and select the Internal Control Evaluation tab located along with the top global menu.



2. Upon the selection, the EA Internal Controls Evaluation page will display initially, and the Evaluation tab will be populated with information from the previous year.



#	Component	Principle	Evaluation Summary	Eval Date	Designed & Implemented	Issues?	Last Updated Date	Last Updated By
1	Control Environment	The oversight body and management should demonstrate a commitment to integrity and ethical values	There might be a little dust on the bottle but don't let it fool you about what's inside.	11/06/2018	Y	Y	12/10/2018 03:31 PM	Bonnie Giampietro
2	Control Environment	The oversight body should oversee the entity's internal control system	I evaluated this Principle. SA also evaluated this principle. John did too.	11/04/2018	Y	Y	12/10/2018 08:26 AM	Bonnie Giampietro
3	Control Environment	Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objective	I also evaluated this Principle	12/20/2018	Y	Y	11/07/2018 10:55 AM	Stephen Roberts

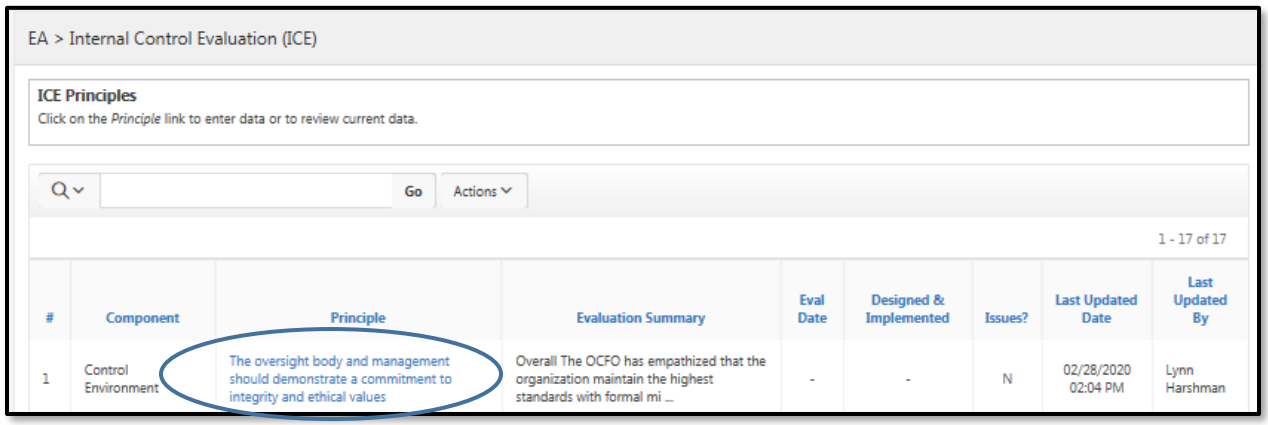
Internal Controls Evaluations Tab

The Summary table provides the following information:

- **#:** The number assigned to each principle listed
- **Component:** Identifies one of the five the components of internal control associated with the seventeen internal control principles
- **Principle:** The name of the principle to be assessed
- **Evaluation Summary:** A brief description of the summary, key information identified and/or activities performed during the evaluation to provide reliable support for assurances that the principles have been addressed. The information and/or, activities must be tangible and documented to be valid, such as testing results, goals and objectives plan, safety managers' reports, annual infrastructure reports, bi-annual. workforce planning survey results, etc. Initially, Evaluation Summary will be populated with information from the previous year.
- **Eval Date:** The date the evaluation was completed
- **Designed & Implemented:** Specifies "Y" or "N" based on the particular principle assessment
- **Issues?:** Specifies "Y" or "N" to determine if a principle has an issue in its operating effectiveness
- **Last Updated Date:** The date and time the principle information was last updated
- **Last Updated By:** Specifies the user who made the last change

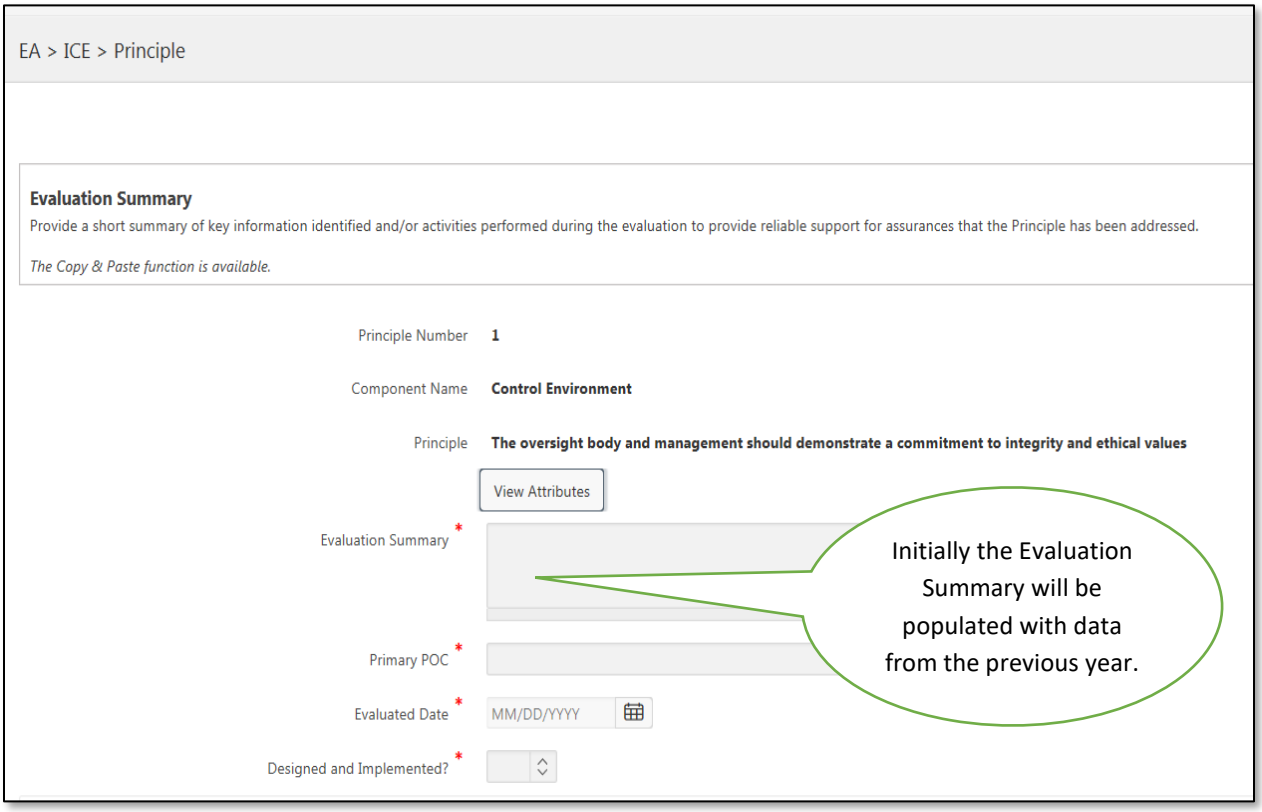
Modifying a Principle

To modify information related to a principle, click on the blue text to launch that principle.



Selecting a Principle

Upon the selection of the desired principle, the EA > ICE > Principle form will display.



Modifying a Principle's Evaluation Summary

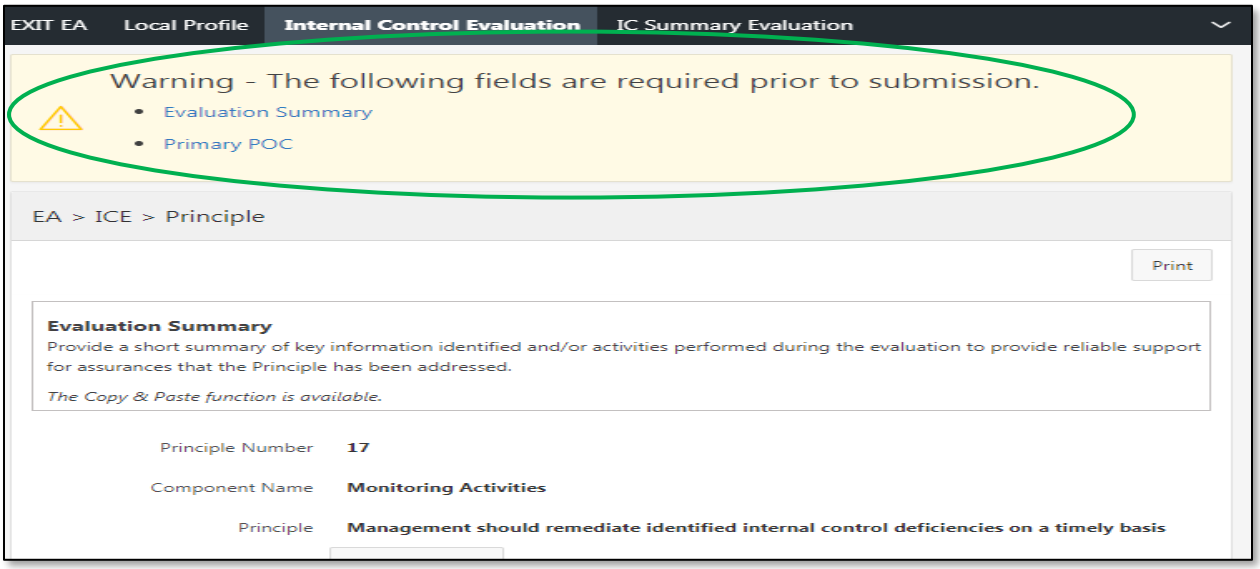
Requirements for each field on the form are described as follows:

- **Principle Number:** The number assigned to each principle listed
- **Component Name:** The component identified with the principle
- **Principle:** The selected principle name
- **View Attributes button:** Select this button to display the Internal Control Attributes. Select Close to exit the dialog box.
- **Evaluation Summary:** (Required) Enter a short summary, key information identified, and/or activities performed during the evaluation to provide reliable support for assurances that the principles have been addressed. The information and/or activities must be tangible and documented to be valid, such as testing results, goals and objectives plan, safety managers' reports, annual infrastructure reports, bi-annual workforce planning survey results, etc.
- **Primary POC:** (Required) Enter the name of the individual responsible for this principle
- **Evaluated Date:** (Required) Enter/Select the date the attribute evaluation was completed
- **Designed and Implemented?:** (Required) The Designed and Implemented column is mandatory and based on your assessment of the particular principle as it relates to your entity (site). Management must summarize its determination whether each principle is designed and implemented effectively to achieve objectives and respond to risks. That determination is a function of management judgment based on (a) the applicability of the principle to the Agency's circumstances; (b) whether the Agency has been able to implement, perform, and apply the principle; and (c) any internal control deficiency that may result.

Please note: A "No" response requires an Issue to be created with a rating of 2 or 3. All required fields will be marked with a red asterisk

To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.

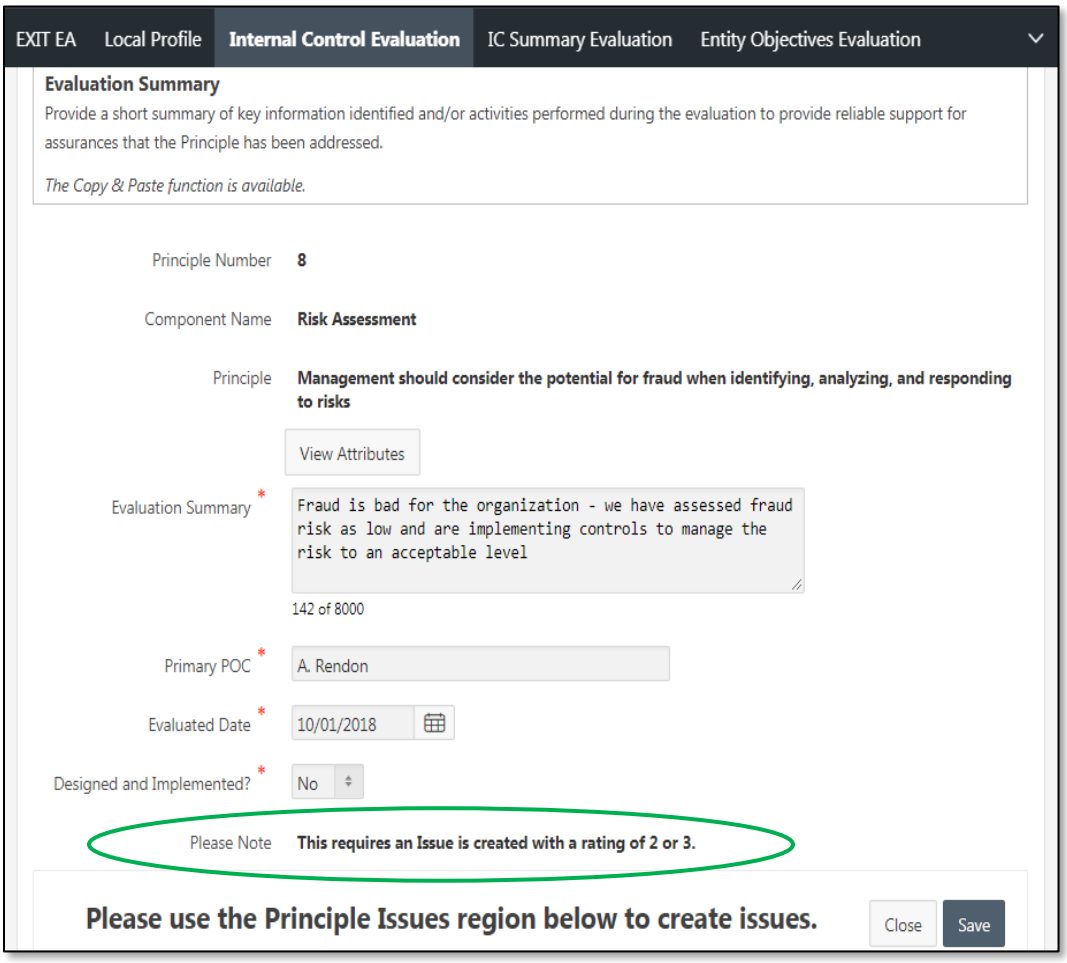
Should a Required field be missed, the system will generate a warning message stating an error has occurred. The Required field(s) will be specified below the warning. To save the issue, provide data for the required field(s) and re-select 'Save.'



Incomplete Evaluation Summary Warning Message

Principle Issues

Users can create and record issue(s) identified for a particular principle. If the response for Designed and Implemented is "No," then an issue with a rating of a 2 or 3 is required, and a corrective action plan (CAP) will be necessary. Instructions on CAPs are provided on page 15.



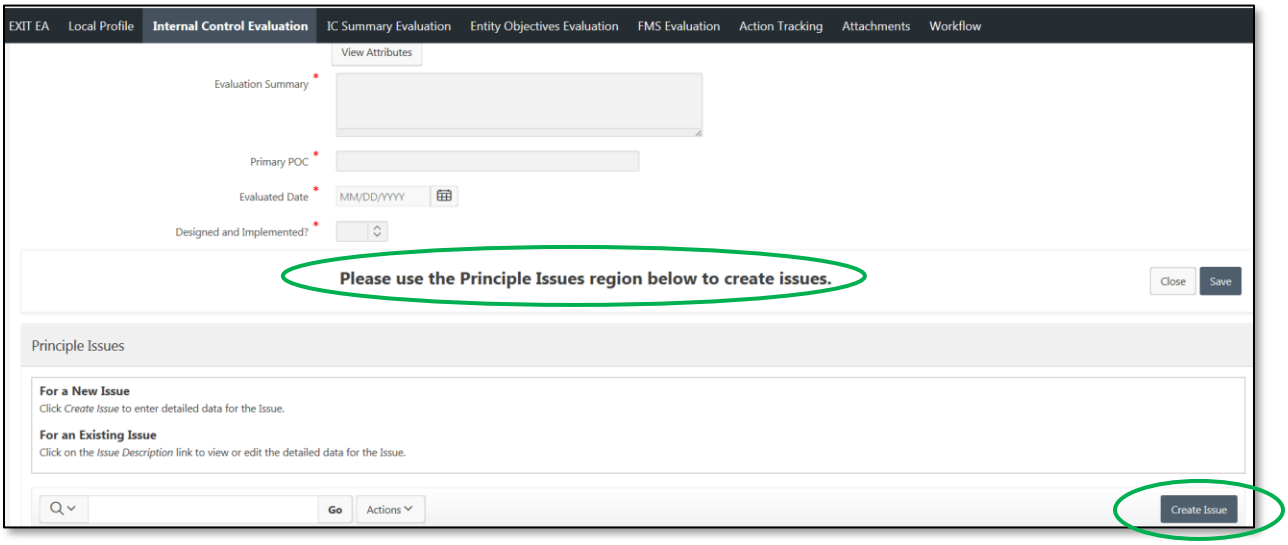
Selecting 'No' will require an Issue & CAP to be created

Below is a list of items to consider when identifying issues:

- Use information gathered and discussions conducted for the evaluation to assist in determining whether or not the entity's management is implementing the principle effectively
- Issues represent areas where certain control objectives are not being met or are trending towards not being met in an efficient, effective manner. In other words, these are areas where controls are breaking down or not functioning properly
- Inability to define a reasonable evaluation may in itself indicate a core control issue

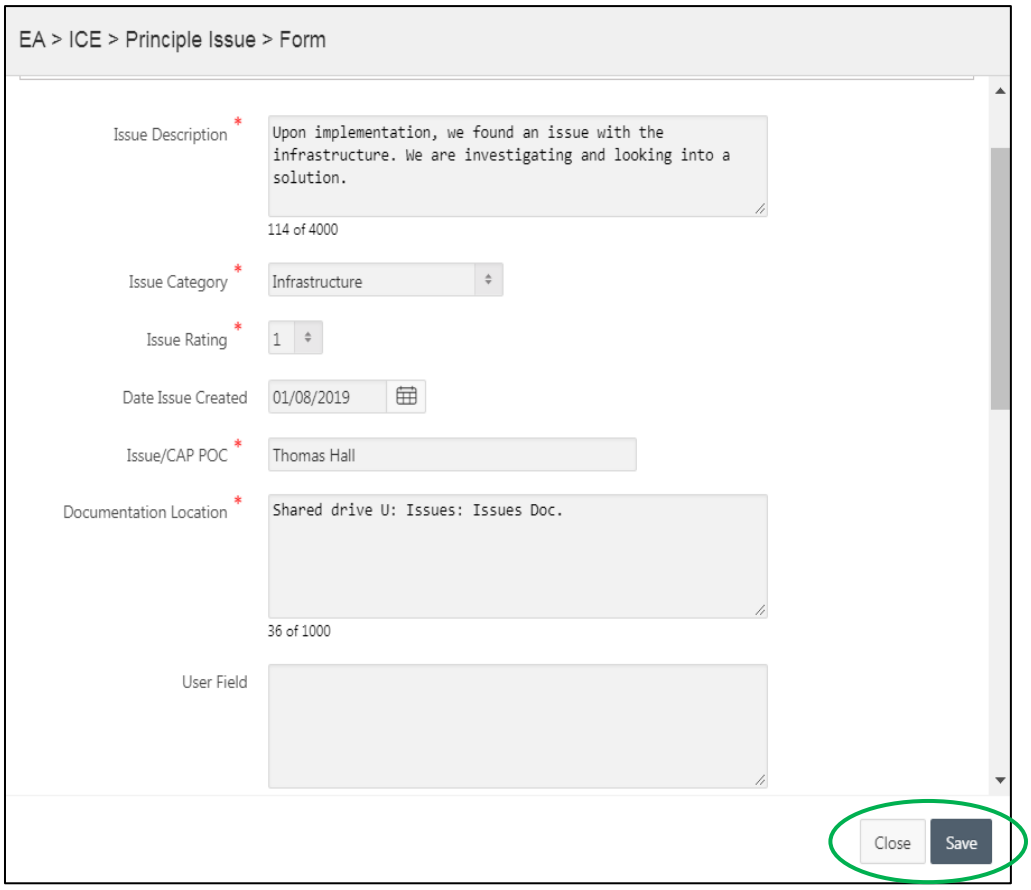
Creating an Issue

On the ICE Summary page, locate and select the 'Create Issue' button.



How to create an Issue

The EA > ICE > Principle Issue > Form dialog box will display.



Issue Form

Requirements for each field on the form are described as follows:

- **Issue Description:** (Required) Provide a brief description of the issue
- **Issue Category:** (Required) Select a category from the dropdown list. The selection of 'Other' will display an 'Issue Category Other' text box to provide additional details
- **Issue Rating:** (Required) Select a rating of 1, 2, or 3 from the dropdown list. Note: Issues rated 2 or 3 require completion of a system-generated CAP. Complete CAP input on the Action Tracking tab or in the CAP Details region. If the CAP was created in the current year, changing an Issue Rating to a 1 will delete all CAP information. The following are definitions of ratings:
    - **Issue level 1** – A situation currently of minor concern and impact, but that has the potential to become more problematic in the future
    - **Issue level 2** – An issue or concern that is currently, or may in the future, cause moderate adverse impact
    - **Issue level 3** – A significant issue or concern that is currently, or may in the future, cause a high adverse impact
    - **Issue level 0 –** This is used to close out an existing issue. An issue with a rating of 0 will not show up on the Summary Screen. When selected, the following warning message appears:

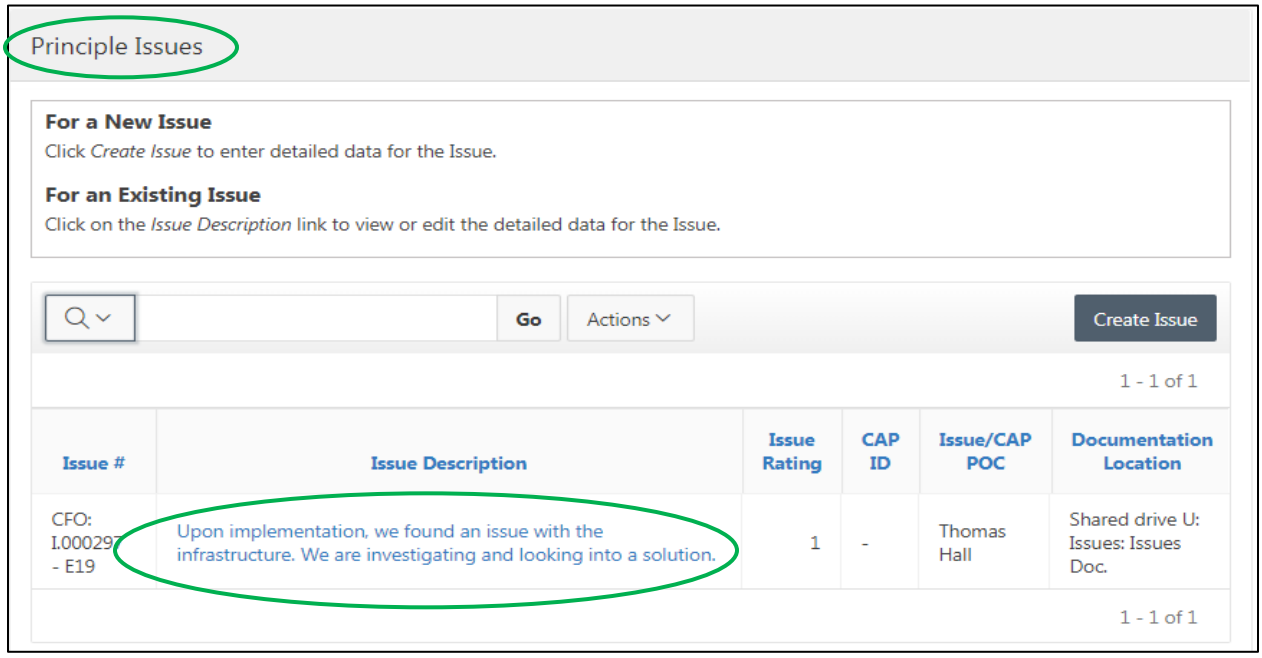
      "Issue Rating of 0 should only be used to close out an Issue that was created in the prior year. Please use the Delete button for current year issues that are no longer valid."
- **Date Issue Created:** (Required) System generated based on the current date when an issue is created, but editable by the user
- **Issue/CAP POC:** (Required) Enter the username of the primary point of contact responsible for completing the evaluation of the Issue/CAP
- **Documentation Location:** (Required) Enter the location of any supplementary documentation that may support the issue.
- **User Field:** Enter any additional information the user finds helpful in performing the evaluation and documentation process specific to the issue

To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.

Saving an Issue

To save an issue, complete the required fields and select the 'Save' button. Should a Required field be missed, the system will generate a warning message stating an error has occurred. The Required field(s) will be specified below the warning. To save the issue, provide data for the required field(s) and re-select 'Save.'

Upon the 'Save' selection, note the issue has been created. The issue details will be captured in the Principle Issues section.



Saved Issues will now appear in the Principle

Please note the summary fields shown in the Principle Issues summary table:

- **Issue #:** System generated numbering schema referencing the following: entity code, issue number, and EA evaluation year (e.g., CFO:I.000297-E19)
- **Issue Description:** (User Input) Provides summary information for the issue description. To modify the issue and/or the CAP, users have the ability to select this field to update the existing issue accordingly.
- **Issue Rating:** (User Input) Specifies the issue rating
- **CAP ID:** (If applicable) System generated numbering schema referencing the following: entity code, CAP number, and EA evaluation year. (e.g., CFO:C.000297-E19)
- **Issue/CAP POC:** (User Input) The username of the primary point of contact responsible for completing the evaluation of the Issue/CAP
- **Documentation Location:** (User Input) The location of any supplementary documentation that may support the issue

Modifying an Existing Issue

Note: *"Changing an Issue Rating to a 1 will delete all CAP Info, unless the CAP was created in a prior year."*.

To edit an issue, complete the following steps:

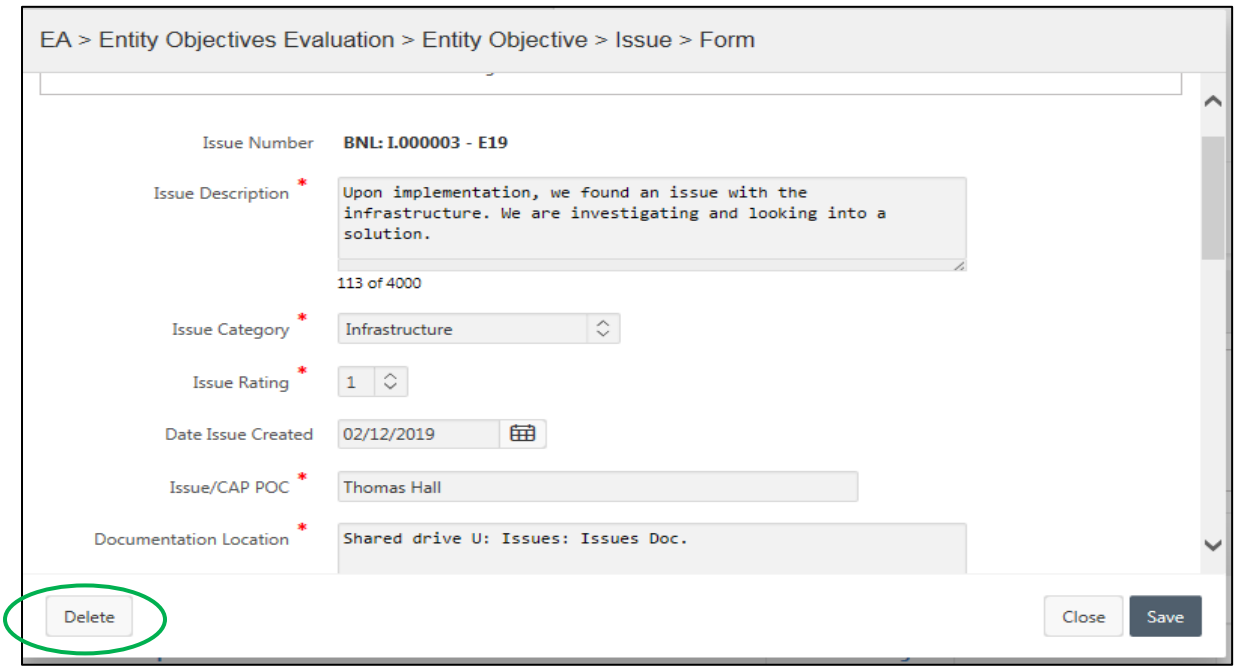
1. Select the principle in which you wish to modify the issue
2. Within the Principle Issues section, locate and click on the 'Issue Description,' which is displayed in the blue text indicating the user has the ability to open and modify
3. The EA > ICE > Principle Issue > Form dialog box will display. Note all fields will be editable except for the Issue #, which is system generated.
4. After the desired changes are made, select 'Save'

Deleting an Existing Issue

Within an EA evaluation, users with the administrator role has the ability to delete an existing issue within the current year. Please note deleting an issue will delete any associated CAP(s) unless created in the prior year.

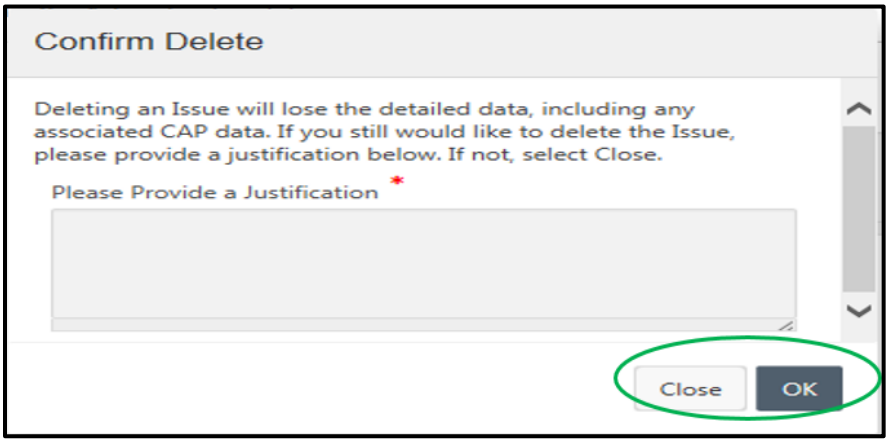
To Delete an Issue:

1. Select the Principle in which you wish to delete the issue
2. Within the Principle Issues section, locate and select the "Issue Description' displayed in the blue text indicating the user can open and modify
3. The EA > ICE > Principle Issue > Form dialog box will display
4. Select the 'Delete' button within the lower-left corner of the dialog box



Deleting an issue

5. A confirmation box will appear, requiring a justification for deleting the issue. Input the justification and click 'OK.' If you wish not to delete the Issue, click 'Cancel.'



Deletion Justification

Closing an Issue

To close an issue, set the value of "Issue Rating" to 0. Please note if the issue had a prior year CAP associated with it, then the CAP must be closed prior to closing the issue.

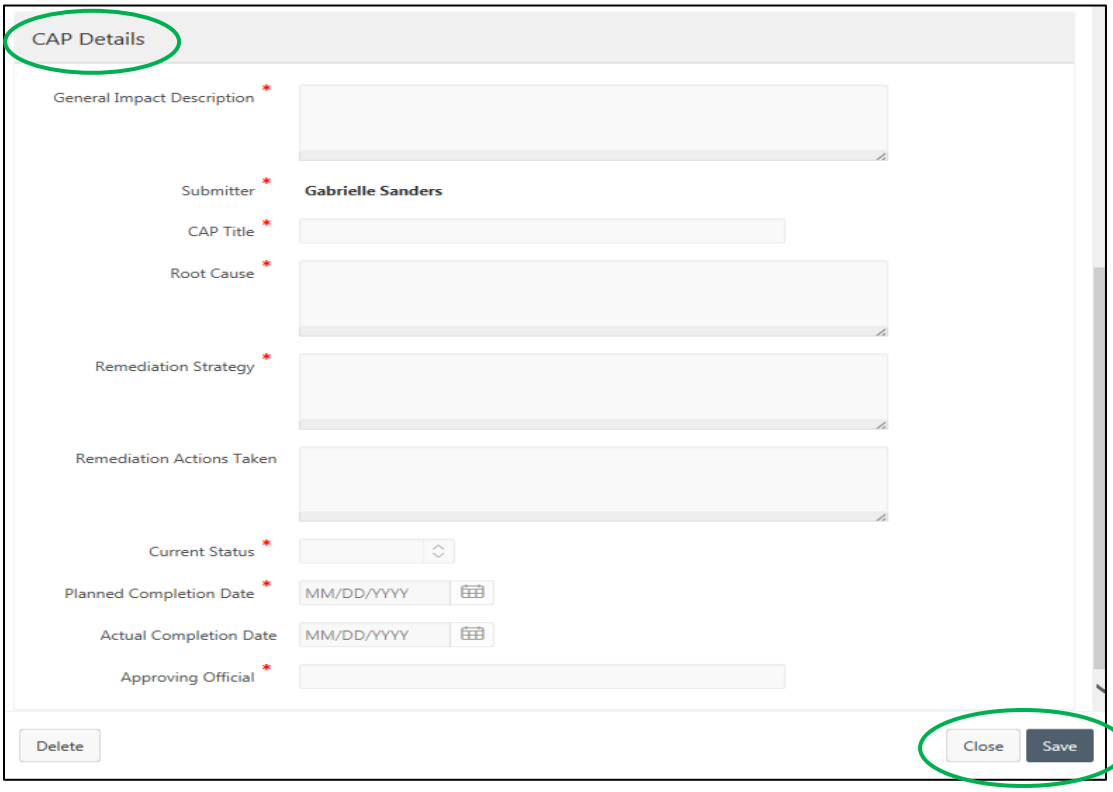
"Current CAP Status must be Canceled or Closed because Issue Rating is set to 0."

If the Issue Rating was changed to a 1 and had a prior year CAP associated with it, the following warning message will display:

"The existing CAP will be retained. Please take action to cancel or close CAP when appropriate."

Creating a CAP

Any issues identified in the Internal Control Evaluation Principle with a rating of 2 or 3 require a CAP. Once an issue is identified with a rating of 2 or 3 in the EA > ICE > Principle Issue > Form, the CAP Details section will automatically appear for data entry.



CAP Details Form

Requirements for each field in the CAP Details section are described as follows:

- **CAP ID:** Automatically populated with an alpha-numeric CAP reference number after the CAP is created
- **General Impact Description:** (Required) Provide a brief description of the impact the issue has and future potential impacts
- **Submitter:** Automatically populated with the individual's name who created the related issue
- **CAP Title:** Provide a name for the CAP
- **Root Cause:** (Required) Provide a brief description or summary of the problem's root cause. It is critical to define the root cause prior to developing a corrective action strategy and milestones. Otherwise, the CAP may fix symptoms rather than addressing the core problem
- **Remediation Strategy:** (Required) Provide a brief summary of the remediation strategy
- **Remediation Actions Taken:** Update the CAP Status to correlate with the current status of the remediation activity
- **Current Status:** (Required) Select the current CAP status from the drop-down menu:
    - **New:** The need to establish a CAP has been discovered through the current year's internal controls evaluation process
    - **In Progress:** Corrective actions have not yet been completed to resolve the issues and mitigate the stated impacts
    - **Implemented:** Corrective actions have been implemented to address newly discovered issues and stated impacts
    - **Closed:** All corrective actions have been completed to resolve the issue and mitigate the stated impacts
    - **Canceled:** CAP is no longer necessary based on the discovery of new or additional information

- **Planned Completion Date:** (Required) Provide the target closure date for the CAP
- **Actual Completion Date:** Provide the actual closure date once the CAP is closed. If the CAP current status is Closed, the actual completion date becomes required
- **Approving Official:** (Required) Provide the individual's name approving the CAP at the field or site level

Saving a CAP

To save a CAP, fill out the required fields and select the 'Save' button at the page's lower-right. Should a required field be missed, the system will generate a warning message. The required field(s) will be specified below the warning. Note, the required fields are not necessary to proceed with saving the CAP data. However, all CAP fields will be required prior to providing the assessment for review and approval.

A line item is automatically generated in the Action Tracking tab for each CAP created. CAP fields can be reviewed and modified on the Internal Control Evaluation or the Action Tracking tabs.

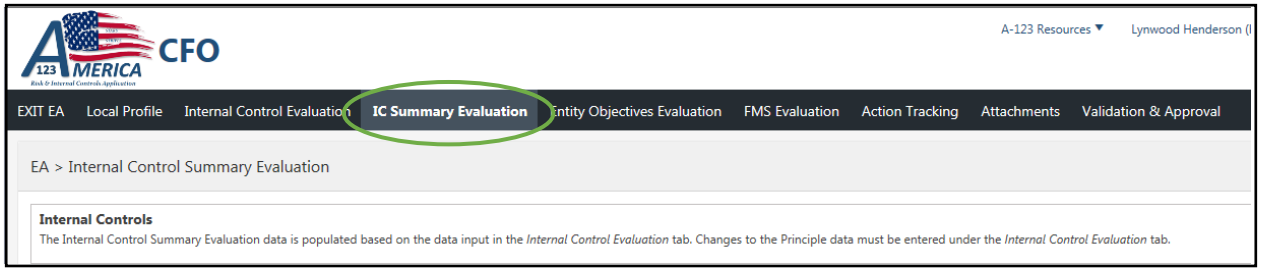
CAPs carried over from previous years need to be reviewed and updated.

Navigating the EA: IC Summary Evaluation

The IC Summary Evaluation tab provides a summary view of the information entered Internal Control Evaluation tab along with two questions at the bottom of the screen asking whether all Components are operating together in an integrated manner and whether the overall system of internal control is effective.

Accessing the Internal Control Evaluation Tab

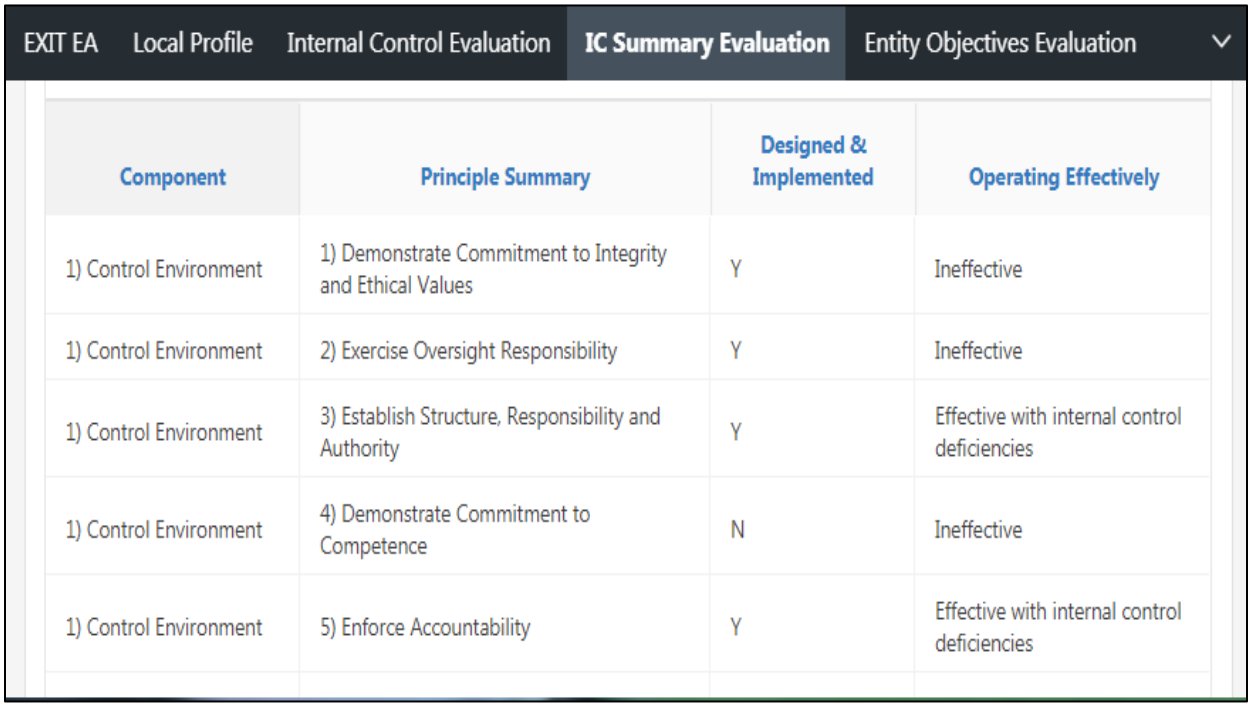
1. Within EA - Entity Assessment, locate and select the IC Summary Evaluation tab located along with the top global menu.



2. Upon the selection, the full IC Summary Evaluation information will display. The IC Summary Evaluation page appears in three sections (Principles Summary, Overall Assessment of a System of Internal Control, and the Additional Questions).

Principles Summary

The table at the top of the IC Summary Evaluation is the summary view of assessing the 17 principles and the scoring based on the Internal Controls data input.



Component	Principle Summary	Designed & Implemented	Operating Effectively
1) Control Environment	1) Demonstrate Commitment to Integrity and Ethical Values	Y	Ineffective
1) Control Environment	2) Exercise Oversight Responsibility	Y	Ineffective
1) Control Environment	3) Establish Structure, Responsibility and Authority	Y	Effective with internal control deficiencies
1) Control Environment	4) Demonstrate Commitment to Competence	N	Ineffective
1) Control Environment	5) Enforce Accountability	Y	Effective with internal control deficiencies

IC Summary Evaluation Tab

The fields shown in the Principles Summary Table are described as follows:

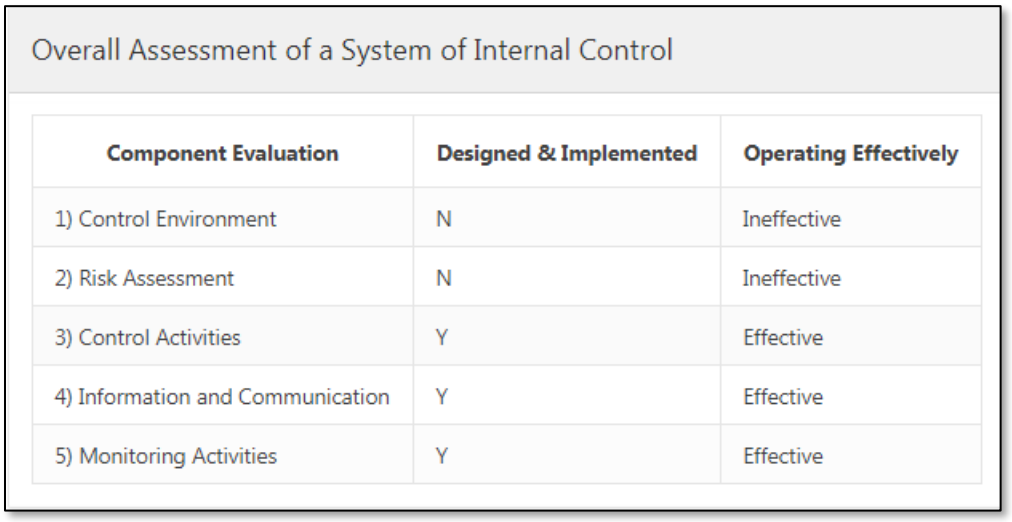
- **Component:** This field is pre-populated with each of the GAO internal control components
- **Principle Summary:** This field is pre-populated with short descriptions of each of the GAO internal control principles
- **Designed & Implemented:** This field is populated automatically based on responses to the Internal Control Evaluation tab
- **Operating Effectively:** This field is populated automatically based on responses to the principles within each component

Overall Assessment of a System of Internal Control

The second table shown in the middle of the IC Summary Evaluation tab is the overall assessment of the five components of internal control and the scoring based on the Internal Controls data input.

The fields shown in the component's summary table are described as follows:

- **Component Evaluation:** This field is pre-populated with each of the GAO internal control components
- **Designed & Implemented:** This field is populated automatically based on responses to the Internal Control Evaluation tab with 'Y' or 'N' responses
- **Operating Effectively:** This field is populated automatically based on responses to the Internal Control Evaluation tab with "Effective" or "Ineffective" responses



Overall Assessment of a System of Internal Control

Component Evaluation	Designed & Implemented	Operating Effectively
1) Control Environment	N	Ineffective
2) Risk Assessment	N	Ineffective
3) Control Activities	Y	Effective
4) Information and Communication	Y	Effective
5) Monitoring Activities	Y	Effective

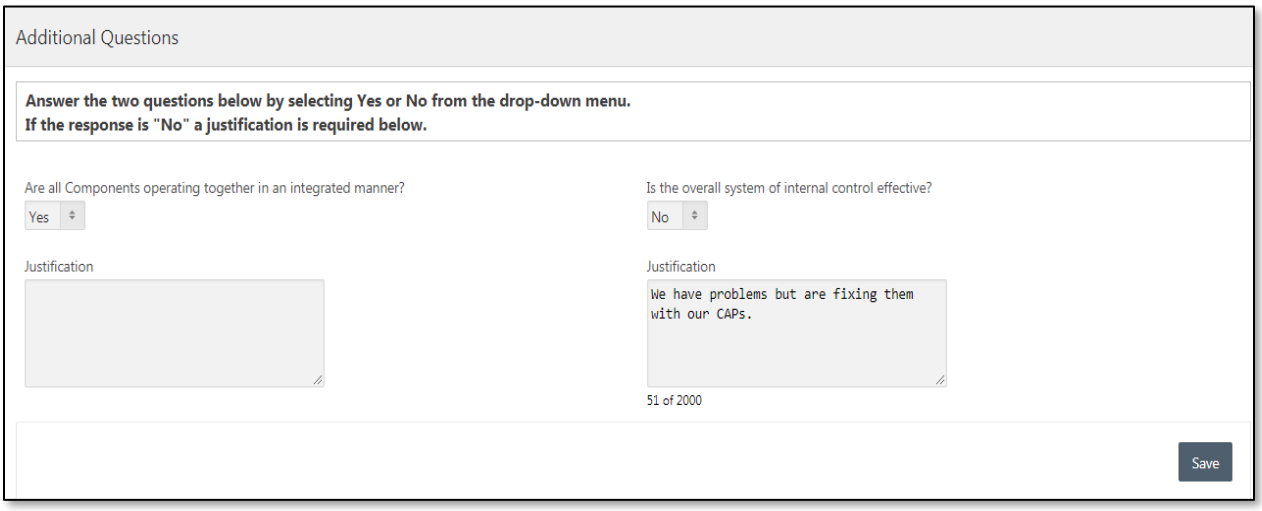
Overall Assessment of 5 Components

Additional Questions

The third section which, appears at the bottom of the IC Summary Evaluation tab, is the Additional Questions section. Those questions are as follows:

1. Are all Components operating together in an integrated manner?
2. Is the overall system of internal control effective?

A response of 'Yes' or 'No' must be selected via the dropdown. The selection of 'No' will prompt a short explanation supporting the 'No' decision.



Internal Controls Questionnaire

Please note the two questions are required and will not pass validation until the questions are completed

Navigating the EA: Entity Objectives Evaluation

The second aspect of the Entity Assessment is an evaluation of each entity's objective (e.g., functions, missions) to determine if there are issues that need to be addressed to assure the objective is being met. There are nine standard entity objective categories identified in the EA that require evaluation by all Departmental Elements:

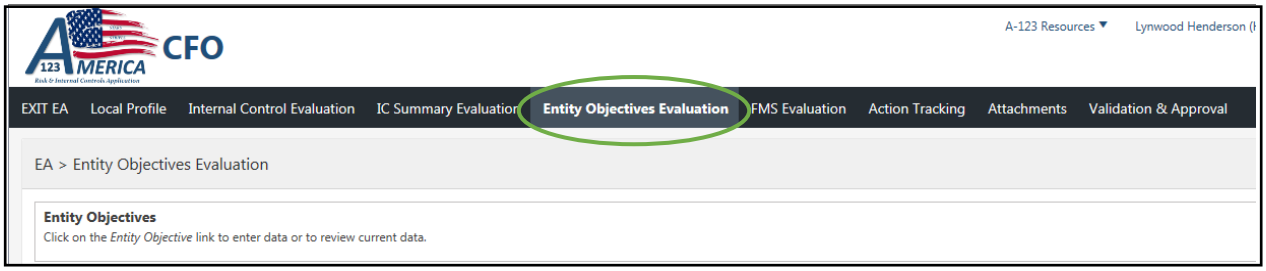
- Fraud Prevention
- Establishment of Entity-Wide Objectives
- Infrastructure Status
- Systems & IT Posture
- S&H Posture
- Security Posture
- Continuity of Operations
- Contractor/Subcontractor Oversight
- Environmental

In addition to the entity objectives that are listed above, some smaller Departmental Elements must complete the following five additional entity objectives in lieu of completing a full FMA module:

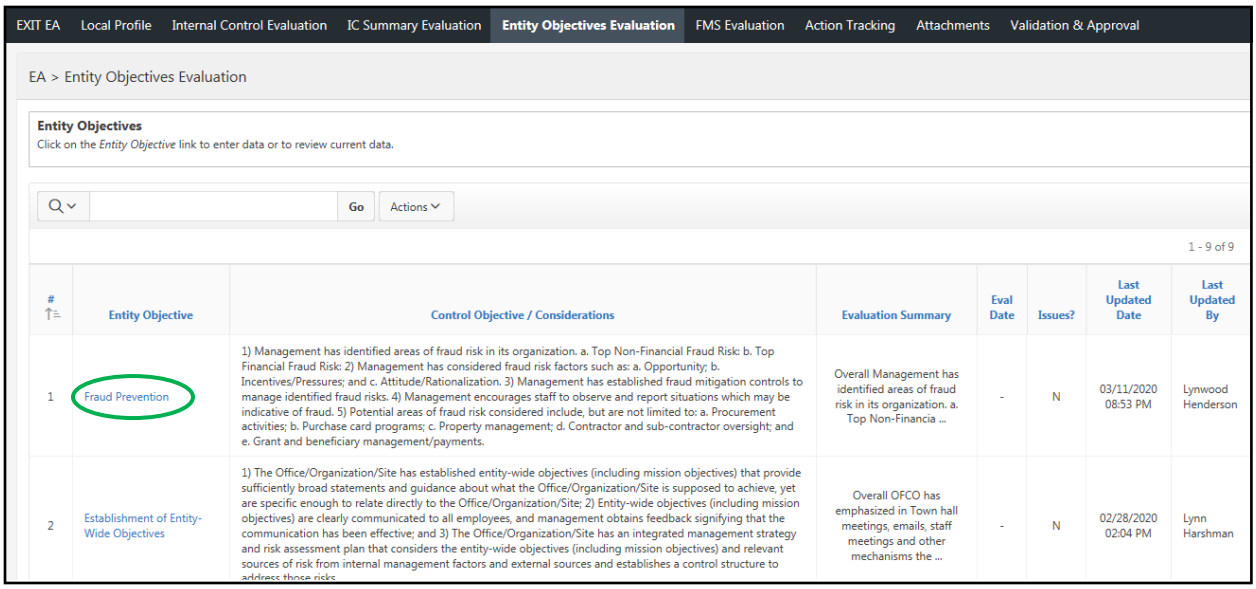
- Funds Management
- Acquisition Management
- Payables Management
- Travel Administration
- Payroll Administration

Accessing the Entity Objectives Evaluation Tab

1. Within the EA module, locate and select the Entity Objectives Evaluation tab.



2. The Entity Objectives Evaluations page will display with either the standard 9 objectives (Default) or 14 objectives (Extended) for the smaller entities that do not complete FMAs.



Entity Objective Evaluation Tab

The Entity Objectives Evaluation summary table provides the following information:

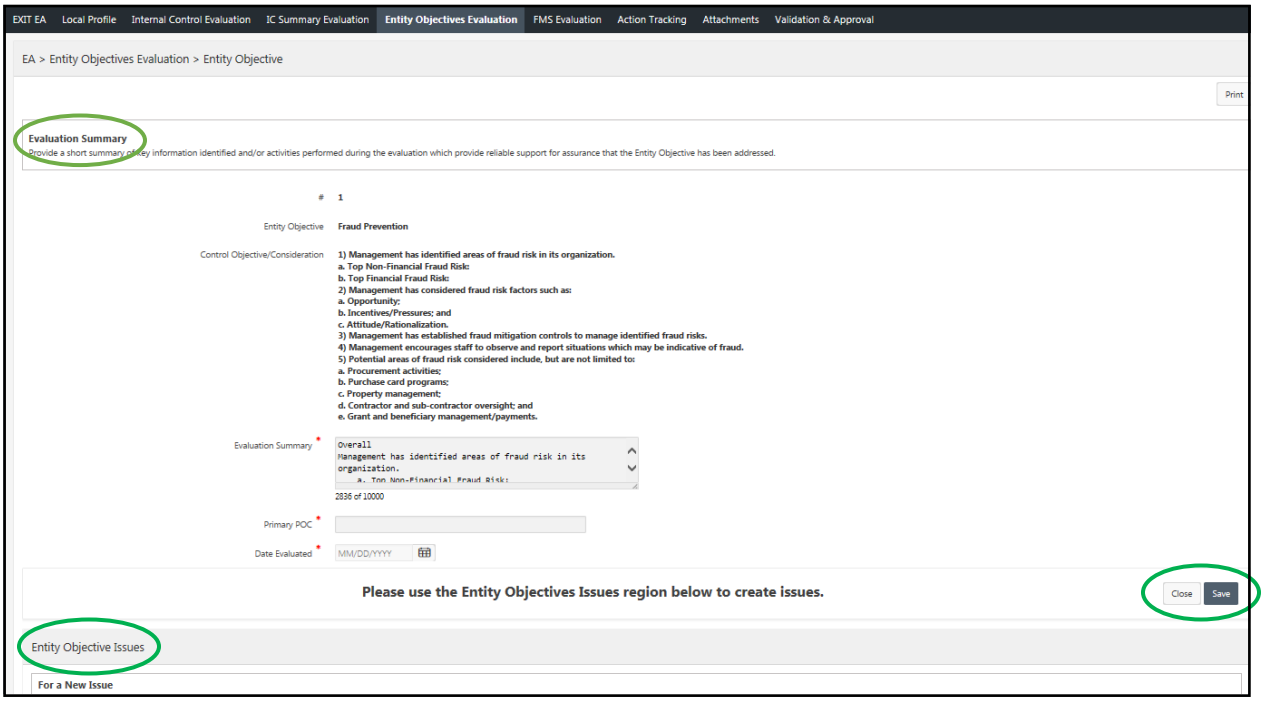
- **#:** The number assigned to each entity objective listed
- **Entity Objective:** The name of the entity objective
- **Control Objective/Considerations:** Identifies the key objectives to be achieved in each area, as well as specific types of control issues that should be considered when performing the evaluation
- **Evaluation Summary:** Presents the key information or activities leveraged/performed to provide reliable support for assurances that the control objectives and considerations have been addressed. This field will be pre-populated with information from the previous year. Care should be taken to assure the data is current and can be updated if necessary

- **Eval Date:** The date the evaluation of the entity objective was completed
- **Issues:** Specifies "Y" or "N" to determine if an entity objective has an issue in its operating effectiveness
- **Last Updated Date:** The date and time the entity objective was last modified
- **Last Updated By:** Specifies the user who made the last change

Modifying an Entity Objective

To modify an entity objective, locate and click on the blue text for the desired entity objective.

Upon the selection of the desired entity objective, the Entity Objective form for that objective will display. The form contains two sections. The top of the form provides the Evaluation Summary input screen. The bottom of the form contains a section to document Entity Objective Issues if any.



Entity Objective Page

The fields in the Evaluation Summary section at the top of the form are described as follows:

- **#:** Pre-populated with the number assigned to the selected entity objective
- **Entity Objective:** Pre-populated with the name of the selected entity objective
- **Control Objective/Considerations:** Pre-populated with the key objectives to be achieved in each area, as well as specific types of control issues that should be considered when performing the evaluation
- **Evaluation Summary:** (Required) Enter the key information or activities leveraged/performed to provide reliable support for assurances that the control objectives and considerations have been addressed. The evaluation summary must be a tangible and documented activity to be valid, such as safety managers' reports, annual infrastructure reports, bi-annual workforce planning survey results, etc. This field will be

pre-populated with information from the previous year. Care should be taken to assure the data is current and can be updated if necessary

- **Primary POC:** (Required) Enter the name of the primary point of contact responsible for completing the evaluation of that particular entity's objective
- **Date Evaluated:** (Required) Record the date the evaluation of the entity objective was completed

Input data on required fields and select the 'Save' button. Should a required field be missed, the system will generate a warning stating an error has occurred. The required field will be specified below the warning. Saving will occur; however, the entity objective will not pass validation until the required field is completed.

Upon the 'Save' selection, the entity objective details will be captured.

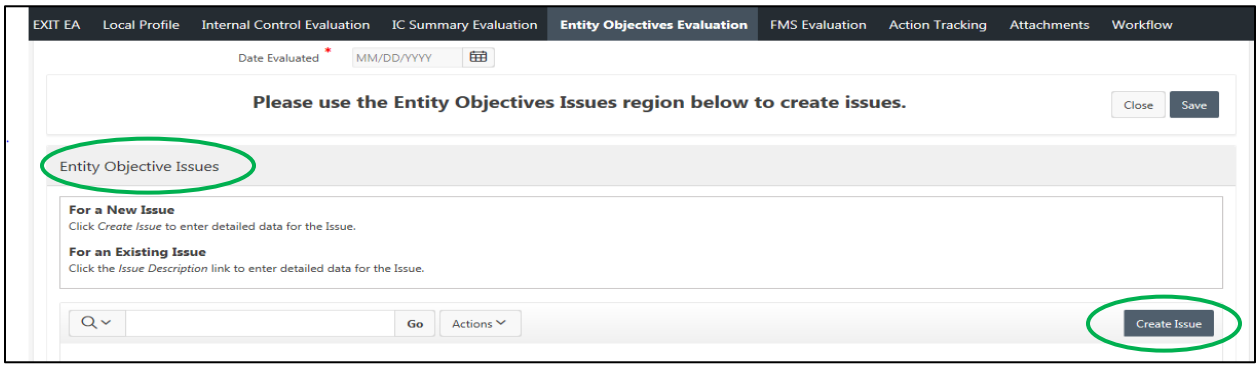
Entity Objective Issues

At the bottom of the page, users will have the ability to create and record a brief description of the issue(s) identified for that particular principle. Below is a list of items to consider when identifying issues:

- Use information gathered for the evaluation to assist in determining whether or not a control is functioning as intended
- Determining the magnitude of the potential impact of issues is not important at this point
- Issues represent areas where certain control objectives are not being met or are trending towards not being met in an efficient, effective manner. In other words, these are areas where controls are breaking down or not functioning properly
- Inability to define a reasonable evaluation may indicate a core control issue

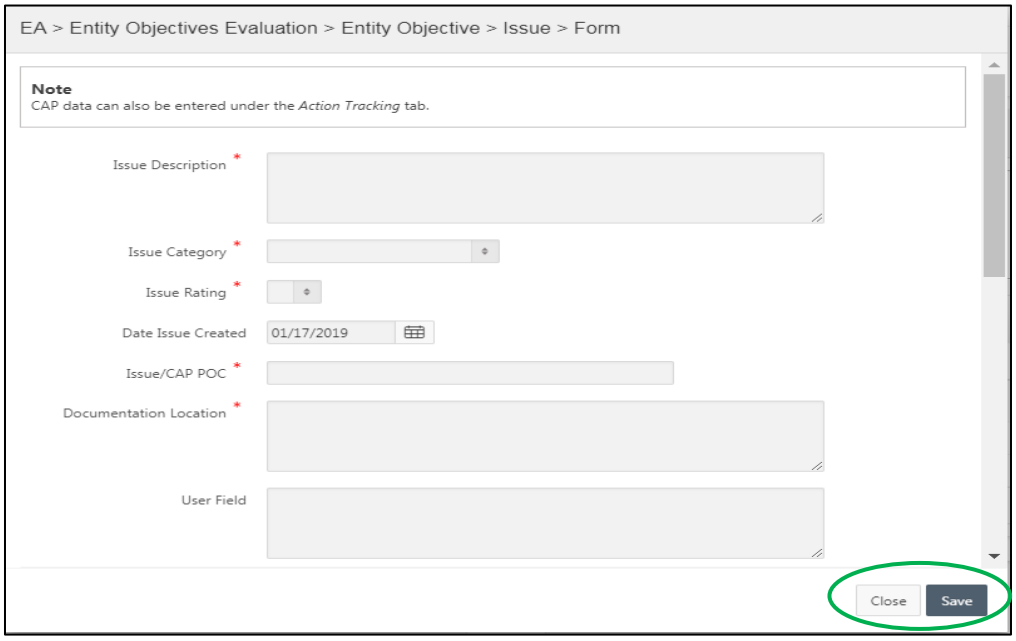
Creating an Issue

On the Entity Objectives Evaluation > Entity Objective page, locate and select the 'Create Issue' button.



How to create an Issue

The EA > Entity Objectives Evaluation > Entity Objective > Issue > Form dialog box will display.



Issues Form

Requirements for each field on the form are described as follows:

- **Issue Description:** (Required) Provide a description of the issue
- **Issue Category:** (Required) Select a category from the dropdown list. The selection of 'Other' will display an 'Issue Category Other' text box to provide additional details.
- **Issue Rating:** (Required) Select a rating of 1, 2, or 3 from the dropdown list. Note: Issues rated 2 or 3 require completion of a system-generated CAP. Complete CAP input on the Action Tracking tab or in the CAP Details region. If the CAP was created in the current year, changing an Issue Rating to a 1 will delete all CAP information. The following are definitions of ratings:
    - **Issue level 1** – A situation currently of minor concern and impact, but that has the potential to become more problematic in the future
    - **Issue level 2** – An issue or concern that is currently, or may in the future, cause moderate adverse impact
    - **Issue level 3** – A significant issue or concern that is currently, or may in the future, cause a high adverse impact
    - **Issue level 0 –** This is used to close out an existing issue. An issue with a rating of 0 will not show up on the Summary Screen. When selected, the following warning message appears:

      "Issue Rating of 0 should only be used to close out an Issue that was created in the prior year. Please use the Delete button for current year issues that are no longer valid."
- **Date Issue Created:** (Required) System generated based on the date when an issue is created, but editable by the user
- **Issue/CAP POC:** (Required) Enter the username of the primary point of contact responsible for completing the evaluation of the particular Issue/CAP
- **Documentation Location:** (Required) Enter the location of any supplementary documentation that may support the issue

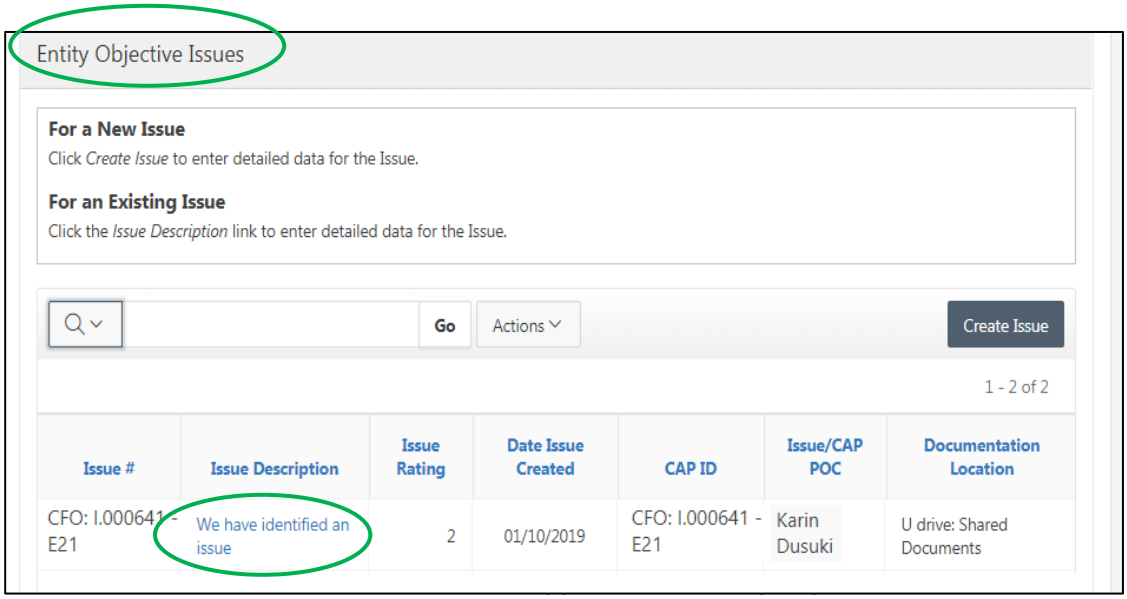
- **User Field:** Enter any additional information the user finds helpful in performing the evaluation and documentation process specific to the issue

To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.

Saving an Issue

To save an issue, fill out the required fields and select the 'Save' button. Please note, to create an Issue, all the required fields within the issues section must be populated prior to saving. Should a required field be excluded, the system will generate a warning stating an error has occurred. The required field(s) will be specified below the warning. To proceed with saving the issue, provide data for the required field(s) and re-select 'Save.'

Upon the 'Save' selection, note the issue has been created. The issue details will be captured in a summary table at the bottom of the Entity Objective Issues section.



The summary fields shown in the Entity Objective Issues summary table are described below:

- **Issue #:** System generated numbering schema referencing the following: entity code, issue number, and EA evaluation year. (e.g., CFO:I.000641-E21)
- **Issue Description:** Provides summary information for the issue description as previously input. To modify the issue and/or the CAP, users have the ability to select this field to update the existing issue accordingly.
- **Issue Rating:** Specifies the issue rating as previously input
- **CAP ID:** (If applicable) System generated numbering schema referencing the following: entity code, CAP number, and EA evaluation year. (e.g., CFO:C.000641-E21)
- **Issue/CAP POC:** The username of the primary point of contact responsible for completing the evaluation of the issue/CAP as previously input
- **Documentation Location:** The location of any supplementary documentation that may support the issue as previously input

Modifying an Existing Issue

Note: "*Changing an Issue Rating to a 1 will delete all CAP Info, unless the CAP was created in a prior year.*"

To edit an issue, complete the following steps:

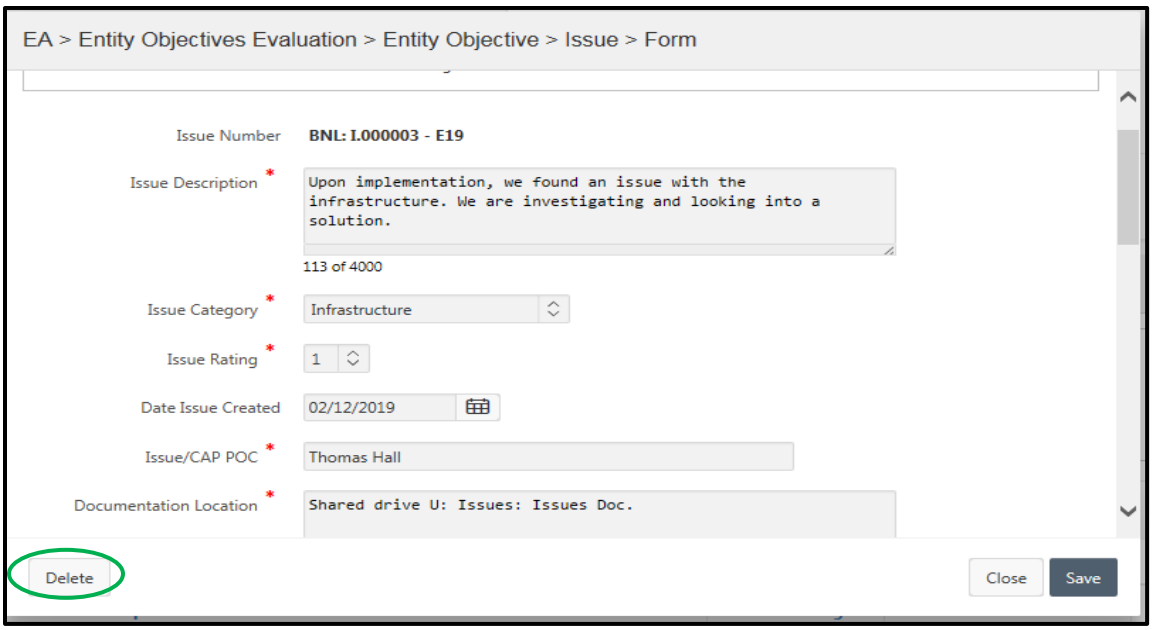
1. Select the entity objective in which you wish to modify the issue
2. Within the Entity Objective Issues section, locate and select the 'Issue Description,' which is displayed in the blue text indicating the user has the ability to open and modify.
3. The EA > Entity Objective Evaluation > Entity Objective > Issue > Form dialog box will display. Note all fields will be editable except for the Issue #, which is system generated.
4. After the desired changes are made, click 'Save'

Deleting an Existing Issue

Within an EA evaluation, users with the administrator role have the ability to delete an existing issue. Please note, deleting an issue will delete any associated CAP(s).

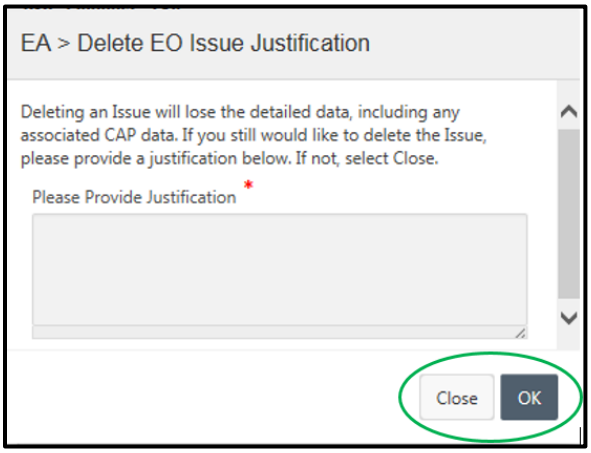
To Delete an issue:

1. Select the entity objective in which you wish to delete the issue
2. Within the Entity Objective Issues section, locate and select the 'Issue Description,' which is displayed in the blue text indicating the user has the ability to open and modify.
3. The EA > Entity Objective Evaluation > Entity Objective > Issue > Form dialog box will display
4. Select the 'Delete' button within the dialog box



Deleting an Issue

5. A confirmation box will appear, requiring a justification for deleting the issue. Input the justification and click 'OK.' If you wish to not delete the Issue, click 'Close.'



Deleting an Issue Justification

Closing an Issue

To close an issue, set the value of "Issue Rating" to 0. Please note if the issue had a prior year CAP associated with it, then the CAP must be closed prior to closing the issue.

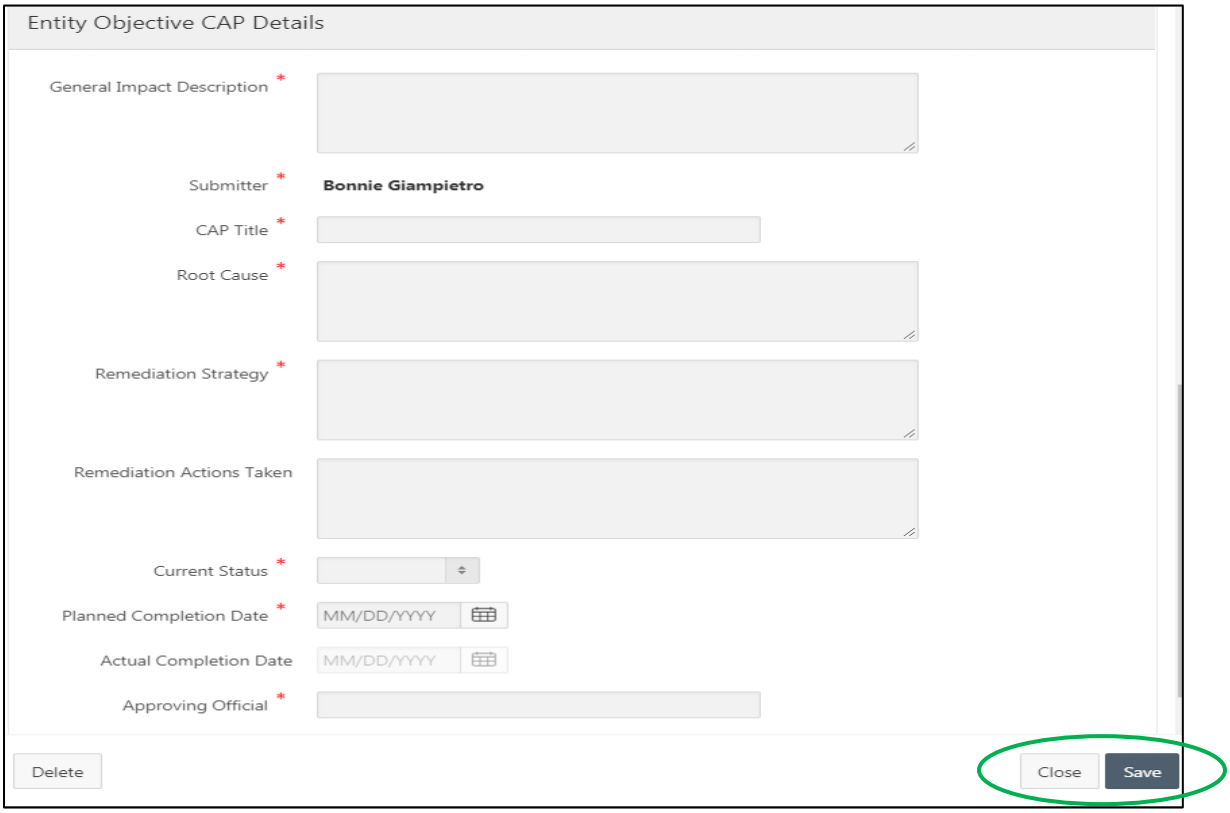
"Current CAP Status must be Canceled or Closed because Issue Rating is set to 0."

If the Issue Rating was changed to a 1 and had a prior year CAP associated with it, the following warning message will display:

"The existing CAP will be retained. Please take action to cancel or close CAP when appropriate."

Creating a CAP

Any issues identified in the Entity Objective Evaluation with a rating of 2 or 3 require a CAP. Once an issue is identified with a rating of 2 or 3 in the EA > Entity Objectives Evaluation > Entity Objective > Issue > Form, the Entity Objective CAP Details section will automatically appear below the issue for data entry.



CAP Details Form

Requirements for each field in the CAP Details section are described as follows:

- **CAP ID:** This will automatically populate with an alpha-numeric CAP reference number after the CAP is created
- **General Impact Description**: (Required) Provide a brief description of the impact the issue is having and future potential impacts
- **Submitter:** Automatically populated with the individual's name who created the related issue
- **CAP Title:** (Required) Provide a name for the CAP
- **Root Cause:** (Required) Provide a brief description or summary of the root cause of the problem. It is critical to define the root cause prior to developing a corrective action strategy and milestones. Otherwise, the CAP may fix symptoms rather than addressing the core problem.
- **Remediation Strategy:** (Required) Provide a brief summary of the remediation strategy
- **Remediation Actions Taken:** Update the CAP Status to correlate with the current status of the remediation activity
- **Current Status:** (Required) Select the current CAP status from the drop-down menu:
  - **New:** The need for the establishment of a CAP has been discovered through the current year's internal controls evaluation process
  - **In Progress:** Corrective actions have not yet been completed to resolve the issues and mitigate the stated impacts
  - **Implemented:** Corrective actions have been implemented to address newly discovered issues and stated impacts
  - **Closed:** All corrective actions have been completed to resolve the issue and mitigate the stated impacts

- **Canceled:** CAP is no longer necessary based on the discovery of new or additional information.
- **Planned Completion Date:** (Required) Provide the target closure date for the CAP
- **Actual Completion Date:** Provide the actual closure date once the CAP is closed. (Required) if the CAP current status is closed, the actual completion date must be provided.
- **Approving Official:** (Required) Provide the name of the individual approving the CAP at the field or site level

Saving a CAP

To save a CAP, fill out the required fields and select the 'Save' button. Should a required field be missed, the system will generate a warning message. The required field(s) will be specified below the warning. Note, the required fields are not necessary to proceed with saving the CAP data. However, all CAP fields will be required prior to finalizing the evaluation for review and approval.

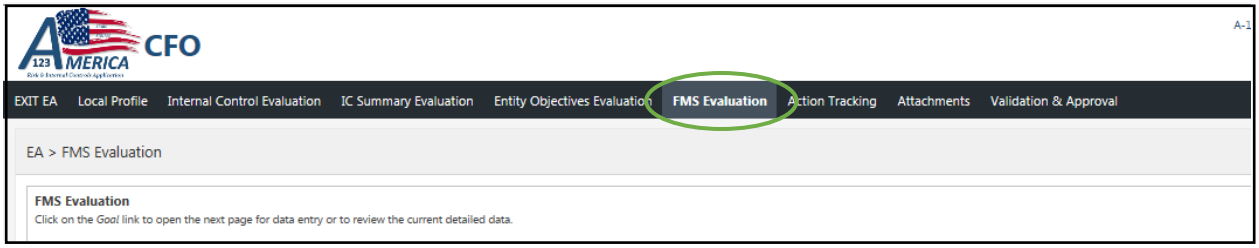
A line item is automatically generated in the Action Tracking tab for each CAP created. CAP fields can be reviewed and modified on the Entity Objectives Evaluation tab or the Action Tracking tab.

Navigating the EA: Financial Management Systems (FMS) Evaluation (If Applicable)

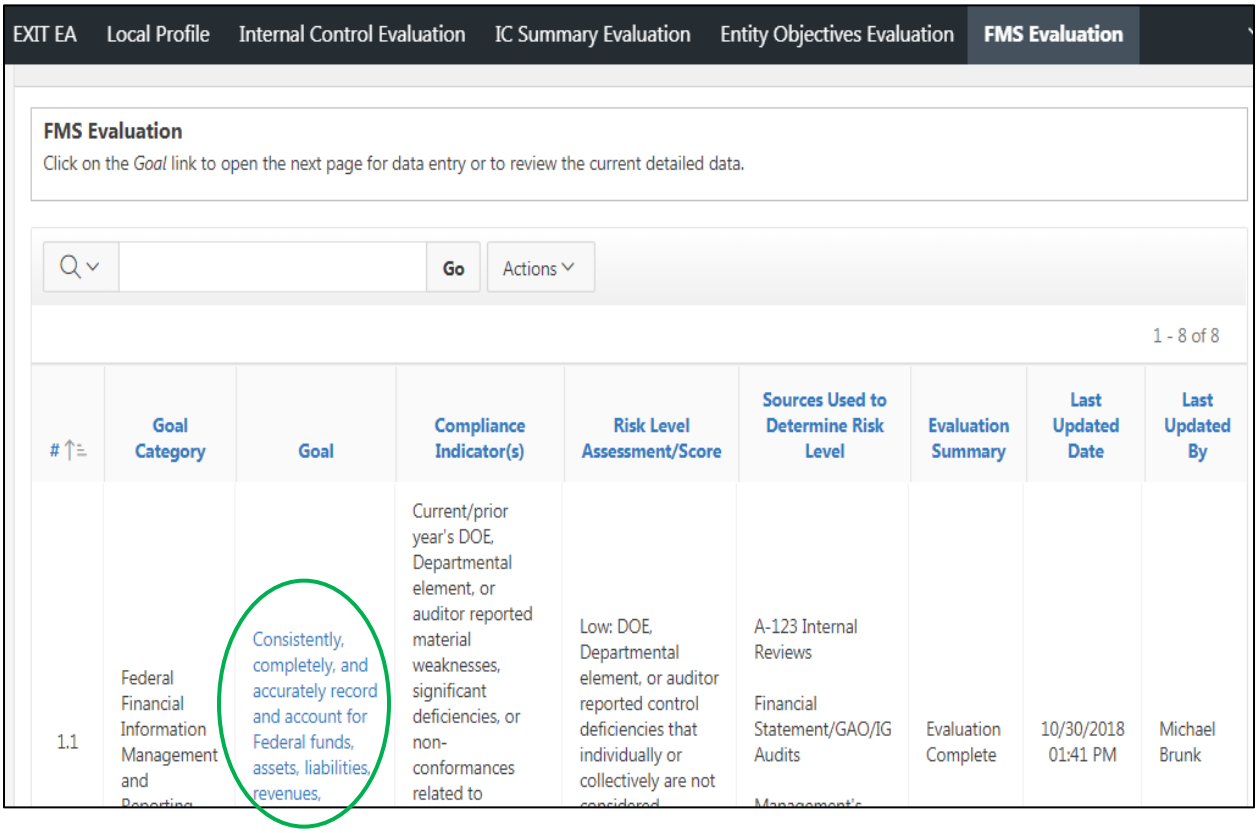
OMB Circular A-123, Appendix D, defines a financial management system as including an agency's overall financial operation, **reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner support business decisions**. Departmental Elements identified in Table 1 of the Internal Controls Guidance must perform a FMS Evaluation to support core requirements of Section IV of FMFIA and FFMIA and will see the FMS Evaluation tab within their Entity Assessment global menu.

Accessing the FMS Evaluation Tab

1. Within the EA module, locate and select the 'FMS Evaluation' tab located along the top global menu.



2. Upon selection, the FMS Evaluation summary page shall display.



FMS Evaluation Tab

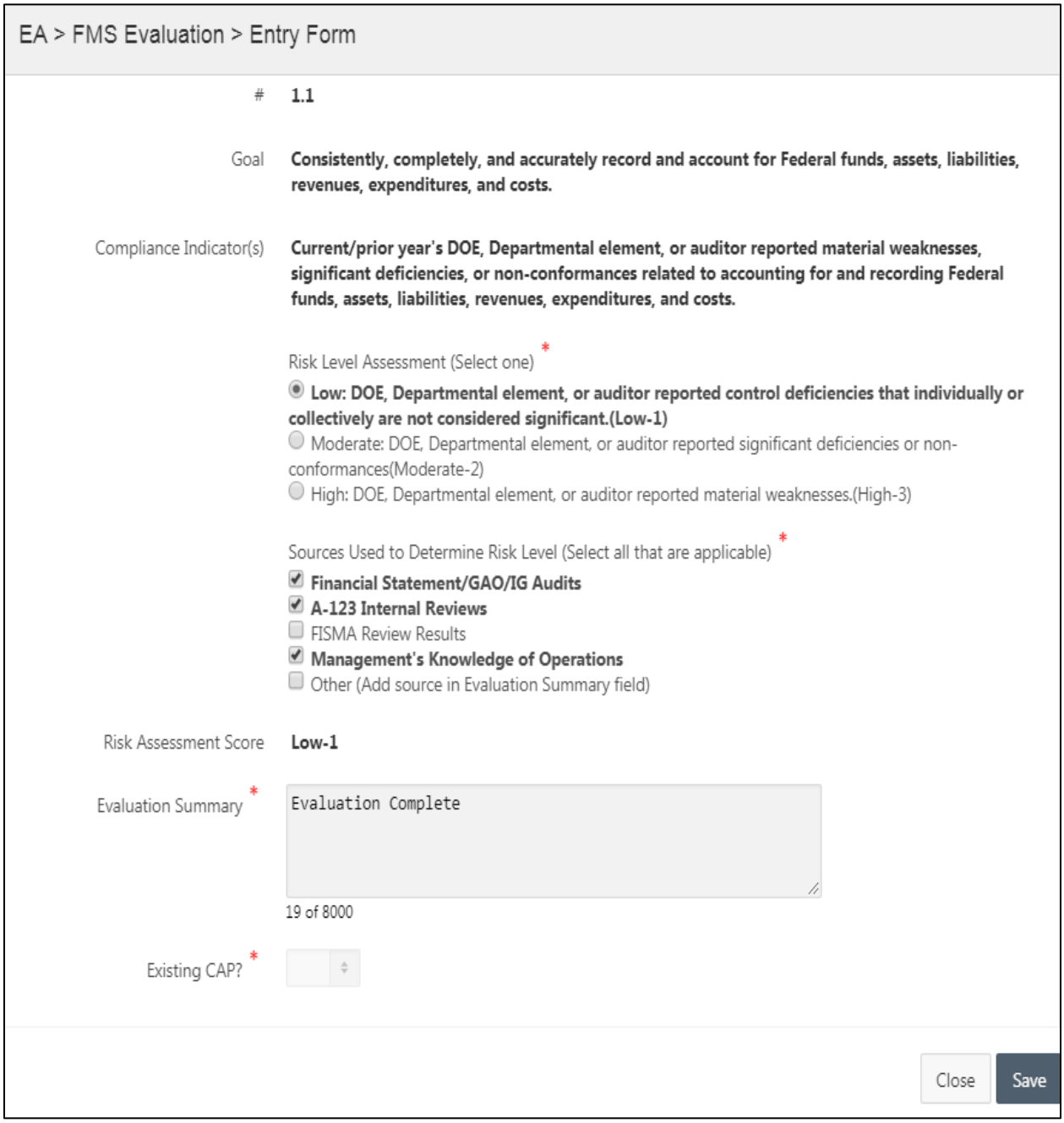
The FMS Evaluation summary page shall display the following fields:

- **#:** The number assigned to each Goal listed
- **Goal Category:** The category associated with the goal
- **Goal:** The name of the FMS Goal
- **Compliance Indicators:** Quantifiable or otherwise observable characteristics used to measure progress towards meeting the financial management goals and demonstrate how well, or at what level, each goal has been achieved.
- **Risk Level Assessment/Score:** Assists in determining the degree of risk related to a financial system complying with FFMIA
- **Sources Used to Determine Risk Level:** Reflects the categories of sources selected from the dropdown menu on the FMS Entry Form
- **Evaluation Summary:** A short description of the tangible evidence used to assess whether Departmental elements are achieving the goals that have been established for Federal Financial Management Systems.
- **Last Updated Date:** The date and time the Goal was last modified
- **Last Updated By:** Specifies the user who made the last change

Modifying a Goal

To modify information related to a Goal, locate and select the desired Goal. Goals will be displayed in the blue text indicating that users have the ability to select and modify the Goal.

Upon the selection of the desired Goal, the EA > FMS Evaluation > Entry Form dialog box will display.



FMS Evaluation Form

Requirements for each field on the form are described as follows:

- **#:** The number assigned to each Goal
- **Goal:** The name of the selected FMS Goal
- **Compliance Indicator(s):** Quantifiable or otherwise observable characteristics used to measure progress towards meeting the financial management goals and demonstrate how well, or at what level, each goal has been achieved.
- **Risk Level Assessment** (Select One): (Required) Select one of the risk level assessments. Note the selection of 2 or 3 will require a CAP identified.
    - **Low:** DOE or Departmental element reported control deficiencies that individually or collectively are not considered significant. (Low-1).
    - **Moderate:** DOE or Departmental element reported significant deficiencies or non-conformances. (Moderate-2).
    - **High:** DOE or Departmental element reported material weaknesses. (High-3).
- **Sources Used to Determine Risk Level** (Select all that are applicable): (Required) Select all sources that are applicable.
    - Financial Statement/GAO/IG Audits
    - A-123 Internal Reviews
    - FISMA Review Results
    - Management's Knowledge of Operations
    - Other (Add source in Evaluation Summary field)
- **Risk Assessment Score:** This field displays a score based on the Risk Level Assessment selection
- **Evaluation Summary:** (Required) Enter a short description of the tangible evidence used to assess whether Departmental elements are achieving the eight goals that have been established for Federal Financial Management Systems. System owners and users should determine whether the financial systems conform to federal FMS requirements. These requirements are intended to advance federal financial management by ensuring that federal financial management systems can provide reliable, consistent handling of financial data. They do so on the basis that is uniform across the federal government from year-to-year, consistently using generally-accepted accounting principles. Thus, the Evaluation Summary column should list a brief description of the documents or tools used to evaluate the effectiveness of those internal controls.

FMS Evaluation CAPS

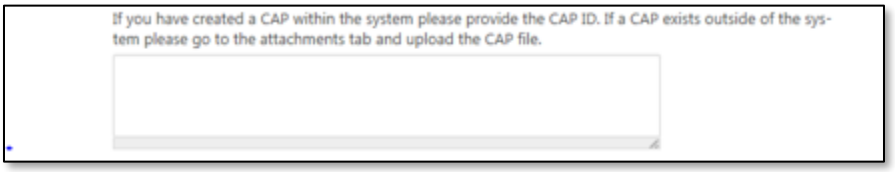
The FMS Evaluation form allows users to specify whether they would like to note an existing CAP or create a new CAP within the system.

Existing CAP: (Required with a Risk Level of 2 or 3). Users will be prompted to either provide the CAP ID outside of the system or create a new CAP within the AMERICA application.

How to select an existing CAP:

1. Within the EA > FMS Evaluation > Entry Form, locate and select the ‘Existing CAP’ question
2. Via the dropdown menu, select ‘Yes’

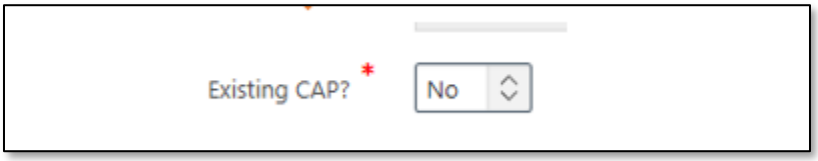
3. A text box will appear: If you have created a CAP within the system, please provide the CAP ID. If a CAP exists outside of the system, please go to the Attachments Tab and upload the CAP file.



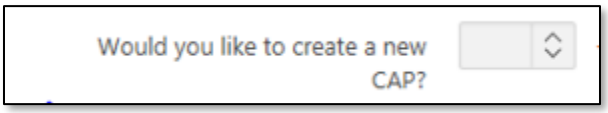
4. Enter the CAP ID information within the provided text box
5. Click the 'Save' button

How to create a new CAP:

1. Within the EA > FMS Evaluation> Entry Form, locate and select the 'Existing CAP' question.

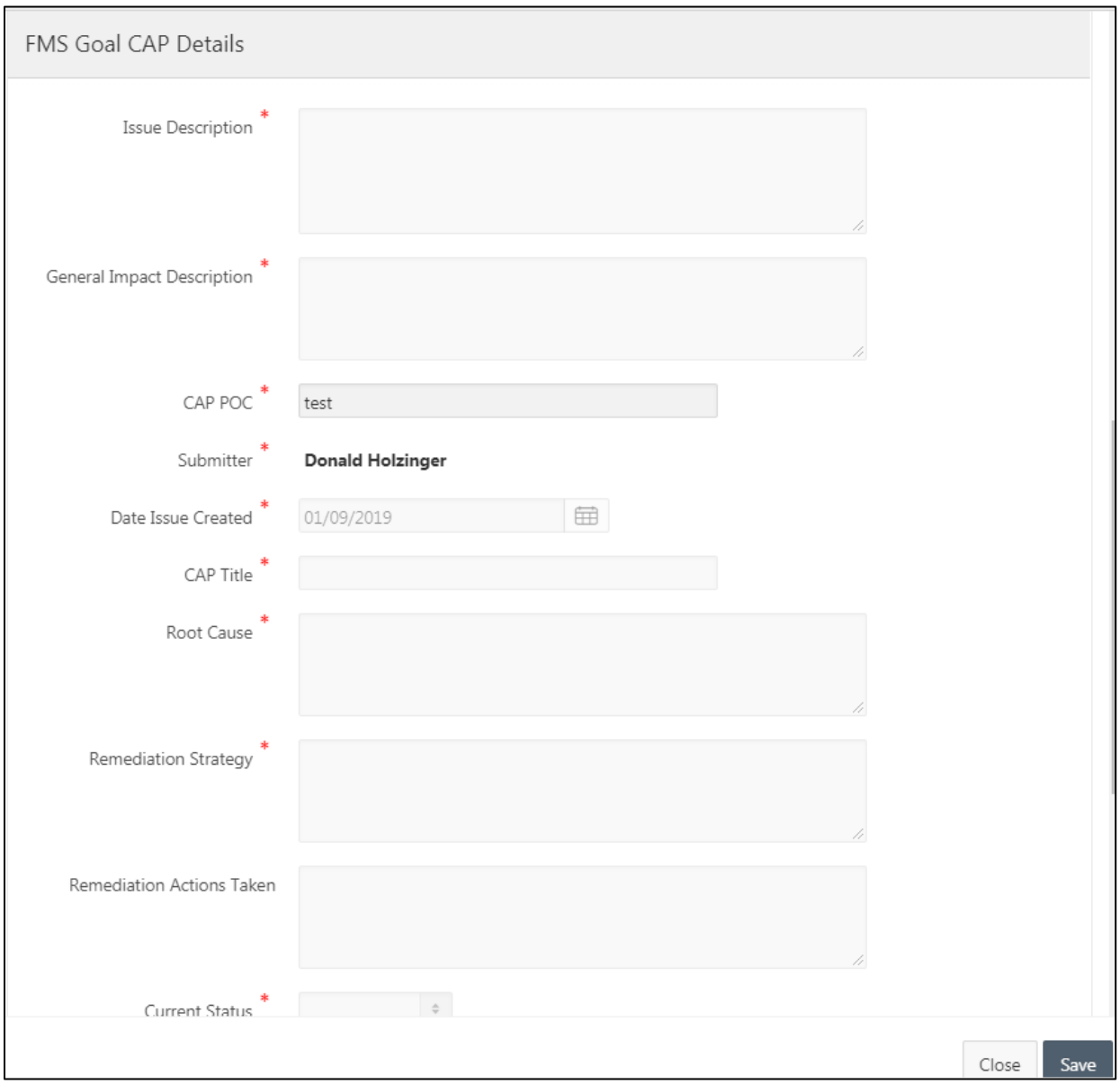


2. Via the dropdown menu, select 'No'
3. A new question will appear: Would you like to create a new CAP?



4. Select 'Yes'

The FMS Goal CAP Details section will then appear for editing. Input data in the required fields.



CAP Details Form

Requirements for each field in the CAP section are described as follows:

- **Issue Description:** (Required) Provide a brief description of the issue
- **General Impact Description:** (Required) Provide a brief description of the impact the issue is having and future potential impacts
- **CAP POC:** (Required) Enter the name of the contact person responsible for recording the action plan
- **Submitter:** Automatically populated with the individual's name who created the CAP
- **Date Issue Created:** (Required) System generated based on the date when an issue is created, but editable by the user
- **CAP Title:** (Required) Provide a name for the CAP

- **Root Cause:** (Required) Provide a brief description or summary of the root cause of the problem. It is critical to define the root cause prior to developing a corrective action strategy and milestones. Otherwise, the CAP may fix symptoms rather than addressing the core problem
- **Remediation Strategy:** (Required) Provide a brief summary of the remediation strategy
- **Remediation Actions Taken:** Update the CAP Status to correlate with the current status of the remediation activity
- **Current Status:** (Required) Select the current CAP status from the drop-down menu:
    - **New:** The need for the establishment of a CAP has been discovered through the current year's internal controls evaluation process
    - **In Progress:** Corrective actions have not yet been completed to resolve the issues and mitigate the stated impacts
    - **Implemented:** Corrective actions have been implemented to address newly discovered issues and stated impacts
    - **Closed:** All corrective actions have been completed to resolve the issue and mitigate the stated impacts
    - **Canceled:** CAP is no longer necessary based on the discovery of new or additional information
- **Planned Completion Date:** (Required) Provide the target closure date for the CAP
- **Actual Completion Date:** Provide the actual closure date once the CAP is closed. If the CAP current status is closed, the actual completion date becomes required
- **Approving Official:** (Required) Provide the name of the individual approving the CAP at the field or site level
- **Documentation Location:** (Required) Enter the location of any supplementary documentation that may support the CAP
- **User Field:** Enter any additional information the user finds helpful in performing the evaluation and documentation process specific to the CAP

  To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.

Prior Year CAPs

Please note if there is a prior year CAP on the goal, setting the Risk Level Assessment to Low will prompt the following warning message:

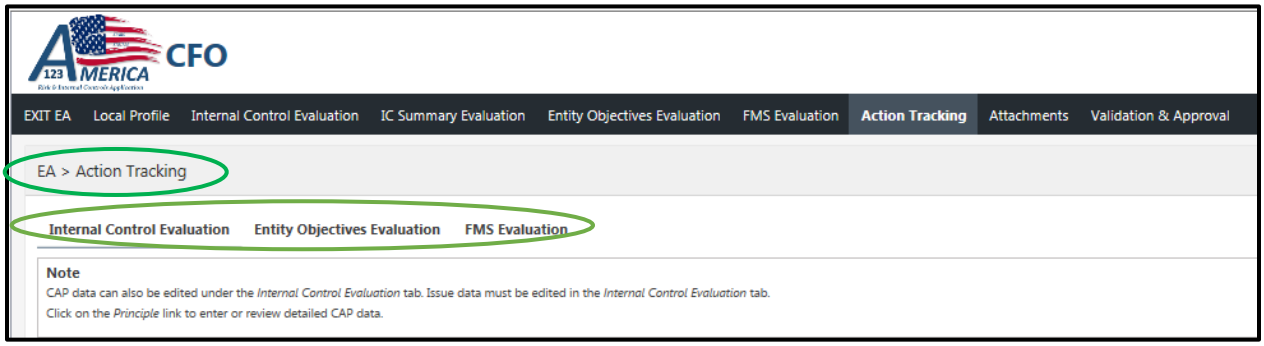
"Changing Risk Level Assessment to Low will delete all CAP Info, unless CAP was created in a prior year."

The new CAP will also appear as a new item in the Action Tracking tab under the FMS Evaluation sub-tab.

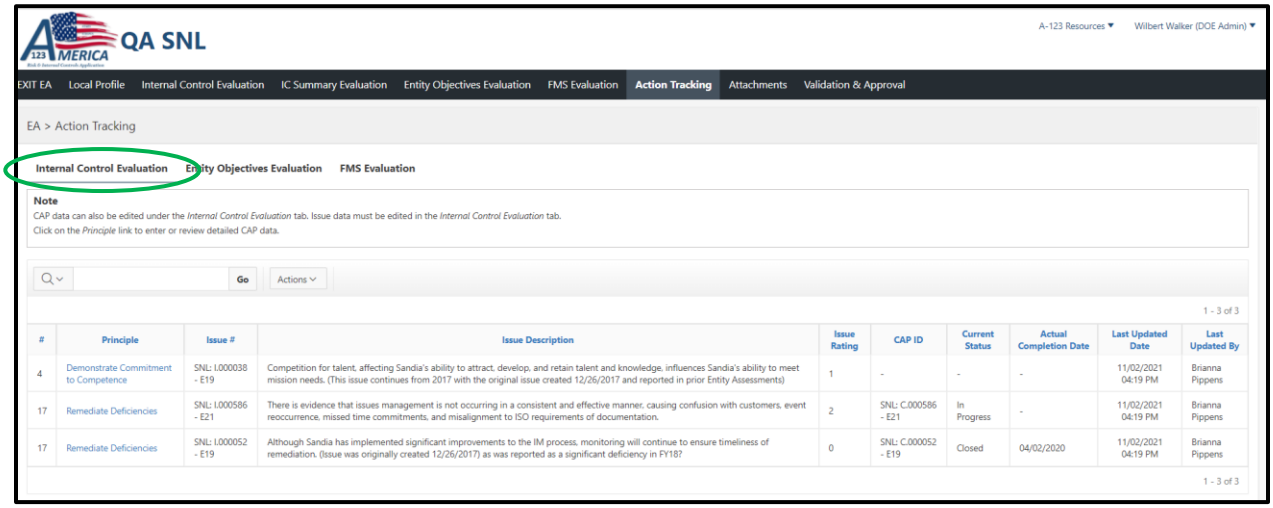
Navigating the EA: Action Tracking

The Action Tracking tab is designed to provide summary-level information of the detailed CAPs maintained locally by each Departmental element. A CAP is automatically created for each issue identified in the EA with a 2 or 3 rating. Please note the list also includes all closed and/or canceled CAPs at the bottom.

The Action Tracking tab provides 3 sub-tabs: Internal Control Evaluation, Entity Objectives Evaluation, and FMS Evaluation (when applicable). Users have the ability to view and navigate to each area's CAP via the sub-tab selections. Each tab provides a list in which users have the capability to track and modify CAPs.



Action Tracking: Internal Control Evaluation



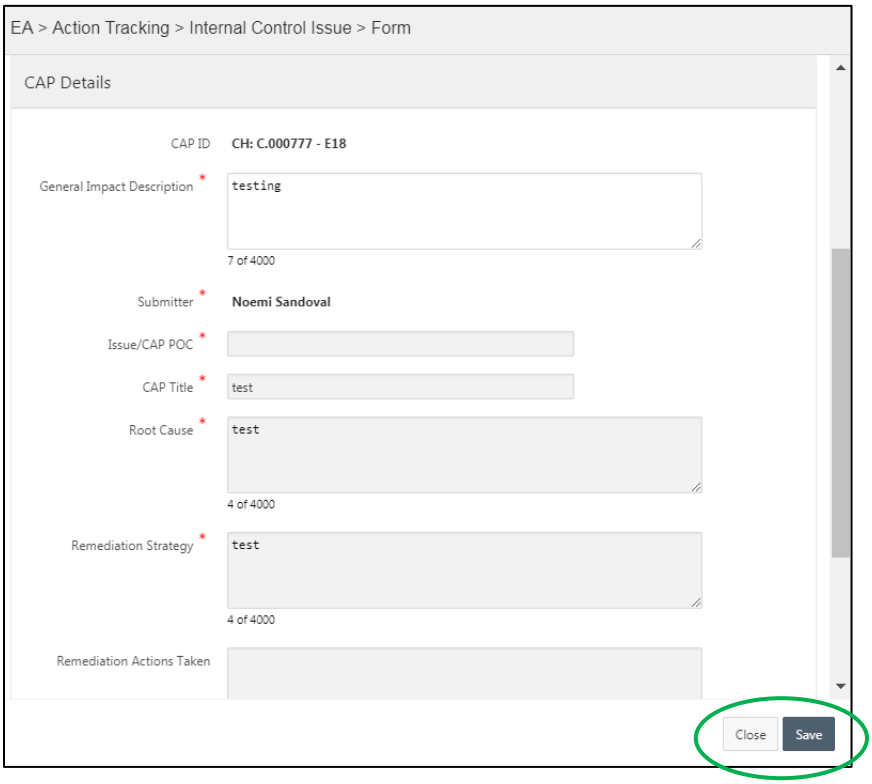
List of Internal Control Evaluation CAPS

The Summary table provides the following information:

- **#:** The number assigned to each principle
- **Principle:** The name of the principle
- **Issue #:** System generated numbering schema referencing an issue
- **Issue Description:** Brief description identified on the Internal Control Evaluation data input screen
- **Issue Rating:** Rating identified on the Internal Control Evaluation data input screen
- **CAP ID:** System generated numbering schema referencing a CAP
- **Actual Completion Date:** Date of when the CAP was closed
- **Current Status:** Status identified on the Internal Control Evaluation data input screen
- **Last Updated Date:** The date and time the principle information was last modified
- **Last Updated By:** Specifies the user who made the last change

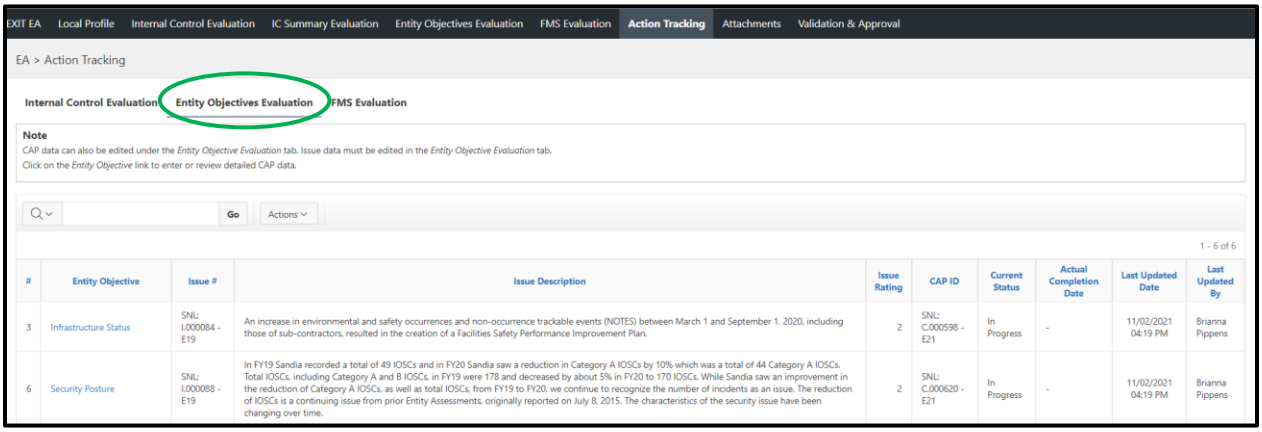
How to Modify Internal Control Evaluation CAP Information:

1. Locate and select the principle/CAP you wish to modify
2. The EA> Action Tracking> Internal Control Issue> Form will display
    a. Please note that only CAP information can be edited on the Action Tracking Form. The Issue information is not editable here. To update the Issue information, you will need to go to the Internal Control Evaluation tab.
3. Locate the CAP Details section, note that the CAP fields are editable, and changes can be made and saved



Internal Control CAP Details Form

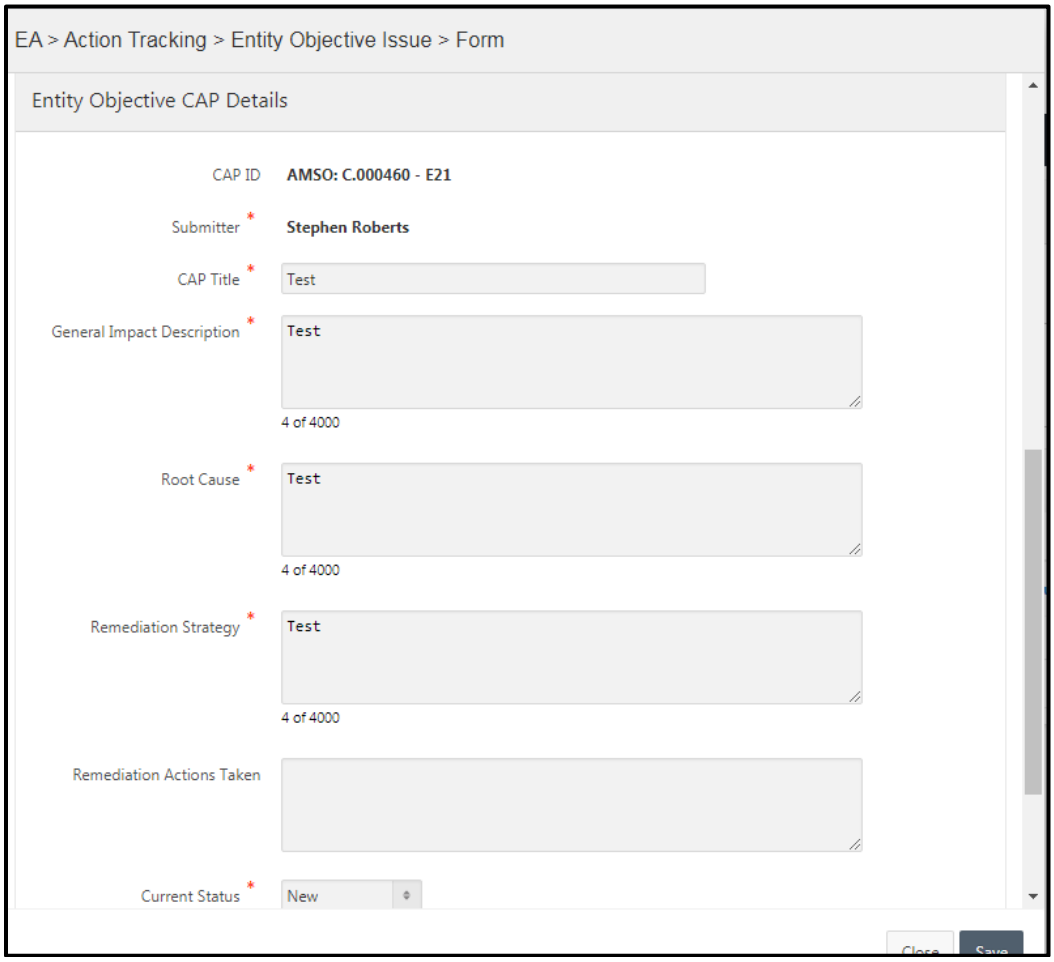
Action Tracking: Entity Objectives Evaluation



List of Entity Objective CAPS

The Summary table provides the following information:

- **#:** The number assigned to the entity objective
- **Entity Objective:** The name of the entity objective
- **Issue #:** System generated numbering schema referencing the issue
- **Issue Description:** Brief description identified on the Entity Objectives Evaluation data input screen
- **Issue Rating:** Issue Rating identified on the Entity Objective Evaluation data input screen
- **CAP ID:** System generated numbering schema referencing the CAP
- **Current Status:** Status identified on the Entity Objective Evaluation data input screen
- **Actual Completion Date:** Date of when the CAP was closed
- **Last Updated Date:** The date and time the entity objective was last modified
- **Last Updated By**: Specifies the user who made the last change

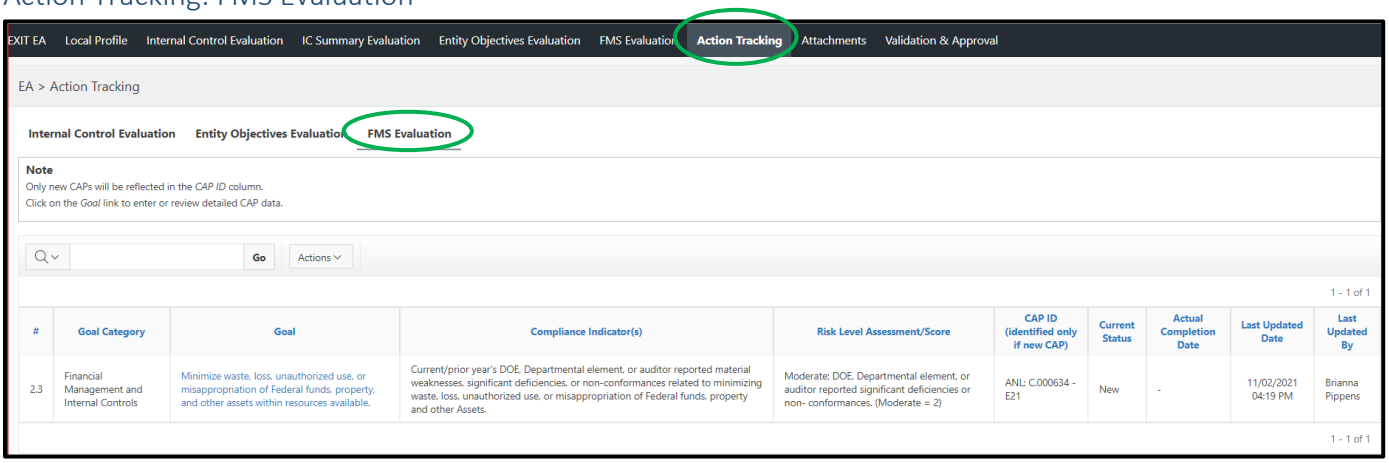


Entity Objective CAP Detail Form

How to Modify Entity Objectives Evaluation CAP Information:

1. Locate and select the entity objective/CAP you wish to modify
2. The EA > Action Tracking > Entity Objective Issue > Form will display
    a. Please note that only CAP information can be edited on the Action Tracking Form. The Issue information is not editable. To update the Issue information, you will need to go to the Entity Objectives Evaluation tab
3. Locate the CAP Details section, note fields are editable, and changes can be made and saved

Action Tracking: FMS Evaluation



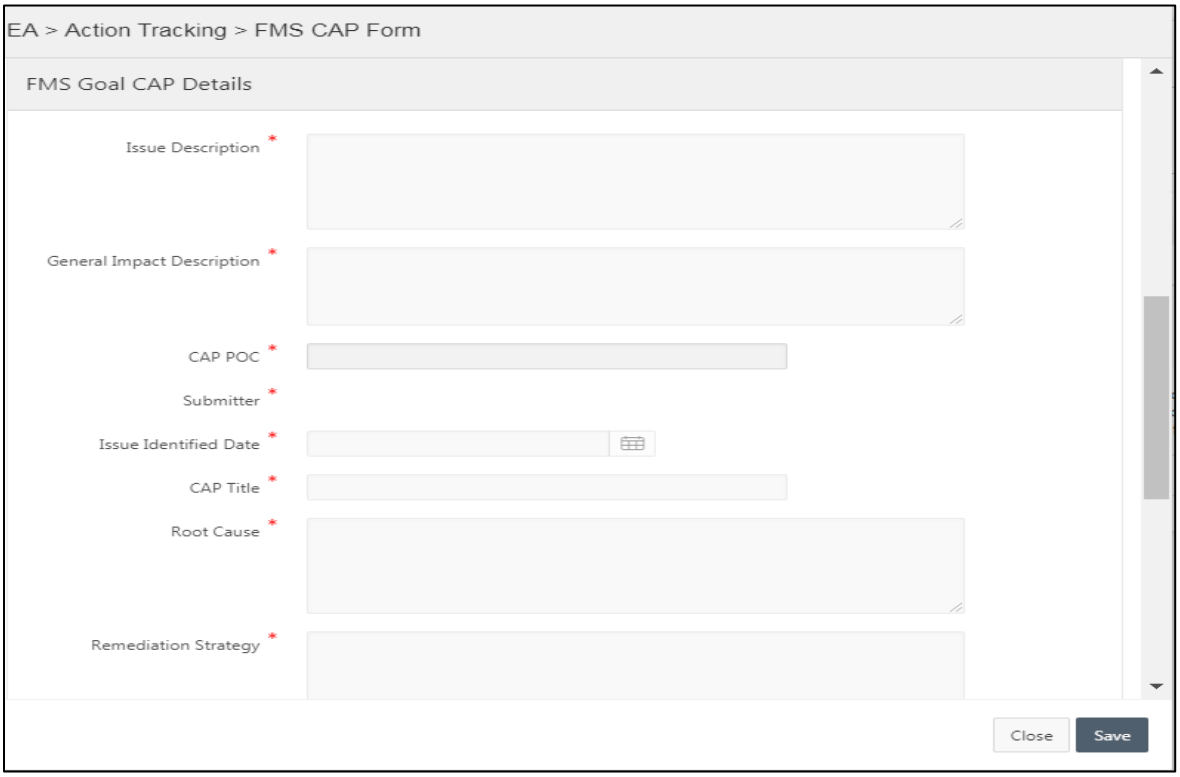
List of FMS CAPs

The Summary table provides the following information:

- **#:** The number assigned to the Goal
- **Goal Category:** The category associated with the goal
- **Goal:** The name of the FMS Goal
- **Compliance Indicator(s):** Quantifiable or otherwise observable characteristics used to measure progress towards meeting the financial management goals and demonstrate how well, or at what level, each goal has been achieved
- **Risk Level Assessment/Score:** Risk Level rating identified on the FMS Evaluation data input screen
- **CAP ID (identified only if new CAP):** System generated numbering schema referencing a CAP
- **Current Status:** Status identified on the FMS Evaluation data input screen
- **Actual Completion Date:** Date of when the CAP was closed
- **Last Updated Date:** The date and time the FMS information was last modified
- **Last Updated By:** Specifies the user who made the last change

How to Modify FMS Evaluation CAP Information:

1. Locate and select the Goal/CAP you wish to modify
2. The EA > Action Tracking > FMS CAP Form will display
    a. Please note that only CAP information can be edited on the Action Tracking Form. The Issue information is not editable. To update the Issue information, you will need to go to the FMS Evaluation tab
3. Locate the CAP Details section, note fields are editable, and changes can be made and saved



FMS CAP Details Screen

Navigating the EA: Attachments

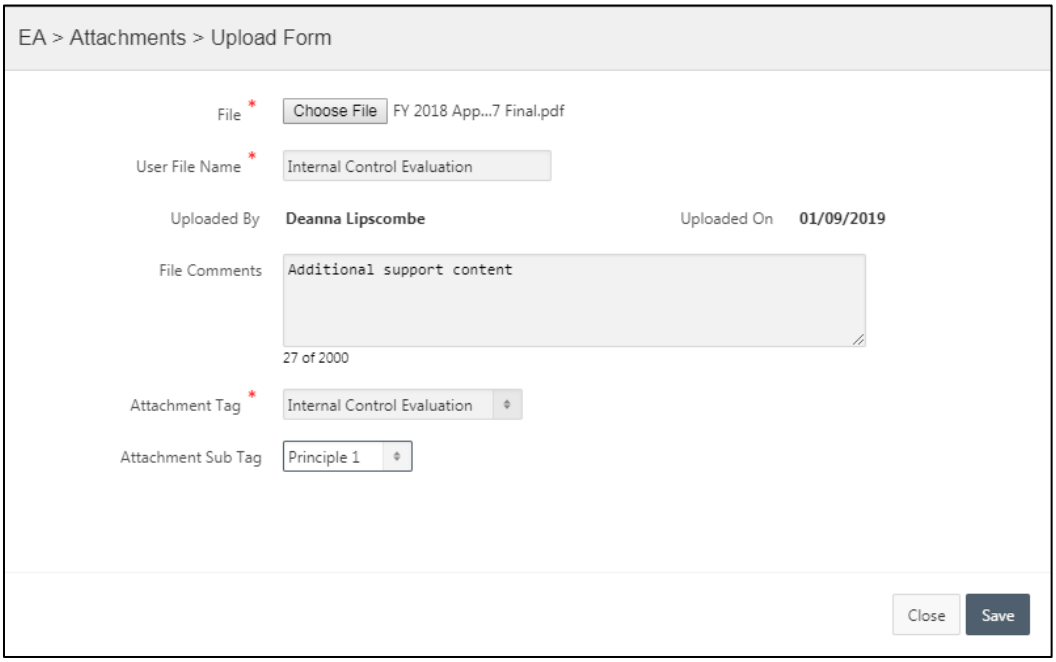
Users will have the ability to add supplementary documents to support their entity data and findings via the Attachments tab. If there are no documents uploaded for a specific EA, upon selecting the Attachments tab, the workspace will read that there are no files uploaded for this assessment.

Uploading a File

Locate and select the 'Upload' button. Provide content in the following fields:

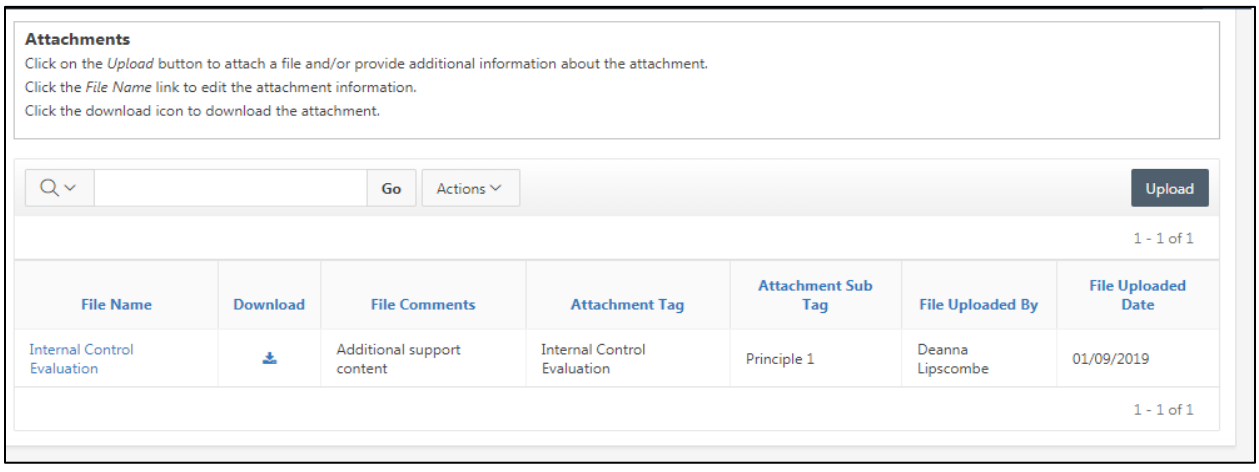
- **File:** (Required) Click on 'Browse', specify the file location to display, and select file to upload
- **User File Name:** (Required) Type in a custom filename
- **File Comments:** Provide an explanation or annotation for the file
- **Attachment Tag:** (Required) Specify which EA tab this attachment is associated with
- **Attachment Sub Tag:** Specify a sub-tag for the attachment

To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.



Once the file is uploaded, it will be hosted on the Attachments tab along with the following summary fields:

- **File Name:** User given name to uniquely identify the file provided
- **Download:** The option to Open or Save the file
- **File Comments:** User explanation or annotation for the file uploaded
- **Attachment Tag:** User selected tag to associate the file with an EA tab
- **Attachment Sub Tag:** User selected sub-tag to associate the file with an EA
- **File Uploaded By:** Specifies the user who uploaded the file
- **File Uploaded Date:** The date and time when the file was uploaded



Modifying a File

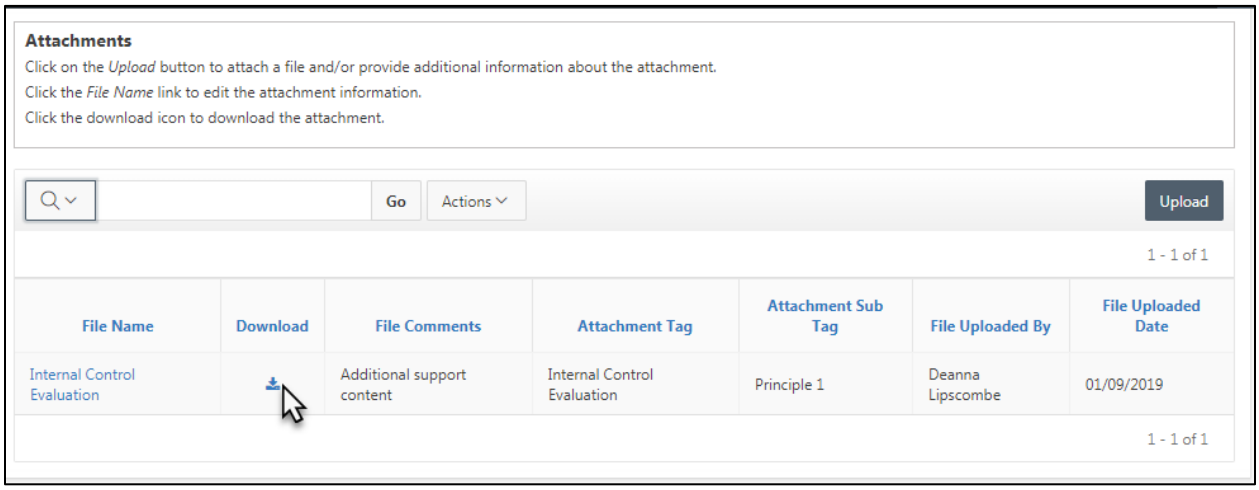
Within the Attachments summary table, locate the file desired. Select the 'File Name' within the summary table. Modify the content in the following fields:

- **File:** (Required) Click on 'Browse', specify the file location to display, and select file to upload
- **User File Name:** (Required) Type in a custom filename
- **File Comments:** Provide an explanation or annotation for the file
- **Attachment Tag:** (Required) Specify which EA tab this attachment is associated with
- **Attachment Sub Tag:** Specify a sub-tag for the attachment

To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.

Downloading a File

1. Within the Attachments summary table, locate the file desired. Select the download icon within the summary table.
2. If asked, choose whether you wish to 'Open' or 'Save' the file



Navigating the EA: Workflow & Validations

Prior to workflow submission, all entity assessments must pass validations.

There are validation rules in place to assure the successful completion of each assessment. Below are the validation rules:

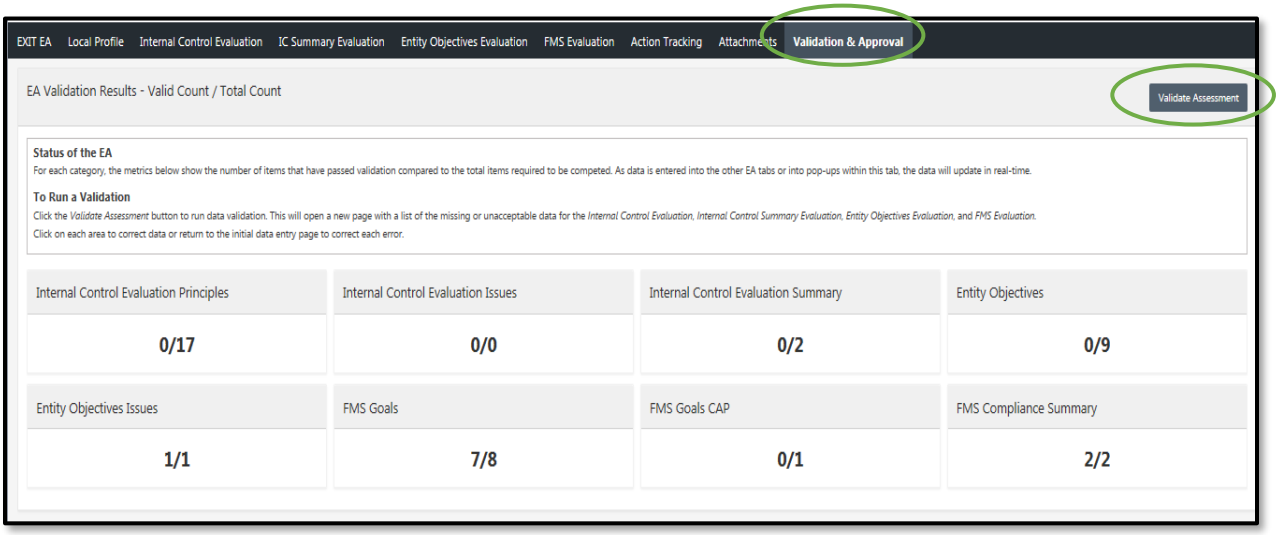
- CAPs must be closed or canceled if the issue rating is changed from 2 or 3 to a 1
- All required fields must be populated
- When Designed & Implemented response is 'No' an associated issue must be created with an issue rating 2 or 3
- All issues rated a 2 or 3 must have an associated CAP
- If the CAP current status is closed, the actual completion date must be provided

A validation can be run at any time and as often as needed. However, a successful validation must be achieved before the submission can be routed to the Approver. View and manage the status of your EA using the validation results table on the Validated and Approval tab. For each category, the metrics will show the number of items that have passed validation compared to the total items required to be

completed. As data is entered into the other EA tabs or pop-ups within this tab, the data will update in real-time.

How to Access the Validations Table

1. Within the EA module, locate and select the Validated and Approval tab
2. The workflow and validations page shall display. Note the top section will display the validation results for each category noting the Valid Count / Total Count



Validation & Approval Valid Count/Total Count

How to View and Validate the Assessment

1. Within the EA module, locate and select the Validated and Approval tab
2. Locate and select the 'Validate Assessment' button

Upon the selection of the 'Validate Assessment' button, the system will provide a listing of needed corrections for each category. Each EA category is hosted on its own tab: Internal Control Evaluation, Entity Objectives, and FMS (if applicable). Each category will host a family of sub-tabs to be viewed and validated. Below is the listing of categories and their sub-tabs:

Internal Control Evaluation

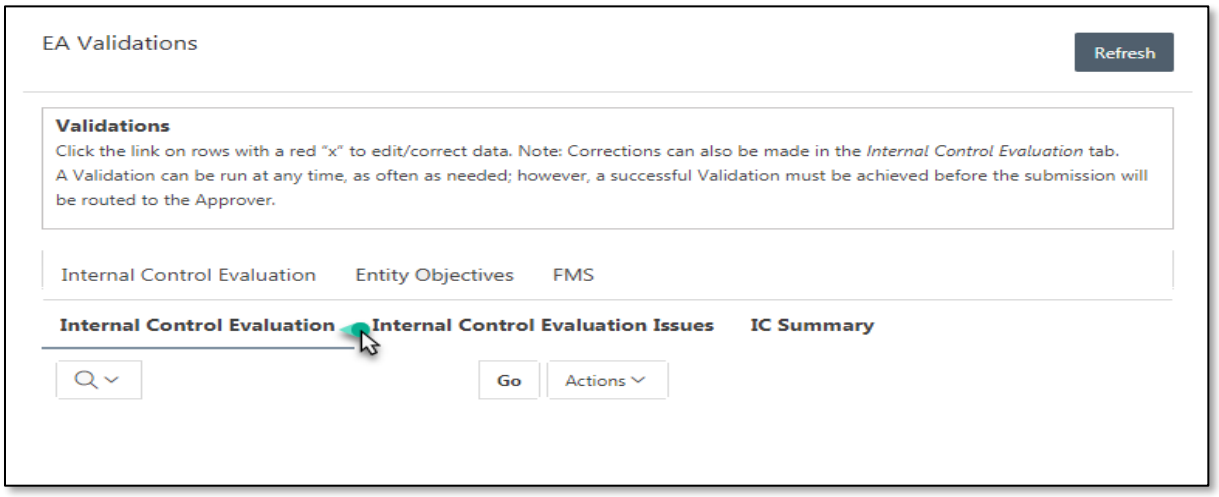
- Internal Control Evaluation
- Internal Control Evaluation Issues
- IC Summary

Entity Objectives

- Entity Objectives Evaluation
- Entity Objectives Issues

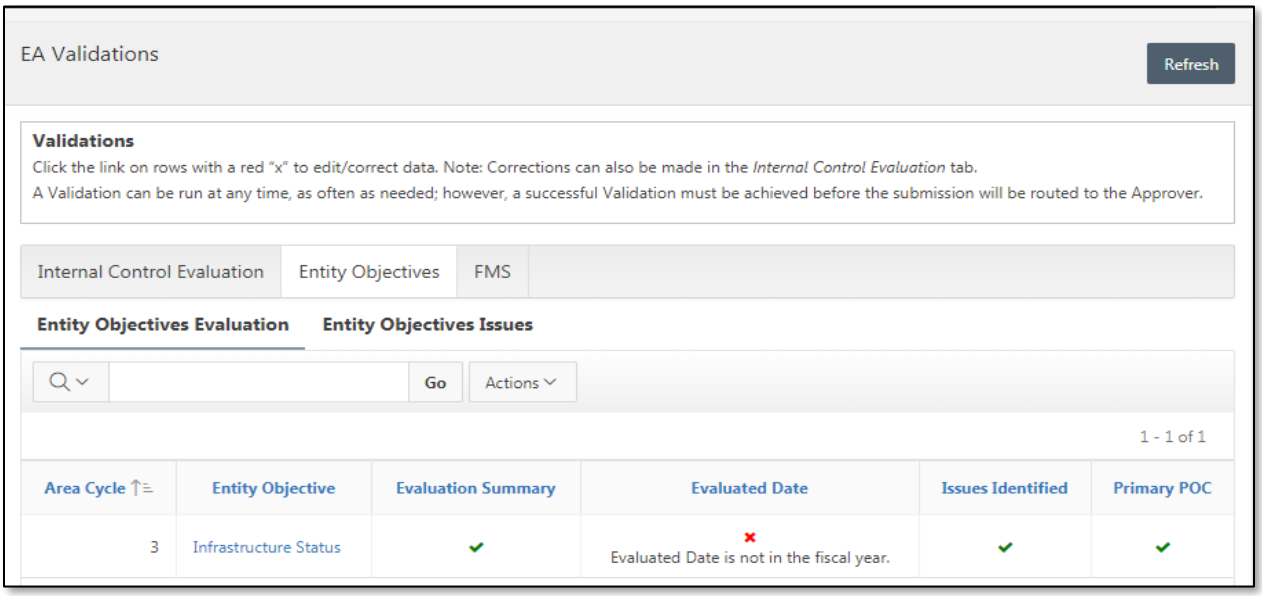
FMS

- FMS Goals
- FMS Goals CAP
- FMS Compliance



EA Validation & Approval: Category and Sub-Tabs Breakdown

Each category and sub-tab will host a series of fields that are required for workflow submission. The required fields and/or other requirements will be identified across the categories via the summary table. Click the blue link on rows with a red "X" to edit/correct data. Note: Corrections can be made within the validations page or the tabs within the global menu.



How to Correct Validations

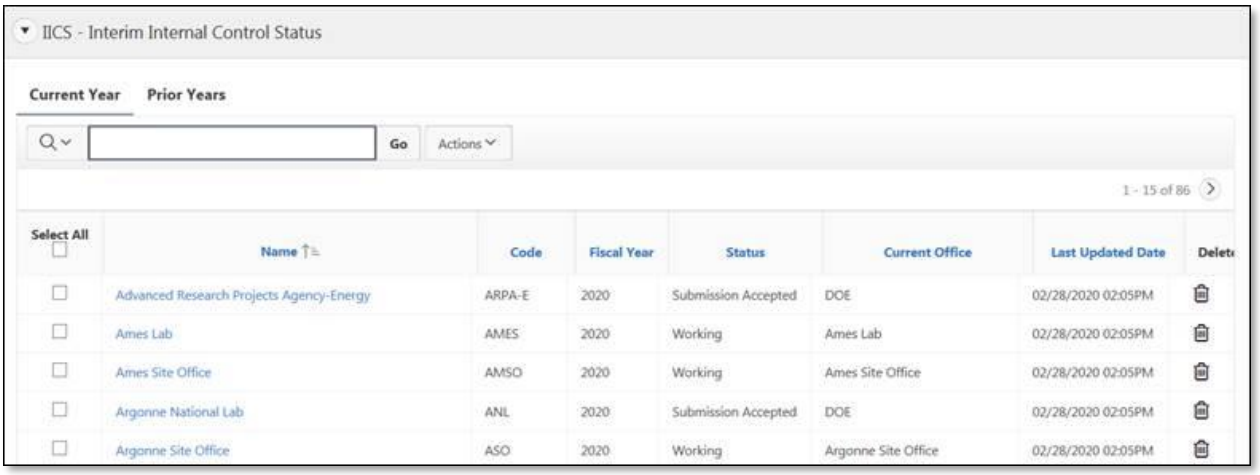
1. Locate the category and row you wish to modify. Note the item(s) identified with a red 'X' as these fields will need to be modified/populated
2. Navigate and select the column shown in the blue text within the row
3. The category entry form will display. Navigate to the fields that need updating
4. Update the fields and select 'Save.'
5. Note upon saving, if the validations were corrected, the row would be removed from the Validations page

Once all validations have been reviewed and are addressed, users may proceed to finalize the assessment for approval via the workflow.

Interim Internal Controls Status (IICS)

An IICS assessment is a questionnaire that provides a mid-year update to CF Headquarters confirming that annual non-financial and financial risk assessments are being performed, risk exposure ratings updated, and whether any issues have been identified that would rise to the level of a significant deficiency or material weakness. The IICS also confirms that corrective actions are being taken on any significant issues identified in the current or prior year assessments.

An IICS is automatically created once the DOE Admin creates the entity's EA. Both the current year and prior year IICS modules are available. To access the IICS available for your organization and downstream entities in your program hierarchy, navigate to the IICS section of the A-123 Home Page.



IICS Module

The following information will display in the summary table:

- **Name:** The assigned entity. The entity name will be displayed in blue text, indicating the user has the ability to open and view the assessment
- **Code:** The entity office code
- **Fiscal Year:** This field is automatically populated with the current fiscal year
- **Status:** The current status of the assessment
    - **Working:** Users are currently working on tasks within the assessment
    - **Pending Approval:** Assessment is waiting for approval from the responsible entity
    - **Submission Accepted:** DOE has accepted the entity's assessment
- **Current Office:** The office currently responsible for the assessment
- **Last Updated Date:** The date the assessment was last updated

To access the desired IICS assessment, click on the blue text with that entity name.

IICS Overview

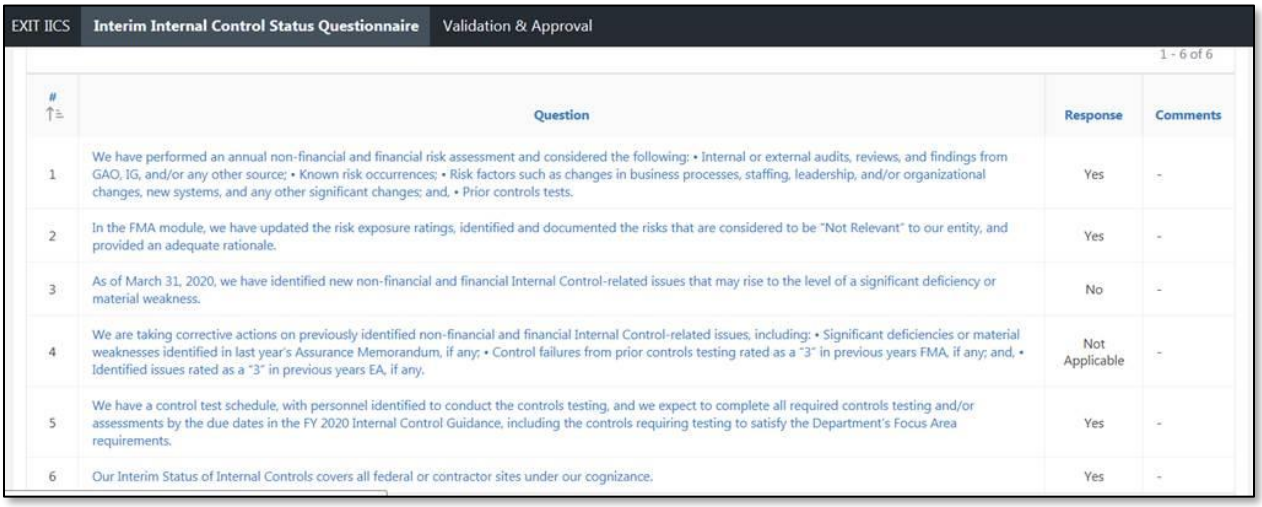
There will be three tabs that will display in the global menu once the desired IICS is selected:

- Exit IICS: Returns you to the homepage
- Interim Internal Control Status Questionnaire
- Validation and Approval

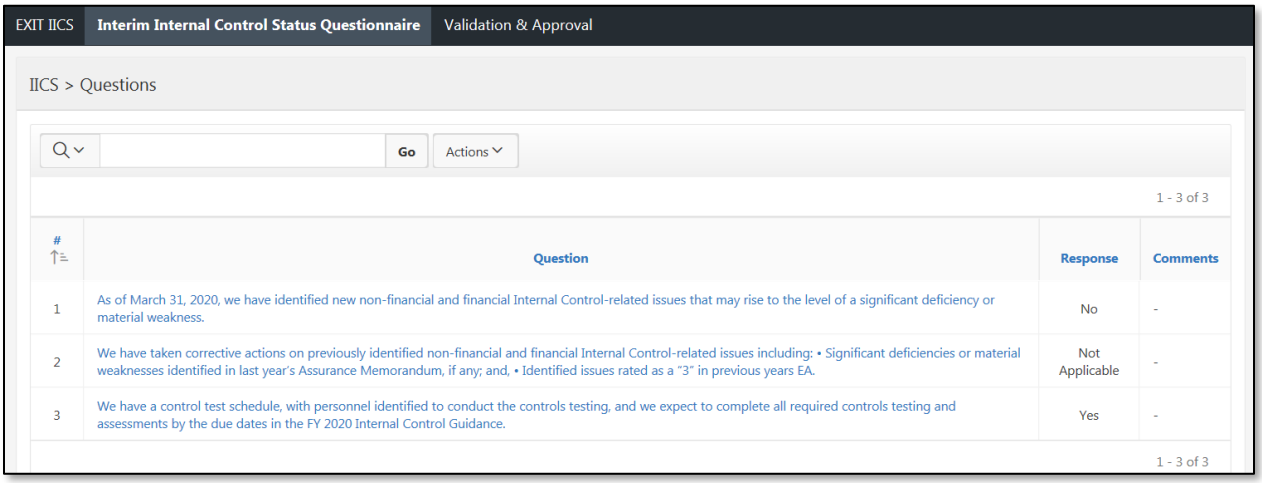
Interim Internal Control Status Questionnaire

The number of questions on the IICS questionnaire depends on the EA Assignment for each entity, determined based on the current year's Internal Controls Guidance. Default EA assignments create an IICS with 6 questions. Smaller organizations that do not do FMAs or an FMS evaluation receive an abbreviated IICS with only 3 questions.

An example of the IICS Questionnaire is provided below. Select the desired question, which is in blue text, to provide a response.



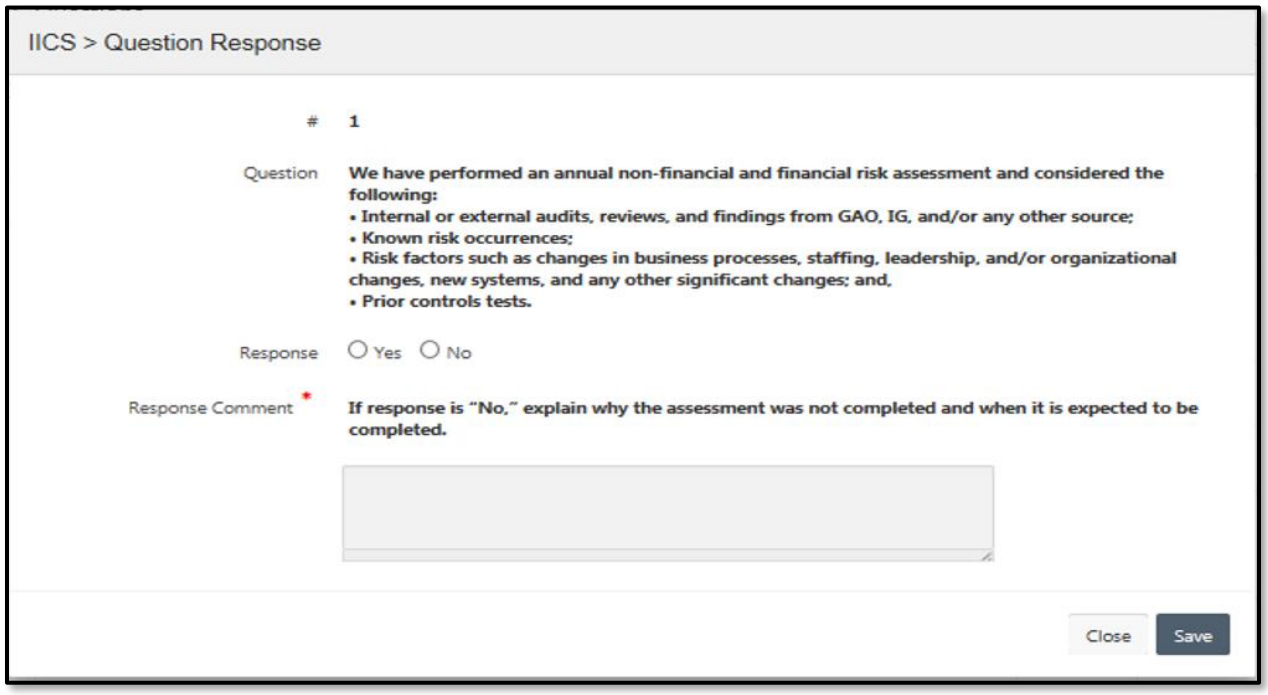
Default - IICS



Abbreviated IICS

Once a question is selected, a popup box will display the following information:

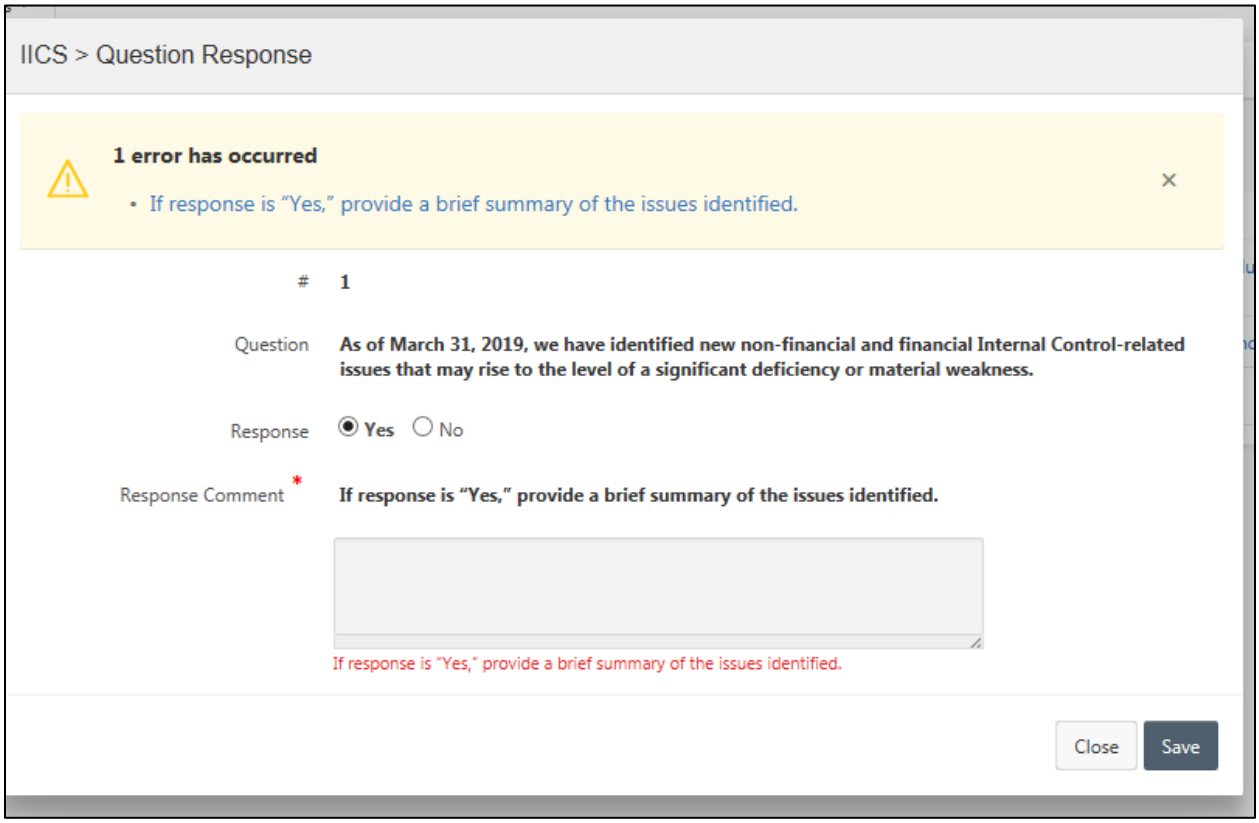
- **#**: The number assigned to the question
- **Question:** The question that is listed on the summary page will display again here for review
- **Response**: (Required) A radio button selection for 'Yes' or 'No'
- **Response Comment**: A response comment may be required based on the Response selection. Be sure to read which response type requires a comment; it varies between 'Yes' and 'No'



IICS Questionnaire

To retain the updates made, select the 'Save' button. To disregard changes made, select the 'Close' button.

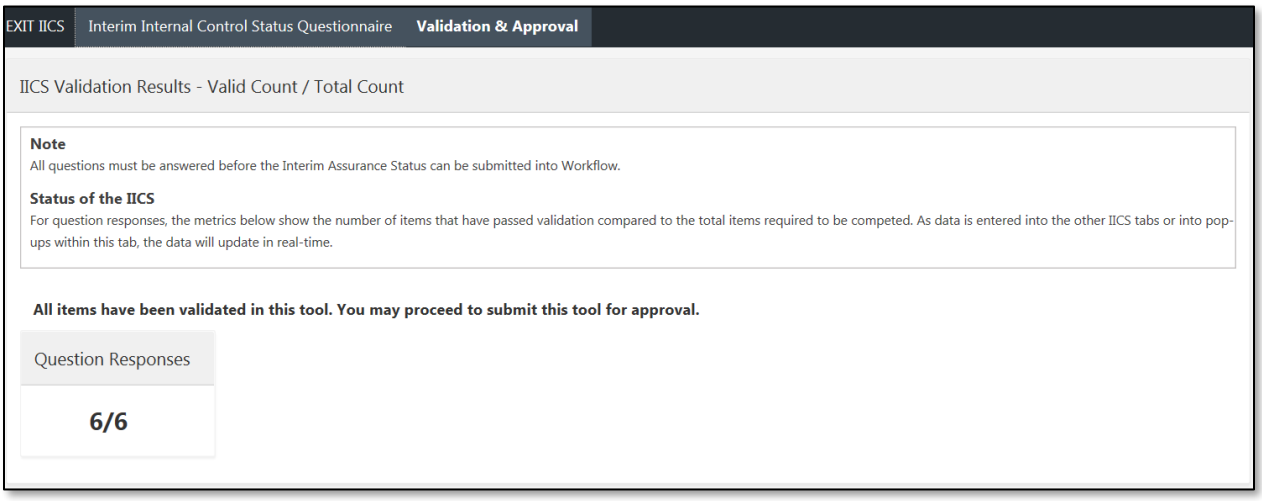
If you attempt to save a response without filling in the required comment, you will receive an error message. This is a hard stop validation, and the radio button response will not be saved until a comment is entered.



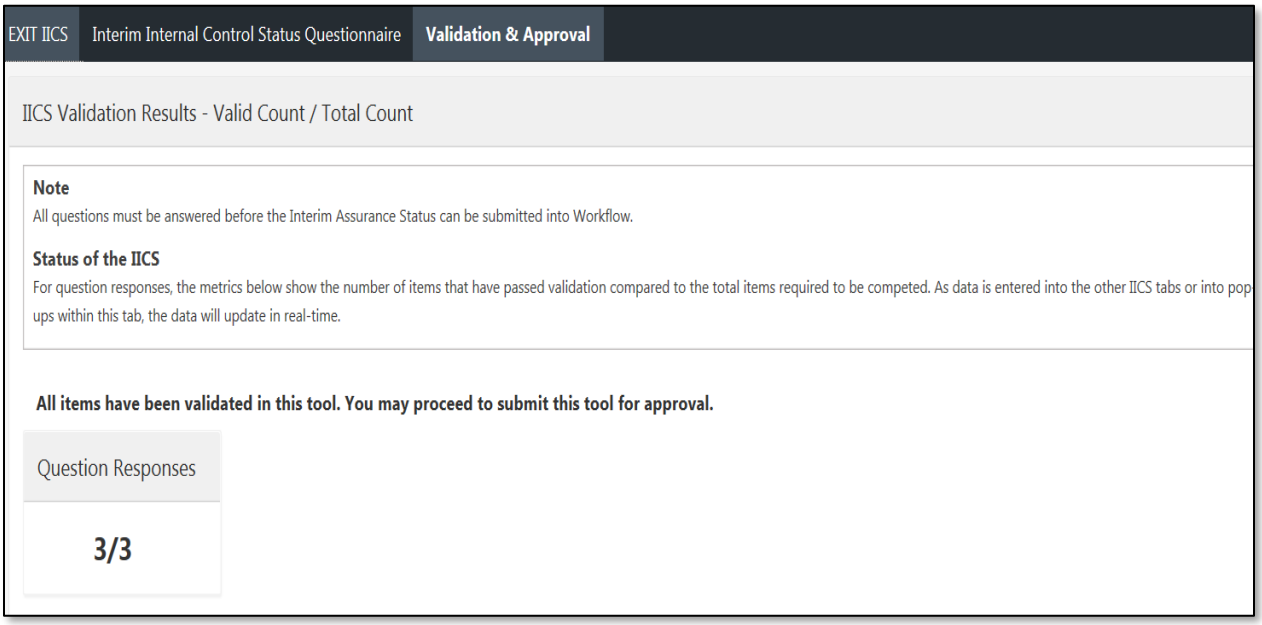
IICS Error Message in response to Issues Identified

IICS Validations

Navigate to the Validation and Approval tab within IICS. Prior to an IICS assessment being submitted into the workflow, it must pass all validations. IICS validations are for the question responses. They will display the valid count/total count. All questions must have a response to complete the validations successfully. If a question has not been answered, navigate back to the Interim Internal Control Status Questionnaire tab to respond.



Example – IICS Default Assignment Validations Page



Example – IICS Abbreviated Assignment Validations Page

Financial Management Assessment (FMA) Module

The Financial Management Assurance (FMA) module records the financial risks and controls evaluations of the Department of Energy (DOE or the Department). It facilitates data updates, data verification, and data analysis.

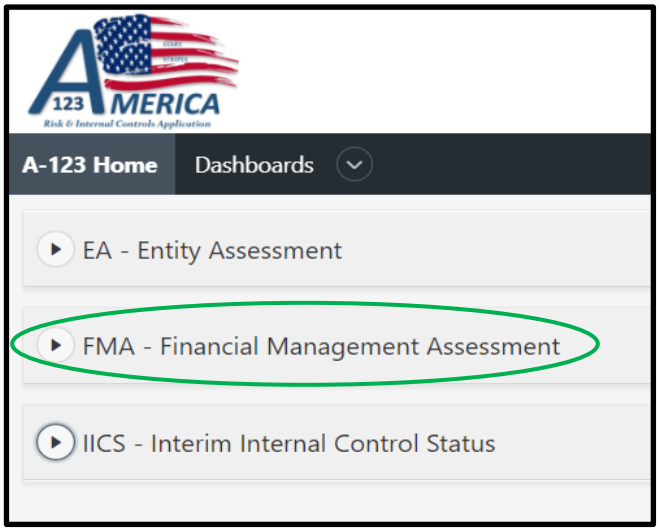
The FMA has two main aspects: The Framework side and the Analysis side.

- The Framework side consists of a Corporate Framework, which is determined by DOE Headquarters. The Corporate Framework consists of Cycles, Processes, Sub-Processes, Corporate Risks, Corporate Controls, and Focus Areas and is managed by the DOE Admins.
- The Analytical side consists of the risk assessment where HQ and Field entities rate various processes, risks, and controls. It also consists of CAPs, which include a remediation strategy for risks not adequately mitigated by their existing controls.

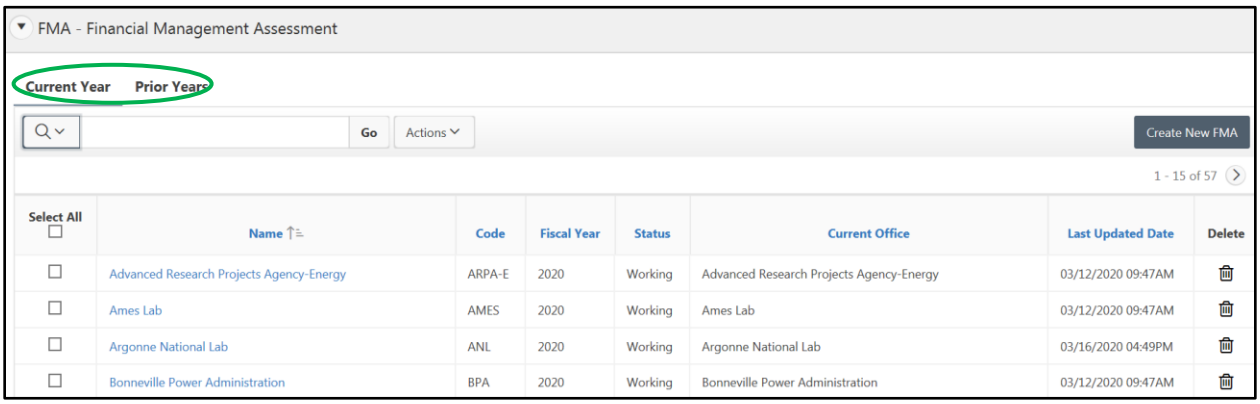
FMA Homepage

First to access the FMA homepage, log into the AMERICA system either through the secure gateway via the iPortal or the direct link https://iportalwc.doe.gov/a123.

Within the AMERICA homepage, navigate to the FMA – Financial Management Assessment tab, located under the A-123 Home Tab.



The A-123 homepage will display all of the FMAs available to each user based on the assigned role(s). Authorized users will have “Read Only” access to downstream FMAs. In addition, Current Year and Prior Year sub-tabs appear at the top of the page. After the Current Year FMAs are approved, these FMAs will be locked and archived under the Prior Years sub-tab and available as “Read Only” for future reference.



FMA – A-123 Homepage

The A-123 Homepage includes the following summary information:

- **Name:** The assigned entity name is displayed in the blue text, indicating the user can open/view the assessment
- **Code:** The entity office code
- **Fiscal Year:** This field is automatically populated with the current fiscal year
- **Status:** The current status of the assessment – Working, Pending Approval, and Submission Accepted
    - Working – Users are currently working within the FMA prior to submission
    - Pending Approval – The FMA is waiting for approval from an Approver consistent with the Workflow hierarchy
    - Submission Accepted - All Approvals have been complete, and DOE has accepted the FMA.
- **Current Office:** The office currently responsible for the assessment
- **Last Updated Date:** The date and time the assessment was last updated

Opening an FMA

To open an FMA, click on Name of the FMA in blue text; or type a Name or Code in the search box, select "Go," then click on Name. The FMA will open to the FMA homepage.

FMA Global Menu

The FMA module is organized into 5 tabs: Local Profile, Assessments, Action Tracking, Attachments, and Validation & Approval. These tabs are shown in the FMA global menu along with the Exit FMA button, which will return the user to the AMERICA homepage.

FMA Global Menu

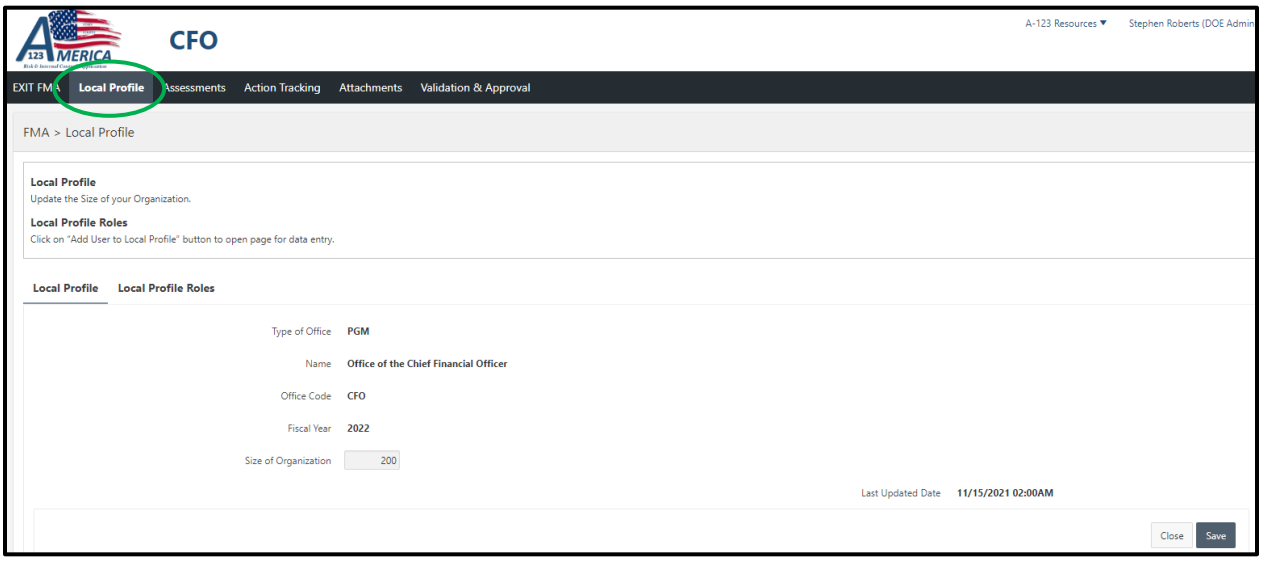
Navigating the FMA: Local Profile

The Local Profile tab is used to record specific entity information and is divided into the entity details (Local Profile) and optional personnel assignments (Local Profile Roles).

Local Profile

The Local Profile tab captures the entity profile information, including the following fields:

- **Type of Office:** This field will automatically populate from the entity name selected during FMA setup
- **Name:** The entity name is selected from a drop-down menu during FMA setup
- **Office Code:** This field will automatically populate from the entity name selected during FMA setup
- **Fiscal Year:** This field will automatically populate with the current fiscal year
- **Size of Organization:** Enter the number of FTEs, or Full-Time Equivalents
- **Last Updated Date:** The date and time the FMA was last updated



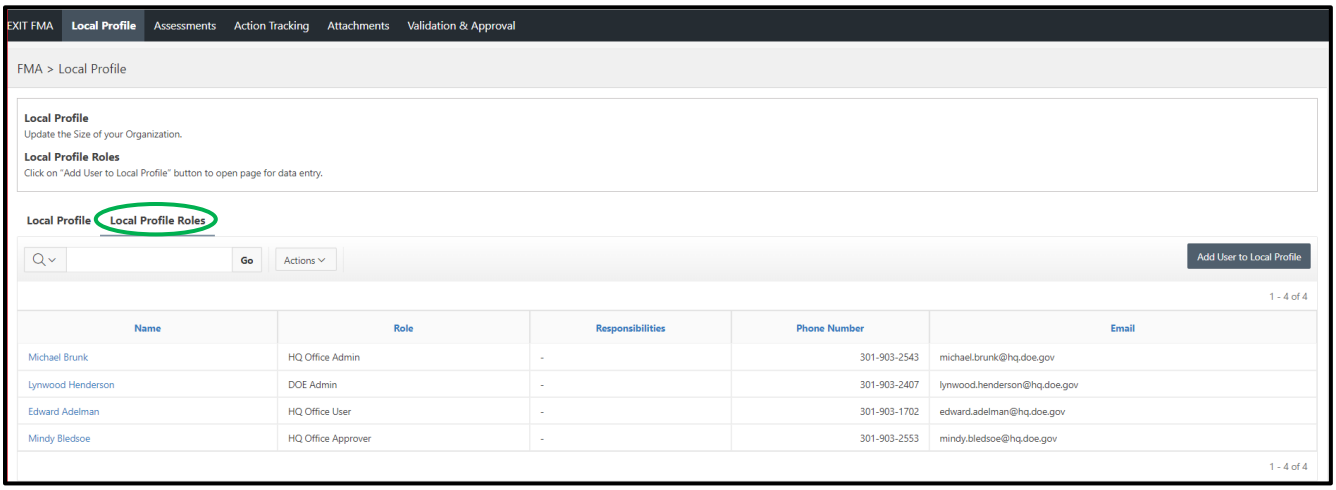
FMA Module - Local Profile

Local Profile Roles

The Local Profile Roles tab captures users' roles and locally-assigned responsibilities for the entity's FMA. Only the Local Admin has the ability to add individuals and responsibilities for their entity personnel in the Local Profile Roles tab. This input is strictly informational and does not control or impact who can enter data into the FMA.

The Local Profile Roles summary table includes the following fields:

- **Name:** The user authorized to access the entity's FMA
- **Role:** System generated per the Name
- **Responsibilities:** The user's responsibilities assigned by the Local Admin (OPTIONAL)
- **Phone Number:** System generated per the Name
- **Email:** System generated per the Name

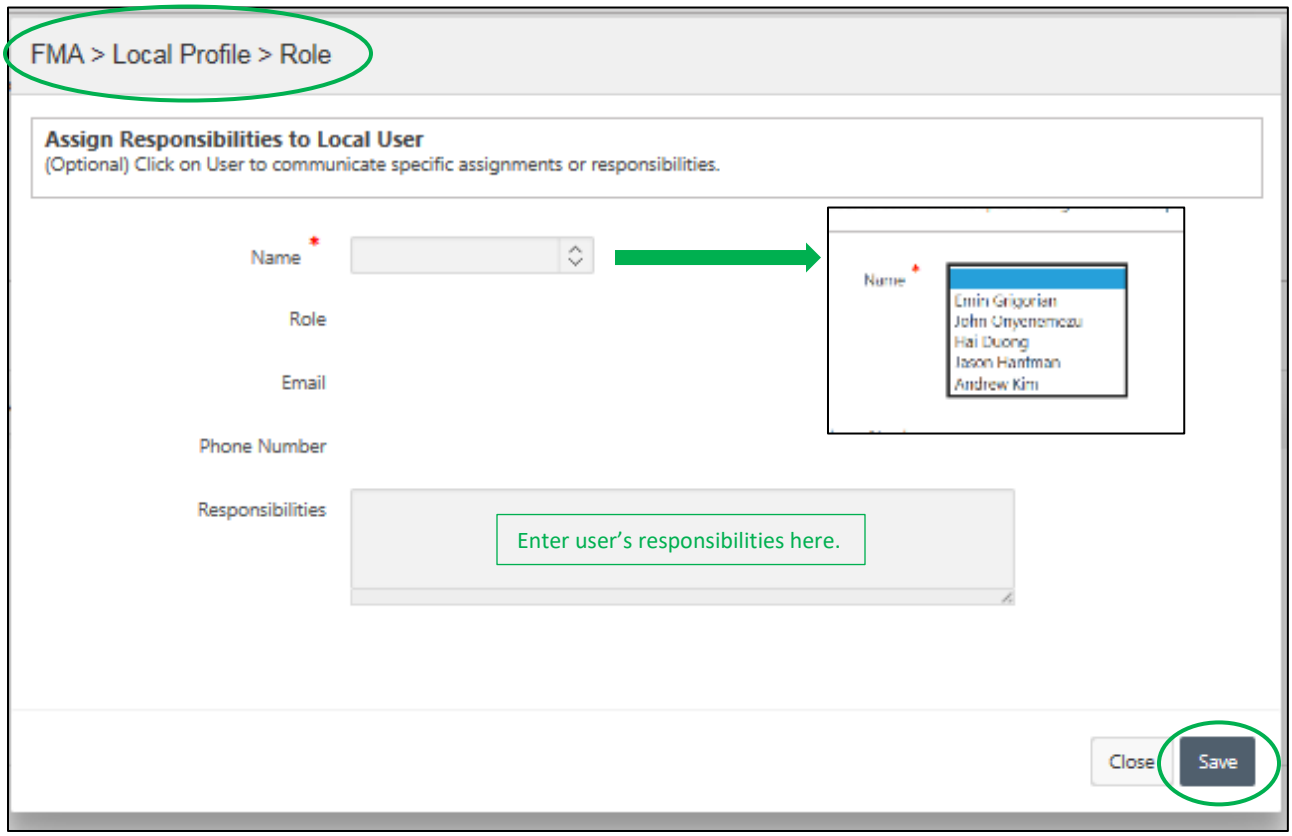


FMA Module - Local Profile Roles

Adding Users to the Local Profile Roles

Only the Local Admin will have the ability to add users to the Local Profile Roles page.

1. Within the Local Profile>Local Profile Roles tab, locate and select the 'Add User to Local Profile' button.
2. The FMA>Local Profile>Role form will display with the following fields:
    a. **Name:** (Required) Selection from dropdown list of persons pre-approved for AMERICA access.
    b. **Role:** System generated per the Name selection
    c. **Email:** System generated per the Name selection
    d. **Phone Number:** System generated per the Name selection
    e. **Responsibilities:** Local Administrator input
3. Locate the 'Name' field. Select the value dropdown next to the field. The value list shown will display users that have been assigned to the entity.
4. Locate and select the desired user. The user role, email, and phone number will populate based on the user selection.
5. Enter the user's Responsibilities within the text box. (Optional)
6. Select the 'Save' button



FMA Module - Local Profile Roles: User Selection and Responsibilities

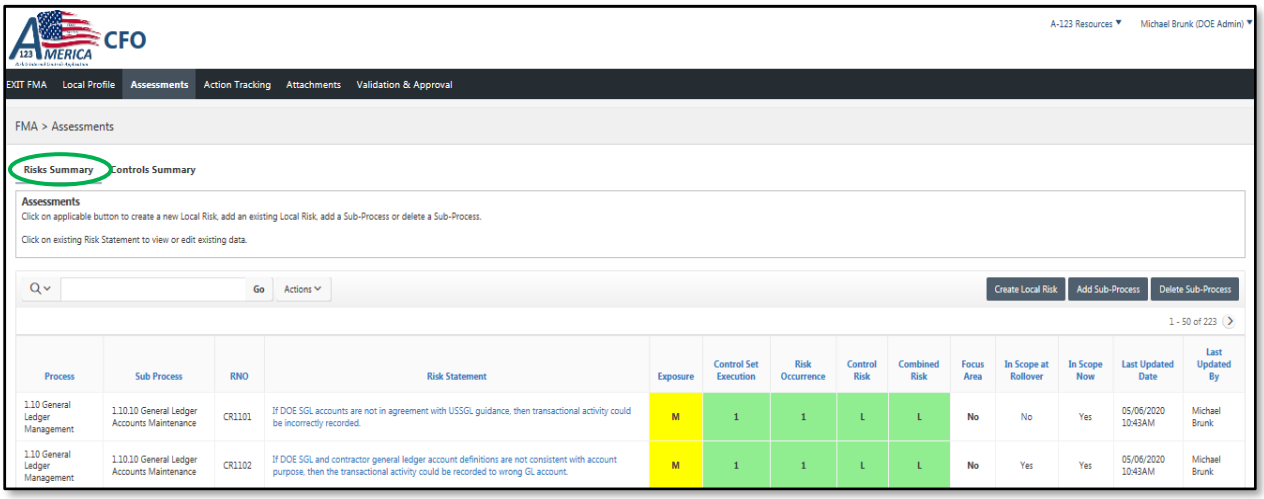
Navigating the FMA: Assessments

The Assessment tab is where the majority of the data entry for the FMA will take place. It is used to document the evaluation of the entity's risks and controls. Within the FMA homepage, select the Assessments tab in the global menu, and the Assessments page will display. The Assessments page includes two sub-tabs:

1. Risks Summary will display a table of the entity's risks and related assessment data plus action buttons to manage the Assessment.
2. Controls Summary will display a table of the entity's controls and related assessment data plus action buttons to manage the Assessment.

Risks Summary View

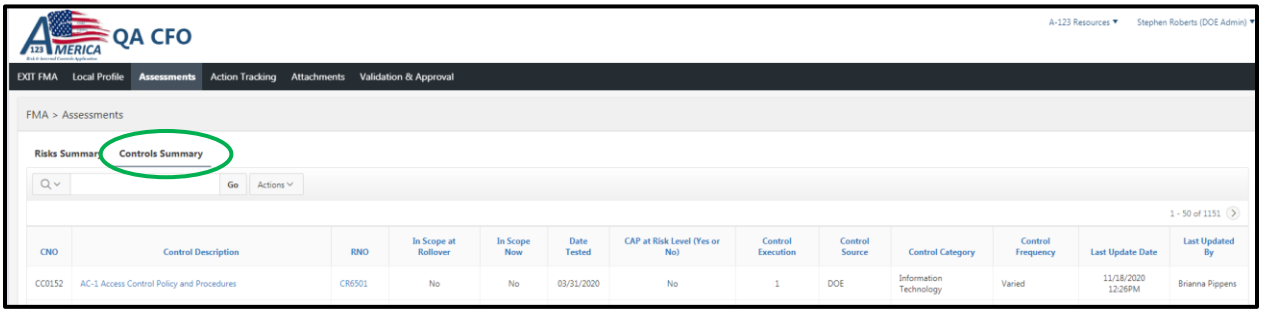
The Risks Summary tab under Assessment provides users a look at all of the Risks in their FMA. The Risks Summary tab is sequentially ordered based on the Process Number. By clicking on the Risk Statement, users can update Risk information.



FMA Module – Risk Summary Page

Controls Summary View

The Controls Summary tab under Assessment provides users a look at all of the Controls in their FMA. The default display is alphabetical based on the Control Number (CNO). By clicking on the CNO, users can update testing as well as other Control information. Clicking on the RNO will take users to the Risk where that Control appears.



FMA Assessment - Controls Summary Page

Assessment Action Buttons

The user's role determines which action buttons are displayed for each user.

- DOE Admin/Local Admin will see all three buttons
- Users will see only the Create Local Risk button
- Approvers will see no action buttons

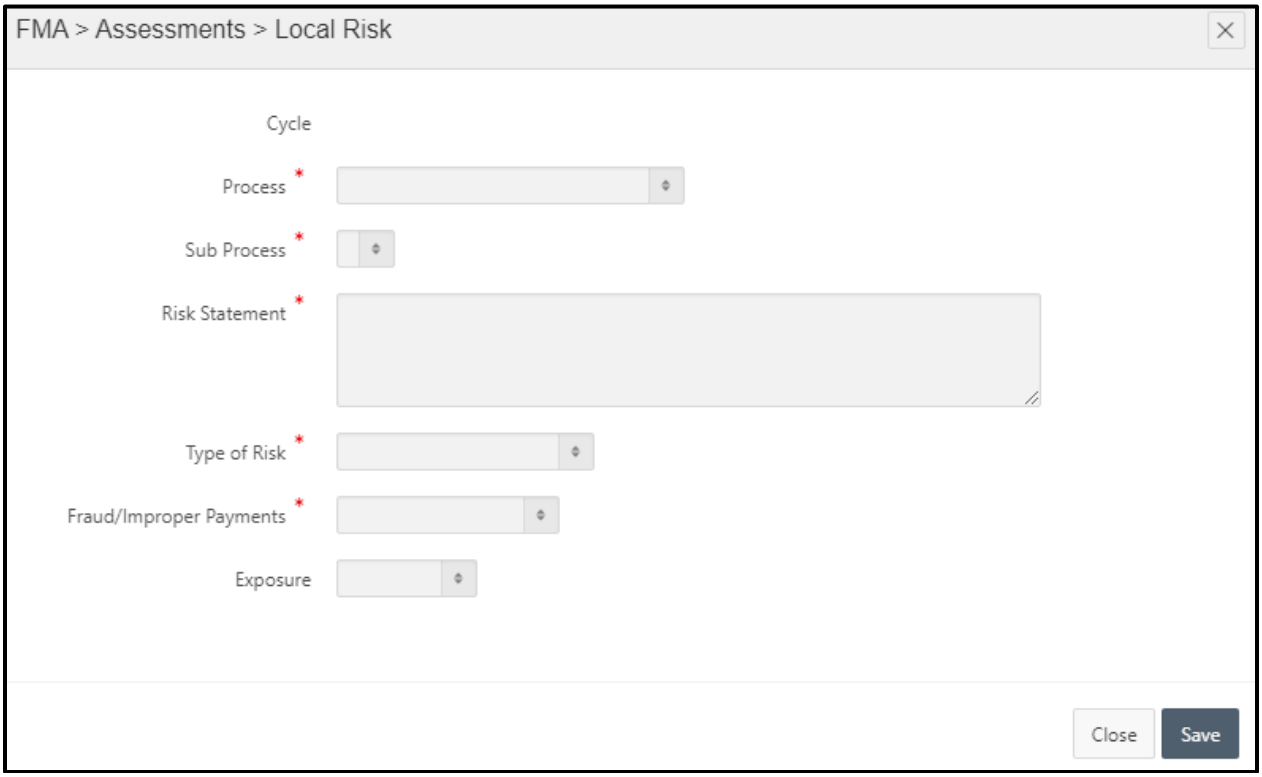
FMA Module - Assessment Buttons

Create Local Risk

The "Create Local Risk" button will create a new entity-specific risk.

1. Within the Assessments page, select the "Create Local Risk" button.
2. The FMA>Assessments>Local Risk form will display with the following fields:
    a. **Cycle**: Automatically populates according to the selection for Process
    b. **Process:** (Required) Select the Process from the dropdown list
    c. **Sub Process**: (Required) Select the Sub Process from the dropdown (based on the Process selection)
    d. **Risk Statement**: (Required) Provide a description of the Local Risk
    e. **Type of Risk**: (Required) Make a selection from the dropdown list: Business, Compliance, Improper Payments, Fraud, Both Fraud and IP, or Information Technology
    Business risks that affect "standard" business operations (budgeting, procurement, payroll, etc.)
    Compliance risks affect activities (e.g., submissions) required by OMB or other internal or external organizations that are performed in a timely and proper manner
    Improper Payments risks affect activities to annually identify, mitigate and/or report programs and activities susceptible to significant improper payments
    Fraud risks affect intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users
    Both Fraud and IP risks are applicable to both Improper Payments and Fraud
    Information Technology risks affect activities surrounding access control, threat detection and deterrence, and availability and reliability of data
    f. **Fraud/Improper Payments**: (Required) Make a selection from the dropdown list: Fraud, Improper Payments, Fraud, Both Fraud and IP, or N/A.
    g. **Exposure**: Make a selection from the dropdown list: Low, Moderate, or High
3. Select the "Save" button

Note: Process, Sub Process, and Risk Statement are required to successfully create the Local Risk. Type of Risk and Exposure can be selected either when the Local Risk is created or evaluated or when the Risk is evaluated, but these fields must be completed to pass Validation before the FMA can be submitted for Approval.



FMA Module - Create a Local Risk

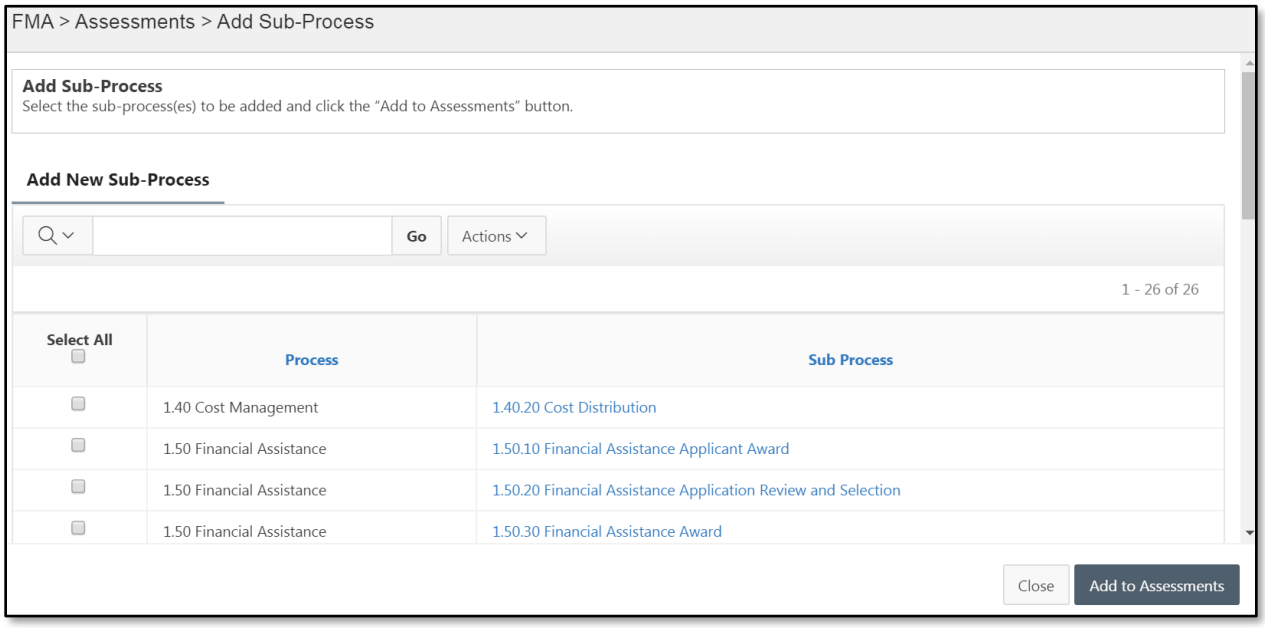
Add Sub-Process

The Add Sub Process button will display a sub-tab: Add New Sub-Process.

Add New Sub-Process

The Add New Sub Process tab is used to add a Sub-Process that was not included in the entity's prior year FMA. When a new Sub-Process is added, any related Risks will be added to the FMA, and data will need to be entered for all required fields.

1. Select the Add Sub-Process button on the Assessments page. The available Sub-Processes will be displayed.
2. Using the selection box(es), select one or more or all Sub-Processes to add to the FMA.
3. Select the "Add to Assessments" button at the bottom right. All selected new Sub-Processes and related risks will be added to the FMA.



FMA Module - Add New Sub-Process

Note: AMERICA requires at least 16 sub-processes. The 16 Sub Processes are:

1.20.10 Budget Formulation
1.20.20 Budget Generation
1.20.30 Funds Distribution
1.20.60 Budget Execution
2.10.10 Requisitioning
2.10.20 Contract Solicitation, Award, & Adjustment
2.10.30 Receipt of Goods and Services
2.10.40 Contract Closeout
2.10.50 Purchase Card Program Management
2.30.30 Invoice Approval
2.40.10 Travel Authorization
2.40.20 Voucher Processing
2.40.30 Travel Closeout
2.40.40 Travel Card Program Management
5.10.20 Time and Attendance Processing
5.10.30 Leave Processing

Delete Sub-Process

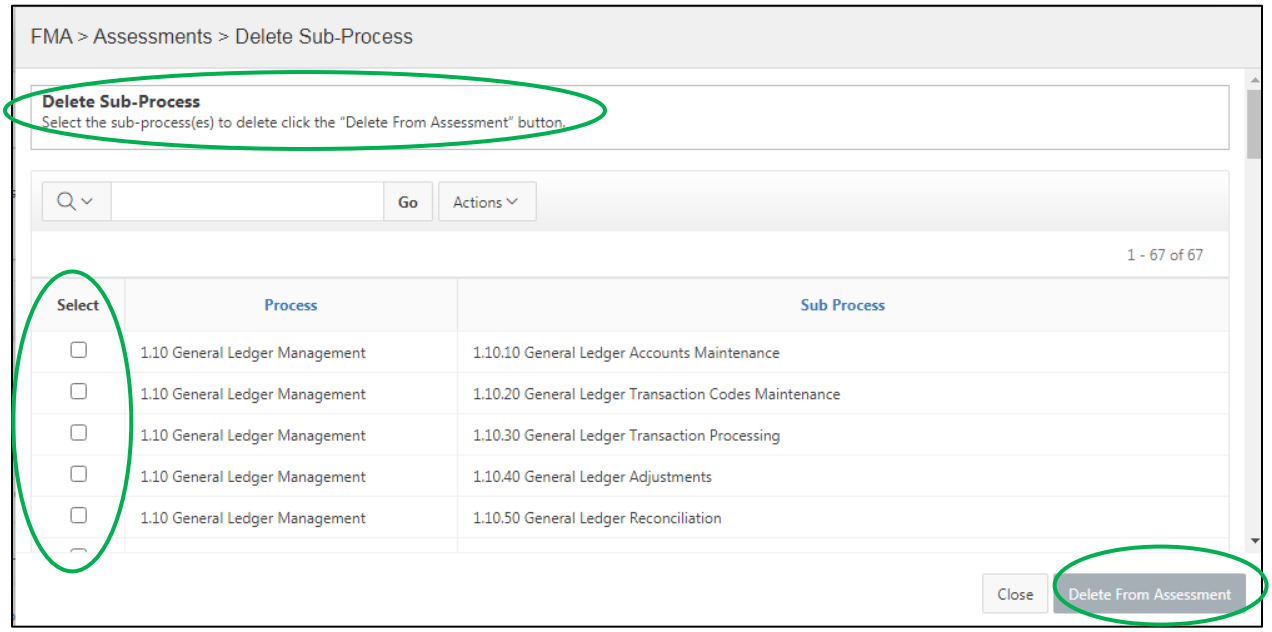
Note: Do not delete any of the required Sub-Processes shown above. Your FMA will not pass Validation.

Corporate Risks cannot be deleted individually; they can only be deleted by Sub-Process grouping. Those Corporate Risks that are not applicable to your site should be marked with an Exposure Rating of Not Relevant (NR), and an explanation of why they are not relevant will need to be added in the "Rationale" field.

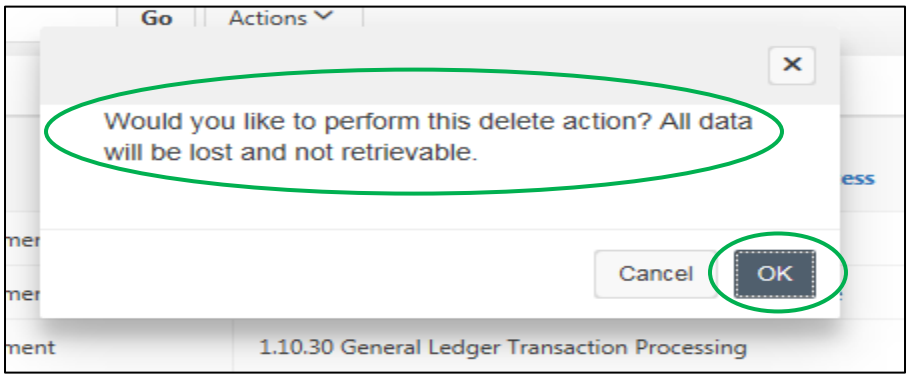
Selecting the 'Delete Sub-Process' button will display a window that has the Sub-Processes that have been added to the Assessment. Only DOE Admin and Local Admin have access to this button.

Note: Deleting a Sub-Process will delete all Corporate Risks and associated data from the FMA. You may select one or multiple Sub Processes to delete from the Assessment. A confirmation message will display.

1. Select the Delete Sub-Process button on the Assessments page. A list of all Sub-Processes in the FMA will display.
2. Use the selection box(es) at the left to select one or more or all of the Sub-Processes.
3. Select the Delete From Assessment button at the bottom right.
4. Select OK to continue with deletion or Cancel to stop deletion.



FMA Module – Delete Sub-Processes



FMA Module – Warning Message

Risk Evaluation Components

Recording the risk evaluation and control testing data occurs in the Assessments tab. The Risks Summary Table on the Assessments page includes all of the entity's risks, along with summary risk data. Rating fields will be color-coded based on the input once the Risk is evaluated and saved. The tiles will display variations of green, yellow, and red.

The Risks Summary Table information includes:

- **Process:** Automatically populated based on the Corporate Framework. The Process is an activity that is part of a Business Cycle. This field cannot be modified.
- **Sub Process:** Automatically populated based on the Corporate Framework. The Sub Process is the Sub-activities or components of a larger process. This field cannot be modified.
- **RNO:** System generated unique identifier used to designate specific risks in the FMA tool Framework. Corporate Risks begin with the letter "CR." Local Risks begin with the sites' abbreviation (e.g., BNL).
- **Risk Statement:** A brief description of the Risk. This field can be modified for Local Risks, but not for Corporate Risks.
- **Exposure:** A measure of Inherent Risk. Inherent Risk is determined by the user and is based on the combination of the likelihood that the risk will occur and the impact should it occur. The value will automatically highlight with the appropriate color.
- **Control Set Execution:** Entered by the user and measures the entire control set, and indicates the ability of the control set to mitigate the risk. The value will automatically highlight with the appropriate color.

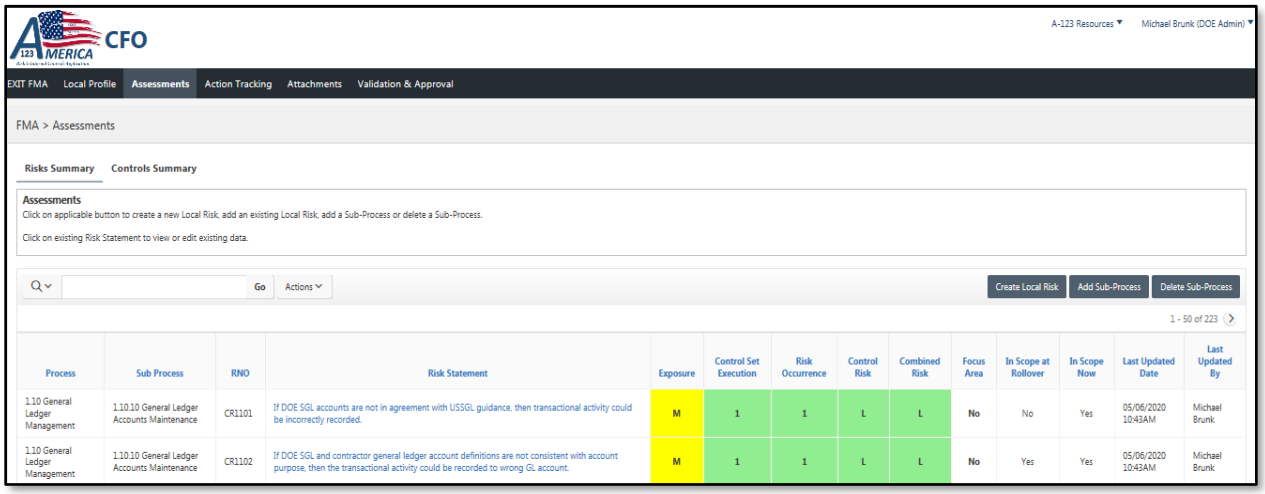
  1 = Passed with No Failures
  2 without CAP = Passed with an Acceptable Level of Failures
  2 with CAP = Passed with an Acceptable Level of Failures
  3 = Failed

  - When a Control Set Execution rating of '2 with CAP' or '3' is selected, an additional CAP Details section will display.

- **Risk Occurrence:** Entered by the user to indicate whether, and to what degree, a risk occurred either during testing or during normal business operations. The value will automatically highlight with the appropriate color.

  1 = Risk did not occur or occurred with minimal impact; 2 = Risk occurred with more than a minimal impact, but within an acceptable threshold; and 3 = Risk occurred with a significant impact and outside of an acceptable threshold. A risk occurrence of 3 automatically requires a CAP.

- **Control Risk:** Rating is automatically calculated using the Risk Occurrence and Control Set Execution ratings. The value will automatically highlight with the appropriate color. **See the FMA Appendix for details.**
- **Combined Risk:** Rating is automatically calculated and measures the residual or end risk to the site considering the level of exposure and effectiveness of controls assigned to mitigate risk. The value will automatically highlight with the appropriate color. **See the FMA Appendix for details.**
- **Focus Area**: Indicates whether or not a Corporate Risk has been defined as a Focus Area Risk for the current year.
- **In Scope at Rollover**: Indicates whether the Risk had testing requirements in the current year at the time of AMERICA Rollover from the prior year (i.e., at the very beginning of the current assessment year). The information in this column is static and does not change based on current year updates.
- **In Scope Now:** Indicates whether the Risk has testing requirements remaining in the current year (i.e., at least one control in the control set needs testing). The information in this column does change based on current year updates.
- **Last Updated Date:** The date and time the Risk was last updated
- **Last Updated By:** Indicates the user who made the last change



FMA Module – Risks Summary Table

Evaluating a Risk

1. Within the FMA>Assessments page, select the desired Risk Statement displayed in the blue text. The Risk Statement Assessment form will display for review and/or data entry.
2. Complete data entry for each of the required fields. Required fields are indicated by a red asterisk. **Note**: Some fields are automatically populated based on FMA data.
3. The form is separated into sections: In Scope for Testing, Process Hierarchy, Risk Assessment, Other Factors to Consider, Control Details / Evaluation, and Control Set Evaluation. If the risk has been designated as a Focus Area, an additional section will display at the bottom. The requirements are listed below.
4. After data entry is complete, select the 'Save' button to save changes.
5. *Select the 'Close' button to discard pending changes.*

In Scope for Testing

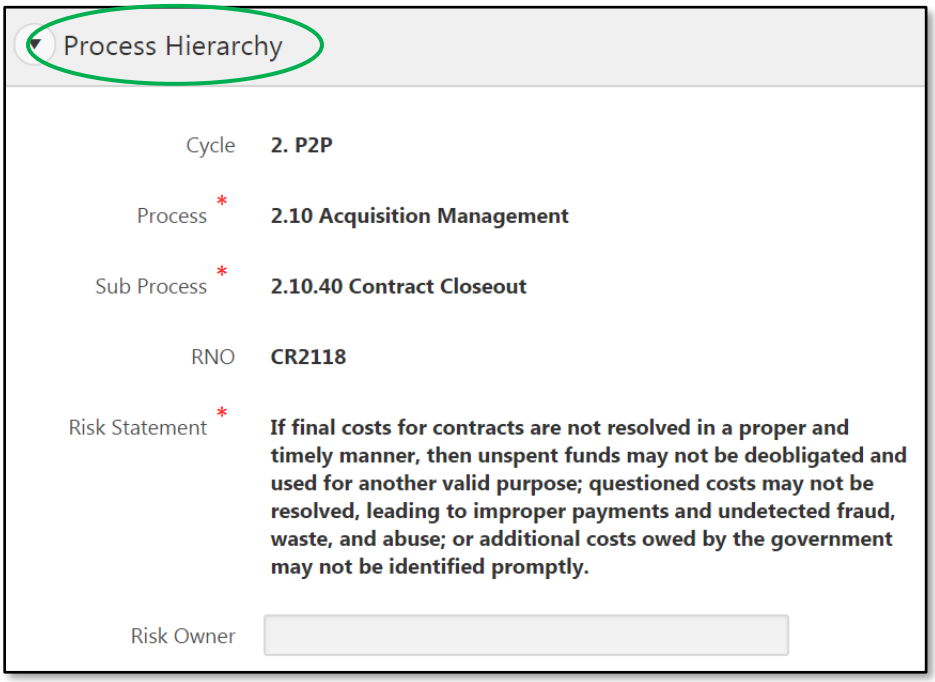
See the FMA Appendix for the calculation of testing requirements.

- **This Year:** Automatically populates based on other form input and indicates testing is required for the current year.
- **Next Year:** Automatically populates based on other form input and indicates testing is required for the next year.
- **Date Risk Added:** Automatically displays the date that the Risk was added to the Assessment. All risks in AMERICA started with a January 2019 date added, regardless of when the risk was originally added to the old FMA tool. Exceptions will be any Risks that organizations have added since AMERICA went live in 2019. Also, if organizations change the Risk Exposure Rating from an existing Risk rated "NR – Not Relevant," the Date Risk Added field will be updated to the current date. This allows previously rated NR risks the one year testing grace period from the date the Risk becomes relevant.

FMA Module – In Scope for Testing Section

Process Hierarchy

- **Cycle:** Automatically populated based on the Corporate Framework. Cycles are the main financial business cycles. Each Cycle represents a distinct type of financial activity with a unique set of Processes associated with it. This field cannot be modified**.**
- **Process:** Automatically populated based on the Corporate Framework. The Process is an activity that is part of a Business Cycle. This field cannot be modified.
- **Sub Process:** Automatically populated based on the Corporate Framework. The Sub Process includes sub-activities or components of a larger process. This field cannot be modified.
- **RNO:** System generated unique identifier used to designate specific risks in the FMA tool Framework.
  - If an RNO starts with the letters "CR" (e.g., CR1101), it is a Corporate Risk, embedded in the FMA Framework by default and can be selected by any DOE site.
  - The Corporate Risk numbering system adheres to the following structure:
    - CR = Corporate Risk
    - 1st position = Cycle
    - 2nd position = Process
    - 3rd and 4th positions = Number Sequence
  - If an RNO starts with the letters of the site code (e.g.,, CFO-R0001 – for the Office of the Chief Financial Officer), it is a Local Risk added at the site level and is only applicable to that specific entity.
- **Risk Statement:** A brief description of the Risk.
  - Corporate Risk statements are automatically populated based on the Corporate Framework.
  - For Local Risk – Risk Statements are provided when first created and can be modified.
- **Risk Owner:** Provide the name of the person responsible for the particular Risk.



FMA Module – Process Hierarchy Section

Risk Assessment

- **Exposure:** (Required) The Exposure rating is a combination of the Likelihood that the risk will occur and the Impact on the site, should it occur.
    - For Corporate Risks – select Low, Moderate, High, or Not Relevant rating from the dropdown.
    - For Local Risks – select a rating of Low, Moderate, or High. A Local Risk cannot be rated as Not Relevant. If a Local Risk is no longer relevant, it should be deleted.
- **Rationale:** Users can provide an explanation for the Exposure rating that was selected.
    - Rationale is only required for Validation if the Exposure selected is NR.
        - When the Exposure is NR, the Risk Assessment section will be the only section displayed for input.
- **Risk Source**: Automatically populated with DOE for Corporate Risks and its Site Code for Local Risks.
- **Type of Risk:** The classification of the Risk can be one of the following: Business, Compliance, and Information Technology.

    - For Corporate Risks - automatically populated based on the Corporate Framework.
    - For Local Risks - make a selection from the dropdown.

Please note Improper Payments, Fraud, and Both Fraud & IP will no longer be included as a dropdown option for FY 22. Any Corporate Risks that were previously marked as three afore mentioned Types of Risks will now be marked as either Business, Compliance, or Information Technology.

NEW in FY 2022

Business risks that affect "standard" business operations (budgeting, procurement, payroll, etc.)
Compliance risks affect activities (e.g., submissions) required by OMB or other internal or external organizations that are performed in a timely and proper manner
Information Technology risks affect activities surrounding access control, threat detection and deterrence, and availability and reliability of data

- **Fraud/Improper Payments:** The further classification of the Risk can be one of the following: Improper Payments, Fraud, Both Fraud & IP, or N/A:

  Improper Payments risks affect activities to annually identify, mitigate and/or report programs and activities susceptible to significant improper payments
  Fraud risks affect intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users
  Both Fraud and IP risks are applicable to both Improper Payments and Fraud

- **Risk User Field 1 and 2:** Available to capture any additional Risk information that the user finds valuable.

FMA Module – Risk Assessment Section

Other Factors to Consider

- **Focus Area**: Automatically populated with "Yes" or "No" based on whether the Risk is a Corporate Focus Area for the current fiscal year. If a Risk is a Focus Area, an additional section will display the Assessments form for data input.
- **Local Request:** An alert issued by local management requiring an assessment of the Risk during the current fiscal year. A choice of "Yes" is akin to making the Risk a "Local Focus Area." Select a "Yes" or "No" response via the dropdown.
- **System Change:** Any local or corporate system or system infrastructure changes directly affecting local operations of supported business functions. Select a "Yes" or "No" response via the dropdown. Examples**:** New computer applications, significant changes to existing computer systems and/or infrastructure, and automation of manual controls.
- **Process Change**: Any local or corporate process changes affecting procedural execution of the business processes. Select a "Yes" or "No" response via the dropdown. Examples**:** Transfer of specific activities to another site and streamlining/eliminating the series of steps needed to perform the business process.
- **Organization Change:** Any local or corporate organizational changes directly affecting local operations. Select a "Yes" or "No" response via the dropdown. Examples: Transfer of responsibilities for specific business activities and creation or elimination of specific units.
- **Other Change**: Management requests or any other local or corporate changes directly affecting local operations (e.g., new or modified management directives and federal government directives or laws). Select a Yes or No response via the dropdown. Examples**:** New or changed laws and/or regulations and new or changed DOE internal policies and/or directives.

- **Audit Findings:** Select a "Yes" or "No" response via the dropdown.

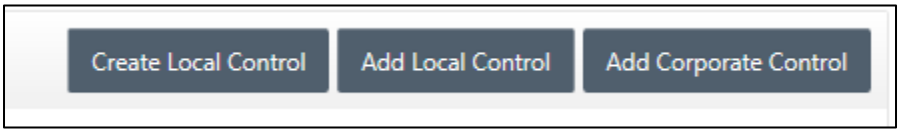
  Note: The default selection is "No" for these fields. Selecting "Yes" for any of the factors will automatically make the Risk and all associated Controls in scope for testing in the current year.

FMA Module – Other Factors to Consider Section

Control Details / Evaluation

Controls are assigned to Risks, and detailed information regarding the control is provided in this section.

- Select the applicable button to create a new Local Control, add an existing Local Control, or add a Corporate Control.



Create Local Control

- Select the Create Local Control button to create a new Local Control.
- The FMA>Assessment>Risk>Control form will display for data input.
- Complete the required fields.
- Select the 'Save' button.
- The Control will then be assigned a system-generated CNO. When a new Local Control is created, the CNO will be the next available number. It will be added to the bottom of the Local Controls pick list so that it can be added to other Risks as well.

The following fields are required:

Control Description: (Required) Provide a unique short description of each control.

***Note**: A Control Description cannot be duplicated. A warning message will occur if the same exact text has already been used.*

Control Category: (Required) Select from the dropdown list: Business, Compliance, Improper Payments, Fraud, Both Fraud & IP, Performance, or Information Technology.

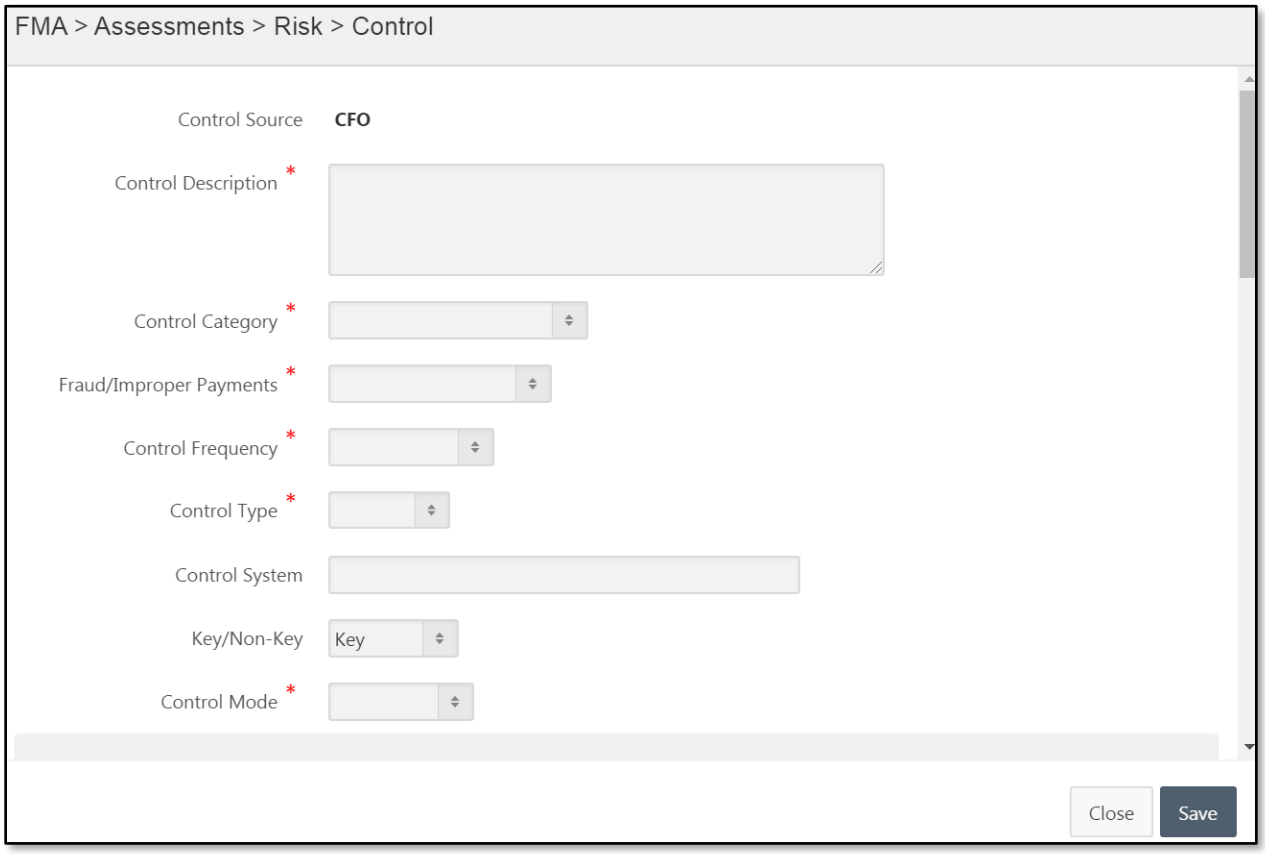
Business controls that affect "standard" business operations (budgeting, procurement, payroll, etc.)
Compliance controls mitigate risks to proper and timely activities (e.g., submissions) required by OMB or other internal or external organizations.

Improper Payments controls to mitigate risks to annually identify, mitigate and/or report programs and activities susceptible to significant improper payments.
Fraud controls mitigate risks involving intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users.
Both Fraud and IP controls mitigate risks to both Improper Payments and Fraud.
Information Technology controls to mitigate risks to activities surrounding access control, threat detection and deterrence, and availability and reliability of data.

Please note for FY23 Fraud, Improper Payments, and Both will be removed from the dropdown list. Any Controls that were previously marked as three afore mentioned Types of Controls will no longer have a Control Category selected. We advise users to change it in the current year.

Fraud/Improper Payments: (Required) Select from the dropdown list: Improper Payments, Fraud, Both Fraud & IP, or N/A.
Control Frequency: (Required) Describes how often a control activity is carried out. Select from the dropdown list: Annual, Bi-weekly, Daily, Monthly, Quarterly, Recurring, Semi-Annual, Varied, or Weekly.
Control Type: (Required) Select either Manual or Auto. Manual Controls are conducted personally by employees, while Automated Controls tend to be automated processes or software (e.g., STARS). Automated Controls require a system to be listed when they are added**.**
Control System: Specify the system(s), e.g., Oracle or Travel Manager. It is only required when the Control Type is Auto.
Key/Non Key: Make a selection from the dropdown. The default is Key.
Control Mode: (Required) Make a selection from the dropdown.

- Detective Controls are designed to discover operational risks with after-the-fact reviews (e.g., quarterly audits).
- Preventive Controls are designed to stop operational risks from occurring at the point of origin.
- The Control Mode is selected by the user directly on the Assessment Tab for both Local and Corporate Controls.



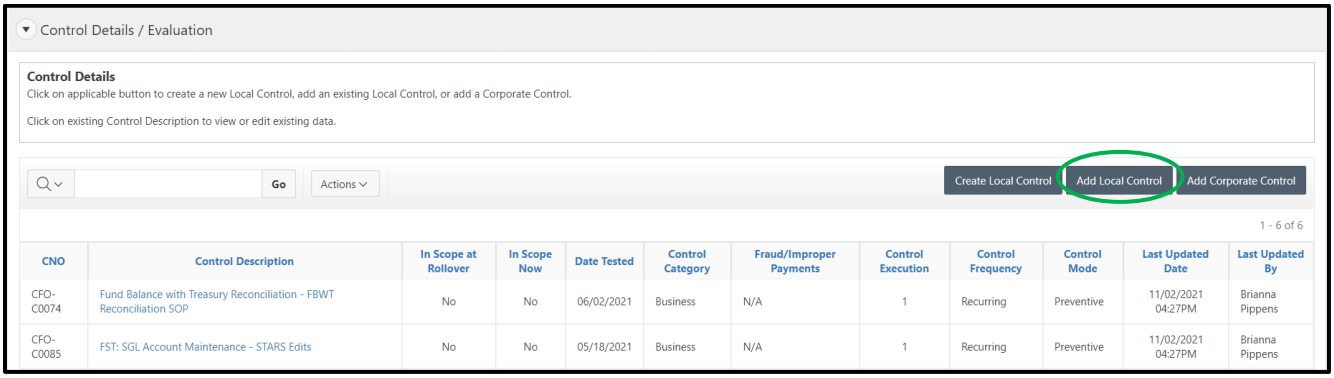
FMA Module - Assessments Risk > Create Local Control

Add Local Control

- Select the Add Local Control button to add an existing Local Control(s) to a particular Risk. A window will display with pre-existing summary information for these controls. Controls already assigned to that risk will not appear because assigning the same Control twice to the same risk is not allowed.
- Note the Historical CNO column which, refers to the number that was used in the prior system. The CNO column will display the new system-generated CNO.
- Using the selection box(es) at the left, select one or more Local Controls.
- Select the Add Controls button at the bottom right.
- The Controls will be displayed in the summary table in the Control Details / Evaluation section.
- If your entity does not have any existing Local Controls to add, the display window will be blank.
- Once added to a risk, they will no longer be able to be added to that same Risk again.

Modification to Controls

Controls can be added to multiple Risks; modifications made to Local Control fields will update for each instance of that Local Control in the FMA. Corporate Control fields that are modified will be updated for each instance of the Corporate Control in the entity's FMA.



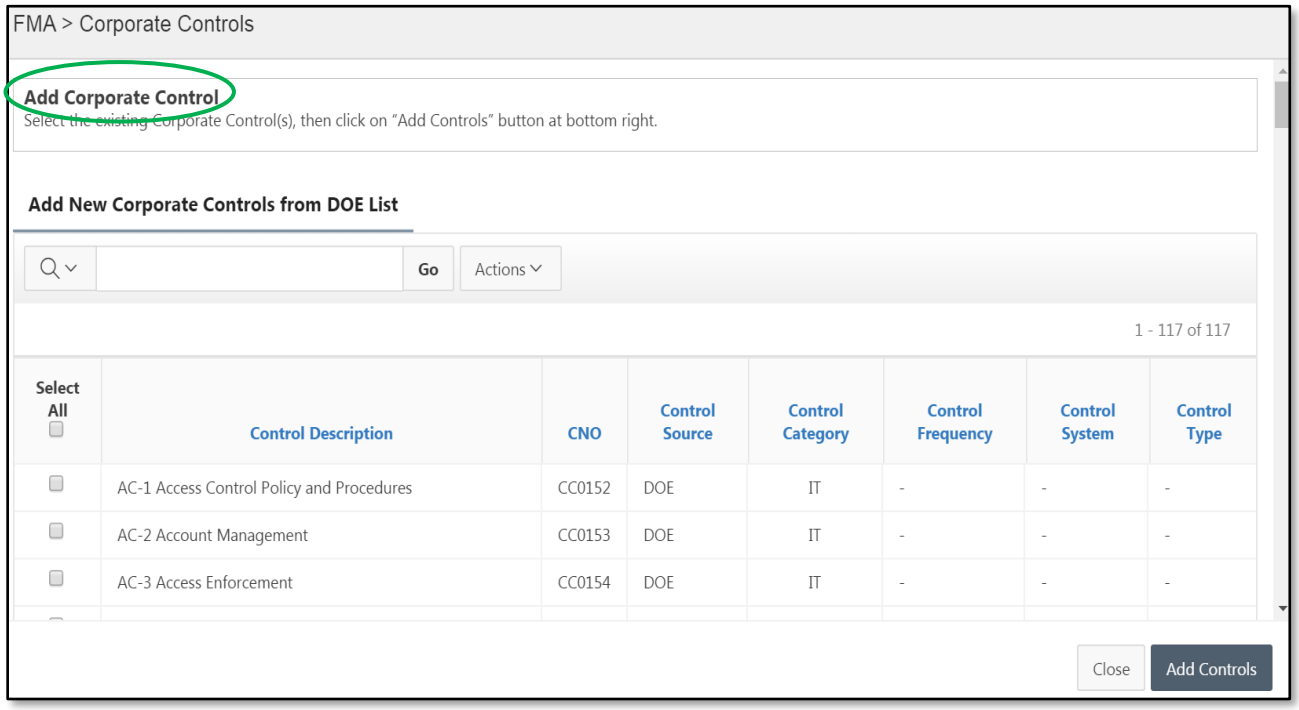
FMA Module – Add Local Controls

Add Corporate Control

Corporate Control is a control that applies to multiple organizations across the DOE complex. Beginning in FY 2019, all Corporate Controls are Information Technology controls. Old non-IT Corporate Controls were converted to Local Controls.

Add Corporate Controls

- Select the Add Corporate Control button to add an existing Corporate Control(s) to a particular Risk. A window will display with pre-existing summary information for these controls. Controls already assigned to that risk will not appear because assigning the same Control twice to the same risk is not allowed.
- Using the Selection box(es) at the left, select one or more Corporate Controls.
- Select the Add Controls button at the bottom right.
- Once added to a risk, they will no longer be able to be added to that same Risk again.
- The Controls will be displayed in the summary table in the Control Details / Evaluation section.



FMA - Add Corporate Controls

Evaluating a Control

- Navigate to the Control Details/Evaluation section of the FMA/Assessment/Risk form.
- Select a Control Description, which is highlighted in the blue text to view or edit existing data.
- The FMA>Assessment/Risk/Control form will open with four sections to be completed or edited.
- Requirements for each field in the Control Details / Evaluation section are as follows:
  CNO: (System Generated) A unique Control Number for each control. The CNO for a Corporate Control begins with the letters "CC" (CCXXXX), and the CNO for a Local Control begins with the reporting entity's Location Code (CFO-CXXXX).
  Historical CNO: Automatically populated for Local Controls that came from the legacy FMA.
  Control Source: Automatically populated based on whether the control is local or corporate.
  Control Description: (Required) Provide a unique short description of each control. A Corporate Control, the description comes pre-loaded in the framework and cannot be changed. For Local Controls, the description was manually entered when it is created and can be edited.
  ***Note**: A Control Description cannot be duplicated. An error will occur if the same exact text has already been used.*
  Control Category: (Required) Select from the dropdown list: Business, Compliance, Improper Payments, Fraud, Both Fraud & IP, Performance, or Information Technology

  Business controls that affect "standard" business operations (budgeting, procurement, payroll, etc.)
  Compliance controls mitigate risks to proper and timely activities (e.g., submissions) required by OMB or other internal or external organizations.
  Improper Payments controls to mitigate risks to annually identify, mitigate and/or report programs and activities susceptible to significant improper payments.
  Fraud controls mitigate risks involving intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users.

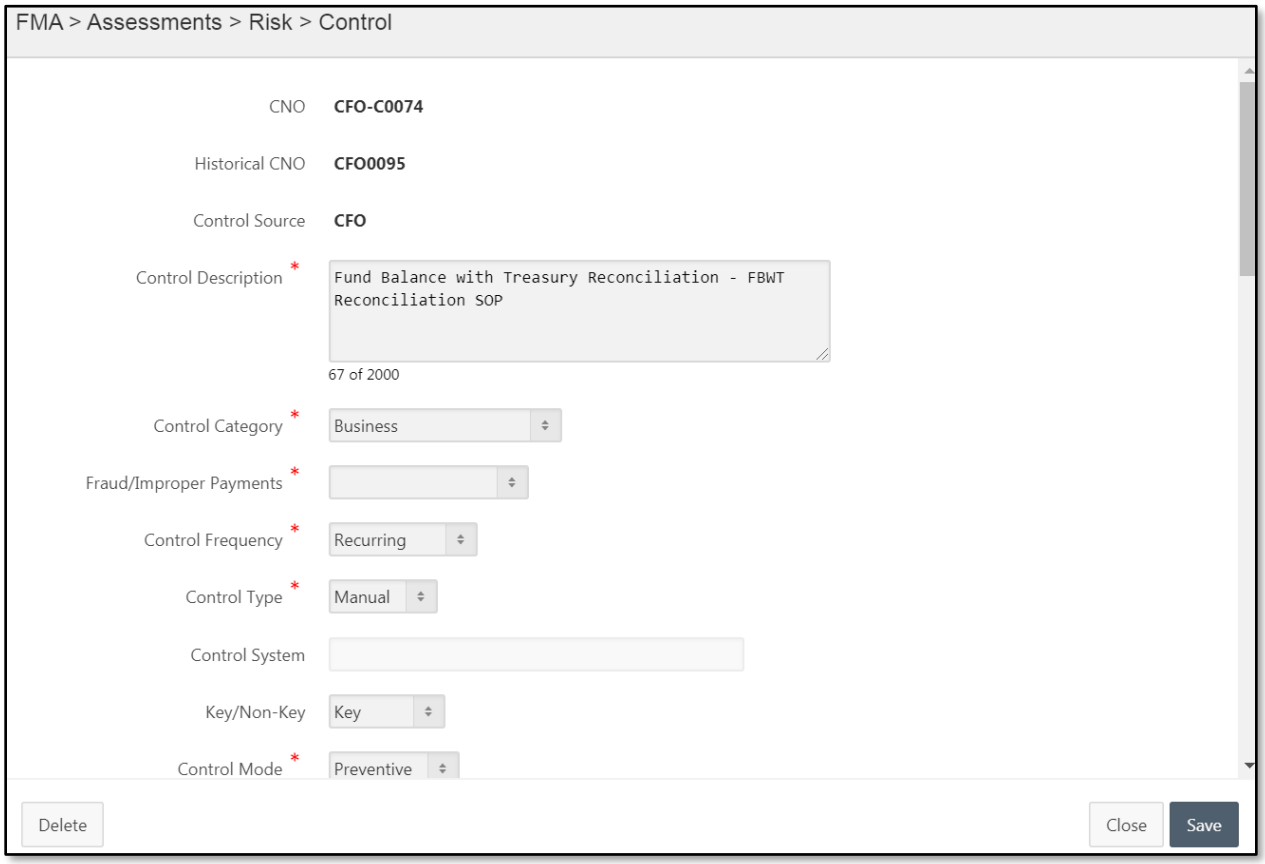
Both Fraud and IP controls mitigate risks to both Improper Payments and Fraud.
Information Technology controls to mitigate risks to activities surrounding access control, threat detection and deterrence, and availability and reliability of data.

- For Corporate Controls – data is pre-loaded in the framework and cannot be changed.
- For Local Controls - selection is made when control is created but can be updated at any time.

Please note for FY23 Fraud, Improper Payments, and Both Fraud and IP will be removed from the dropdown list. Any Controls that were previously marked as three afore mentioned Types of Controls will no longer have a Control Category selected. We advise users to change it in the current year.

Fraud/Improper Payments: (Required) Select from the dropdown list: Improper Payments, Fraud, Both Fraud & IP, or N/A. If the control mitigates IP, Fraud, or Both, make the proper selection. Otherwise, choose N/A.
Control Frequency: (Required) Describes how often a control activity is carried out. Select from the dropdown list: Annual, Bi-weekly, Daily, Monthly, Quarterly, Recurring, Semi-Annual, Varied, or Weekly.
Control Type: (Required) Select either Manual or Auto. Manual Controls are conducted personally by employees, while Automatic Controls tend to be automated processes or software (e.g., STARS). Automated Controls require a system to be listed when they are added**.**
Control System: Specify the system name, e.g., Oracle or Travel Manager. Only required when the Control Type is Auto.
Key/Non Key: Select from the dropdown. The default is Key.
Control Mode: (Required) Select from the dropdown for both Local and Corporate Controls.

- Detective Controls are designed to discover operational risks with after-the-fact reviews (e.g.,, quarterly audits).
- Preventive Controls are designed to stop operational risks from occurring at the point of origin.



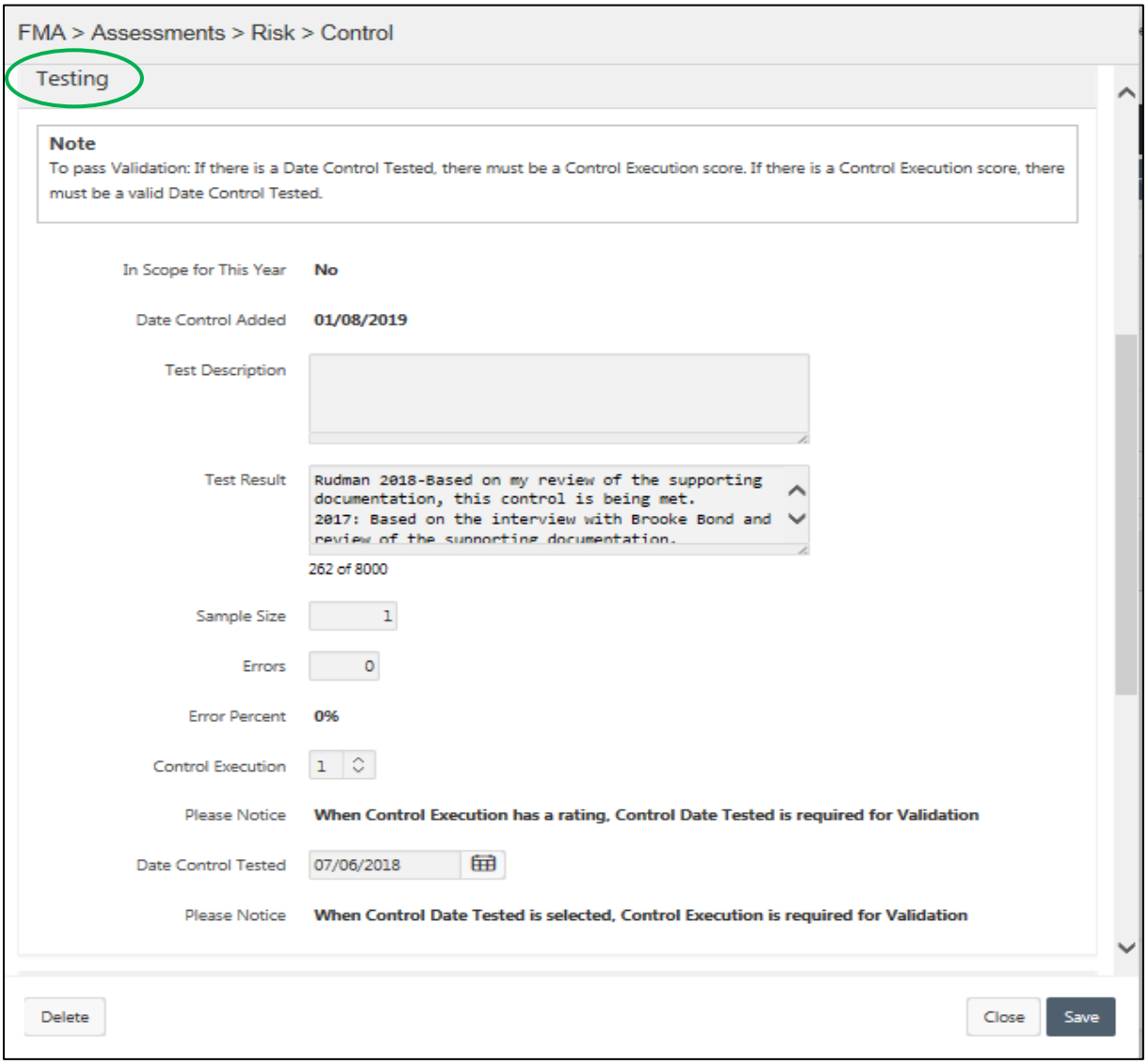
FMA Module - Evaluate a Control

Testing

In Scope Now: Automatically populated based on other field inputs. The field will display Yes, No, or Overdue. **See the FMA Appendix for details.**
Date Control Added: Automatically populated with the date the Control was added to the Risk. Many dates will show as January of 2019 when the data was migrated from the old system.
Test Description: Provide a description of the testing process used for a control at an appropriate level of detail.
Test Result: Provide a description of the results based on the outcome of the control test.
Sample Size: Enter the total population size of evidence samples used in a test process.
Errors: Enter the number of failures that occurred in a controls test.
Error Percent: Automatically calculates the number of errors in a controls test as a percentage of the total population of evidence samples. Calculation is: Error / Sample Size *100%.
Control Execution: Control Execution ratings reflect the score given to an individual control when tested. When Control Execution has a rating, Control Date Tested is required for validation. Select from dropdown: 1, 2, or 3.

1 = Passed with No Failures; 2 = Passed with an Acceptable Level of Failures; 3 = Failed.

Date Control Tested: Provide a test date at the individual control level. When Control Date Tested is selected, a Control Execution rating is required for validation.

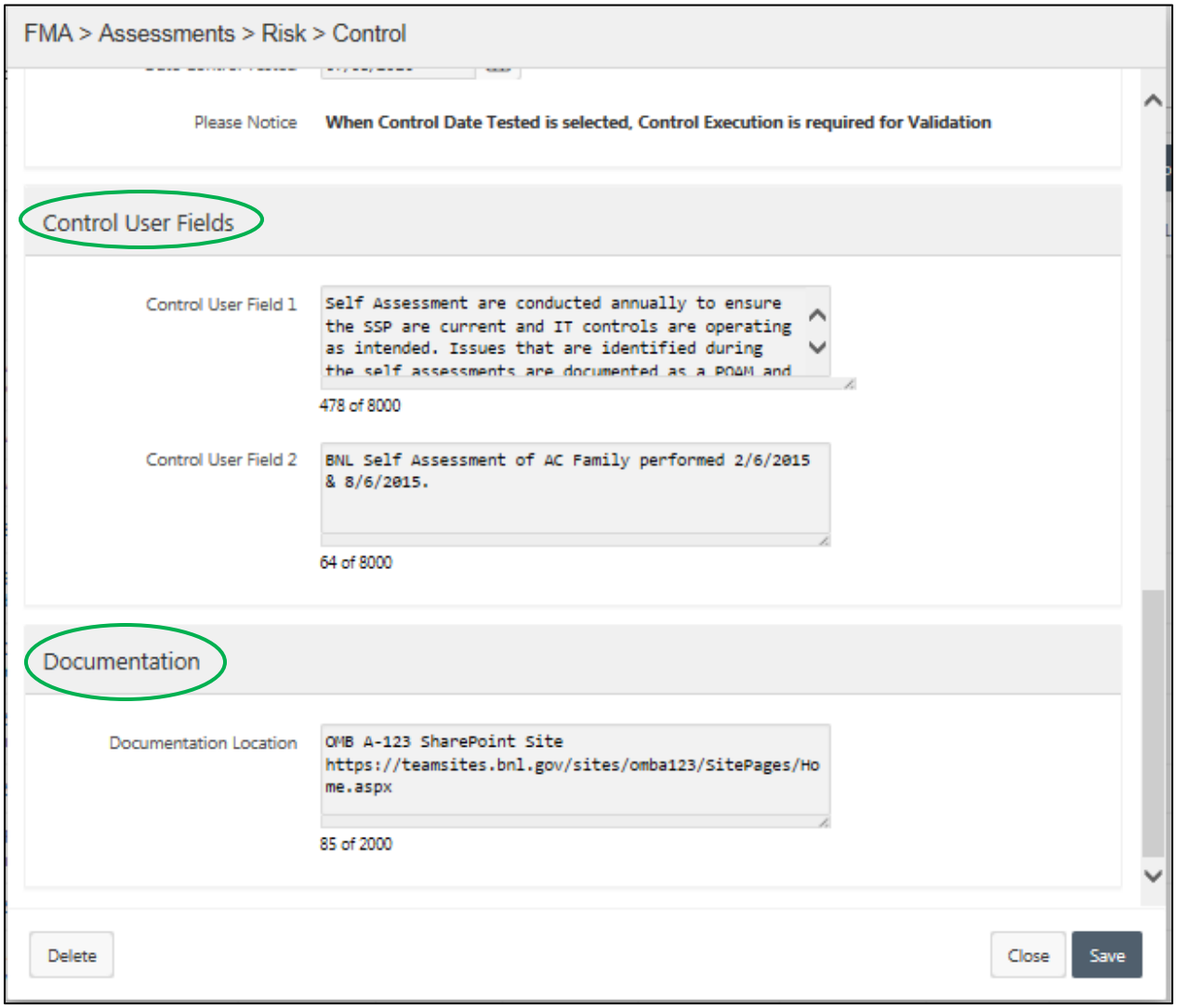


FMA Module - Control Testing Section

User Fields and Documentation Location

Control User Field 1 and 2: Available to capture any additional control information that the user finds valuable. **Note**: Use Control Field 1 to indicate why a control that was Due or Overdue for testing was not tested.

Documentation Location: Provide input for referencing the location of the documentation relevant to the control test.



FMA Module - Control User Fields and Documentation Sections

Control Set Evaluation

Control Set Execution: Make a selection from the dropdown list. This field measures the entire control set and indicates the ability of the control set to mitigate the risk.

1 = Passed with No Failures
2 without CAP = Passed with an Acceptable Level of Failures
2 with CAP = Passed without an Acceptable Level of Failures but requires a CAP
3 = Failed

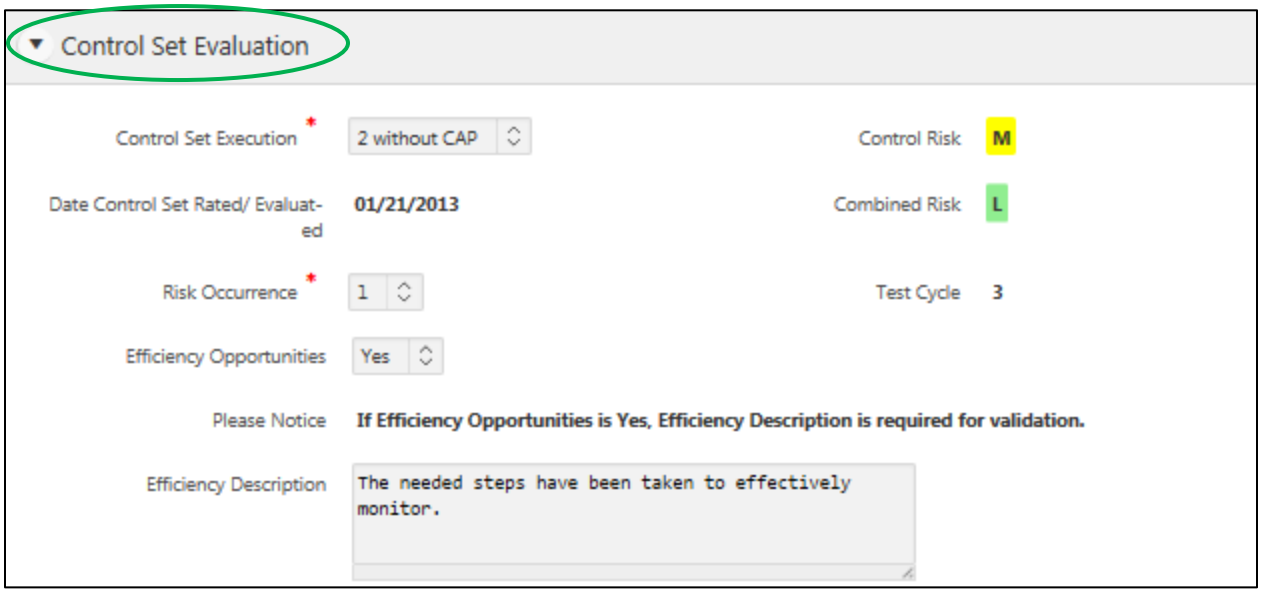
- When a Control Set Execution rating of '2 with CAP' or '3' is selected, an additional CAP Details section will display.

Date Control Set Rated/Evaluated: This field is automatically populated based on the Control Details section's oldest date for the Date Control Tested field.

Risk Occurrence: Make a selection from the dropdown list. Determined during testing or through observation during normal business operations. Measures to what degree the risk occurred:

1 = Risk did not occur or occurred with minimal impact; 2 = Risk occurred with more than a minimal impact, but within an acceptable threshold; and 3 = Risk occurred with a significant impact and outside of an acceptable threshold. A risk occurrence of 3 automatically requires a CAP.

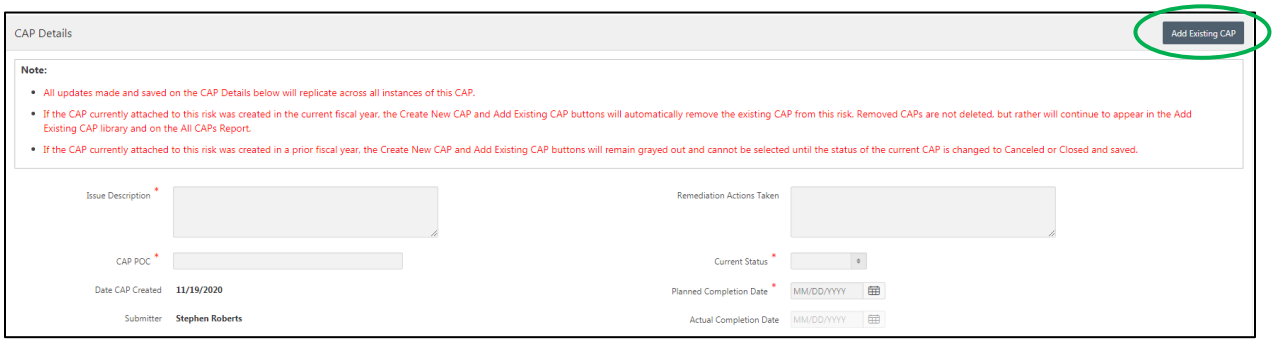
Efficiency Opportunities: Select "Yes" or leave this field blank with regards to whether there are efficiency opportunities.
Efficiency Description: A brief description is required if the Efficiency Opportunities selection is 'Yes.'
Control Risk: An automatically calculated field that measures a control set's ability to mitigate risk. Control Risk is calculated using the Risk Occurrence and Control Set Execution ratings. The value will automatically highlight the appropriate rating and color. **See the FMA Appendix for details.**
Combined Risk: Rating is automatically calculated measuring the residual or end risk to the site considering the level of exposure and effectiveness of controls assigned to mitigate a risk. The value will automatically highlight the appropriate rating and color. **See the FMA Appendix for details.**
Test Cycle: Automatically calculated number between 1 and 3 years based on the Combined Risk rating. This number is used along with the control-set test date to provide the results for the In Scope This Year and Next Year fields. **See the FMA Appendix for details.**



FMA Module - Control Set Evaluation Section

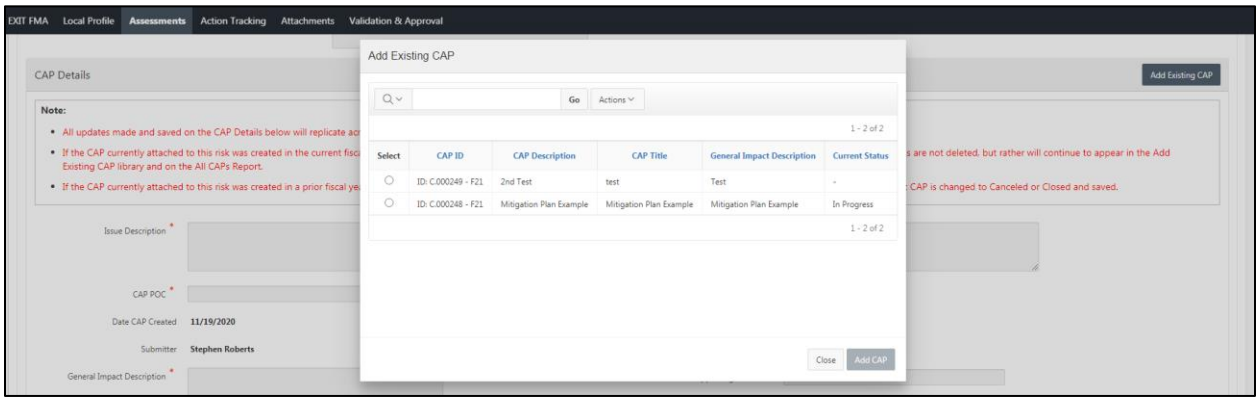
CAP Details

When a Risk Occurrence is 3 or the Control Set Execution rating is a '2 with CAP' or '3,' a CAP is required, and the CAP Details section will display.



Add Existing CAP

If an existing CAP is already in AMERICA relevant to this Risk, click “Add Existing CAP”.



This will bring up a pop-up menu with a list of all existing CAPs for the current year. From this menu, click the CAP to associate it with the risk.

Create a New CAP

Input in this section is linked to the Action Tracking tab. Requirements for each field in the CAP Section are described as follows:

Issue Description: (Required) Provide a brief description of the issue. This issue statement will also automatically populate on the Action Tracking tab. A CAP cannot be created without this input.
CAP POC: (Required) Populate this field with the name of the primary point of contact responsible for completing the evaluation of that particular CAP.
CAP Reference Number: Automatically populated once the CAP has been created. System generated identifier (ex. CFO: C.000003-F19).
Date CAP Created: Automatically populated with the date the CAP is created.
Submitter: Automatically populated with the name of the user that created the CAP.
Note: CAP Reference, Date CAP Created, and Submitter will only display once the CAP has been saved.
General Impact Description: (Required) Provide a brief description of the impact the issue is having and future potential impacts if any.

Source/Type: Make a selection from the dropdown:

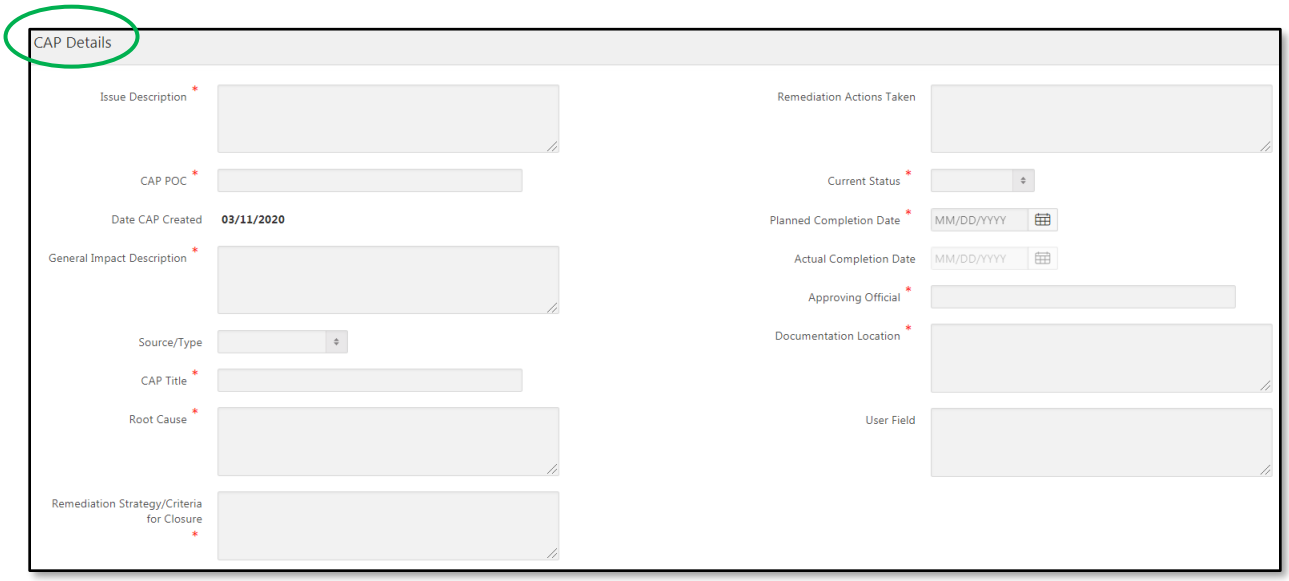
- Audit
- Corrective
- Program Feedback
- QA Feedback

CAP Title: (Required) Provide a name for the CAP
Root Cause: (Required) Provide a brief description or summary of the root cause of the problem. It is critical to define the root cause prior to developing a corrective action strategy and milestones.
Remediation Strategy/Criteria for Closure: (Required) Provide a brief summary of the remediation strategy and the criteria required in order to close the CAP
Remediation Actions Taken: Describe the remediation actions taken
Current Status: (Required) Select the current CAP status from the drop-down menu:

- **New**: The need for the establishment of a CAP has been discovered through the current year's internal controls evaluation process
- **In Progress**: Corrective actions have not yet been completed to resolve the issues and mitigate the stated impacts
- **Implemented**: Corrective actions have been implemented to address issues and stated impacts, but the criteria for closure have not been met
- **Closed**: All corrective actions have been completed to resolve the issue and mitigate the stated impacts
- **Canceled**: CAP is no longer necessary based on the discovery of new or additional information

Planned Completion Date: (Required) Provide the target closure date for the CAP
Actual Completion Date: (Required if Current Status is Closed) Provide the actual closure date once CAP is closed. This field can only be updated when the Current Status selection is "Closed."
Approving Official: (Required) Provide the name of the individual certifying the CAP
Documentation Location: (Required) Provide the location of the documents or any information that is considered beneficial in supporting the CAP
User Field: This field can be used to keep a record of any additional information the user finds helpful

To retain the updates made, select the 'Save' button. To discard changes made, select the 'Close' button.

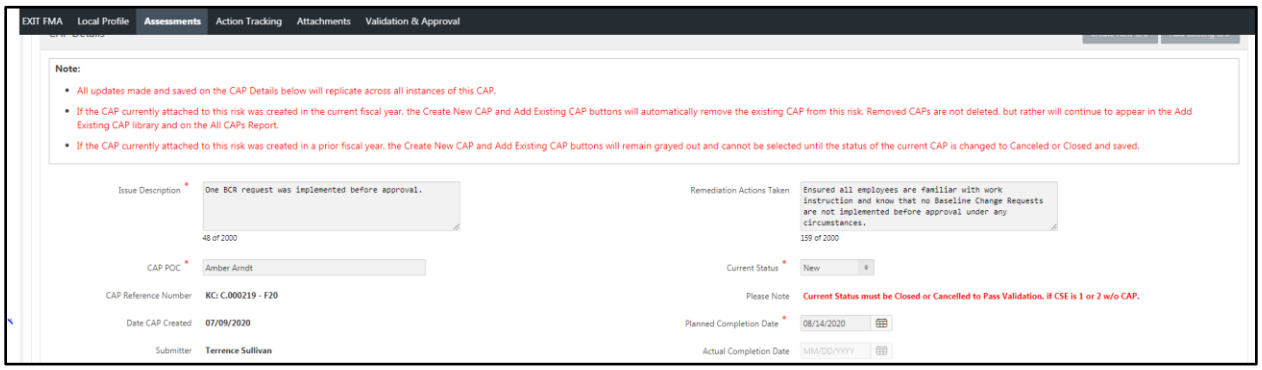


FMA Module - CAP Details Section

Modifying an Existing CAP

If a risk has a prior year CAP associated with it, the CAP details information will carry over into the current year. In the CAP detail section, you can modify the CAP information. Please note if you change the CAP rating from a 2 or 3 to a 1, then the following error message will appear:

"*Current Status must be Closed or Canceled if CSE is 1 or 2 w/o CAP*"

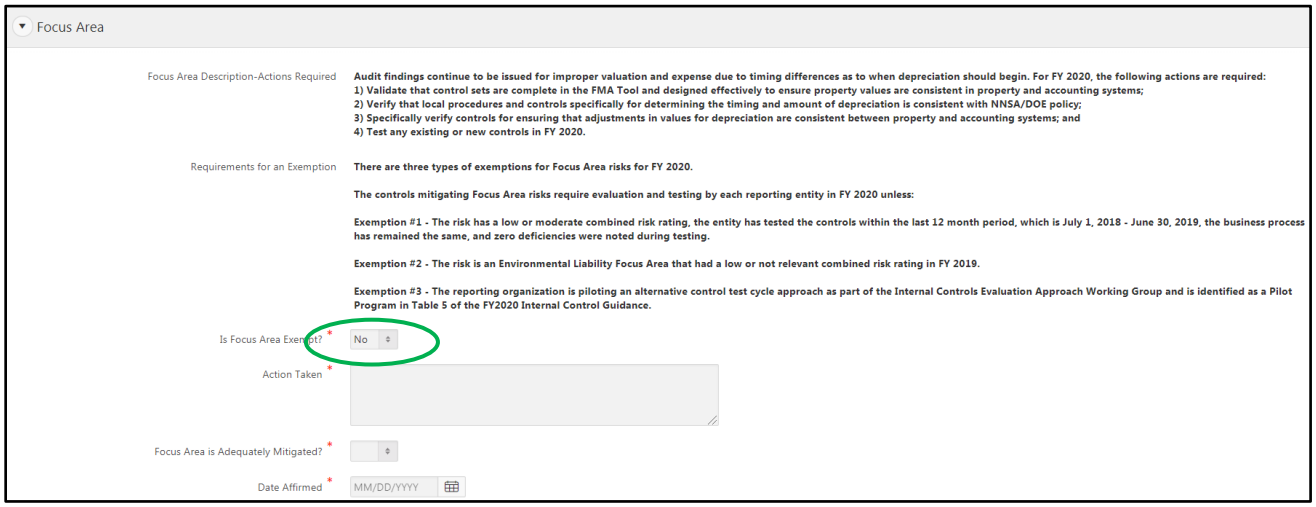


Focus Areas

Focus Areas are select Corporate Risks that require specific actions to be taken in the current fiscal year. For all Focus Area Risks, an additional section will display on the Assessment form. All Focus Area Risks must be assessed or tested regardless of risk rating or test cycle. The field requirements are as follows:

- **Focus Area Description-Actions Required:** Auto populated with information on why this risk is a Focus Area and what actions are required by the site
- **Requirements for an Exemption:** Auto populated with information regarding possible exemption from performing testing in the current year

- **Is Focus Area Exempt?**: Select 'Yes' from the dropdown if the site meets one of the exemptions that are for the current fiscal year. The default setting is 'No.' Please refer to the IC Evaluations Guidance for more details on current FY Focus Area Exemptions.
- **Action Taken:** (Required) Provide information on the actions taken to address a Focus Area.
- **Focus Area is Adequately Mitigated**?: Select 'Yes' or 'No' from the dropdown
- **Date Affirmed**: Enter a date within the current assessment year



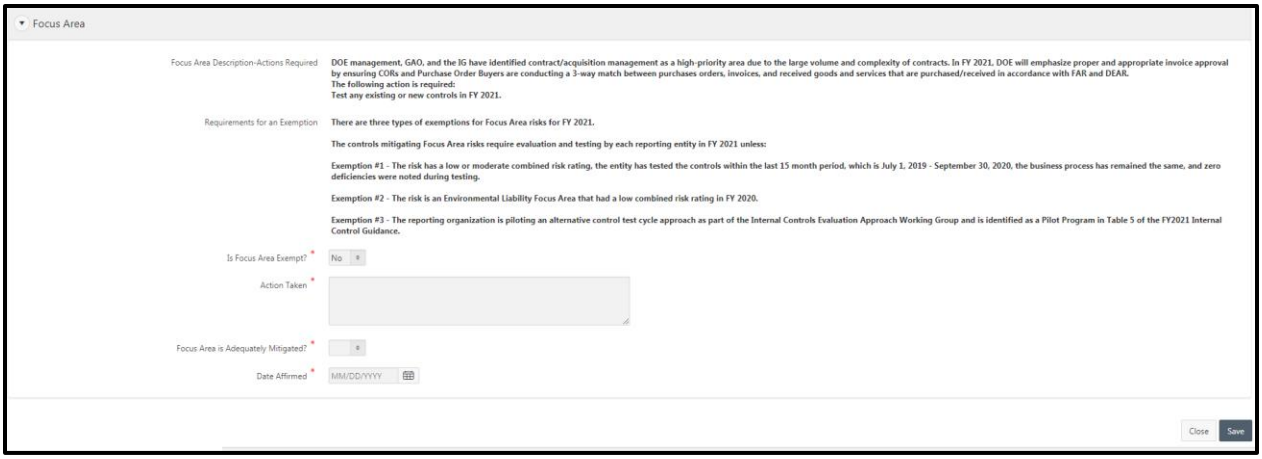
FMA Module - Focus Area Section with "No" Exemption (default)

If a Risk is a Focus Area, it is automatically 'Yes' for In Scope this Year. If a Risk is a Focus Area but the Exposure rating selection is 'NR,' the Focus Area will no longer be in scope for the current year; it will display NR for In Scope this Year. **See the FMA Appendix for details.**

To retain the updates made, select the 'Save' button. To discard changes made, select the 'Close' button.

Focus Area Exemptions

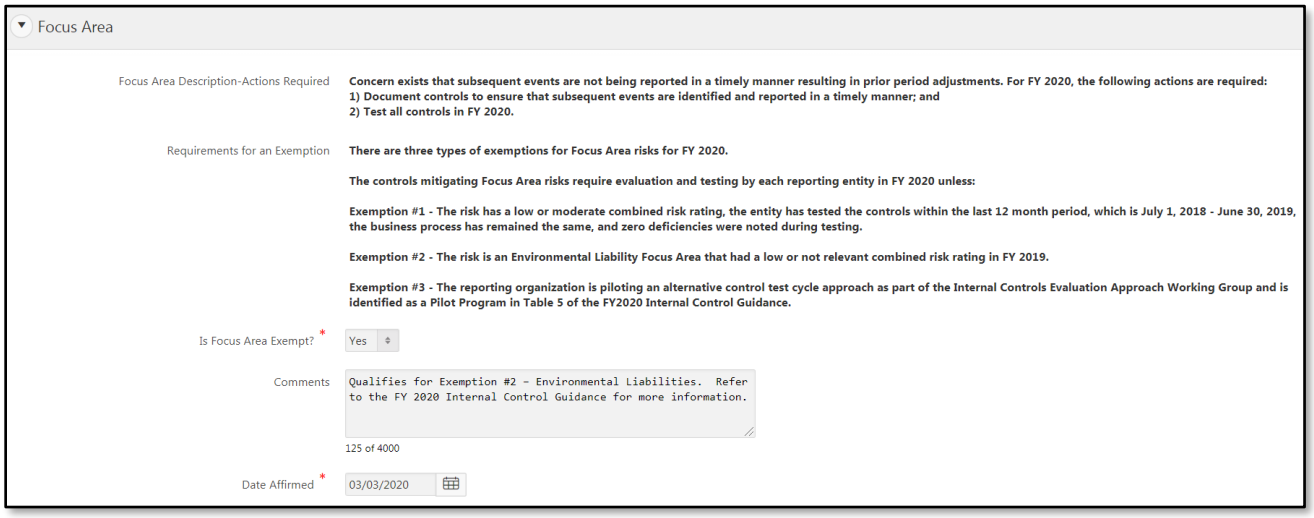
If the site meets the exemption requirements for Focus Area Risks, testing in the current assessment year will not be necessary. Exemption requirements are listed in the Annual Internal Controls Guidance and are also in AMERICA at each Focus Area Risk. For FY 2021, certain exemptions for select sites have been pre-populated in AMERICA. Because of this activity, there will be a disconnect between the **In Scope at Rollover** and the **In Scope Now** columns for those Focus Area Risks. Here is an example:



Although no actual testing was done and no testing information was input into AMERICA, the Controls (and the Focus Area Risk) are no longer in scope for the current year because the exemption was pre-populated.

To take a Focus Area Exemption:

- Carefully read the exemption language to be sure the site meets the conditions
- Select 'Yes' for Is Focus Area Exempt?
- In the Comments box, enter which exemption you are claiming (e.g.,, Qualifies for Exemption #1 - The risk has a low or moderate combined risk rating, the entity has tested the controls within the last 12 month period, which is July 1, 2018 - June 30, 2019, the business process has remained the same, and zero deficiencies were noted during testing.)
- In the 'Date Affirmed' field, enter the current date
- Select 'Save



FMA Module – Focus Area Section with "Yes" Exemption

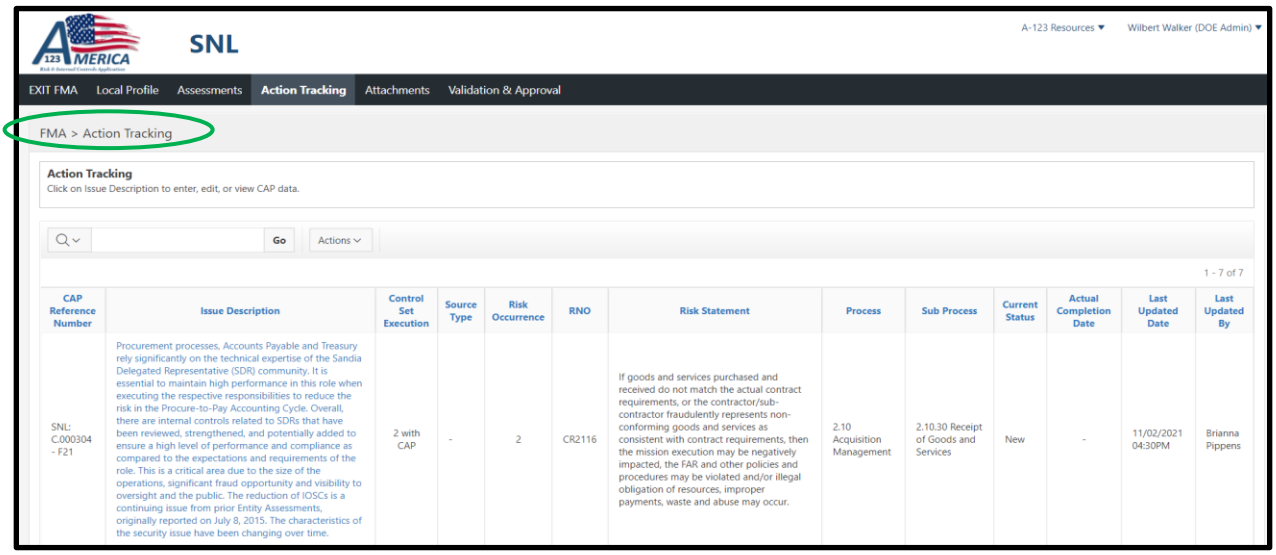
Navigating the FMA: Action Tracking

The Action Tracking tab of the FMA records CAPs for Risks that reporting entities have identified as being deficient based on the Control Set Execution rating of a '2 with CAP' or '3,' or a Risk Occurrence rating of '3.' Select the Action Tracking tab in the Global Menu.

A summary table will display with CAP information. The following fields will display:

CAP Reference Number: System generated identifier (e.g., CFO: C.000003-F19)
Issue Description: Brief description of the Issue from the CAP Details in the Assessments tab
CAP Rating: The CAP Rating from the Control Set Evaluation in the Assessments tab
RNO: System generated unique identifier used to designate specific risks in the FMA tool Framework
Risk Statement: Brief description of the Risk
Process: Automatically populated based on the Corporate Framework. The Process is an activity that is part of a business cycle. This field cannot be modified
Sub Process: Automatically populated based on the Corporate Framework. The Sub Process is the Sub-activities or components of a larger process. This field cannot be modified
Current Status: Current CAP status is provided in the Assessments tab

Last Updated Date: The date and time the CAP was last updated
Last Updated By: Specifies the user who made the last change



FMA Module – Action Tracking

Please note all Closed or Canceled CAPs will appear at the bottom of the list. These CAPs will not count toward active CAPs. For FY 22 the addition of the "Actual Completion Date" column will now display on the Action Tracking Form.

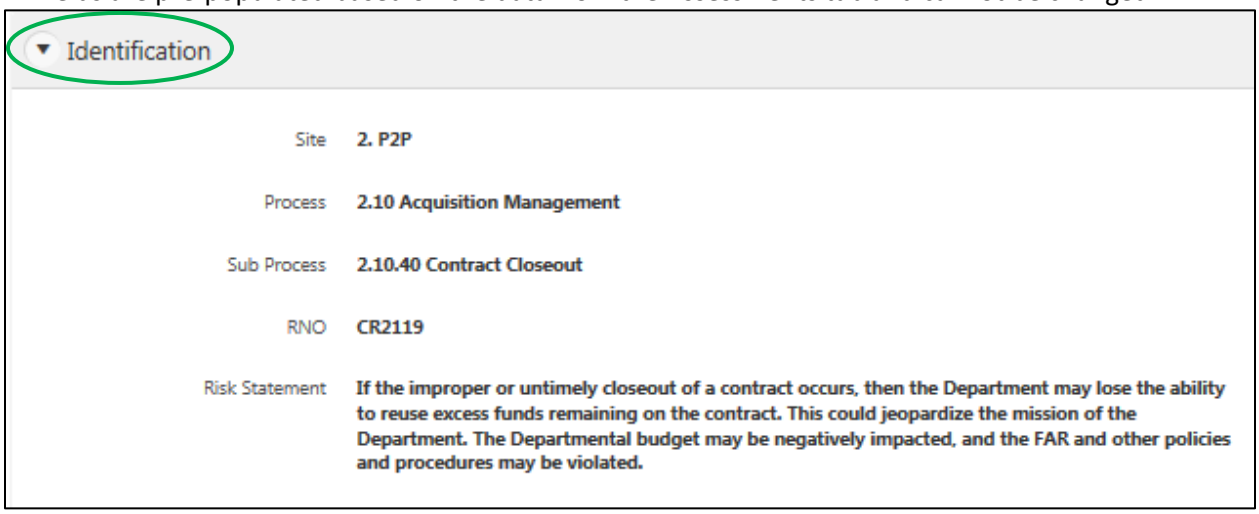
NEW in FY 2022

Evaluate a CAP

Select the Issue Description for the CAP, which will be highlighted in the blue text. The FMA Action Tracking CAP form is separated into 6 sections. The majority of the CAP data can also be updated under the Assessments tab. If data was already provided on the Assessments tab> CAP Details, that input will display and can be updated.

Identification

All fields are pre-populated based on the data from the Assessments tab and cannot be changed.



FMA – Action Tracking CAP Identification

Description

The field requirements are as follows:

CAP Reference Number: Automatically populated once the CAP has been created. System generated identifier (e.g., CFO: C.000003-F19)

Issue Description: (Required) Provide a description of the issue

CAP POC: (Required) Populate this field with the name of the primary point of contact responsible for completing the evaluation of that particular CAP

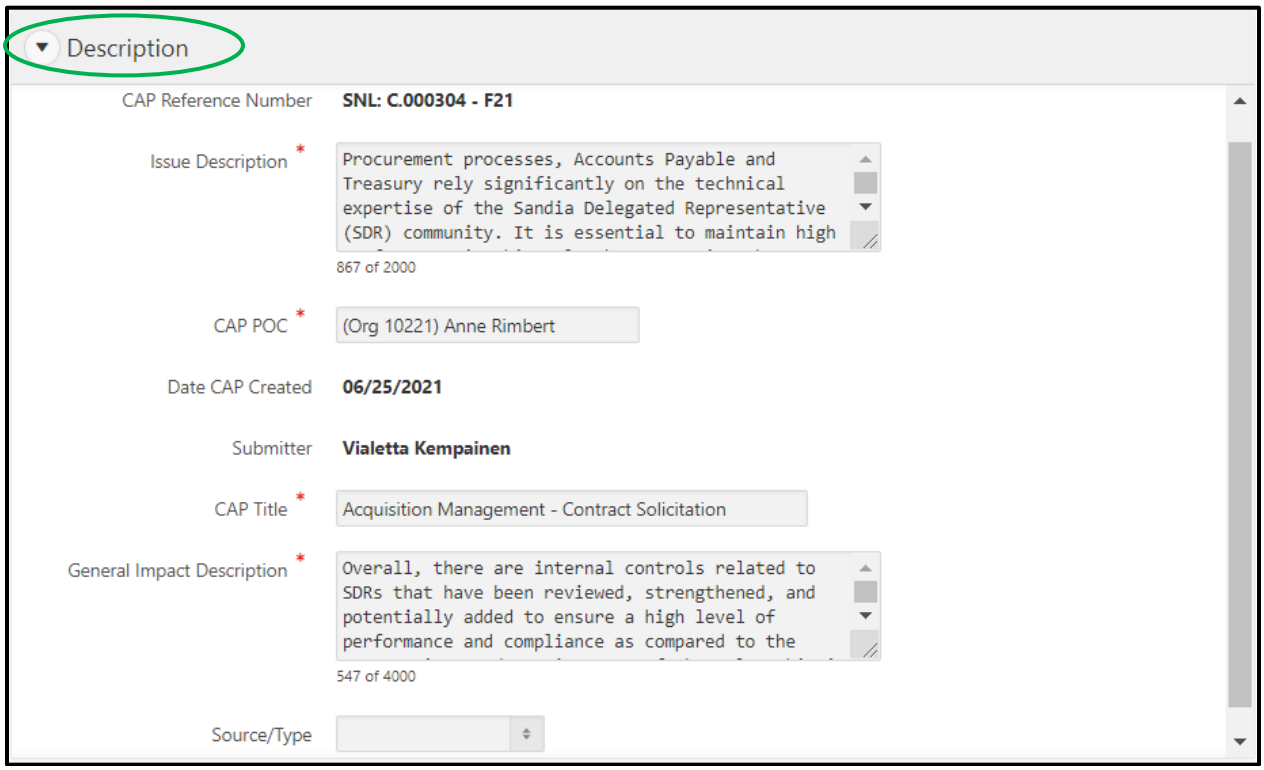
Date CAP Created: Automatically populated with the date the CAP was created

Submitter: Automatically populated with the name of the user that created the CAP

CAP Title: (Required) Provide a name for the CAP

General Impact Description: (Required) Provide a brief description of the impact the issue is having and future potential impacts, if any

To retain the updates made, select the 'Save' button. To discard changes made, select the 'Close' button.



FMA – Action Tracking CAP Description

Area Impacted

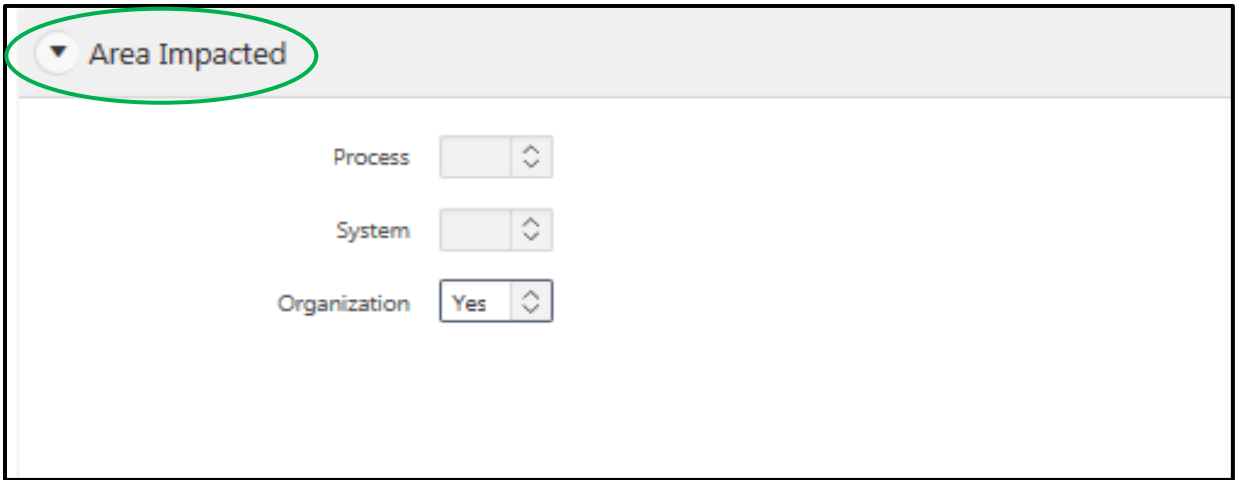
These fields are only on the Action Tracking form and cannot be updated on the Assessments tab in the CAP Details. The only dropdown selection for these fields is 'Yes.'

Process: Mark 'Yes' if the process area is impacted

System: Mark 'Yes' if the system area is impacted

Organization: Mark 'Yes' if the organization area is impacted

Note: More than one selection can be made.

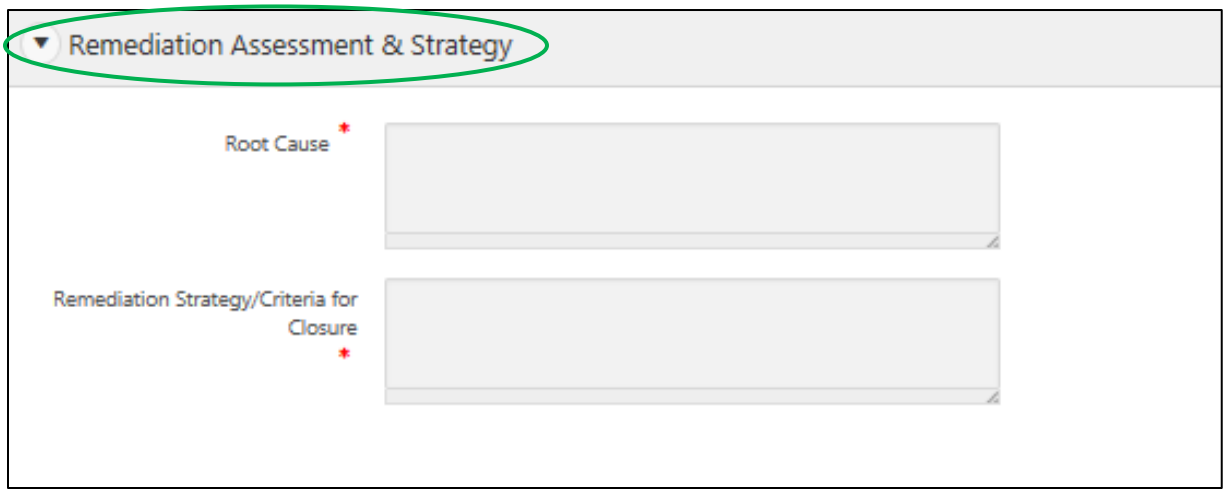


FMA – Action Tracking CAP Area Impacted

Remediation Assessment & Strategy

Root Cause: (Required) Provide a brief description or summary of the root cause of the problem. It is critical to define the root cause prior to developing a corrective action strategy and milestones.
Remediation Strategy/Criteria for Closure: (Required) Provide a brief summary of the remediation strategy and the criteria required in order to close the CAP

To retain the updates made, select the 'Save' button. To discard changes made, select the 'Close' button.



FMA – Action Tracking CAP Remediation Assessment & Strategy

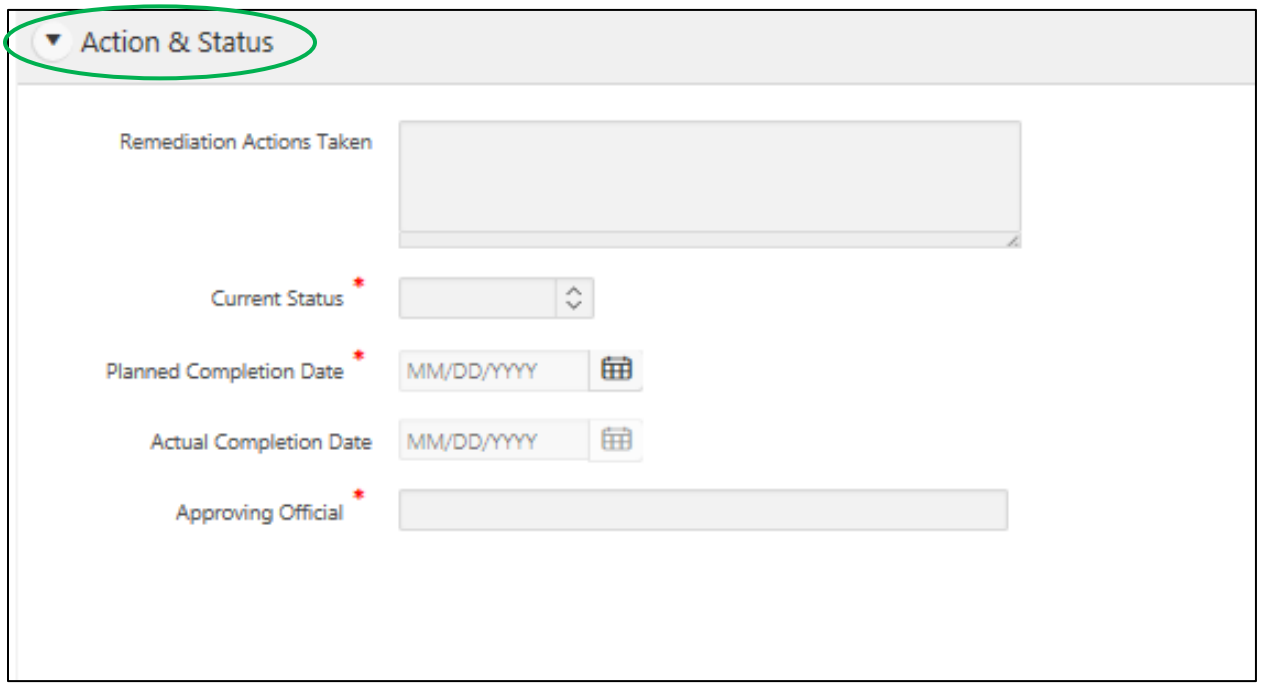
Action & Status

Remediation Actions Taken: Describe the remediation actions taken to date.
Current Status: (Required) Select the current CAP status from the drop-down menu:

- **New**: The need for the establishment of a CAP has been discovered through the current year's internal controls evaluation process.
- **In Progress**: Corrective actions have not yet been completed to resolve the issues and mitigate the stated impacts
- **Implemented**: Corrective actions have been implemented to address issues and stated impacts, but the criteria for closure have not been met
- **Closed**: All corrective actions have been completed to resolve the issue and mitigate the stated impacts
- **Canceled**: CAP is no longer necessary based on the discovery of new or additional information

Planned Completion Date: (Required) Provide the target closure date for the CAP.
Actual Completion Date: (Required if Current Status is Closed) Provide the actual closure date once CAP is closed. This field can only be updated when the Current Status selection is "Closed."
Approving Official: (Required) Provide the name of the individual certifying the CAP.

To retain the updates made, select the 'Save' button. To discard changes made, select the 'Close' button.

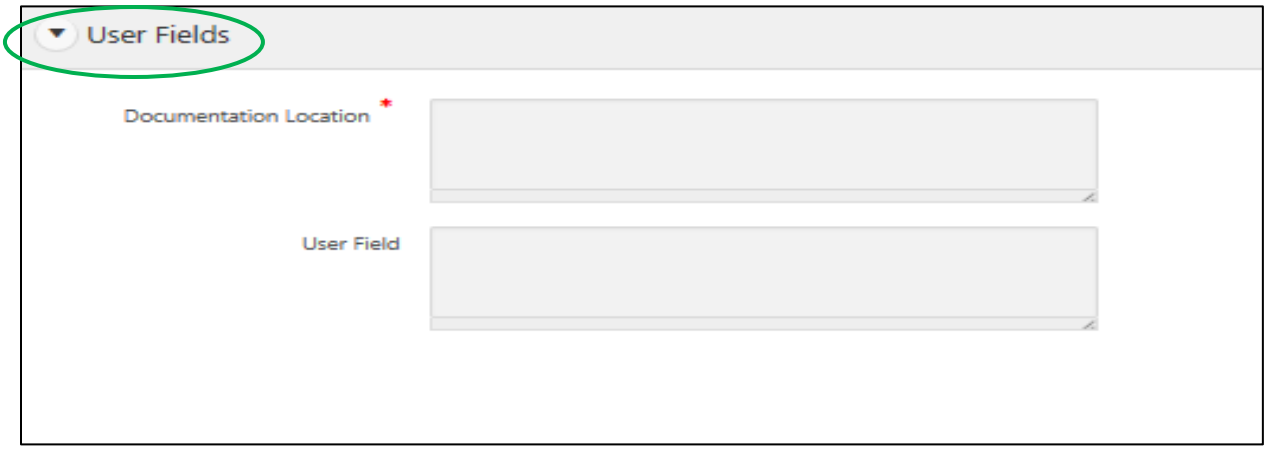


FMA - Action Tracking CAP Action & Status

User Fields

Documentation Location: (Required) Provide the location of the documents or any information that is considered beneficial in supporting the CAP
User Field: This field can be used to keep a record of any additional information the user finds helpful.

To retain the updates made, select the 'Save' button. To discard changes made, select the 'Close' button.



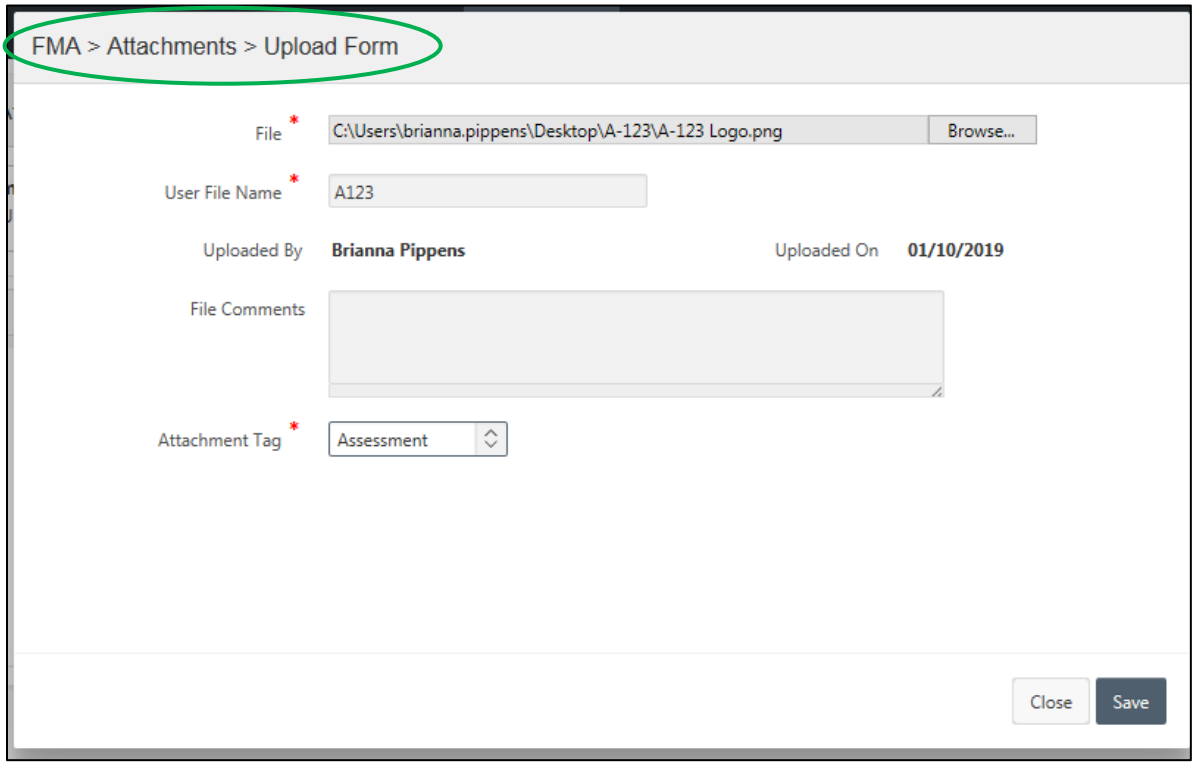
FMA - Action Tracking CAP User Fields

Navigating the FMA: Attachments

Users have the ability to add supplementary documents to support their FMA assessment activities via the Attachments tab. If there are no documents uploaded for a specific FMA, the workspace will read that there are no documents uploaded upon selecting the Attachments tab.

Uploading a File

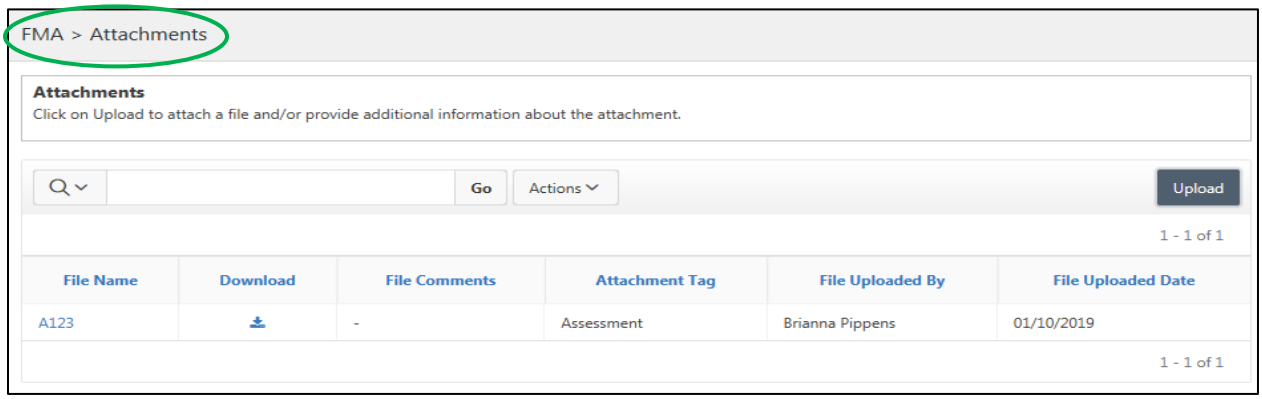
1. Locate and select the 'Upload' button
2. Provide content in the following fields:
   File: (Required) Click on 'Browse,' specify the file location to display, and select a file to upload
   User File Name: (Required) Provide a custom filename
   File Comments: Provide an explanation or annotation for the file
   Attachment Tag: (Required) Select from the dropdown list to indicate the subject for the attachment
3. Select the 'Save' button to save and upload the attachment
4. *To discard changes made, select the 'Close' button*



FMA Module - Attachments Upload Form

Once the file is uploaded, it will be hosted on the Attachments summary page along with the following summary fields:

- **File Name:** User given name to uniquely identify the file provided
- **Download:** The option to Open or Save the file
- **File Comments:** User explanation or annotation for the file uploaded
- **Attachment Tag:** Selected from the dropdown list to indicate the subject for the attachment
- **File Uploaded By:** Specifies the user who uploaded the file
- **File Uploaded Date**: The date and time when the file was uploaded



FMA Module - Attachments Summary

Modifying a File

1. Within the Attachments summary table, locate the file desired.
2. Select the 'File Name' within the summary table.
3. Content may be modified in the following fields:

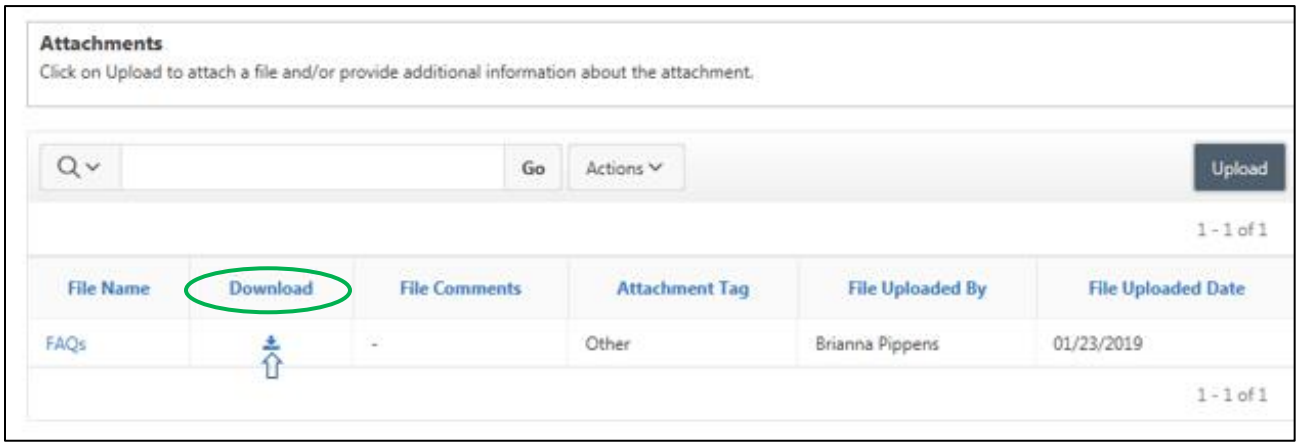
   User File Name: (Required) Type in a custom filename
   File Comments: (Optional but recommended) Provide an explanation or annotation for the file
   Attachment Tag: (Required) Select from the dropdown list to indicate the subject for the attachment

4. Select the 'Save' button to save updates.
5. *To discard changes made, select the 'Close' button.*

AMERICA was not designed as a document repository for all of your sites' documents. Upload only attachments that are pertinent to the validation and approval of your assessment.

Downloading a File

1. Within the Attachments summary table, locate the file desired
2. Select the download icon within the summary table



FMA - Download an Attachment

Navigating the FMA: Validation & Approval

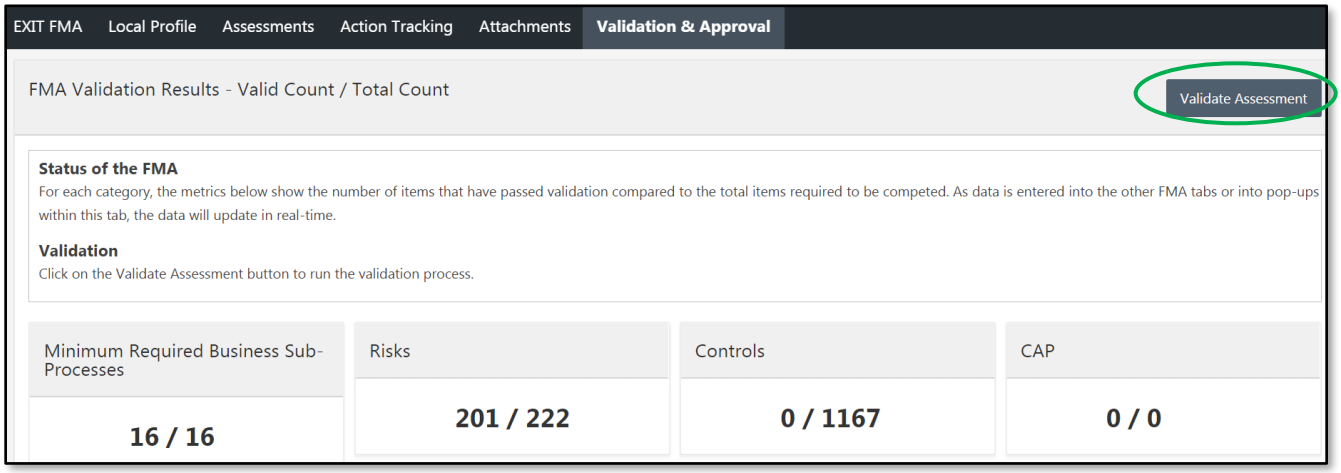
The Validation & Approval tab provides the ability to check the status of FMA validations, run a validation, and view Workflow History.

Validation

Prior to workflow submission, all FMA Assessments must pass validation. The 'Validate Assessment' button allows you to run validations at any time and as often as needed. However, a successful validation of your entity's FMA is required in order to proceed into workflow.

Note: The Validate Assessment button no longer appears once the FMA has fulfilled all of the validation requirements and is ready to enter into workflow.

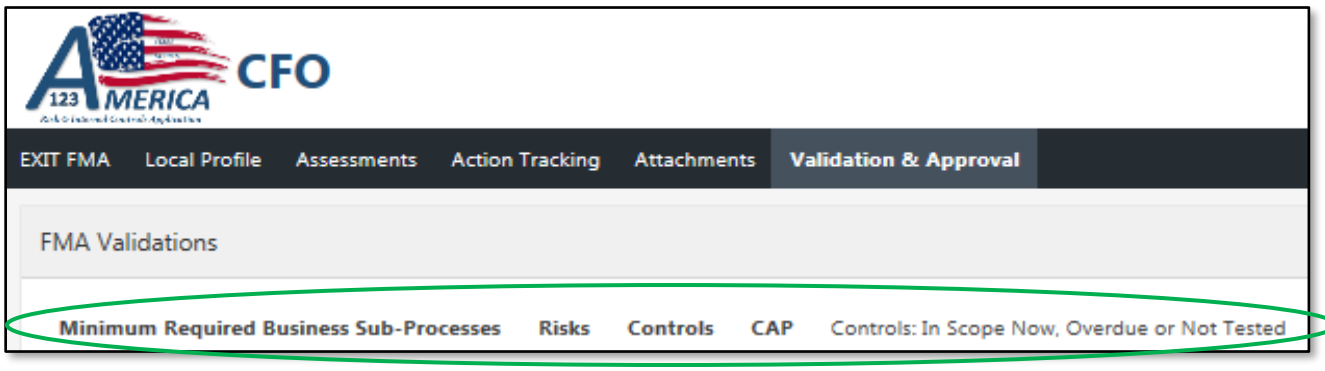
For each Validation category, metrics will show the number of items that have passed validation compared to the total items required to be completed. As data is entered into the other FMA tabs or pop-ups within this tab, the validation data will update in real-time.



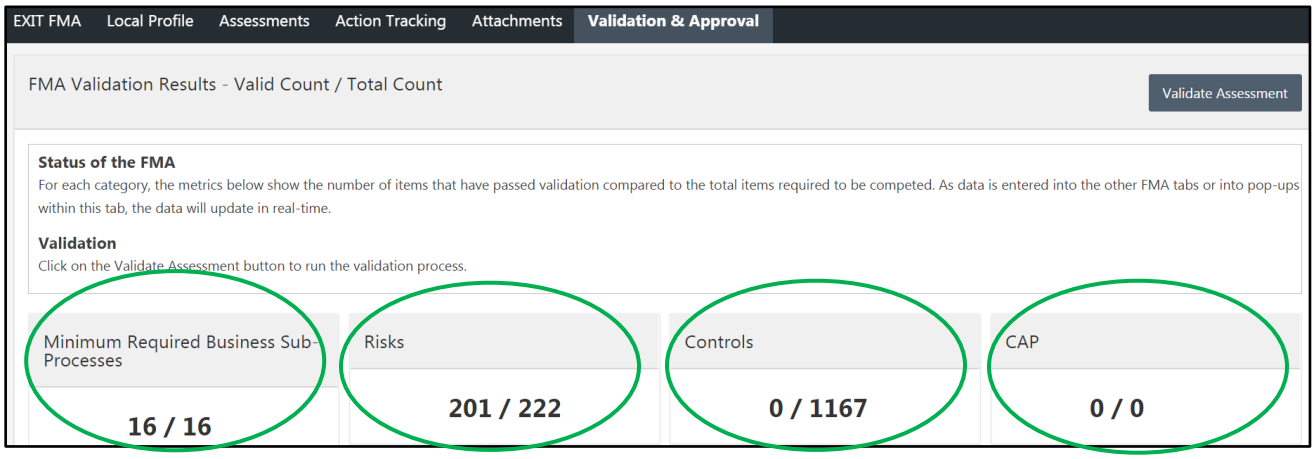
FMA - Validation & Approval Page

How to Access the Validations Table

1. Within the FMA module, select the Validation & Approval tab
2. The Validations and Workflow page will display
3. The top section will display the validation results for each category noting the Valid Count / Total Count
4. Select the "Validate Assessment" button. An updated status of each Validation category is displayed
5. FMA has four validation categories: Minimum Required Business Sub-Processes, Risks, Controls, and CAP. Each Validation category is a sub-tab. In FY 2020, a fifth tab, "Controls: In Scope Now, Overdue, or Not Tested," was added for informational only. This new tab is not a Validation. The FMA will pass Validation even if there are Controls that are In Scope Now or Overdue. Select each category to display the items that need to be addressed



FMA: Validation & Approval Page after Clicking "Validate Assessment"



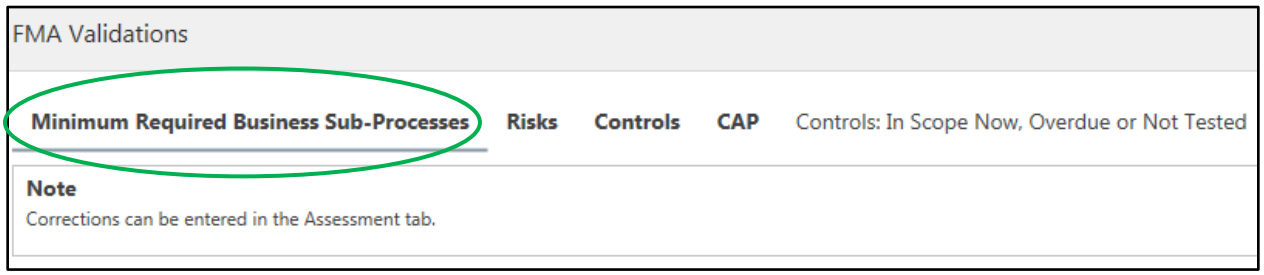
FMA Module - Validations Table

Minimum Required Business Sub-Processes

There are 16 required Sub-Processes that must be added to your entity's Assessment. If a Sub-Process has been added to the Assessment, there will be a green checkmark. If the Sub-Process has not been added to the Assessment, a red **X** will display.

To add the missing Sub-Process(es):

1. Navigate to the Assessments page
2. Select the Add Sub-Process button
3. Select the Sub-Process and Save
4. NOTE: Once all required Sub-Processes are added, the Validation will show 16/16 in the Minimum Required Business Sub-Processes category



FMA Module - Validations Minimum Required Business Sub Processes

Risks

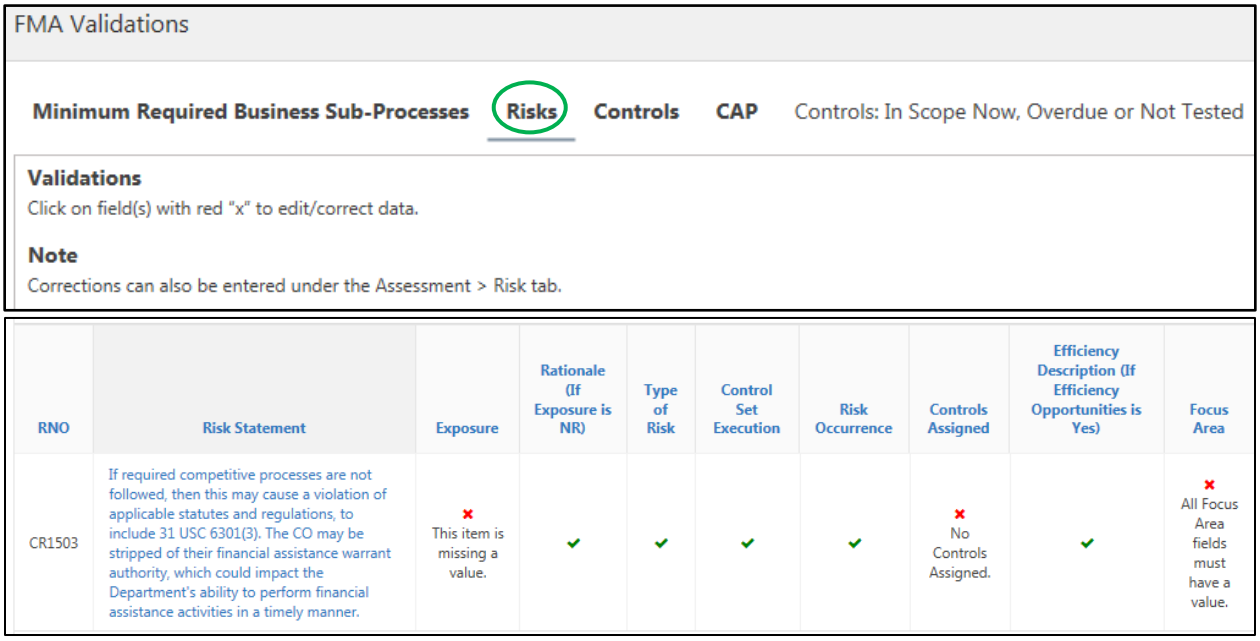
Risk validations are checking the individual Risks for 3 different things:

- All required fields have been addressed
- At least one Control has been added to the Risk
- All the required Focus Area fields have been addressed for Focus Area Risks

If the field has been addressed, there will be a green checkmark. If the validation has not been addressed, a red **X** will display.

To correct Risk Validations:

1. Navigate and select the Risk Statement shown in the blue text within the row
2. The category entry form will display. Navigate to the fields that need updating.
3. Update the fields and select 'Save'
4. Note upon saving, if the validations were corrected, the row would be removed from the validations page



FMA Module - Risk Validations

Controls

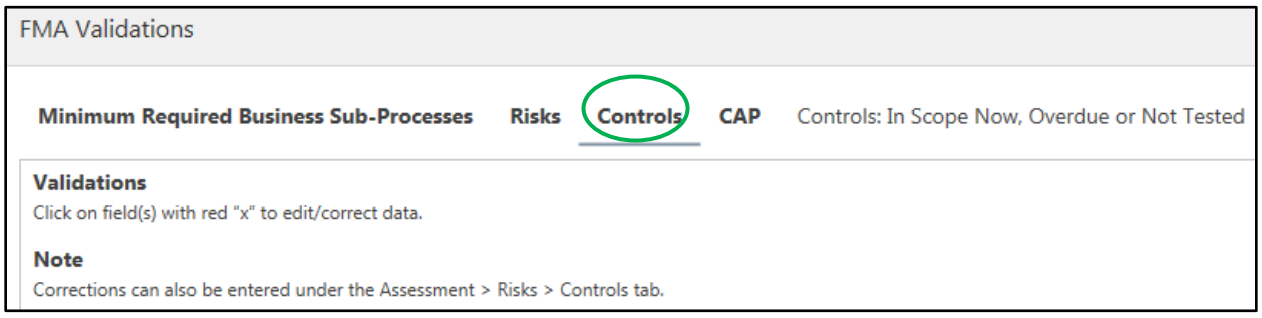
Control validations are checking that all required fields have been addressed for each individual Control.

If the field has been addressed, there will be a green checkmark. If the validation has not been addressed, a red **X** will display.

To correct Controls validations:

1. Navigate and select the Control Description shown in the blue text within the row
2. The category entry form will display. Navigate to the fields that need updating
3. Update the fields and select 'Save'
4. Note upon saving, if the validations were corrected, the row would be removed from the Validations page

Note: Controls that are In Scope for testing in the current year that was not tested will not appear as needing validation and will not stop the user from submitting.



FMA Module - Controls Validations

CAP

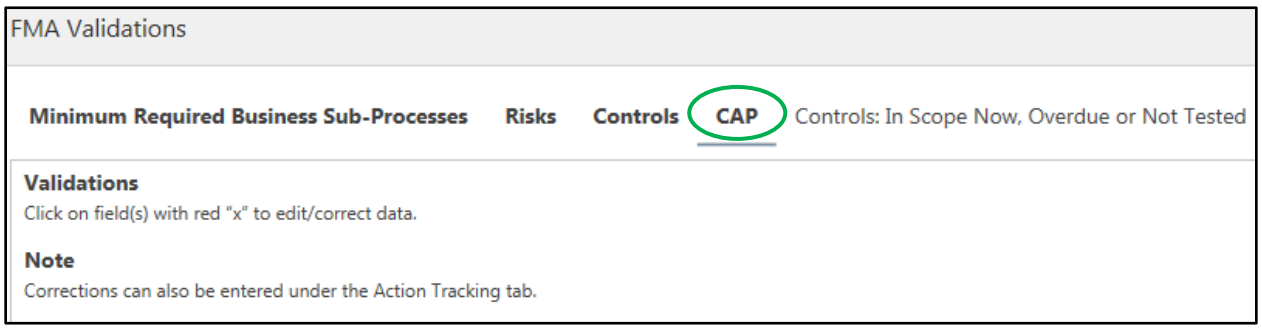
CAP validations are checking that all required fields have been addressed for each individual CAP. Please remember if a prior year CAP Issue rating changed to a 1, it must be Canceled or closed; otherwise, the following error message will appear:

"*Current Status must be Closed or Canceled if CSE is 1 or 2 w/o CAP*"

If the field has been addressed, there will be a green checkmark. If the validation has not been addressed, a red **X** will display.

To correct CAP validations:

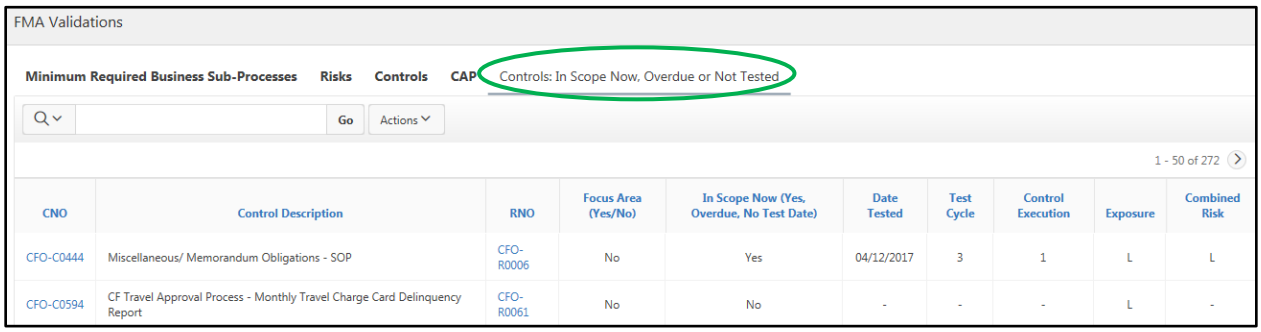
1. Navigate and select the Issue Description shown in the blue text within the row
2. The category entry form will display. Navigate to the fields that need updating.
3. Update the fields and select 'Save'
4. Note upon saving, if the validations were corrected, the row would be removed from the Validations page



FMA - CAP Validations

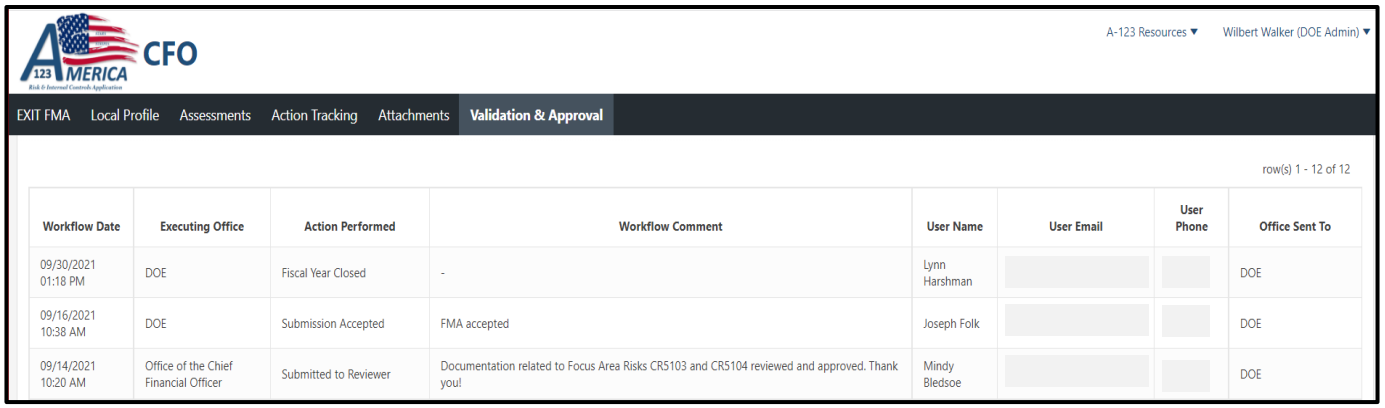
Once all validations have been addressed, the FMA may be submitted for approval via Workflow.

The new fifth tab, "Controls: In Scope Now, Overdue, or Not Tested," is informational only. The FMA will pass Validation even if there are Controls that are In Scope Now or Overdue. This tab displays those Controls still requiring testing in the current year and those that have yet to be tested.



Workflow History

The Workflow History provides the Approval hierarchy for the organization's FMA. See AMERICA User Guide – Workflow and Reports for additional information on Workflow.



Appendix A: Field Calculations

There are many fields that have automatic calculations based on other field inputs. This section will give more detail on how these fields are populated.

Control Risk Rating

Control Risk Rating			
Risk Occurrence	**Control Set Execution**		**Control Risk**
1	1	=	L
1	2	=	L
1	3	=	M
2	2	=	M
3	2	=	H
3	3	=	H
2	1	=	L
2	3	=	H
3	1	=	M

Test Cycle

Test Cycle Calculation		
Combined Risk		**Test Cycle**
H	=	1
M	=	2
L	=	3
(Blank)	=	(Blank)

Combined Risk Rating

Combined Risk Rating			
Exposure Risk	**Control Risk**		**Combined Risk**
L	L	=	L
L	M	=	L
L	H	=	M
M	L	=	L
M	M	=	M
M	H	=	H
H	L	=	M
H	M	=	H
H	H	=	H
NR	Not Considered	=	NR

Risk Level: In Scope This Year

Consideration 1	Consideration 2	Consideration 3	Consideration 4		Final Value
Date Risk Added	**Test Cycle**	**Date Control Set Rated/ Evaluated**	**Combined Risk**		**Current Year**
Date Risk Added + 1 < Fiscal Year	(Blank)	(Blank)	Not Considered	=	Overdue
Date Risk Added + 1 = Fiscal Year	(Blank)	(Blank)	Not Considered	=	Yes
Not Considered	Test Cycle + Year Control Set Tested = Fiscal Year	Test Cycle + Year Control Set Tested = Fiscal Year	H, M, or L	=	Yes
Date Risk Added = Fiscal Year	(Blank)	(Blank)	Not Considered	=	No
Not Considered	Test Cycle + Year Control Set Tested > Fiscal Year	Test Cycle + Year Control Set Tested > Fiscal Year	H, M, or L	=	No
Not Considered	Not Considered	Not Considered	NR	=	NR

***Note**: Focus Area Risks automatically populate with "Yes" for In Scope for This Year.*

Risk Level: In Scope Next Year

Consideration 1	Consideration 2	Consideration 3	Consideration 4		Final Value
Date Risk Added	**Test Cycle**	**Date Control Set Rated/ Evaluated**	**Combined Risk**		**Next Year**
Not Considered	Test Cycle + Year Control Set Tested = Fiscal Year + 1	Test Cycle + Year Control Set Tested = Fiscal Year + 1	H, M, or L	=	Yes
Date Risk Added = Fiscal Year	(Blank)	(Blank)	Not Considered	=	Yes
Not Considered	Not Considered	Not Considered	NR	=	NR
-	-	-	-	=	No

Control Level: In Scope This Year

Consideration 1	Consideration 2	Consideration 3	Consideration 4	Consideration 5		Final Value
Year Control Added	**Test Cycle**	**Date Control Tested**	**Combined Risk**	**Control Execution**		**Current**
Year Control Added + 1 < Fiscal Year	(Blank)	(Blank)	Not Considered	Not Considered	=	Overdue
Not Considered	Test Cycle + Year Tested < Fiscal Year	Test Cycle + Year Tested < Fiscal Year	H, M, or L	1, 2, or 3	=	Overdue
Year Control Added + 1 = Fiscal Year	(Blank)	(Blank)	Not Considered	Not Considered	=	Yes
Not Considered	Test Cycle + Year Tested = Fiscal Year	Test Cycle + Year Tested = Fiscal Year	H, M, or L	1, 2, or 3	=	Yes
Year Control Added = Fiscal Year	(Blank)	(Blank)	Not Considered	Not Considered	=	No
Not Considered	Test Cycle + Year Tested > Fiscal Year	Test Cycle + Year Tested > Fiscal Year	H, M, or L	1, 2, or 3	=	No

Appendix B: Color Indicators

There are several fields within the FMA module that are color coded based on the data value.

Exposure	Low	Moderate	High
Control Set Execution	1	2 without CAP 2 with CAP	3
Risk Occurrence	1	2	3
Control Risk	Low	Moderate	High
Combined Risk	Low	Moderate	High

Appendix E – Fraud Risk Management

A. Purpose and Background

Fraud poses a risk to the integrity of Federal programs and can erode public trust in government. Effective fraud risk management helps to make sure that the Department's services are fulfilling intended purposes, funds are spent effectively, and assets are safeguarded. In FY 2022, DOE continues to place emphasis on fraud prevention, detection, and mitigation to decrease fraud and to comply with the *Payment Integrity Information Act of 2019* (PIIA). PIIA indicates that the guidelines required to be established under section 3(a) of FRDAA shall continue to be in effect on or after the date of enactment of PIIA, which requires agencies to:

- Conduct an evaluation of fraud risks using a risk-based approach to design and implement control activities to mitigate identified fraud risks;
- Collect and analyze data from reporting mechanisms on detected fraud to monitor fraud trends and use that data and information to continuously improve fraud prevention controls; and,
- Use the results of monitoring, evaluations, audits, and investigations to improve fraud prevention, detection, and response.

B. GAO Fraud Framework

To help combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks in the Fraud Framework. The Fraud Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, and highlights opportunities for federal managers to take a more strategic, risk-based approach to managing fraud risks and developing effective antifraud controls. The Fraud Framework describes leading practices for establishing an organizational structure and culture that are conducive to fraud risk management, designing and implementing controls to prevent and detect potential fraud, and monitoring and evaluating to provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud.

DOE reporting organizations should adhere to the leading practices in the GAO Fraud Framework as part of the efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. Reporting organizations are responsible for determining the extent to which the leading practices from the Fraud Framework are relevant to each office and for tailoring the practices, as appropriate. In doing so, reporting organizations should consider the specific risks the entity faces, applicable laws and regulations, and the associated benefits and costs of implementing each practice.

For details on the GAO Fraud Framework, refer to GAO-15-593SP, *A Framework for Managing Fraud Risks in Federal Programs*.

Figure 1 GAO Fraud Risk Framework and Select Leading Practices

DOE entities may use Treasury's *Program Integrity: Antifraud Playbook* (Playbook) to assist with the implementation of leading practices from the GAO Framework. The Playbook offers guidance to entities on how to proactively manage fraud risk in order to prevent fraud. The Playbook also clarifies and operationalizes concepts put forward in other guidance, including the GAO Fraud Framework, in order to help entities adopt the leading practices. Reporting organizations are not required to implement the Playbook sequentially, or in its entirety. The Playbook may be used to best fit the needs of the entity, and may be utilized differently based on the organization's level of maturity.

C. DOE Fraud Risk & Data Analytics Framework

As part of the Department's effort to improve its fraud risk mitigation activities since 2017, DOE developed a fraud risk framework modeled after the GAO's Fraud Framework. It will manage and integrate the fraud risk framework with internal control activities at all levels throughout the Department.

The phased approach will occur over the next several years and the Department will progress to the next phase once all the conditions have been met in the previous phase. Adjustments will be made as necessary to achieve the best results.

Phase I began in FY 2020-2021. The OCFO invoked '*commitment*' per the first component of the GAO Fraud Framework. DOE Senior Management are engaged in the overall fraud risk management as the roles and responsibilities of the Department Internal Control and Assessment Review Council (DICARC) were expanded to perform additional duties as the Senior Risk Management Council (SRMC). A DOE Senior Assessment Team (SAT), a subset group of DICARC/SRMC, will implement DOE's fraud risk framework considering recommendations from the Fraud Risk Working Group (FRWG). The FRWG consists of representatives from Headquarters Offices, Field Offices, and M&O contractors as shown in ***Figure 2***. The DICARC/SRMC and the SAT, coupled with OCFO's Internal Controls & Fraud Risk Management Division (ICFRMD), will serve as the designated entities to lead fraud risk management activities for the Department.

In FY 2022, OCFO will continue to support the DICARC and SRMC in leading the effort for implementing DOE's Fraud Risk Framework based on recommendations from the FRWG. The DICARC/SRMC and the SAT, coupled with OCFO's Internal Controls & Fraud Risk Management Division (ICFRMD), will serve as the designated entities to lead fraud risk management activities for the Department. **Reporting organizations will identify and provide the name of their Risk POC to the OCFO** in accordance with Table 2, *DOE Internal Controls and Risk Profile Important FY 2022 Dates.*

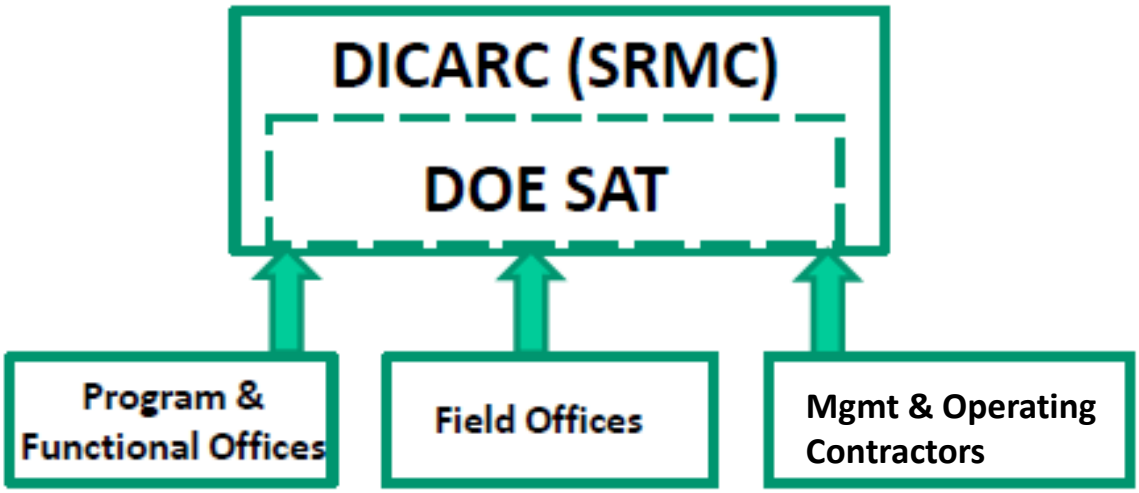
NEW in FY 2022

Phase II focuses on evaluating fraud risk occurrences across DOE along with preparing and providing direction on DOE's antifraud strategy. The SAT supported by the FRWG will prepare a Department Fraud Risk Profile. The SAT and FRWG are slated to begin recurring quarterly meetings starting in January 2022. In phase III DOE will continue to mature and monitor the fraud risk framework.

Continuous evolution of the DOE Fraud Risk Framework is expected by establishing data analytics with leadership and expertise across the Department. There will be continuous monitoring of fraud risks as DOE corporate fraud risks and potential controls are refined along with the anti-fraud strategy.

As DOE's Fraud Risk Framework continues to improve, recommended best practices and lessons learned will be considered in order to further mature and integrate ERM and internal controls.

Figure 2 DOE SAT as a subset of SRMC leveraging recommendations from various working groups



D. Fraud Communication Requirements

DOE internal controls reporting organizations are expected to report allegations and actual instances of fraud, waste, abuse, corruption, criminal acts, or mismanagement related to DOE programs to the Department's Office of the Inspector General (OIG) in accordance with DOE Order 221.1B. The DOE OIG is responsible for investigating any fraudulent acts involving DOE, contractors or subcontractors, or any crime affecting the programs, operations, Government funds, or employees of those entities. Entities can report suspected or actual fraud to the OIG anonymously and confidentially through the OIG Hotline[1]. **Organizations should report allegations of suspected or actual fraud promptly to the Department OIG**.

E. Fraud Trends Across the Department

The Department continues efforts to combat and prevent fraud, waste, and abuse. One particular fraud risk that continues to emerge as a threat to the Department is business email compromise (BEC). BECs involve the impersonation of legitimate DOE personnel or vendors to request changes in the payment information in order to route Department funds to a fraudulent bank account. Fraudsters use information available online to impersonate a legitimate Department vendor/employee, create a spoofed email address similar to the legitimate vendor/employee email address, and then send an email to a DOE entity requesting a change in banking information.

BEC fraudulent activities continue to adversely impact the Department and Government as a whole. Reporting organizations should review the *Business Email Compromise Checklist* on the final page of this appendix. The checklist contains immediate actions in the event of a BEC, as well as potential controls for prevention and recognition. Reporting organizations should consider the risk of business email compromise fraud and establish or enhance controls to manage the risk as warranted.

The Government Accountability Office (GAO) has identified nine fraud scheme categories in recent audits that may impact the Department of Energy. Reporting organizations should consider the actions they are taking to mitigate the potential risks of these fraud schemes from occurring. The fraud schemes are found in ***Table 1***.

Table 1 GAO Contracting Fraud Schemes Categories[2]

Bid Rigging	Payroll Schemes	Kickback and Gratuities
Conflicts of Interests	Misrepresentation of Eligibility	Theft
Product Quality	Contract Progress Schemes	Billing Schemes

The DOE OIG also identified common fraud schemes that entities should consider:

- Non-Deliverables – where a recipient fails to produce what is required from the statement of work or the grants/contract is closed out without holding the recipient/contractor accountable.
- Bid Rigging or Collusion – two or more contractors/subcontractors/grantees work together and attempt to extort the Department of funds.

[1] Contact OIG Hotline via email: ighotline@hq.doe.gov or phone: (202) 586-4073, toll free: (800) 541-1625, and fax: FAX: (202) 586-4902.
A webform may also be filled out using the following web address: https://www.energy.gov/ig/complaint-form.
[2] The definitions are found in Appendix G, Glossary.

- Fraud in the Inducement – when a grantee lies about their capabilities in order to receive Department funding.
- Ghost Employees – paying government funds to employees that don't exist.
- Fictitious Invoices/Laundering – fake companies send fictitious bills to the prime contractors/grantee for reimbursement.
- Kickbacks/ Bribes/ Extortion/ Conflict of Interest by Federal officials in the award and administration of grants/ contracts.
- Foreign Corrupt Practices on the part of U.S. or foreign officials.

Due to the current pandemic, there has been a rise of vulnerability to BEC and targeted phishing on most teleworkers. The following should be considered to avoid becoming a victim to these common fraud schemes:

- Use DOE equipment for DOE business only - Do not connect unauthorized devices, e.g. smartphones and USB devices, to your DOE equipment.
- Update your work devices - Check that your devices and software are up-to-date.
- Communicate your working hours - Establish and disclose your hours of availability for your team's awareness.
- Observe your surroundings - Avoid having sensitive work-related conversations in public areas.
- Encrypt email messages containing sensitive information - Ensure your online activities are encrypted and use telework capabilities provided.
- Avoid leaving DOE equipment unattended at any time - Lock your screen when walking away and store your work device in a secure location.
- Practice good phishing hygiene - Avoid clicking on suspicious links and attachments from unsolicited emails.
- Be cautious of unfamiliar e-mails regarding the COVID-19 pandemic.

F. Fraud Requirements in the FMA Review

DOE maintains an emphasis on fraud prevention in the Financial Management Assessment (FMA) Module within AMERICA to further increase fraud prevention activities across the Department. In FY 2022, entities are responsible for reviewing controls to determine if a fraud and/or improper payments risk is mitigated. Any controls that mitigate a fraud and/or improper payments risk should be designated as such in the FMA Module Assessment tab by **selecting the appropriate designation from the *Fraud/ Improper Payments* dropdown option for controls**. If a control is designed to mitigate a fraud and/ or improper payment risk and the control fails testing, or fails related to the detection of potential fraud, the organization will notify their assigned OCFO Analyst on the control failure and the remediation plan to confirm a control is designed and operating effectively to mitigate the risk. Entities should also continue to improve data integrity by removing all Fraud/ Improper Payment selections from the *Control Category* field and identify from the dropdown menu whether the control is *Business, Compliance, Performance*, or *Information Technology*. For more information on how to assign a fraud and/or improper payment control type in AMERICA, see Appendix C.

In FY 2022, the *Fraud/Improper Payments/Both Fraud & IP* dropdown options have been removed from the *Type of Risk* field. **Local risks** which were reported as *Fraud, Improper Payments,* or *Both Fraud & IP* in the *Type of Risk* field at the end of FY 2021 have been changed to *Business*. Organizations affected by this change will need to review and update these **local risks,** if needed. Affected organizations will be notified in December of the local risks affected by this change and **must** identify in the FMA Module

local risks that are subject to fraud, improper payment, or both by **selecting from the dropdown menu of the *Fraud/Improper Payments* field**.

G. Fraud Requirements in the Entity Review

To sustain increased fraud prevention activities across the Department, emphasis remains in this area in the EA Module. In the Entity Objective Evaluation tab, organizations must evaluate the Fraud Prevention entity objective. This evaluation is in addition to the assessment of fraud risk under the GAO Green Book Principle #8, "management should consider the potential for fraud when identifying, analyzing, and responding to risks," in the Internal Controls Evaluation tab. The Fraud Prevention entity objective has several considerations that should be evaluated by reporting organizations.

1. *Top financial and top non-financial fraud risks* - organizations must identify the top financial and non-financial fraud risks. The top fraud risks identified in an entity's EA Module should be consistent with the fraud risks included in the FY 2022 Risk Profile deliverable.
2. *Fraud risk factors* - entities should consider the fraud risk factors from the GAO Green Book. While the following fraud risk factors don't necessarily indicate that fraud exists, they are often present when fraud occurs.
    - Incentive/Pressure: management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud
    - Opportunity: circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud
    - Attitude/Rationalization: individuals involved are able to rationalize committing fraud
3. *Fraud mitigation controls for identified fraud risks* – organizations should determine if controls are in place to mitigate identified fraud risks. For controls reported in the FMA Module that manage a fraud risk, organizations should assign a fraud and/or improper payments control type.
4. *Management's commitment to reporting fraud* – entities should evaluate whether the organization is encouraging the reporting of suspected fraud to the DOE OIG in accordance with DOE Order 221.1B, "Reporting Fraud, Waste and Abuse to the Office of Inspector General."
5. *Additional potential areas of fraud risk* – organizations should specifically consider potential fraud risks in the following areas that are more susceptible to fraud at DOE:
    - Procurement activities
    - Purchase card programs
    - Property management
    - Contractor and sub-contractor oversight
    - Grant and beneficiary management/payments
    - Time and attendance

    Entities that complete an FMA Module should assess and evaluate the potential fraud risks in the FMA. Organizations that are not required to complete an FMA Module should list mitigating control activities in the EA Module.

H. Fraud Requirements in the Risk Profile

Management has overall responsibility for establishing internal controls to manage the risk of fraud. When developing the FY 2022 Risk Profile, organizations must consider the potential for fraud and should follow the guidance set forth by the GAO Fraud Framework and GAO Green Book.

In FY 2022, all entities must identify the top financial and non-financial fraud risk in the Risk Profile deliverable along with other identified significant risks. **Organizations must identify whether each risk has a fraud impact by selecting Financial, Non-financial, Top Financial, or Top Non-financial fraud impact by completing the *Fraud Impact* column in the Risk Profile.** If a risk does not have a fraud impact, then organizations should select "N/A" from the drop-down menu. While financial fraud risks are often well known, there can be difficulties in identifying non-financial fraud risks. Examples of potential non-financial fraud risks are included below:

- Theft of PII or classified information
- False claims or false statements (For example, a contractor makes false statements to win a bid, an employee provides false statements to be hired, or a grantee provides false claims to be awarded a grant)
- Employees pressured to issue knowingly incorrect non-financial data/reports
- Product substitution or counterfeit parts (For example, a subcontractor fraudulently provides the wrong parts or parts of a lesser material)
- Employee sabotage or employee vandalism[3]

[3] Black's Law Dictionary defines vandalism as mindless and malicious harm and injury to another's property.

Business Email Compromise Checklist

Have you been a victim of CEO or Wire Transfer Fraud, commonly known as Business Email Compromise (BEC)? Review the checklist below for immediate actions, as well as, ideas for prevention and recognition:

IMMEDIATE ACTIONS

Reporting the Incident

- ☐ Contact your bank
  - ☐ Determine the appropriate contact at your bank, who has the authority to recall a wire transfer
  - ☐ Notify your bank you have been the victim of a Business Email Compromise
    - AND -
  - ☐ Request a wire recall or SWIFT Recall Message
    - AND -
  - ☐ Request they fully cooperate with law enforcement
- ☐ Report the incident (or attempt) to the FBI at www.IC3.gov
  - ☐ Provide all details for the beneficiary: account numbers, contact information, names
- ☐ Contact your local FBI Field Office

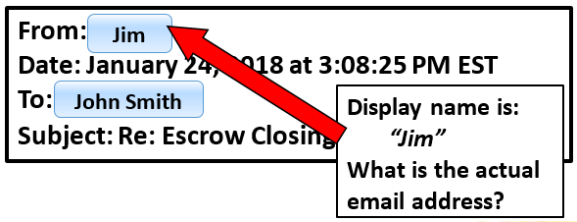
Internal Actions

- ☐ Review all IP logs accessing the relevant infrastructure (internal mail servers or other publically accessible infrastructure) looking for unusual activity
- ☐ Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?
- ☐ Review the relevant email account(s) which may have been spoofed or otherwise compromised for any rules such as "auto forward" or "auto delete"
- ☐ Inform employees/agents of the situation and require they contact clients and customers who are near the wire transfer stage
- ☐ Review all requests that asked for a change in payment type or location.

***Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend. ***

PREVENTION & RECOGNITION

- ☐ Hover you cursor over, or expand contact details on, suspicious email addresses – Looking for indications of Display Name Deception or Spoofing



- ☐ DO NOT hover on ***links*** within emails, as simply hovering *may* execute commands.
- ☐ Call a known/trusted phone number or meet in person to confirm that the wire transfer information provided to you, matches the other party's information
- ☐ Does the Routing Number or SWIFT Number provided to you, resolve to the expected bank used by the other party?

  (Example: Have you received wire information for an account at a Hong Kong bank; however, your other party only banks in the U.S?)

  Possible websites to verify a Routing or SWIFT Number:
  a. Any reputable search engine
  b. The Federal Reserve www.FRBServices.org
  c. American Bankers Association https://routingnumber.aba.com

- ☐ Regularly check your email account log-in activity for possible signs of email compromise
- ☐ Develop an intrusion detection system to identify emails from extensions that are similar to your company email.
- ☐ Regularly check your email account for new "rules", such as email forwarding and/or auto delete
- ☐ Be cautious of "new" customers, suppliers, clients and/or others you don't know who ask you to:
  a. …open or download any documents they send
  - OR -
  b. …sign into a separate window or click on a link to view an invoice or document
  - OR -
  c. …provide sensitive Personal or Corporate information
- ☐ Verify the wire instructions you provide to your customers/clients are accurate for both the pertinent bank and pertinent account.
  a. Where did you get the account data?
  b. Is this the correct account number?

Appendix F – Financial Management Systems Evaluation Guidance

Background

Section 4 of the *Federal Managers' Financial Integrity Act of 1982* (FMFIA) requires agencies to include a separate report on the conformance of the agency's accounting system as prescribed by the Comptroller General of the Government Accountability Office (GAO). The *Federal Financial Management Improvement Act of 1996* (FFMIA) expands upon financial management system (FMS) evaluations. FFMIA, Section 803 (a) addresses areas of compliance for financial management systems. They are (1) Federal FMS requirements; (2) Applicable Federal Accounting Standards; and, (3) United States Standard General Ledger.

The Office of Management and Budget (OMB) Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996,* defines an FMS as an agency's overall financial operation, **reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions**. Financial management systems include hardware, applications and system software, personnel, procedures, data, and reporting functions. The financial management system can be fully integrated with other management information systems (i.e., mixed systems) where transactions automatically flow into the accounting general ledger. The financial management system could also include manual processes to post transactions from other management systems into the accounting general ledger.

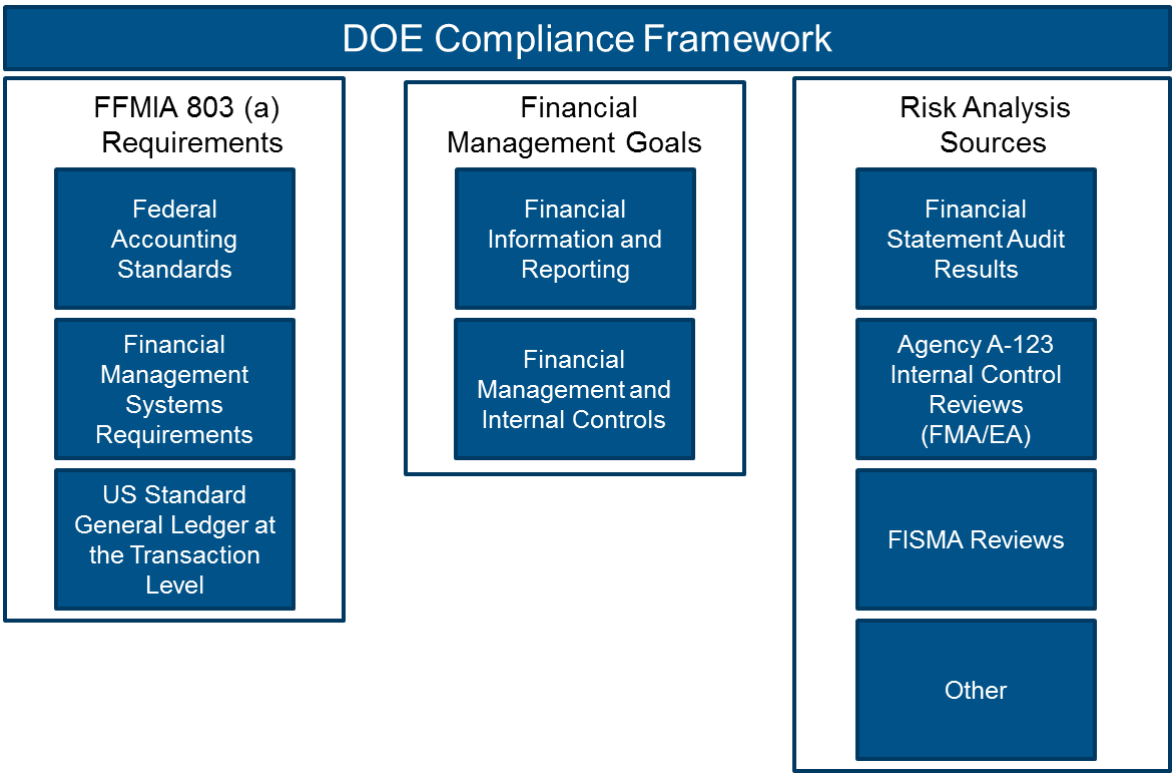
Owners and users of financial management systems will perform financial management system evaluations. Refer to Table 1 in the *DOE Internal Control Evaluations Guidance* for organizations that are required to perform financial management system evaluations. For questions, refer to your assigned OCFO Analyst. Headquarter's organizations, Field/Site Offices, and Major/Integrated Contractors use and/or provide information into one or more of the Department's financial management systems. If an entity's system (including integrated and major contractor systems) feed into a Department of Energy (DOE) financial management system, then those systems are subject to an FMS Evaluation. As a result, users of financial management systems span into all organizations throughout the Department including the Field/Site Offices and Major/Integrated Contractors.

Department of Energy's Compliance Framework

DOE's compliance framework (Figure 1) is based on the compliance framework published in OMB Circular A-123, Appendix D. DOE's compliance framework consists of three pillars, which are FFMIA 803 (a) Requirements, Financial Management Goals, and Risk Analysis Sources.

Section 803 (a) requirements are the (1) Federal FMS requirements; (2) Applicable Federal Accounting Standards; and, (3) United States Standard General Ledger. The financial management categories are groupings of related goals. The two financial management categories are (1) Financial Information and Reporting and (2) Financial Management and Internal Controls. Each financial management category consists of four goals (Figure 3). The Risk Analysis Sources are the documents that Departmental elements and Major/Integrated Contractors may use as sources of information when assessing whether the organization is achieving a prescribed goal. When performing assessments, organizations should use the compliance indicators (Figure 3) identified for each goal. An entity's FMS evaluation should capture the results of its evaluation for applicable systems – a separate FMS evaluation for each FMS system is not necessary.

Figure 1: DOE Compliance Framework



Deliverable Requirements

As depicted in the *DOE Internal Control Evaluations Guidance*, Table 1, Headquarters, Field Offices and Major/Integrated Contractors are responsible for completing a financial management system evaluation. Organizations will record the results of financial management system evaluations in the Financial Management System Evaluation Tab of the Entity Assessment Module of the AMERICA Application. Organizations are expected to provide summary evaluation results as depicted in Figure 2.

Figure 2: Example Financial Management Evaluation Summary

Financial Information Management and Reporting, Goal 1

Rating: 2

Source: External Reviews, IG/GAO Audits

During the Internal Control testing period for July 1, 2019 – June 30, 2020, there were 3 IG/GAO audits that revealed 2 significant deficiencies related to the accurate recording and accounting for PPE. The 2 significant deficiencies were linked to inappropriate depreciation. A corrective action plan has been prepared and is CAP # in DARTS.

Financial Management and Internal Controls, Goal 1

Rating: 1

Source: A-123 Internal Reviews

During the Internal Control testing period for July 1, 2019 – June 30, 2020, FMA reviews did not reveal any problems and there were not any issues identified by external organizations.

Instructions for Financial Management System Evaluations

The Financial Management Systems Worksheet (Figure 3) is designed to assist organizations with financial management system assessments. An explanation of each area as they appear in the AMERICA Application is listed below:

Goal: This column identifies each of the eight goals that FMS owners and users should assess to determine whether an organization is achieving each goal that supports the financial management categories.

Compliance Indicator(s): This column identifies possible areas of consideration that FMS owners and users should consider when assessing the risk of non-compliance for each category to support the assessment of the eight financial management goals.

Risk Level Assessment: FMS owners and users will use this column to select a risk rating category that reflects the organization's risk of non-compliance for each goal. An organization will select low, moderate, or high.

Sources Used In Determining Risk Level: This column is also referred to as the Risk Analysis Sources in the DOE Compliance Framework. FMS owners and users may use any of the listed sources as a basis for the assessment. Organizations may select multiple sources.

Risk Assessment Score: This column is auto-populated based on the risk rating category that is selected in the Risk Level Assessment column. Selecting low, moderate, or high will result in a 1, 2, or 3, respectively. The lower the score the lower the risk of non-compliance for a particular goal.

Evaluation Summary: FMS owners and users should provide a summary synopsis that will serve as the basis of the assessment. An example is provided in Figure 2.

Figure 3: Financial Management System Evaluation Worksheet

Financial Management System (FMS) Evaluation

Departmental elements will check only one of these boxes.

Departmental elements may check more than one of these boxes.

Goal	Compliance Indicator(s)	Risk Level Assessment	Sources Used in Determining Risk Level	Risk Assessment Score	Evaluation Summary
1. Federal Financial Information Management and Reporting					
1.1 Consistently, completely, and accurately record and account for Federal funds, assets, liabilities, revenues, expenditures, and costs.	Current/prior year's DOE, Departmental element, or auditor reported material weaknesses, significant deficiencies, or non-conformances related to accounting for and recording Federal funds, assets, liabilities, revenues, expenditures, and costs.	☐ **Low:** DOE, Departmental element, or auditor reported zero control deficiencies or reported control deficiencies that individually or collectively are not considered significant. ☐ **Moderate:** DOE, Departmental element, or auditor reported significant deficiencies or non-conformances ☐ **High:** DOE, Departmental element, or auditor reported material weaknesses.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)	Need numerical score based on entry at left in the Risk Level Assessment column. Low = 1 Moderate = 2 High = 3	Test Field: Sites write their words here.
1.2 Provide timely and reliable Federal financial management information of appropriate form and content to DOE program managers for managing current Departmental programs and activities.	Current/prior year's DOE or Departmental element reported material weaknesses, significant deficiencies, or non-conformances related to internal reporting of financial management information used for managing current Government programs and activities.	☐ **Low:** DOE or Departmental element reported zero control deficiencies or reported control deficiencies that individually or collectively are not considered significant. ☐ **Moderate:** DOE or Departmental element reported significant deficiencies or non-conformances. ☐ **High:** DOE or Departmental element reported material weaknesses.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		
1.3 Provide timely and reliable Federal financial management information of appropriate form and content for continuing use by stakeholders external to the Department, including the President, the Congress, and the public.	Financial Information (Departmental Element) and/or Financial Statements (DOE & PMAs): a. Departmental element submitted financial information that supports the DOE financial statements or audit opinion on the DOE financial statements. b. Departmental element submitted financial information to DOE in accordance with the prescribed timeline or unaudited interim DOE financial statements submitted to OMB within 21 calendar days after the end of the first three quarters of the fiscal	☐ **Low:** Accurate financial data submitted by Departmental elements is in accordance with the prescribed timeline to DOE or an Unmodified audit is provided on DOE financial statements and the financial statements are submitted on time to GAO, OMB, and Congress. ☐ **Moderate:** Departmental elements have provided late financial data for the current quarter/year to DOE or DOE has not submitted financial reports on time for the current quarter/year to GAO, OMB, and Congress. ☐ **High:** Departmental elements have provided Inaccurate or late financial data for the current and prior quarters/years to DOE or DOE has received a Qualified, Disclaimer, or Adverse opinion on the financial	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		

Goal	Compliance Indicator(s)	Risk Level Assessment	Sources Used in Determining Risk Level	Risk Assessment Score	Evaluation Summary
	year and Agency Financial Report submitted to OMB, GAO, and the Congress by November 15.	statements or DOE has not submitted financial reports on time for the current and prior quarters/year to GAO, OMB, and Congress.			
1.4 Provide timely and reliable Federal financial management information of appropriate form and content that can be linked to strategic goals and performance information.	Departmental element costs as submitted to DOE or DOE costs, as presented in the Statement of Net Costs, in accordance with OMB Circular No. A-136, are clearly linked to DOE strategic goals, which are free from Departmental element or DOE-reported material weaknesses, significant deficiencies, or non-conformances. Additionally, financial and performance information that is submitted by Departmental elements or DOE is presented in the performance section of the Agency Financial Report or Performance & Accountability Report, is free from reported material weaknesses, significant deficiencies, or non-conformances.	☐ **Low:** DOE, Departmental element, or auditor reported zero control deficiencies or reported control deficiencies that individually or collectively are not considered significant. ☐ **Moderate:** DOE, Departmental element, or auditor reported significant deficiencies or non-conformances. ☐ **High:** DOE, Departmental element, or auditor reported material weaknesses.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		
2. Financial Management and Internal Controls					
2.1 Provide internal control to restrict Federal obligations and outlays to those authorized by law and within the amount available.	Current/prior year's DOE, Departmental element, or auditor reported material weaknesses, significant deficiencies, or non-conformances related to restricting DOE obligations and outlays to those authorized by law and within the amount available or an Anti-deficiency Act (ADA) was required to be submitted.	☐ **Low:** DOE, Departmental element, or auditor reported zero control deficiencies or reported control deficiencies that individually or collectively are not considered significant and/or an ADA Violation was not submitted within the last two fiscal years preceding the current fiscal year. ☐ **Moderate:** DOE, Departmental element, or auditor reported significant deficiencies or non- conformances and/or an ADA violation was submitted within the last two fiscal years preceding the current fiscal year. ☐ **High:** DOE, Departmental element, or auditor reported material weaknesses and/or an ADA violation was required to be submitted for the current fiscal year.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		
2.2 Perform Federal financial management operations effectively within resources available.	Current/prior year's instances of non-compliance with laws and regulations related to prompt payments or debts owed to the Federal Government.	☐ **Low:** No reported instances of non-compliance with laws and regulations. ☐ **Moderate:** Instances of non-compliance with laws and regulations were reported in the current year.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results		

Goal	Compliance Indicator(s)	Risk Level Assessment	Sources Used in Determining Risk Level	Risk Assessment Score	Evaluation Summary
		☐ **High:** Instances of non-compliance with laws and regulations were reported in the current year and prior years.	☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		
2.3 Minimize waste, loss, unauthorized use, or misappropriation of Federal funds, property, and other assets within resources available.	Current/prior year's DOE, Departmental element, or auditor reported material weaknesses, significant deficiencies, or non-conformances related to minimizing waste, loss, unauthorized use, or misappropriation of Federal funds, property and other Assets.	☐ **Low:** DOE, Departmental element, or auditor reported zero control deficiencies or reported control deficiencies that are not significant. ☐ **Moderate:** DOE, Departmental element, or auditor reported significant deficiencies or non- conformances. ☐ **High:** DOE, Departmental element, or auditor reported material weaknesses.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		
2.4 Minimize Federal financial management system security risks to an acceptable level.	FISMA or other (for example, National Institute of Standards and Technology-related) significant deficiencies impacting financial management systems in the DOE or Departmental element's Security Certification and Accreditation of Federal Information Systems.	☐ **Low:** DOE, Departmental element, or auditor reported zero control deficiencies or reported control deficiencies that individually or collectively are not considered significant. ☐ **Moderate:** DOE, Departmental element, or auditor reported control deficiencies. ☐ **High:** DOE, Departmental element, or auditor reported non-conformances, significant deficiencies, or material weaknesses.	☐ Financial Statement/GAO/IG Audits ☐ A-123 Internal Reviews ☐ FISMA Review Results ☐ Management's Knowledge of Operations ☐ Other (Add source in Evaluation Summary Column)		
Risk Assessment Total	**Total of scores in the "Risk Assessment" column plus the words:** **Low Risk of Non-compliance (if score is 12 or less)** **Moderate Risk of Non-compliance (if score is between 13 and 19)** **High Risk of Non-compliance (if score is 20 or higher)**				

Compliance Summary

1. Federal Financial Information Management and Reporting ☐ Substantial Compliance ☐ Non-Compliance (with CAPs noted)
2. Financial Management and Internal Controls ☐ Substantial Compliance ☐ Non-Compliance (with CAPs noted)

Appendix G – Glossary of Terms

AMERICA	An application that automates and streamlines the Department's management, reporting, and analysis of risks and controls in compliance with OMB Circular A-123.
Assurance Memorandum	Annual statement of assurance provided by reporting organizations that expresses the overall adequacy and effectiveness of the system of internal controls. For the required Assurance Memorandum content, see Appendix D, *Assurance Memorandum Templates*.
Basis of Evaluation	The key information or activities performed to provide support for assurances that the control objectives and considerations were addressed. The Basis of Evaluation should be a documented activity. Examples include reports, bi-annual workforce planning survey results, other reports, memos, reviews, assessments, evaluations, plans, emails, meeting minutes, certificates, and documented signatures.
Bid-rigging	Agency officials or contractors bidding on a contract conspire to influence the purchase of goods or services to avoid competitive bidding controls. Bid-rigging typically involves contractors agreeing to artificially increase the prices of goods or services offered in bids to the government or bidding in such a way to guarantee a specific contractor wins the contract.
Billing Schemes	Contractors obtaining payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.
Budget to Close (B2C)	The cycle comprises financial and/or accounting processes used to manage financial data and resources such as: General Ledger Management; Funds Management; Fund Balance with Treasury; Cost Management; Grants Administration; and Loan Administration. Specific areas involved in the cycle are budgeting, journal entries, costing reconciliations, financial reporting and closing activities at month, quarter, and year-end.
Combined Risk Assessment	The residual risk considering the control environment and a measure of the end risk to DOE. In the FMA Module, the combined risk is a calculated field based on exposure risk and control risk. If an organization has not performed control testing, the combined risk rating defaults to the exposure risk rating. Once control testing is conducted and recorded, the combined risk will automatically calculate. H – High risk, ineffective risk mitigation; M – Moderate risk; and L – Low risk, effective risk mitigation. The diagram demonstrates the calculation of High, Moderate, and Low combined risk ratings.

Exposure Risk				
	H	Moderate	High	High
	M	Low	Moderate	High
	L	Low	Low	Moderate
		L	M	H
		Control Risk		

Conflicts of Interest

Agency officials or government contractors inappropriately awarding business to vendors in which they have an unreported direct or indirect interest, potentially resulting in higher contract costs or purchases of goods or services not needed. Conflicts of interest can arise at the individual or organizational level. Organizational conflict of interest can occur when a contractor has a preexisting relationship with a potential subcontractor or vendor that results in in appropriate award of subcontracts at higher cost to the government.

Contract Progress Schemes

Contractors inappropriately obtaining payments by purposefully misrepresenting the extent of project completion.

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 the assigned functions, to achieve control objectives and address related risks. There are three types of control deficiencies:

Design Deficiency – 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.

Implementation Deficiency – Exists when a properly designed control is not implemented correctly in the internal control system.

Operating Deficiency – 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.

Control Execution

A rating resulting from individual control testing. Control Execution ratings are defined in the FMA Module as:

1 – Passed with no failures.
2 – Passed with failures within acceptable threshold.
3 – Failed.

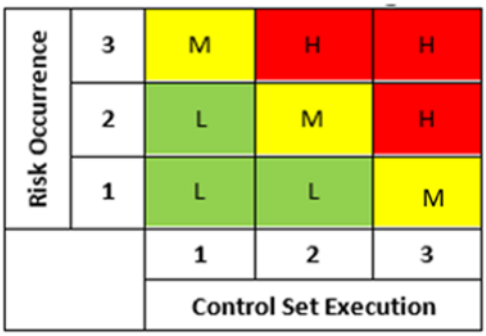
Control Objective

Identifies the key objectives to be achieved by the internal control in each area, as well as specific types of control issues that should be considered

when performing the evaluation and the goal to be achieved to minimize, manage, or mitigate risks. Each objective considers the nature of the activity, the organization's mission, and the cost and benefits of each control in determining desired control objectives.

Control Risk Assessment

A measure of the risk considering the effectiveness of the controls to mitigate that risk and the risk occurrence. In the FMA Module, control risk is calculated based on the **Control Set Execution** and **Risk Occurrence scores**. The diagram demonstrates the calculation of High, Moderate, and Low control risk ratings:



Control Set Execution: Rating based on an assessment of the testing results of all individual controls within a control set.
1 - Passed with no failures;
2 - Passed with failures within acceptable threshold; or
3 - Failed.

Risk Occurrence: Determined through observation during normal business operations. Ask, did the risk occur during normal business operations within the current testing year?
1 - No risk occurrence;
2 - Risk occurred within acceptable threshold; or
3 - Risk occurred outside the acceptable threshold.
Example scenarios for rating risk occurrence and control set execution are available on the Internal Controls iPortal space under the Resources tab.

Corporate Risk

A risk that is pre-populated into the FMA Module to facilitate the FMA Evaluation. The FMA Module also allows each organization to add local risks.

Corrective Action Plan (CAP)

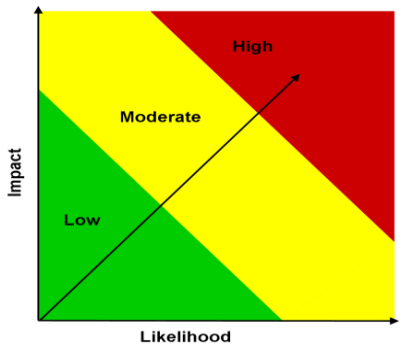
A plan to correct a control deficiency. A CAP must be prepared and tracked for all significant control deficiencies identified during the internal control evaluations process. A CAP Summary for significant deficiencies and material weaknesses identified in the Assurance Memorandum must be provided with the memorandum.

Data Analytics

Process of examining data sets in order to find trends and draw conclusions about the information.

Departmental Element

Refers to DOE Headquarters Offices, Power Marketing Administrations, Field, and/or Operations Offices.

Entity	Refers to DOE reporting organizations and includes DOE Headquarters Offices, Field Offices, Site Offices, Power Marking Administrations, Operations Offices, and Major/Integrated Contractors.
Entity Assessment (EA) Module	The central location for documenting and reporting the results of evaluations of the entity's internal controls and objectives as well as financial management system evaluations.
Entity Evaluation	Detailed evaluation of an organization's key administrative, operational, or programmatic activities, to determine whether adequate control techniques exist and are implemented to achieve cost-effective compliance with FMFIA and FFMIA.
Entity Level Controls	Controls that have a pervasive effect on an entity's internal control system and pertains to multiple components.
Enterprise Risk Management (ERM)	An agency-wide approach to addressing the full spectrum of DOE external and internal risks by understanding the combined impact of all organization risks as an interrelated portfolio, rather than addressing risks in individual programs.
Evaluation Summary	Presents the key information or activities leveraged/performed to provide reliable support for assurances that the control objectives and considerations have been addressed.
Exposure Risk Assessment	A combined measure of the **likelihood** and **impact** to DOE should the risk occur (regardless of the strength of the controls to mitigate the risk). In the FMA Module, this is a professional judgment rating of High, Moderate, Low, or Not Relevant (NR). The NR rating is for corporately defined risks that may not impact all organizations. No assessment is required with a rating of NR, although a short rationale will need to be provided. **General environment:** Environment that assumes no mitigating controls are in place. **Likelihood:** The measure of the relative potential that the risk might occur given the general environment. **Impact:** The measure of the magnitude and nature of the effect the risk might cause given the general environment. 

Federal Managers' Financial Integrity Act (FMFIA)	Federal Act that requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency (including DOE). DOE Order 413.1b, *Internal Control Program,* requires the Department to establish and maintain an internal control program to evaluate internal controls and report the status of significant issues up through the chain of command to the President and Congress. To support Departmental reporting, Heads of organizations, including the National Nuclear Security Administration (NNSA), are required to report on the status of the organization's internal controls, including reportable issues identified and progress made in correcting prior reportable issues. FMFIA provides for: • Evaluation of an agency's internal controls in accordance with Government Accountability Office (GAO) standards; • Annual reporting by the head of each executive agency to the President; • Identification of material weaknesses and the plans for correcting them; and, • Agencies to provide for internal control assessments on an on-going basis.
Federal Financial Management Improvement Act (FFMIA)	Federal Act that requires each agency to implement and maintain financial management systems that comply substantially with the: • Federal financial management systems requirements; • Applicable Federal accounting standards; and, • United States Government Standard General Ledger (USSGL) at the transaction level.
Financial Management Assessment (FMA) Evaluation	An evaluation of internal controls over reporting that tests an entity's controls in order to provide assurance on the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.
Financial Management Assessment (FMA) Module	The central location for documenting the evaluation of the relevant financial business processes, sub processes, and risks facing each reporting entity, as well as the key controls and testing information for each process that are relied upon to mitigate the risks.
Financial Management Systems	OMB Circular A-123, Appendix D*, Compliance with the Federal Financial Management Improvement Act of 1996,* defines a "financial management system" as including "an agency's overall financial operation, reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions, including hardware, applications and system software, personnel, procedures, data, and reporting functions. The financial management system may fully integrate with other management information systems (i.e., mixed systems) where transactions automatically flow into an accounting general ledger. The financial management system could also include manual processes to post transactions from other management systems into the accounting general ledger."

	The financial system encompasses processes and records that: • Identify and record all valid transactions; • Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting; • Measure the value of transactions in a manner that permits recording the proper monetary value in the financial statements; and • Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period."
Financial Management Systems (FMS) Evaluation	In accordance with the FMFIA, entity owners of a financial management system included in the Department's FMS Inventory, and users of an FMS, are required to conduct an FMS Evaluation as part of the annual internal controls evaluation process.
Focus Area	Specific areas of emphasis which require additional assessment in the FMA Module.
Improper Payment	When the payment funds go to the wrong recipient, the recipient receives the incorrect amount of funds, or the recipient uses the funds in an improper manner resulting in unintentional payment errors or intentional fraud and abuse.
Interim Internal Controls Status (IICS) Assessment	A questionnaire that provides a mid-year update confirming that annual non-financial and financial risk assessments are being performed, risk exposure ratings updated, corrective actions are being taken on any significant issues identified in the current or prior year assessments, and whether any issues have been identified that would rise to the level of a significant deficiency or material weakness.
Internal Control	An integrated component of management that provides reasonable assurance that the following objectives are being achieved: • Effectiveness and efficiency of operations; • Reliability of reporting; and • Compliance with applicable laws and regulations.
Inherent Risk	The exposure arising from a risk before any action is taken to manage it.
Inquiry	A detailed discussion with knowledgeable personnel to determine if controls are in place and functioning
Inspection	Scrutiny of specific business processes and documents through consideration and analysis for approval authorities that indicate the effectiveness of controls.
Key Control	A control or set of controls that address the relevant assertions for a material activity or significant risk. At the point that management is ready to test controls, and in order to focus test work, management must identify the key controls in place.

Kickbacks and Gratuities	Contractors making undisclosed payments to agency officials or other government contractors or giving something of value to reward a business decision.
Local Risk	A risk in the FMA that is added by a reporting organization because the risk is applicable to that organization and the risk is not captured in a corporate risk
Material Non-conformance	Exists when *financial systems* do not substantially comply with federal financial management system requirements or where control deficiencies impact financial systems' ability to comply. The EA Module defines the conformance criteria and captures identified non-conformances.
Material Weakness	A significant deficiency that the Entity Head determines to be significant enough to report outside of the Entity as a material weakness. There are four types: **Material Weakness in Internal Control Over Operations** – Includes, but is not limited to, conditions that: • Impact the operating effectiveness of Entity Level Controls; • Impair fulfillment of essential operations or mission; • Deprive the public of needed services; and • Significantly weakens established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest. **Material Weakness in Internal Control Over Reporting** – A significant deficiency, in which the Entity's Head determines significant enough to impact internal or external decision-making and reports outside of the Entity as a material weakness. **Material Weakness in Internal Control Over Financial Reporting** – A significant 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. **Material Weakness in Internal Control Over Compliance** – A condition where management lacks a process that reasonably assures 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 Entity objectives.
Major/Integrated Contractors	DOE contractors with responsibility for the management and/or operation of a Department-owned or leased facility.
Misrepresentation of Eligibility	Contractors purposefully reporting incorrect information in bid proposal to falsely claim eligibility to perform the work, such as status as a small business
Minimum Evaluation Standard	The basis by which testing cycles for the FMA Evaluation are determined. The minimum evaluation standard is based on the combined risk rating of risks

	identified both corporate risks automatically populated by the FMA Module and local risks identified by the individual entity for each standard process and sub-process. Controls for processes that have risks with a combined risk rating of High are tested each year. Controls for a process that has risks with a combined risk rating of Moderate are tested at least once every two years. Controls for processes that have risks with a combined risk rating of **Low** are tested at least once every three years. All controls in all business processes and sub-processes must be on a three-year testing cycle, including processes with a Low exposure rating and no control risk rating. If an organization has not tested a control in the past two years, the control will receive testing in the current year.
Mitigate	To put controls in place that would reduce the probability or impact of a given risk from being realized.
Mixed System	OMB Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, defines as a "hybrid of financial and non-financial portions of the overall financial management system."
Non-Conformance	Exists when the Entity has identified potentially significant deficiencies in the scope of the internal controls' evaluations conducted, which would warrant disclosure to assure limitations are understood
OMB Circular A-123 Observation	Prescribes guidance for internal control and risk management requirements. The viewing of a specific business process in action, and in particular the control activities associated with the process, to test the effectiveness of an internal control.
Payment Integrity Information Act (PIIA)	Federal act requiring agency leaders to assess and identify high-risk or otherwise significant programs and activities and share these findings in an annual publication.
Payroll Schemes	Contractors obtaining payment through submission of false claims for compensation, such as misrepresenting employee labor in order to charge for more work hours and increase profit.
Procure to Pay (P2P)	The cycle comprises the purchasing and payment processes including Acquisition Management; Inventory Management; Payables Management; and Travel Administration. Specific areas involved in this cycle are approving requisitions, issuing RFP's, maintaining, and selecting vendors, awarding contracts, maintaining obligations, receiving and managing goods or services, approving and paying invoices, tracking funds, monitoring continuing resolutions, and managing travel and purchase cards.

Product Quality	Contractors purposefully conducting work in a way that results in the delivery of goods of a lesser quality than required by the contract.
Projects to Assets (P2A)	The cycle comprises processes related to the oversight of projects resulting in an asset and the management of project costs and property. Processes included in this cycle are Project Cost Management, and Property Management. Specific areas that fall within this process cycle are managing large projects including capturing all costs and managing to budget; capturing costs for reimbursable expenses; creating and monitoring assets; monitoring depreciation; and controlling property.
Quote to Cash (Q2C)	The cycle comprises processes related to working capital management and capturing revenue as a receivable to be managed and collected. The cycle consists of Revenue Management and Receivable Management processes. Specific areas that fall within this process cycle include invoicing for reimbursable expenses, along with other expected revenues through to managing accounts receivable and receiving cash.
Reasonable Assurance	Judgment by management based upon available information that the systems of internal controls are operating as intended under FMFIA.
Remediation Activity	An action put in place that would address the correction of a control deficiency identified through an internal controls assessment.
Re-performance	An objective execution of procedures or controls performed as part of a test of the effectiveness of the entity's internal control.
Residual Risk	The amount of risk that remains after action has been taken to manage it
Risk Assessment	A systematic process of evaluating the potential risks that may impact the ability of an organization to achieve objectives or goals.
Risk Factor	Identification of changes that may affect the exposure risk or effectiveness of existing controls in mitigating the risk. Risk factors include system, process, organization, or other changes (e.g., Inspector General (IG) or GAO audits).
Risk Profile	A prioritized inventory of the most significant risks identified that the Agency faces toward achieving its strategic objectives arising from its activities and operations and identifies appropriate options for addressing significant risks.
Risk Register	An inventory of potential risks the Agency may face when striving to achieve its strategic objectives.
Risk Response	A determination by management on how a risk should be managed, considering the potential impact of the risk and the likelihood of occurrence, as well as the cost associated with mitigating the risk. **Types of risk responses**: *Acceptance* Take no action to respond to the risk based on insignificance of risk, requirement to complete the work, or benefits and opportunities exceed the risk

Avoidance – Action is taken to stop the operational process, or the part of the operational process causing the risk.

Reduce – Action is taken to reduce the likelihood or impact of the risk.

Share – Action is taken to share the risks with another entity within the organization or with one or more external parties.

Transfer – Action to transfer the responsibility for ownership and handling the risk to an organization other than the current entity that owns the risk.

Risk Tolerance The level of variation in performance that management is willing to accept, relative to achieving objectives. Management should establish its risk tolerance level before the placement of controls.

Sabotage The intentional and deliberate destruction of property or the obstruction of an activity.

Sampling Used to select the appropriate number of transactions to test for each control. Sampling methods for consideration are:

- **Random**- A method of selecting a sample whereby each item in the population of transactions is given an equal chance of selection regardless of the population size.
- **Judgmental**- A method of sample selection whereby the sampled items are selected based on a deliberate choice based on the profile of the population of transactions. This method provides validation that high-risk or other items of interest are included in the selected sample and reviewed as part of testing the control.
- **Systematic**- A method of sample selection whereby a uniform interval is selected throughout the population. The appropriate interval is determined by dividing the number of items in the population by the sample size.

Scope Limitation Exists when the entity has identified potentially significant deficiencies in the scope of the internal control evaluations conducted, which would warrant disclosure to assure limitations are understood. Scope limitations may be determined by the entity or may be required by the Office of the Chief Financial Officer (OCFO) in certain circumstances.

Significant Deficiency A deficiency or a combination of deficiencies in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

Special Purpose (SPC) The cycle comprises processes which are unique and cannot be categorized under other process cycles. These processes require significant attention due to the impact on the financial statements and scope of responsibility. The cycle consists of the Environmental Management (EM) Liability process.

Standard Process A business process that is pre-populated in the FMA Module.

Standard Sub-process	A sub-component of a standard process, also pre-populated in the FMA Module.
Statement of Assurance	Annual statement required by FMFIA and included in the DOE Agency Financial Report (AFR) that represents the Secretary's informed judgment as to the overall adequacy and effectiveness of DOE internal controls. The AFR reports the results of evaluations made on DOE entity, financial, and financial management systems controls, including identified material weaknesses or material non-conformances and corrective action progress made on existing material weaknesses and material non-conformances.
Testing Activity	Procedure to determine if internal control systems work in accordance with internal control objectives.
Theft	Contractors stealing or misappropriating government resources, such as cash or other assets.
Vandalism	The mindless and malicious harm and injury to another's property.

Appendix H – Management Priorities

A. Background

Appendix H provides guidance on the preparation and updates of the Department of Energy's (DOE) Management Priorities included in DOE's annual Agency Financial Report (AFR). This appendix is **applicable to Management Priority Owners and Management Priority lead offices only**.

Management Priorities represent the most important strategic management issues facing the Department and are reviewed and identified by DOE's Senior Risk Management Council (SRMC), the Departmental Internal Control and Assessment Review Council (DICARC). The DICARC considers the results and any significant deficiencies and/ or material weaknesses reported in the Departmental Elements' Assurance Memoranda. The DICARC also consults and considers the DOE Inspector General's (IG) Management Challenges and the Government Accountability Office's (GAO) biennial High Risk Series update when assembling DOE's Management Priorities.

B. Management Priorities

Each DOE Management Priority is assigned a Senior Executive owner and lead responsible office to track the action progress and prepare annual enterprise updates for inclusion in the AFR. In FY 2022, the owner or lead responsible office for each Management Priority will provide updates to the Office of the Chief Financial Officer (OCFO) during the third and fourth quarters of the fiscal year. The lead responsible office of the Management Priority will update the narrative with an enterprise perspective and approve each priority update prior to delivering to the OCFO. See ***Table 1*** for the list of Management Priorities reported along with the assigned lead responsible offices.

Table 1 DOE's Management Priorities and Lead Responsible Offices

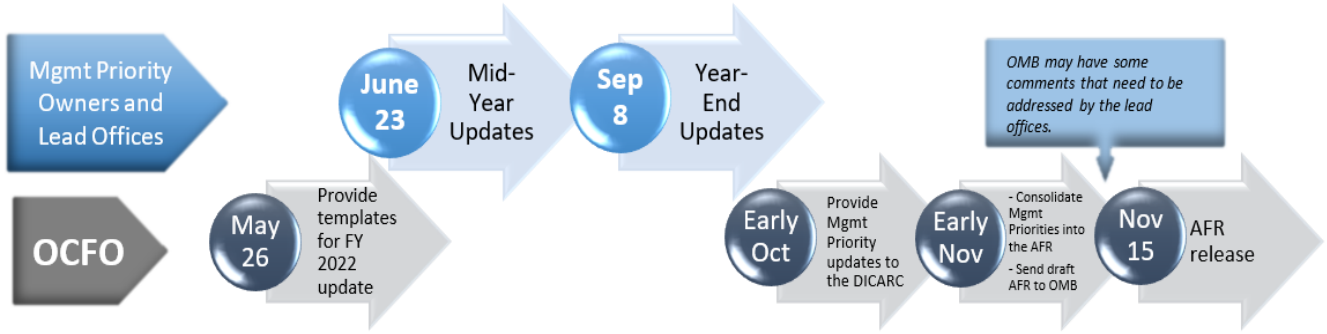
Management Priorities	Lead Responsible Offices
Cybersecurity	CIO
Human Capital Management & Diversity and Inclusion	HC & ED
Contractor & Major Project Management	MA
Infrastructure	MA
Nuclear Waste Disposal	NE & GC
Safety & Security	AU (including Program Office input)
Nuclear Stockpile Stewardship	NNSA
Environmental Cleanup	EM
Climate Change	EERE & MA
Energy Justice	ED

C. Management Priorities Update Process

In the third quarter of FY 2022, the OCFO will provide the lead responsible offices and owners with Management Priorities published in the FY 2021 AFR. The lead responsible offices and owners will update the narrative (using tracked changes) based on significant activities and results performed in FY 2022. In the fourth quarter, OCFO will provide each lead responsible offices and owners with relevant significant deficiencies and/ or material weaknesses reported by Departmental Elements along with the top risks throughout DOE for potential consideration and incorporation into Management Priorities updates. Lead responsible offices and owners will consider the enterprise reported results and provide a fourth quarter

Management Priorities update (using tracked changes) to the OCFO. ***Figure 1*** shows an illustration of the process with timelines for both the OCFO and the Management Priority owners and lead offices.

Figure 1 Management Priority Process with Timeline



The OCFO will provide the Management Priorities updates to the DICARC for consideration along with the OIG Management Challenges and the GAO High Risk List. The DICARC will meet in October 2022 and determine whether to revise, edit, or maintain DOE's Management Priorities. The Management Priorities updates determined by the DICARC will be reported in the FY 2022 DOE AFR and will serve as the starting point for the FY 2023 update process.

D. Guideline on writing the Management Priority narrative

The Management Priority narrative is composed of the *Title Header*, *Key Challenges*, and *Departmental Initiatives*. Refer to ***Table 2*** for the description of each section.

Table 2 Management Priorities Narrative Structure

Structure	Instructions
Management Priority Title Header	Provide succinct and descriptive management priority title. If prior Management Priority has changed, update if needed, or enter create new title for new management priority.
Key Challenges	**Introduction:** Provide a narrative description of the management priority in terms of the key challenges DOE faces (what risks or vulnerabilities do the challenges present to DOE?). Summarize the specific elements and contributors of the challenges associated with the management priority. **Body:** Use bullets and sub-bullets to provide additional detail for each area under the key challenges.
Departmental Initiatives	**Introduction:** Provide a summarized description of the Department's efforts taken and on-going initiatives to improve and/ or address the key challenges identified with the management priority. **Body:** Use bullets and sub-bullets to provide additional detail on specific elements or factors associated with challenges or initiatives.

The next succeeding tables provide consideration for word usage and formatting.

Table 3 Considerations for Word Usage

Item #	Topic	Word Usage Considerations
1	Active Voice	Use ***ACTIVE*** voice. **Correct:** "DOE implemented controls to restrict access to the accounting system by unauthorized personnel." **Incorrect:** "DOE has implemented controls that will restrict access to the accounting system by unauthorized personnel."
2	Bulleted Lists	Begin with an action verb when possible. (Particularly for describing the initiatives taken) Strive for a consistent tone in the opening sentence of each bullet under a particular key challenge/initiative: ▪ "Improved X by…" ▪ "Completed X to…" ▪ "Developed X to…" ***OR*** ▪ "Improving X by…" ▪ "Completing X to…" ▪ "Developing X to…"
3	Buzz Words	***Avoid*** buzz words, such as: ▪ Allow ▪ Cultivate ▪ Driver ▪ Engage ▪ Ensure ▪ Stakeholders ▪ Utilize
4	Other Words	Other words to ***avoid*** include: ▪ Additional, additionally, in addition ▪ Amplify ▪ Any ▪ As follows, following (when referencing a location within document) ▪ Customer ▪ Enable ▪ Etc. ▪ Everything ▪ Few ▪ Furthermore ▪ Great ▪ However ▪ Invaluable ▪ Many ▪ Rigorous ▪ Required (Use "needed," where applicable) ▪ Robust ▪ Should (when unnecessary, delete) ▪ Show, showed ▪ Some ▪ Soon ▪ That (when unnecessary, delete) ▪ Therefore ▪ Their ▪ Whether
5	Acronyms	▪ Consider using if term is referenced multiple times throughout section (three or more times). ▪ Consider writing out if only used a couple of times.
6	Pronouns	***Avoid*** using pronouns, such as: I, you, she, it, this

Table 4 Considerations for Formatting

Item #	Topic	Formatting Considerations
1	Spacing	Single space after periods
2	Bullets	Spacing for bulleted lists: • First level indent is 0.00" ○ Second level indent is 0.25"
3	Bullets	Do not begin a bullet with "the"
4	Publications	Italicize publications
5	Quotations	Only use quotation marks around direct quotes
6	Numbering	Spell out numbers less than 10 (one, two, three, …nine, 10, 11, 12…)

E. Management Priorities Due Dates

Table 5 provides a summary of the Management Priorities key dates and deliverables for FY 2022. Management Priority owners and lead responsible offices should contact the Internal Controls Fraud Risk & Management Division (email: CFO-ICFRMD@hq.doe.gov) if there are any issues in meeting the below deadlines.

Table 5 Key Dates and Deliverables for FY 2022

FY 2022 Key Dates	Deliverables
June 23	Lead responsible offices provide OCFO **mid-year updates** to the Management Priorities using provided templates based on FY 2022 enterprise activities performed and planned.
September 8	Lead responsible offices provide OCFO **year-end updates** to the Management Priorities.
Early to Mid-November	Be prepared to provide responses for potential OMB comments.