Department of Energy
Washington, DC 20585

January 28, 2020

MEMORANDUM FOR DISTRIBUTION

FROM: R. M. HENDRICKSON
DEPUTY CHIEF FINANCIAL OFFICER

SUBJECT: Federal Managers' Financial Integrity Act of 1982 and DOE FY 2020 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 2020 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*.

This guidance is in alignment with the President's Management Agenda Cross-Agency Priority Goal #6, *Shifting from Low-Value to High-Value Work* and DOE's Internal Control Program is executing several initiatives to reduce burden on reporting organizations while maintaining effective internal controls for the Department. The initiatives are:

- Implementing a pilot program with four labs to evaluate alternative control test cycle approaches, analytical and business process approaches;
- Eliminating controls testing on environmental liabilities focus areas risks in the Financial Management Assessment Module for 29 organizations with low combined risk ratings;
- Reducing the number of entity objective evaluations in the Entity Assessment Module from ten to nine; and,
- Eliminating the deliverable for Field/Operations Offices Risk Profile to the OCFO since the risk profiles are provided to the respective program office at Headquarters.

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 14, 2020,** Headquarters Offices on **September 15, 2020,** and each Under Secretary on **September 30, 2020**. 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 attached 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:
S1 Chief of Staff
S2 Chief of Staff
Under Secretary of Energy
Under Secretary for Science
Under Secretary for Nuclear Security, Administrator NNSA
Assistant Secretary for Congressional and Intergovernmental Affairs
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 for Electricity
Assistant Secretary for International Affairs
Assistant Secretary for Cybersecurity, Energy Security & Emergency Response
Associate Under Secretary for Environment, Health, Safety, and Security
Chief Human Capital Officer
Chief Information Officer
Chief Risk Officer
Inspector General
General Counsel
Executive Director, Loan Programs Office
Director, Office of Advanced Research Projects Agency – Energy
Director, Office of Artificial Intelligence and Technology
Director, Office of Economic Impact and Diversity
Director, Office of Enterprise Assessments
Director, Office of Hearings and Appeals
Director, Office of Indian Energy Policy & Programs
Director, Office of Intelligence and Counterintelligence
Director, Office of Legacy Management
Director, Office of Management
Director, Office of Policy
Director, Office of Project Management Oversight and Assessments
Director, Office of Public Affairs
Director, Office of Science
Director, Office of Small and Disadvantaged Business Utilization
Director, Office of Technology Transitions
Director, National Laboratory Operations Board
Administrator, Energy Information Administration
Administrator, Bonneville Power Administration
Administrator, Southeastern Power Administration
Administrator, Southwestern Power Administration
Administrator, Western Area Power Administration
Chairman, Federal Energy Regulatory Commission
Manager, Carlsbad Field Office
Manager, Idaho Operations Office
Manager, Richland Operations Office
Manager, Savannah River Operations Office
Manager, Science Consolidated Science Center
Manager, Naval Reactors Laboratory Field Office
Director, EM Consolidated Business Center
Director, Golden Field Office
Director, National Energy Technology Laboratory
Project Manager, Strategic Petroleum Reserve Project Management

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

Internal Control Evaluations

Fiscal Year 2020 Guidance

Summary of Key Dates and Deliverables

FY 2020 Key Dates	Deliverables
March 13	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and Power Marketing Administrations (PMA) upload Risk Profile excel template and signed PDF version, with consideration of reporting from Field Offices, Site Offices, and M&O Contractors as applicable, to the Internal Controls iPortal Space and to the respective Under Secretaries, if applicable.
April 3	Under Secretaries provide Risk Profile excel template and signed PDF version to the Internal Controls iPortal Space based on the input of the reporting offices.
April 17	Departmental Elements provide Interim Internal Control Status using the AMERICA Application.
May 8	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review in mid-May.
June 15	OCFO provides the lead responsible offices Management Priorities from the DOE FY 2019 AFR in required update templates.
June 29	Lead responsible offices provide OCFO with mid-year updates on Management Priorities using provided templates based on FY 2020 significant enterprise activities performed and planned. **Note:** Applicable to Management Priority Owners Only.
July 17	M&O Contractors and Field Offices provide FMA Module and EA Module using the AMERICA Application. Reporting organizations should follow subsequent timelines that are published by the cognizant organization to assure FMA and EA Modules are provided to DOE on time.
July 31	Field Offices provide draft Assurance Memoranda using iPortal, considering and incorporating Site Offices and M&O Contractors.
August 7	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and PMAs provide FMA Module and EA Module using the AMERICA Application.
August 14	Field Offices upload the signed Assurance Memoranda to the Internal Controls iPortal Space.
August 17	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and PMAs provide draft Assurance Memoranda using iPortal and eDOCs.
September 15	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and PMAs upload the signed Assurance Memoranda to the Internal Controls iPortal Space and eDOCs.
September 22	Lead responsible offices update Management Priorities with year-end updates and relevant Field and Headquarter Offices reported deficiencies/weaknesses using provided templates. **Note:** Applicable to Management Priority Owners Only.
September 30	Under Secretaries upload the signed Assurance Memoranda to the Internal Controls iPortal Space and eDOCs.
October 1	Organizations that resolve or identify a significant deficiency or material weakness, after June 30, 2020, but no later than September 30, 2020 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:** Following DICARC recommendation, the final Management Priorities are incorporated into the AFR and proceed through Exec Sec Concurrence Process.

Table of Contents

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.

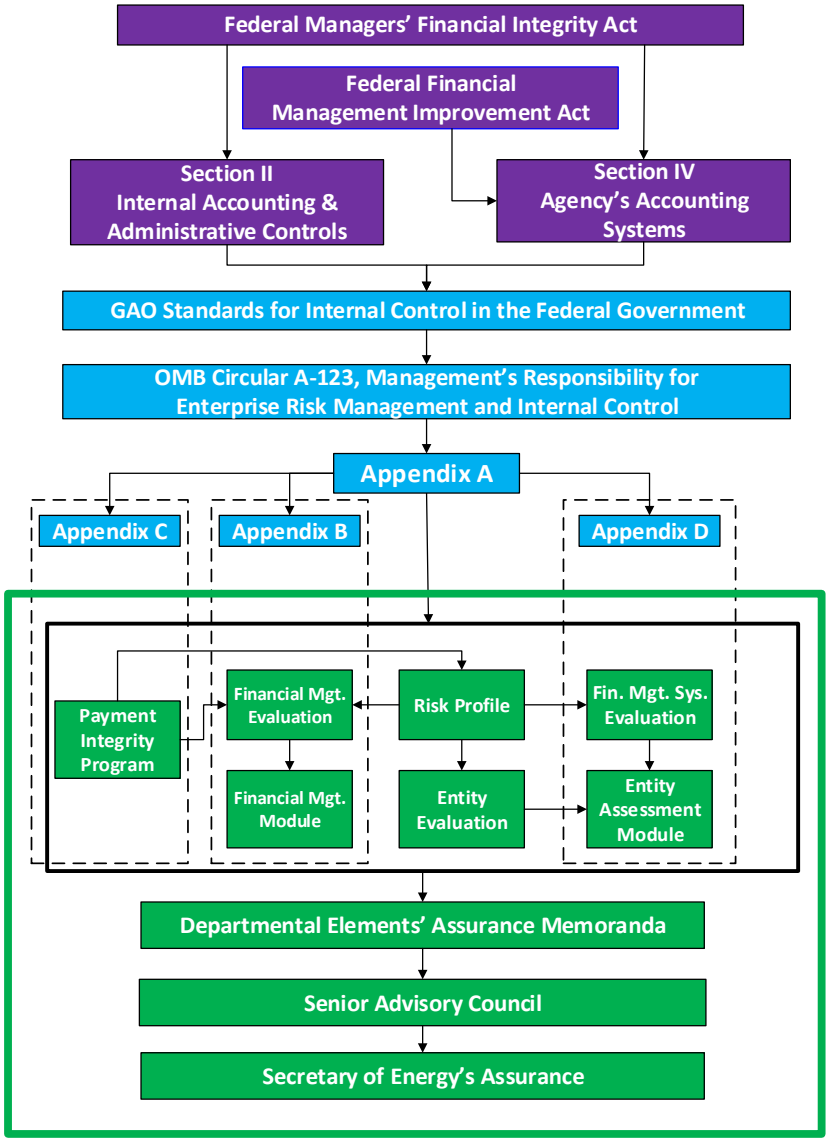
FMFIA requires each agency to:

- 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) meets 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 2020, 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 report 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 steamline 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 in order to provide reasonable assurance over internal controls over financial reporting (ICOFR). 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.

To implement OMB's updates to the revised Appendix A, the Department is adopting a phased approach towards implementation. As part of the President's Management Agenda Cross Agency Priority Goal 6, *Shifting from Low-Value to High-Value Work*, the OCFO will conduct a data call with Departmental elements in FY 2020 to assist in identifying significant external and internal reports produced by the Department. The objective of the data call is to assist in transitioning to the revised Appendix A, identify and determine the DOE external and internal reports that will receive internal controls testing, and support the reporting of quality data. Appendix A transition plan, information on the reporting data call, and the categories of reports needed for identification will be provided to organizations later in FY 2020.

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. In FY 2020, reporting organizations will provide 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 OCFO will receive separate and detailed guidance for DOE's

Improper Payment Program by the start of Q4 FY 2020. For further details on improper payments, Internal Controls Points-of-Contact (POC) may reference DOE's FY 2019 Improper Payment Program guidance and should coordinate with the organization's Improper Payment POC.

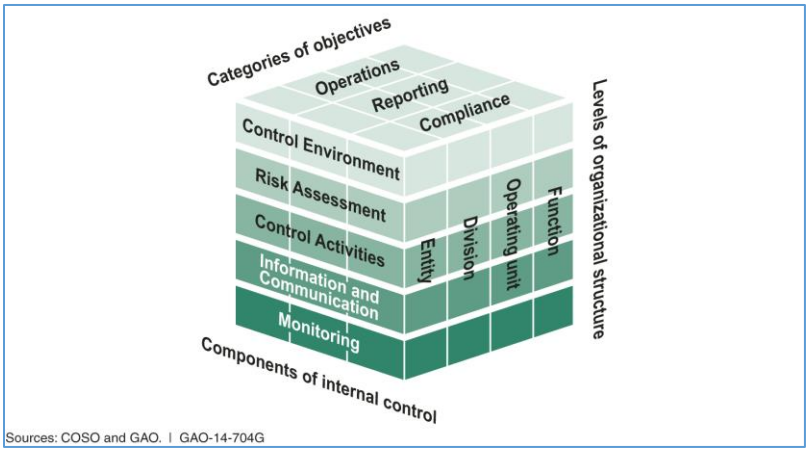
C. GAO Standards for Internal Control

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



The columns labeled on the top of the cube represents the three categories of an entity's objectives. The rows represents the five components of internal control. The levels of organizational structure represents the third dimension of the cube. Each component of internal control applies to the three categories of objectives and the organizational structure.

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 *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 2020, DOE consolidated fraud risk management requirements into a single appendix (Appendix E) in the Internal Controls Evaluation Guidance to provide further information on fraud related requirements and the GAO's Fraud Risk Framework. Appendix E also presents information on fraud communication requirements, fraud trends across DOE, and fraud specific requirements for the Financial Management Assessment (FMA) Module, Entity Assessment (EA) Module, and Risk Profile.

NEW in FY 2020

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

DOE is working to incorporate OMB Memorandum M-18-23, *Shifting From Low-Value to High-Value Work* that states agencies should identify opportunities to streamline operations and incorporate flexibility for the components, complementing the broader Government-wide efforts of the Cross-Agency Priority Goal to shift resources to high-value work. Consistent with this goal, the Department initiated the Internal Controls Evaluation Approach Working Group in FY 2019 to evaluate alternative control test cycle approaches. Four labs volunteered to serve as pilot organizations to conduct alternative control test cycle approaches – including both analytical and business process approaches – as part of the DOE FMA. The pilot labs will provide updates to the working group, which will provide recommendations to the DOE Internal Controls Program to focus resources on higher rated risks, while also maintaining effective internal controls on lower rated risks.

To streamline efforts, in FY 2020 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 organizations that have a combined risk rating of moderate or high for specific risks. POC's should refer to Table 5 in Section B, Focus Area Guidance for a complete listing of reporting organizations exempt from the environmental liabilities focus areas in FY 2020.

In FY 2020, the control risk rating matrix is revised in the FMA Module to focus attention on the highest rated risks and reduce efforts on lower rated risks. Under the revised control risk rating matrix, risks with lower risk occurrence and control set execution scores may receive lower control risk ratings than under the previous matrix, resulting in less frequent testing for lower rated risks in the FMA Module. For more information on the revised FY 2020 control risk rating and combined risk rating matrices, refer to Section IV: Financial Management Assessment (FMA) Evaluation.

Consistent with Government-wide efforts to shift to high-value work, the OCFO reviewed the ten entity objective categories for evaluation in the EA Module. The review determined that the Segregation of Duties entity objective overlapped with the EA Internal Controls Evaluation of Green Book Principle #10 and the FMA Evaluation of select business sub-processes. In FY 2020, the Segregation of Duties entity objective is removed and reporting organizations will evaluate nine entity objective categories. Issues identified with the Segregation of Duties entity objective in FY 2019 and associated CAPs have been moved to Principle #10 in the EA Module Internal Control Evaluation tab for FY 2020. For more information on the revised FY 2020 entity objectives, refer to Section V: Entity Assessment Evaluation.

F. Key Internal Control and Risk Profile Requirements

This guidance provides the FY 2020 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 in the EA Module);
- Interim Internal Controls Status (IICS) Memoranda (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;[2]
- Small Departmental Elements are not required to perform FMA evaluations, these Elements though 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 EA and IICS deliverables to the OCFO, but should check with the cognizant Field and Headquarters Offices to determine if a deliverable is required to either cognizant organization; and,
- Major/Integrated Contractors and Field Offices are required to provide a Risk Profile to the cognizant Field Office but are not required to provide the Risk Profile to the OCFO.

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 of Energy				✓		✓
	Office of the Under Secretary for Science				✓		✓
	Office of the Under Secretary for Nuclear Security and National Nuclear Security Administration				✓		✓
Headquarters Offices	Advanced Research Projects Agency Energy	✓	✓	✓	✓	✓	✓
	Artificial Intelligence & Technology	✓	✓	✓	✓	✓	✓
	Chief Financial Officer	✓	✓	✓	✓	✓	✓
	Chief Information Officer	✓	✓	✓	✓	✓	✓
	Cybersecurity, Energy Security & Emergency Response	✓	✓	✓	✓	✓	✓
	Electricity Delivery and Energy Reliability	✓	✓	✓	✓	✓	✓
	Energy Efficiency and Renewable Energy	✓	✓	✓	✓	✓	✓
	Environment, Health,Safety and Security	✓	✓	✓	✓	✓	✓
	Environmental Management	✓	✓	✓	✓	✓	✓
	Federal Energy Regulatory Commission						✓
	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	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		✓		✓	✓	✓

[2] Major/Integrated Contractors are DOE contractors with responsibility for the management and/or operation of a Department-owned or leased facility.
[3] Kansas City, Livermore, Los Alamos, Nevada, NNSA Production, Sandia, Ames, Argonne, Brookhaven, Fermi, Bay Area, Princeton, Oak Ridge National Lab, Pacific Northwest, Thomas Jefferson.
[4] Internal Control deliverables to OCFO are identified for each organization. Major/Integrated Contractors and Site Offices should check with the cognizant organization for specific reporting requirements that are not identified in Table 1.

Departmental Elements & Reporting Organizations		FMA Evaluation	Entity Evaluation	FMS	Risk Profile	Interim Internal Control Status	Assurance Memorandum
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 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	✓	✓	✓		✓	✓
Site Offices							
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 Laboratories	✓	✓	✓			
	Naval Nuclear Laboratories	✓	✓	✓			
	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	✓	✓	✓			

G. Important Dates and Transmittal Methods

Table 2 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 for the delay to include any potential significant deficiency or material weakness to the OCFO Internal Controls POC for the organization. Management quality assurance reviews will take place at every level prior to providing Internal Control deliverables and Risk Profiles.

Table 2: DOE Internal Controls and Risk Profile Important Dates

FY 2020 Key Dates	Deliverables
March 13	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and Power Marketing Administrations (PMA) upload Risk Profile excel template and signed PDF version, with consideration of reporting from Field Offices, Site Offices, and M&O Contractors as applicable, to the Internal Controls iPortal Space and to the respective Under Secretaries, if applicable.
April 3	Under Secretaries provide Risk Profile excel template and signed PDF version to the Internal Controls iPortal Space based on the input of the reporting offices.
April 17	Departmental Elements provide Interim Internal Control Status using the AMERICA Application.
May 8	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review in mid-May.
June 15	OCFO provides the lead responsible offices Management Priorities from the FY 2019 AFR in required update templates. **Note:** Applicable to Management Priority Owners.

FY 2020 Key Dates	Deliverables
June 29	Lead responsible offices provide OCFO with mid-year updates on Management Priorities using provided templates based on FY 2020 significant enterprise activities performed and planned. **Note:** Applicable to Management Priority Owners Only.
July 17	M&O Contractors and Field Offices provide FMA Module and EA Module using the AMERICA Application. Reporting organizations should follow subsequent timelines that are published by the cognizant organization to assure FMA and EA Modules are provided to DOE on time.
July 31	Field Offices provide draft Assurance Memoranda using iPortal, considering and incorporating Site Offices and M&O Contractors.
August 7	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and PMAs provide FMA Module and EA Module using the AMERICA Application.
August 14	Field Offices upload signed Assurance Memoranda to the Internal Controls iPortal Space.
August 17	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and PMAs provide draft Assurance Memoranda using iPortal and eDOCs.
September 15	Under Secretaries Headquarters Offices, Functional Headquarters Offices, and PMAs upload the signed Assurance Memoranda to the Internal Controls iPortal Space and eDOCs.
September 22	Lead responsible offices update Management Priorities with year-end updates and relevant Field and Headquarter Offices reported deficiencies/weaknesses using provided templates. **Note:** Applicable to Management Priority Owners Only.
September 30	Under Secretaries upload the signed Assurance Memoranda to the Internal Controls iPortal Space and eDOCs.
October 1	Organizations that resolve or identify a significant deficiency or material weakness, after June 30, 2020, but no later than September 30, 2020 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; Following DICARC recommendation, the final Management Priorities are incorporated into the AFR and proceed through Exec Sec Concurrence Process.

Entities (Federal and contracting organizations) should provide the Internal Control Deliverables that are listed in Table 2*: DOE Internal Controls and Risk Profile Important 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	Electronic Delivery & Upload to iPortal	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 Interim Internal Control Status	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	Upload to iPortal	Field Office Assurance Memorandum addressed To: Lead Program Secretarial Office with copies to the Cognizant Secretarial Office(s).
	Signed PDF	Upload to iPortal and eDOCS	Headquarters and PMAs 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 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;
- Internal audits and/or management reviews;
- Process flows and descriptions;
- Test documentation more detailed than what is included in the FMA and EA Modules; and,
- Evidence collected during testing.

Organizations must have vigorous and strong 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 a sufficient amount of detail that will provide an understanding of the test and results.

New in FY 2020: Reporting entities are required to upload documentation to AMERICA which supports the FMA Evaluation for select business sub-processes. Such documentation may include business

process narratives or flowcharts, risk analyses, test plans, and other applicable documents that support the organization's assessment and evaluation. Entities are not expected to provide 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. For further information on the business sub-processes which require supporting documentation to be uploaded, refer to Section IV: Financial Management Assessment (FMA) Evaluation.

III. Risk Profile

OMB Circular A-123 requires each agency to prepare an annual prioritized and ranked Risk Profile, which is used as part of the annual Strategic Review with OMB in May and provided to OMB in early June 2020. The Risk Profile must identify the most significant risks to achieving agency strategic objectives and the appropriate options for addressing the significant 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 must identify the most significant risks and provide a Risk Profile in accordance with the guidance in Appendix A, *Risk Profile Template*, to the cognizant Field Office. Field Offices, taking into consideration the Major/Integrated Contractors must identify the most significant risks and provide a Risk Profile to the responsible Headquarters Office in accordance with the due dates in Table 2.

Each Headquarters Office, PMA, and Under Secretary must prepare a Risk Profile identifying no more than the top ten significant risks. 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 discussed as part of the annual Strategic Review in mid-May and for input to OMB by June 3, 2020.

Risk Profiles are updated and prepared on an annual basis. Appendix A, *Risk Profile Template*, provides the Risk Profile template and detailed instructions for developing the Risk Profile. In our continuous efforts to improve risk profiles, in FY 2020 the Risk Profile template is similar to the prior year template with the exception of five new columns. These columns have been added for FY 2020 to identify risks that have a financial or nonfinancial fraud impact (Column E), links risks to strategic objectives (column G), identify the organizations accepting shared or transferred risks (Column L), provide further detail on where risks are being evaluated in AMERICA (Column N), and performs validations (Column U).

In FY 2020, 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.**

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 2020 internal control testing and attested in the FY 2020 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). 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 new Current Evaluation Details column (Column N).

Fraud Considerations in the Risk Profile

In FY 2020, reporting organizations must continue to identify the top financial and non-financial fraud risks in the Risk Profile. These on-going fraud risk statements must be included in each entity's Risk Profile deliverable along with other identified significant risks. Organizations must identify risks with a financial or nonfinancial fraud impact by completing the new *Fraud Sub-Category* column in the FY 2020 Risk Profile. Organizations will then select *financial* or *nonfinancial* from a drop-down menu identifying whether a risk has a financial or nonfinancial **fraud impact**. If a risk does not have a financial or nonfinancial fraud impact, 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, and corporate risks to the entity.

New in FY 2020: Reporting entities are required to upload documentation to AMERICA which supports the FMA Evaluation for select business sub-processes. 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.

This year reporting organizations which complete the FMA Module will upload supporting documentation for the Receipt of Goods and Services (2.10.30) sub-process into AMERICA. Reporting organizations will provide documentation for the corporate risk (CR2116) that includes Receipt of Goods and Services as well as local risks added to this sub-process. Entities that tested CR2116 in FY 2019 and meet the focus area exemption for FY 2020 will provide the evaluation documentation used in FY 2019. Organizations that have assessed the focus area risk as **Not Relevant** do not need to provide further documentation.

While supporting documentation should be referenced for identified sub-processes and corporate risks, only such documentation that supports the assessment and evaluation of the Receipt of Goods and Services sub-process should be uploaded to AMERICA for OCFO review in FY 2020. Supporting documentation should be uploaded to the FMA Module using the **Attachments** tab in AMERICA. Documentation for the Receipt of Goods and Services sub-process is required due to its continued importance across the Department as a Focus Area, its widespread applicability to organizations that contract for good or services, and numerous control set deficiencies identified and reported in FY 2019.

B. Revised Control Risk Matrix

The control risk rating matrix has been revised in the FMA Module to focus attention on the highest rated risks and reduce the frequency of testing on lower rated ones. As seen in Figure 3, under the revised control risk rating matrix, risks with lower risk occurrence and control set execution scores will likely receive a lower control risk rating than under the previous matrix. For example, a risk occurrence score of 2 and a control set execution score of 1 will now result in a low overall control risk rating. The revised control risk ratings may lower the combined risk ratings and result in less frequent testing for lower rated risks in the FMA Module.

NEW in FY 2020

Figure 3: DOE Revised Control Risk Matrix

New FY 2020 Control Risk Matrix:

Risk Occurrence			
3	M	H	H
2	L	M	H
1	L	L	M
	1	2	3
	Control Set Execution		

Previous Control Risk Matrix:

Risk Occurrence			
3	H	H	H
2	M	M	H
1	L	M	M
	1	2	3
	Control Set Execution		

C. Requirements for FY 2020

In FY 2020, 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, beginning **April 1, 2020** entities must mark the appropriate area in the **Assessment** tab, 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 and continue testing the controls into the fourth quarter even though the FMA Module has been provided to OCFO. **Points-of-Contacts should coordinate with the respective OCFO analysts to update the FMA Module with fourth quarter testing information after the results have been provided to OCFO**. 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. Entities should pay careful attention to the

NEW in FY 2020

revised Acquisition-related corporate risk statements in the FMA Module when performing risk assessments. In FY 2020, the Acquisition-related risks identified in the prior year for deletion as a corporate risk no longer reside in the FMA Module. If the risks were applicable to an organization and the entity did not convert the corporate risk into a local risk in FY 2019, then the organization will need to add the risk by creating a new local risk in FY 2020.

2. *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.
3. *Evaluate risks and test controls in cycle for the processes/sub-processes identified in Table 4* - The processes/sub-processes listed in Table 4 will continue to be included in the 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 rationale in the **Assessment** tab. 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 4: 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	✓	✓	✓

4. *Fraud and Improper Payments Consideration* - Effective fraud risk management monitors that taxpayer dollars and government services serve the intended purposes. In FY 2020, entities are 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. In FY 2020, the fraud and improper payments options have been removed and a drop-down box has been added where fraud and/or improper payment designations should be made. This will require reporting organizations to review fraud and improper payments controls and select the appropriate control type designation from the drop-down box. Entities **must** also identify in the FMA Module **local risks** that are subject to

fraud, improper payment, or both. If a control is designed to mitigate a fraud and/or improper payment risk and the control fails testing, or fails related to actual potential fraud, the organization will notify the OCFO 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.

5. *Complete Current Year Test Requirements* – Using the ***Assessment Tab*** (*Control View available in FY 2021)* in 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 no later than June 30. Entities should remain cognizant that *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 and may continue testing the controls into the fourth quarter although the FMA Module has been provided to OCFO.
6. *Complete Focus Area Testing and Actions* – Organizations must complete testing and other required actions to address the FY 2020 focus area risks and document the actions taken in the **Assessment** tab of the FMA Module. In FY 2020, the environmental liabilities focus areas will not be required for select organizations that have a combined risk rating as low or not relevant. With the notable exception of the environmental liabilities focus area exemption, the DOE and NNSA focus areas **will remain the same** for FY 2020. 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 6: FY 2020 Focus Areas. Section D, Focus Area Guidance, provides more details on focus areas and assessment requirements.

7. *Develop Corrective Action Plans As Applicable* - A Corrective Action Plan (CAP) is required for each risk with a control set execution score of 3. Organizations also have the option of developing formal corrective action plans (CAP) 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, 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 Impact 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.

8. *Upload Relevant and Appropriate Supporting Documentation* – Beginning in FY 2020, organizations are responsible for **uploading requested documentation** in AMERICA for the Receipt of Goods and Services sub-process (2.10.30). 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, Supporting Documentation.

D. Focus Area Guidance

In FY 2020, assessment of the environmental liabilities focus areas is not required for select entities. **Reporting organizations that had a low or not relevant combined risk rating for environmental liabilities focus area risks are fully exempt from testing the environmental liabilities focus areas in FY 2020.** 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 2020 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 areas are identified in Table 5. Organizations not listed in Table 5 did not identify at least one of the environmental liabilities focus areas as relevant in FY 2019, and thus are not responsible for addressing these risks as focus areas in FY 2020 **assuming the exposure risk rating is not relevant**. Reporting organizations piloting an alternative control test cycle approach as part of the Internal Controls Evaluation Approach Working Group are exempt from each FY 2020 Focus Area and are identified as **Pilot Programs** in Table 5.

Table 5: 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
Savannah River Site (SRS)	Savannah River Operations Office (SR)
Chicago Field Office (CH)	Richland-Office of River Protection (RL)
Pacific Northwest National Lab (PNNL)	Argonne National Lab (ANL)
Office of Legacy Management (LM)	EM Consolidated Business Center (EMCBC)
National Energy Technology Lab (NETL)	Brookhaven National Lab (BNL)
Idaho Operations Office (ID)	Oak Ridge Office (OR)
East Tennessee Technology Park (ETTP)	Oak Ridge National Laboratory (ORNL)
Fermi National Accelerator Lab (FNAL)	Pantex Plant & Y-12 National Security Complex (PX/Y12)
Thomas Jefferson National Accelerator Facility (TJNAF)	Kansas City National Security Campus (KC)
Western Area Power Administration (WAPA)	Nevada National Security Site (NNSS)
Princeton Plasma Physics Lab (PPPL)	Office of the Chief Financial Officer (CFO)
NNSA Complex (NNSA ALB)	Bonneville Power Administration (BPA)
Naval Reactors Laboratory Field Office (NRLFO)	

SLAC National Accelerator Laboratory (SLAC) ***Pilot Program***	
Lawrence Livermore National Lab (LLNL) ***Pilot Program***	
Lawrence Berkley National Lab (LBNL) ***Pilot Program***	
Sandia National Lab (SNL) ***Pilot Program***	

The environmental liabilities focus areas that are exempted from testing in FY 2020 will be appropriately flagged and addressed in AMERICA by OCFO and no further action will be required by the corresponding entities.

Table 6: FY 2020 Focus Areas

FY 2020 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)
Contract Solicitation, Award, and Adjustment • Project Monitoring-Cost/timeline issues (CR4106) • Project Monitoring-Improper transfer of assets (CR4110)
Property Management • Property Recognition and Recording-Inconsistent property values (CR4201) • Property Recognition and Recording-Improper recording of assets (CR4202)
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)

FY 2020 Focus Areas
Improper Payments • SPC: Payment Disbursing-Incorrect implementation of OMB requirements (CR6601)

The DOE and NNSA focus areas will remain the same for FY 2020 with the exception of changes to the acquisition-related focus area risks. The Department annually identifies Focus Areas for the FMA evaluation process based on repeat audit findings or areas of high risk that require further management evaluation. In the prior year, the acquisition-related corporate risks were revised and resulted in revisions, deletions, and additions to the acquisition management focus areas for FY 2020. In FY 2020, CR2117 is deleted and combined into CR2116, and CR2119 is deleted and combined with CR2118. The risk language is also revised for focus areas CR2115, CR2121, and CR6404.

The Focus Area processes and risks are identified in Table 6. For the 29 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 2020 unless the organization has tested the controls within the **last 12 month period**, which is July 1, 2018 – June 30, 2019. For risks that have a low or moderate combined risk rating, and the entity has tested the controls within the last 12 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 the following verbiage** into the Action Taken dialogue box in the **Focus Area** tab: **The controls have been tested within the last 12 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 12 month period, then the controls mitigating the focus areas risk will require testing **regardless of the risk rating or test cycle**.

E. FMA IT Corporate Controls

For FY 2020, the Information Technology (IT) will remain corporate controls within the FMA Module. The IT corporate controls are updated to keep DOE compliant with the National Institute of Standards and Technology (NIST) SP 800-53, Revision 4 cyber requirements. Table 7 identifies the changes to the IT corporate controls.

Table 7: FY 2020 IT Corporate Controls Update

CNO	Control Description	Status
CC0153	AC-2 Account Management	Per NIST SP 800-53, Rev 4, the corporate control encompasses CC0259.
CC0154	AC-3 Access Enforcement	Per NIST SP 800-53, Rev 4, the corporate control encompasses CC0259.
CC0174	CA-2 Security Assessments	Per NIST SP 800-53, Rev 4, the corporate control encompasses CC0176.

[6] IT corporate controls are updated based on NIST SP 800-53, Rev 4.

CC0176	CA-4 Security Certification	The corporate control is no longer a separate control and OCFO deleted it from the AMERICA for FY 2020. Per NIST SP 800-53, Rev 4, CC0174 encompasses this corporate control.
CC0216	PL-2 Security Planning Policy and Procedures	Per NIST SP 800-53, Rev 4, the corporate control encompasses CC0217.
CC0217	PL-3 System Security Plan Update	The corporate control is no longer a separate control and OCFO deleted it from AMERICA for FY 2020. Per NIST SP 800-53, Rev 4, CC0216 encompasses this corporate control.
CC0219	PL-5 Privacy Impact Assessment	The corporate control is no longer a separate control and OCFO deleted it from AMERICA for FY 2020. A new corporate control will be created to replace this control.
CC0259	SI-9 Information Input Restrictions	The corporate control is no longer a separate control and OCFO deleted it from AMERICA for FY 2020. Per NIST SP 800-53, Rev 4, CC0153, CC0154, CC0271, and CC0272 will encompasses this corporate control.
CC0271	AC-5 Separation of Duties	Per NIST SP 800-53, Rev 4, the corporate control encompasses CC0259.
CC0272	AC-6 Least Privilege	Per NIST SP 800-53, Rev 4, the corporate control encompasses CC0259.

Entities with financial systems will select the **Information Technology** sub-processes applicable to the site, evaluate the appropriate risks, and test controls. Risks rated as **NR** 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. For a complete listing of the IT corporate controls that should mitigate the IT corporate risks, refer to the *IT Corporate Risks and Controls Worksheet* that is located in the A-123 Resources section within AMERICA .

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 required last year, each reporting organization, as shown in Table 1, Listing of Required Internal Control Evaluations by Organization, 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 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 Activity-Level Objectives (Entity Missions)
- Infrastructure Status
- Systems & IT Posture
- Safety & Health (S&H) Posture
- Security Posture
- Continuity of Operations
- Contractor/Subcontractor Oversight
- Environmental

Entities denoted with single asterisks (*) in Table 1 must complete five accompanying entity objectives:

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

Consistent with Government-wide efforts to shift to high-value work, the OCFO reviewed the prior ten entity objective categories for evaluation in the EA Module. The review determined that the Segregation of Duties entity objective overlapped with the EA Internal Controls Evaluation of Green Book Principle #10 and the FMA Evaluation of select business sub-processes. In FY 2020, the Segregation of Duties entity objective is removed and reporting organizations will evaluate nine entity objective categories. Issues identified with the Segregation of Duties entity objective in FY 2019 and associated CAPs have been moved to Principle #10 within the EA Module Internal Control Evaluation tab in AMERICA for FY 2020.

The results of the evaluation for the nine (or fourteen 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

Organizations identified as owners of an FMS included in Table 8, DOE Financial Management Systems, **and users** of an FMS 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 2020.

Table 8: 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**
Funds Distribution System 2.0 (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.

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. 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 each 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, 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 in 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
- 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 Appendix F, *FMS Evaluation Worksheet*, 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. In FY 2020,

the risk level assessment narratives have been modified from the prior year to reflect instances where there are no significant deficiencies.

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 impact 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 9, 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 9: 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, but 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.	FMA, EA	Yes

Deficiency Title	Definition	Applicable to	Reported in Assurance Memorandum
	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?		
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 8, Deficiency Classifications, and a summary of the corrective action plans developed to address such issues will accompany the Assurance Memorandum. Further, in the FY 2020 Assurance Memorandum, organizations will 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 have been added 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

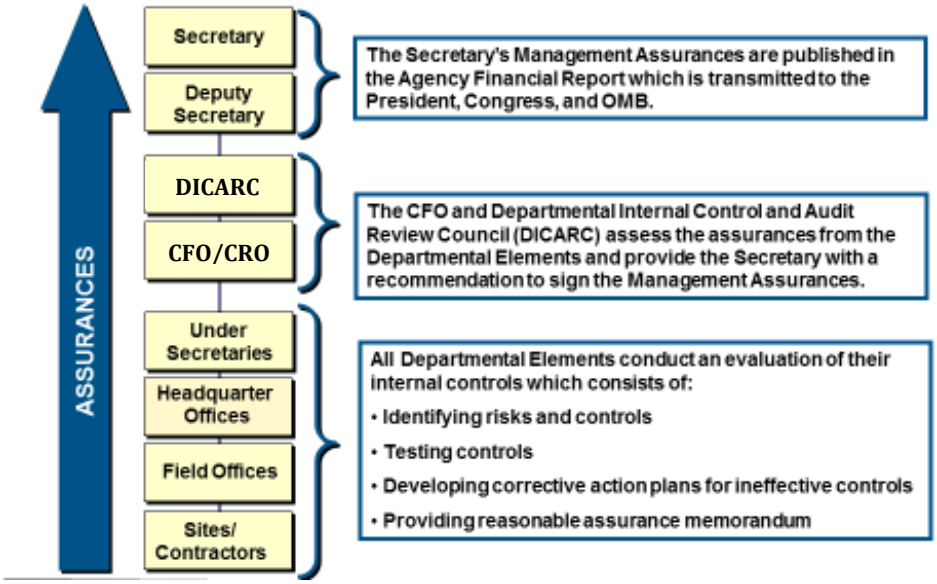
that the controls are operating effectively. Organizational assurance statements include an evaluation of the effectiveness of internal control over operations, reporting and compliance as of June 30. Organizations remain responsible to provide an update to the assurance statements when a significant 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 not later than October 1, 2020, 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, Chief Risk Officer (CRO), 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, large Headquarters Offices and smaller Headquarters Offices to use in preparation of the Assurance Memorandum. PMAs should continue to use the large Headquarters Office template in FY 2020.
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 2020, 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 organization must sign the Assurance Memorandum**. Headquarters-level entities that report to an Under Secretary will provide the Assurance Memorandum to the respective Under Secretary for signature.

Summary of Changes in FY 2020 Internal Controls Guidance

Documentation Requirements: In FY 2020, reporting entities are required to upload to AMERICA documentation which supports the FMA Evaluation for select business sub-processes. 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. For more information on the business sub-processes which require supporting documentation to be uploaded, refer to Section IV: Financial Management Assessment (FMA) Evaluation.

Environmental Liability Focus Area Exemptions: In FY 2020, the environmental liabilities focus areas are not required for select entities. Reporting organizations that had a low combined risk rating for environmental liabilities focus area risks are fully exempt from testing these focus areas in FY 2020. Organizations that reported environmental liabilities focus area risks with a combination of low and moderate/high combined risk ratings are only partially exempt. The partially exempt organizations are only required in FY 2020 to address the environmental liability focus areas with a moderate or high combined risk rating. For the entities where the environmental liabilities focus areas are not required in FY 2020, they will be removed as required focus areas in the organizations' FMA Module.

Fraud Risk Management Appendix: A new fraud risk management appendix (Appendix E) has been included in the FY 2020 Internal Controls Evaluation Guidance to provide information on fraud related requirements and the GAO Fraud Risk Framework. The appendix also presents information on fraud communication requirements, fraud trends across DOE, and fraud specific requirements for the FMA Module, EA Module, and Risk Profile.

Revised Risk and Control Type Designations: Reporting organizations are now able to tag risks and controls with multiple designations. Similar to the prior year, risks and controls will require a designation to be selected from the drop-down box in AMERICA. In FY 2020, risks and controls will have an alternative drop-down box where a fraud and/or improper payment designation can be assigned. For more information on where to assign a risk and control type in AMERICA, refer to Appendix C.

Revised Control Risk Matrices: The control risk rating matrix has been revised in the FMA Module to focus attention on the highest rated risks and reduce the frequency of testing on lower rated risks. Under the revised control risk rating matrix, risks with lower risk occurrence and control set execution scores will likely receive a lower control risk rating than under the previous matrix. For example, a risk occurrence score of 2 and a control set execution score of 1 will now result in a low overall control risk rating. The revised control risk ratings may lower the combined risk ratings and result in less frequent testing for lower rated risks in the FMA Module.

Risk Profile Approval Requirement: In FY 2020, 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 from the Head of the Departmental Element on the Risk Profile template. Organizations will provide both the completed Risk Profile excel template and the PDF version with management's signature.

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 Headquarter Offices and Field Offices must use to provide assurances on the effectives of the reporting organization's System of Internal Controls.
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 performs 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.
Appendix I, *Corporate Risk Table Guidance*	The appendix lists the corporate risks in the FMA Module and identifies which risks are applicable to reporting organizations.

Appendix A – Risk Profile Template

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 arising from activities and operations and the appropriate options for addressing those significant risks. This guidance provides the Risk Profile template and accompanying instructions to produce a Risk Profile compliant with OMB and DOE requirements.

The results of the completed risks assessments are recorded in the Risk Profile template and present reporting organizations' prioritized risks. OMB Circular A-123 requires that risks be analyzed in relation to the achievement of objectives in the following areas:

- **Strategic**: DOE Strategic Plan 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 external reporting.

Fraud Considerations in the Risk Profile

To ensure fraud risks are considered in FY 2020, all entities must identify the top financial and non-financial fraud risk. These two fraud risk statements must be included in each entity's Risk Profile along with other identified significant risks. Regardless of the residual risk ratings, the top financial and non-financial fraud risk must be identified and included in the FY 2020 Risk Profile. See Appendix E for additional information on fraud risk considerations.

In FY 2020, a new column has been added to the Risk Profile template to indicate the type of fraud risk category. The new Fraud Sub-Category column (Column E) will allow organizations to select whether a risk has a financial or non-financial fraud impact. If a risk does not have a fraud impact, then organizations should select "N/A" from the drop-down menu.

Deliverable Requirements

In FY 2020, 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 approval and sign-off. Reporting organizations 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 should be provided to the CFO via iPortal and not through the A-123 Application, AMERICA.

Major/Integrated contractors should provide a Risk Profile, identifying the most significant risks, to each respective Field Office. Field Offices, taking into consideration the Major/Integrated contractors under their purview, must provide a Risk Profile identifying the most significant risks to the responsible HQ Office. Each Headquarters Office taking into consideration the Field Offices under their purview, must provide a Risk Profile identifying no more than 10 of the most significant risks (not including fraud risks) to the Internal Controls iPortal Space and to the respective Under Secretaries, if applicable.

Each lower-level organizational element will produce a Risk Profile and provide it to the higher-level organization for consideration and consolidation. 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 as part of the annual Strategic Review with OMB in May and provided to OMB in early June 2020. Risk Profiles will continue to be formally updated and prepared on an annual basis.

Table 1 Important Dates for Risk Profile Deliverable:

FY 2020 Key Dates	Deliverables
March 13	All HQ Offices upload Risk Profile Excel and signed PDF versions using the provided templates, with consideration of reporting Field Offices as applicable, to the Internal Controls iPortal Space and to the respective Under Secretaries, if applicable.
April 3	Under Secretaries provide Risk Profile Excel and signed PDF versions using the provided templates, to the Internal Controls iPortal Space based on the input of the reporting offices.
May 8	Department completes DOE Risk Profile as required by OMB to prepare for the Annual Strategic Review in mid-May.

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 FY 2020 internal control testing and attested in the FY 2020 assurance statement. If a control existed in last year's Risk Profile submission, the Departmental Element may apply the focus area exemption to the existing control and treat it in the same manner as the 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 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.

In FY 2020, entities should 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:

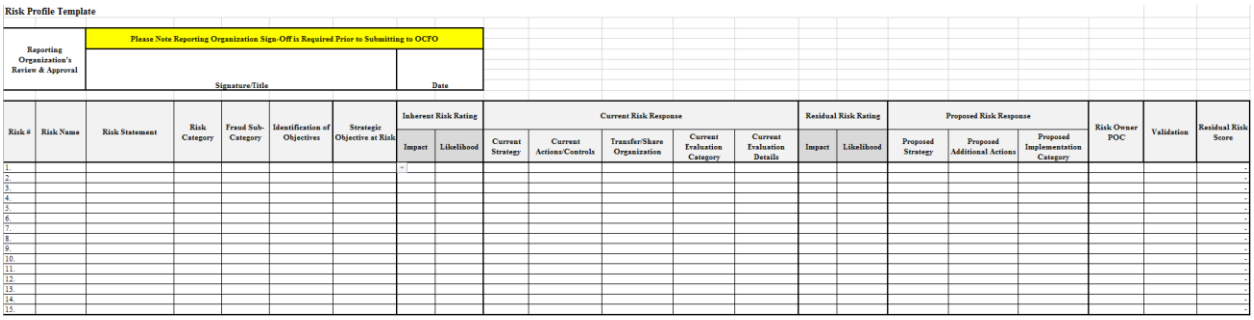
- What are my organization's goals and objectives that support the DOE Strategic Plan?
- What events could happen that would prevent my organization from achieving its goals and objectives aligned with the DOE Strategic Plan?

- 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 GAO *Standards for Internal Control in the Federal Government* (Green Book) define 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 followed by instructions explaining how to complete each column in the FY 2020 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



Risk Profile Template

Reporting Organization's Review & Approval	Please Note Reporting Organization Sign-Off is Required Prior to Submitting to OCFO	
	Signature/Title	Date

Risk #	Risk Name	Risk Statement	Risk Category	Fraud Sub-Category	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.																					-
2.																					-
3.																					-
4.																					-
5.																					-
6.																					-
7.																					-
8.																					-
9.																					-
10.																					-
11.																					-
12.																					-
13.																					-
14.																					-
15.																					-

NOTE: Verify that the file is "Enabled" by clicking on "File," "Enable Content," "Enable All Content" before entering data into the template.

Risk Number (Column A): This column is automatically populated and associates a unique number with each 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.

These 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 eight management priorities identified in the Agency Financial Report (contract and major project management; security; environmental cleanup; nuclear waste disposal; cybersecurity; infrastructure; human capital management; and safety culture) along with seven other common risk categories (Political, Reputational, IT, Grants/Loans, COOP, Fraud, and Financial). These management priorities along with the other listed categories serve as proxies for risk categories and will be used to aggregate risks. Only select one risk category. 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.

Fraud Sub-Category (Column E): Use this column to identify if the risk is a financial fraud or non-financial fraud related risk. 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).

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 external 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 (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-the 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 2018-2022. Only select one strategic objective, and for instances where multiple strategic objectives may seem to apply, use best judgement to select the most relevant strategic objective.

Inherent Risk Rating: Inherent risk is the exposure arising from a risk before any action is taken to manage it beyond normal operations. 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 "the risk of doing business" and will be measured using the impact and likelihood metrics described below.

Impact (Column H): 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 Figure 2, *Impacts*, to rate the impact of the risk.

Figure 2: Impacts

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.

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 Figure 3, *Likelihood*, to rate the likelihood of the identified risk:

Figure 3: Likelihood

Likelihood	Definition
1 – Very Low	Risk event **rarely** to occur.
2 – Low	Risk event **unlikely** to occur.
3 – Moderate	Risk event **possible** to occur.
4 – High	Risk event **highly likely** to occur.
5 – Very High	Risk event **almost certain** to occur.

Current Risk Response 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 Figure 4, *Risk Responses)*

Figure 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 FY 2020 internal control testing and included in the FY 2020 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 Risk response is to "Transfer" or "Share," then this field should be used to identify the organization to which the risk is transferred or shared. 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), 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 (Figure 2, *Impacts* and Figure 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 measurements 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 Figure 2). 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 Figure 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 from the drop down menu a proposed residual risk strategy from the options found in Figure 4, *Risk Responses*. For risks where no actions were taken to address the inherent or residual risk, the proposed risk response (Columns Q-S) 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: the (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 in the Fraud Sub-Category column (Column E) from the dropdown menu. The column will also identify if a Strategic Objective at Risk (Column G) or a Transfer/Share Organization (Column L) is applicable and missing. Additionally, the column will identify if there are errors in the values selected for the residual risk ratings. If the Residual Risk Impact and/or Likelihood values are greater than the Inherent Risk Impact and/or Likelihood values, then this field will produce an error and adjustments will be required. 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).

Appendix D – Assurance Memorandum Templates

1. Format for Large Headquarters Assurance Memorandum

Department of Energy
Washington, DC 20585

Date

MEMORANDUM FOR THE SECRETARY

THROUGH: **[if applicable] [Under Secretary's Name], [Under Secretarial Office Name]**

FROM: **[Head of HQ Element's Name], [Head of HQ Element's Title]**

SUBJECT: **Assurances of Internal Control - Federal Managers' Financial Integrity Act (FMFIA); OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; and [if applicable] Federal Financial Management Improvement Act of 1996 (FFMIA)**

FMFIA (Section II - Operations, Reporting, and Compliance):
In order to meet the objectives of the FMFIA, I am responsible for managing risks and maintaining effective internal control for **[HQ Element Name]**. I have completed a summary management review of the internal controls over operations, reporting, and compliance. The review was performed in conformity with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; OMB Circular A-123, Appendix A, *Management of Reporting and Data Integrity Risk;* OMB Circular A-123, Appendix B, *A Risk Management Framework for Government Charge Card Programs;* and Departmental guidelines. The review included an evaluation of whether the internal controls were in compliance with underlying management principles, which incorporate the Government Accountability Office's *Standards for Internal Control in the Federal Government*. The review included the consideration of the results of audit reports, internal management reviews, computer security reviews, **[include if applicable]** assurances from field elements under my cognizance, and all other known information. In addition, our review considered the areas of (1) environmental management, (2) nuclear safety management, and (3) non-nuclear safety management.

The results of the review indicate **[there is or there is not]** reasonable assurance that the internal controls over operations, reporting, and compliance were working effectively and that program and administrative functions were performed in an economical and efficient manner consistent with applicable laws; property, funds and other resources were safeguarded against fraud, waste, loss, unauthorized use or misappropriation; obligations and costs were proper; and accountability for assets was maintained. In addition, **[HQ Element Name]** has established safeguards, internal controls, and the appropriate

policies and controls to mitigate the risk of fraud and inappropriate charge card practices. The concept of reasonable assurance recognizes that internal controls must be cost effective, and there is always some potential for errors or irregularities to go undetected.

I have reported the results of my entity's Financial Management Assessment and Entity Assessment evaluations in AMERICA, and reviewed the results of the evaluations, including a review of any control deficiencies. The above review identified **[no or number identified]** significant deficiencies and **[no or number identified]** material weaknesses. **[Include if applicable]** Any significant deficiencies or material weaknesses identified during the evaluations are summarized and disclosed in the below *Corrective Action Plan (CAP) Summary* template.

[Include if applicable] In addition, evaluations performed by **[Field Element Name]** under my cognizance, identified **[no or number identified]** significant deficiencies and **[no or number identified]** material weaknesses. Details of the significant deficiencies or material weaknesses are located in the **[Field Element Name]** assurance memoranda.

If a significant deficiency or material weakness is identified, or an existing significant deficiency or material weakness is remediated during the time period June 30, 2020 - September 30, 2020, an updated Assurance Memorandum will be provided.

Based on the results of all the above evaluations, there **[is or is not]** reasonable assurance that processes are in place to identify risks and establish controls or integrate existing controls to mitigate the identified risks. For those risks for which formal internal controls were identified as part of the Risk Profile, there **[is or is not]** reasonable assurance that the internal controls were designed and operating effectively.

FMFIA (Section IV – Financial Management Systems) and FFMIA:
[HQ Element Name] has conducted an evaluation of financial management systems in accordance with OMB Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, and DOE guidelines. The results of the review indicate that systems generally **[conform or do not conform]** with Federal financial management system requirements. In addition, **[include if applicable]** the financial management systems of field elements under my cognizance are **[in or not in]** conformance with DOE accounting policies and procedures.

The financial management systems evaluation **[did or did not]** disclose financial management system reportable non-conformances. **[Include this statement if applicable]** Any non-conformances identified during the evaluations are summarized and disclosed in the below *Corrective Action Plan Summary* template.

Corrective Action Plan Summary for Element Name

Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details[1]	
Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details	
Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details	
Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details	

[1] In this field, describe the current status of remediation activities and any planned remediation activities for the following fiscal year. Also note if the CAP has been closed.

2. Format for Field Assurance Memorandum

Department of Energy
Washington, DC 20585

Date

MEMORANDUM FOR **[Head of HQ Element's Name], [Head of HQ Element's Title]**

FROM: **[Head of Field Element's Name], [Head of Field Element's Title]**

SUBJECT: **Assurances of Internal Control - Federal Managers' Financial Integrity Act (FMFIA), OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; and [if applicable] Federal Financial Management Improvement Act of 1996 (FFMIA)**

FMFIA (Section II – Operations, Reporting, and Compliance):
In order to meet the objectives of the FMFIA, I am responsible for managing risks and maintaining effective internal control for **[Field Element Name]**. I have completed a summary management review of the internal controls over operations, reporting, and compliance. The review was performed in conformity with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; OMB Circular A-123, Appendix A, *Management of Reporting and Data Integrity Risk;* OMB Circular A-123, Appendix B, *A Risk Management Framework for Government Charge Card Programs;* and Departmental guidelines. The review included an evaluation of whether the internal controls were in compliance with underlying management principles, which incorporate the Government Accountability Office's *Standards for Internal Controls in the Federal Government*. The review included the consideration of the results of audit reports, internal management reviews, computer security reviews, **[include if applicable]** assurances from major contractors under my cognizance, and all other known information. In addition, our review considered the areas of (1) environmental management, (2) nuclear safety management, and (3) non-nuclear safety management.

The results of the review indicate **[there is or there is not]** reasonable assurance that the internal controls over operations, reporting, and compliance were working effectively and that program and administrative functions were performed in an economical and efficient manner consistent with applicable laws; property, funds and other resources were safeguarded against fraud, waste, loss, unauthorized use or misappropriation; obligations and costs were proper; and accountability for assets was maintained. In addition, **[Field Element Name]** has established safeguards, internal controls, and the appropriate policies and controls to mitigate the risk of fraud and inappropriate charge card practices. The concept of reasonable assurance recognizes that internal controls must be cost effective, and there is always some potential for errors or irregularities to go undetected.

I have reported the results of my entity's Financial Management Assessment and Entity Assessment evaluations in AMERICA, and reviewed the results of the evaluations, including a review of any control deficiencies.

The above review identified **[no or number identified]** significant deficiencies and **[no or number identified]** material weaknesses. **[Include if applicable]** Any significant deficiencies or material weaknesses identified during the evaluations are summarized and disclosed in the below *Corrective Action Plan (CAP) Summary* template.

In addition, evaluations performed by the management of **[Field Element Name]** is responsible for establishing and maintaining adequate internal controls for any site(s) under our cognizance. My office has completed its evaluation of internal controls over operations, reporting, and compliance, which includes safeguarding of assets and compliance with applicable laws and regulations, as required by OMB Circular A-123 and Departmental requirements. This assessment covers the **[Field Element Name]** as well as the following federal or contractor sites under our cognizance: **[List names of Sites or Major/Integrated Contractors]**.

[Include if applicable] In addition, evaluations performed by **[Major/Integrated Contractor Name]** under my cognizance, identified **[no or number identified]** significant deficiencies and **[no or number identified]** material weaknesses. Details of the significant deficiencies or material weaknesses are located in the **[Major/Integrated Contractor Name]** assurance memoranda.

If a significant deficiency or material weakness is identified, or an existing significant deficiency or material weakness is remediated during the time period June 30, 2020 - September 30, 2020, an updated Assurance Memorandum will be provided.

Based on the results of all the above evaluations, there **[is or is not]** reasonable assurance that processes are in place to identify risks and establish controls or integrate existing controls to the identified risks. For those risks for which formal internal controls were identified as part of the Risk Profile, there **[is or is not]** reasonable assurance that the internal controls were operating effectively.

FMFIA (Section IV – Financial Management Systems)

[Field Element Name] has conducted an evaluation of financial management systems in accordance with OMB Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, and DOE guidelines. The results of the review indicate that systems generally **[conform or do not conform]** with Federal financial management system requirements. In addition, **[include if applicable]** the financial management systems of major/integrated contractors under my cognizance are **[in or not in]** conformance with applicable DOE financial requirements as contained in the terms and conditions of their respective Management and Operating (M&O) contracts.

The financial management systems evaluation **[did or did not]** disclose financial management system reportable non-conformances. **[Include this statement if applicable]** Any non-conformances identified during the evaluations are summarized and disclosed in the below *Corrective Action Plan Summary* template.

Corrective Action Plan Summary for Element Name

Title	
Assurance	Choose Operations, Reporting, Compliance, or FMS
Type	Choose significant deficiency, material weakness, or non-conformance
Status	Choose New or Existing
CAP Details[2]	
Title	
Assurance	Choose Operations, Reporting, Compliance, or FMS
Type	Choose significant deficiency, material weakness, or non-conformance
Status	Choose New or Existing
CAP Details	
Title	
Assurance	Choose Operations, Reporting, Compliance, or FMS
Type	Choose significant deficiency, material weakness, or non-conformance
Status	Choose New or Existing
CAP Details	
Title	
Assurance	Choose Operations, Reporting, Compliance, or FMS
Type	Choose significant deficiency, material weakness, or non-conformance
Status	Choose New or Existing
CAP Details	

[2] In this field, describe the current status of remediation activities and any planned remediation activities for the following fiscal year. Also note if the CAP has been closed.

3. Format for Small Headquarters Office Assurance Memorandum

Department of Energy
Washington, DC 20585

Date

MEMORANDUM FOR THE SECRETARY

THROUGH: **[if applicable] [Under Secretary's Name], [Under Secretarial Office Name]**

FROM: **[Head of HQ Element's Name], [Head of HQ Element's Title]**

SUBJECT: **Assurances of Internal Control - Federal Managers' Financial Integrity Act (FMFIA) and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control***

FMFIA (Section II - Operations, Reporting, and Compliance):
In order to meet the objectives of the FMFIA, I am responsible for managing risks and maintaining effective internal control for **[HQ Element Name].** I have completed a summary management review of the internal controls over operations, reporting, and compliance. The review was performed in conformity with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; OMB Circular A-123, Appendix A, *Management of Reporting and Data Integrity Risk;* OMB Circular A-123, Appendix B, *A Risk Management Framework for Government Charge Card Programs;* and Departmental guidelines. The review included an evaluation of whether the internal controls were in compliance with underlying management principles, which incorporate the Government Accountability Office's *Standards for Internal Control in the Federal Government*. The review included the consideration of the results of audit reports, internal management reviews, computer security reviews, and all other known information. In addition, our review considered the areas of (1) environmental management, (2) nuclear safety management, and (3) non-nuclear safety management.

The results of the review indicate **[there is or there is not]** reasonable assurance that the internal controls over operations, reporting, and compliance were working effectively and that program and administrative functions were performed in an economical and efficient manner consistent with applicable laws; property, funds and other resources were safeguarded against fraud, waste, loss, unauthorized use or misappropriation; obligations and costs were proper; and accountability for assets was maintained. In addition, **[HQ Element Name]** has established safeguards, internal controls, and the appropriate policies and controls to mitigate the risk of fraud and inappropriate charge card practices. The concept of reasonable assurance recognizes that internal controls must be cost effective, and there is always some potential for errors or irregularities to go undetected.

I have reported the results of my entity's Entity Assessment evaluations in AMERICA, and reviewed the results of the evaluations, including a review of any control deficiencies. The above review identified **[no or number identified]** significant

deficiencies and **[no or number identified]** material weaknesses. **[Include if applicable]** Any significant deficiencies or material weaknesses identified during the evaluations are summarized and disclosed in the below *Corrective Action Plan (CAP) Summary* template.

If a significant deficiency or material weakness is identified, or an existing significant deficiency or material weakness is remediated during the time period June 30, 2020 - September 30, 2020, an updated Assurance Memorandum will be provided.

Based on the results of all the above evaluations, there **[is or is not]** reasonable assurance that processes are in place to identify risks and establish controls or integrate existing controls to mitigate the identified risks. For those risks for which formal internal controls were identified as part of the Risk Profile, there **[is or is not]** reasonable assurance that the internal controls were designed and operating effectively.

Corrective Action Plan Summary for Element Name

Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details[3]	
Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details	
Title	
Assurance	**Choose Operations, Reporting, Compliance, or FMS**
Type	**Choose significant deficiency, material weakness, or non-conformance**
Status	**Choose New or Existing**
CAP Details	

[3] In this field, describe the current status of remediation activities and any planned remediation activities for the following fiscal year. Also note if the CAP has been closed.

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 2020, DOE continues to place emphasis on fraud prevention, detection, and mitigation to decrease fraud and to comply with the Fraud Reduction and Data Analytics Act of 2015 (FRDAA). The FRDAA requires the establishment of financial and administrative controls related to fraud and improper payments. More specifically, FRDAA states that agencies are required 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.

The FRDAA requires the Director of the Office of Management and Budget (OMB) to establish guidelines for agencies to establish controls to identify and assess fraud risks and design and implement control activities that incorporate the leading practices identified by the Government Accountability Office (GAO) *Framework for Managing Fraud Risks in Federal Programs* (Fraud Framework). The OMB established guidelines in OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

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.

Figure 1: GAO Fraud Risk Framework and Select Leading Practices

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

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. 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. **Organizations should report allegations of suspected or actual fraud promptly to the Department OIG**.

D. Fraud Trends Across the Department

In FY 2020, the Department continues efforts to combat and prevent fraud, waste, and abuse. One particular fraud risk emerging 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. Since June 2016, worldwide losses from BEC frauds total over $26 billion[1]. 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 an 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 DOE OIG identified additional 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.
- 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.

E. 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 2020, 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.

New in FY 2020: Reporting organizations will be able to tag controls with two designations. Similar to the prior year, all controls will require a control type designation (e.g. business, compliance) to be selected from the drop-down box in AMERICA. In FY 2020, the fraud and improper payments options have been removed and a new drop-down box has been added where fraud and/or improper payment designations should be made. This will require reporting organizations to review fraud and improper payments controls and select the appropriate control type designation from the additional drop-down box. For more information on how to assign a fraud and/or improper payment control type in AMERICA, see Appendix C.

Reporting organizations are also responsible for reviewing local risks to determine if they have a fraud and/or improper payments impact. In FY 2020, entities will be able to assign an additional risk type of fraud, improper payments, or both, to any local risk. The tagging of all local risks with a fraud and/or improper payments impact will provide for an easier identification of fraud risks across reporting organizations.

[1]Statistics from the FBI's public service announcement on September 10, 2019.

F. 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 2020 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. If the controls are already evaluated and reported in the FMA Module, organizations do not need to report them in the EA Module.
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

    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.

G. Fraud Requirements in the Risk Profile

Management has overall responsibility for establishing internal controls to manage the risk of fraud. When developing the FY 2020 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 2020, all entities must identify the top financial and non-financial fraud risk in the Risk Profile deliverable. DOE reporting organizations are required to identify and include the top two fraud risks along with other identified significant risks, regardless of the residual risk scores. 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); and
- Employee sabotage or employee vandalism.

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

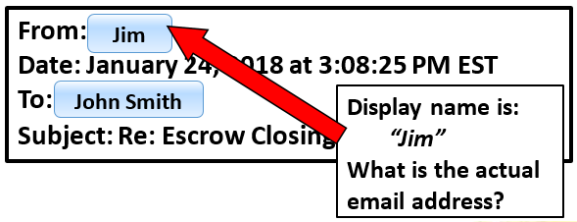
Internal Actions

- ☐ 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.

OMB Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996,* defines a financial management system (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 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.

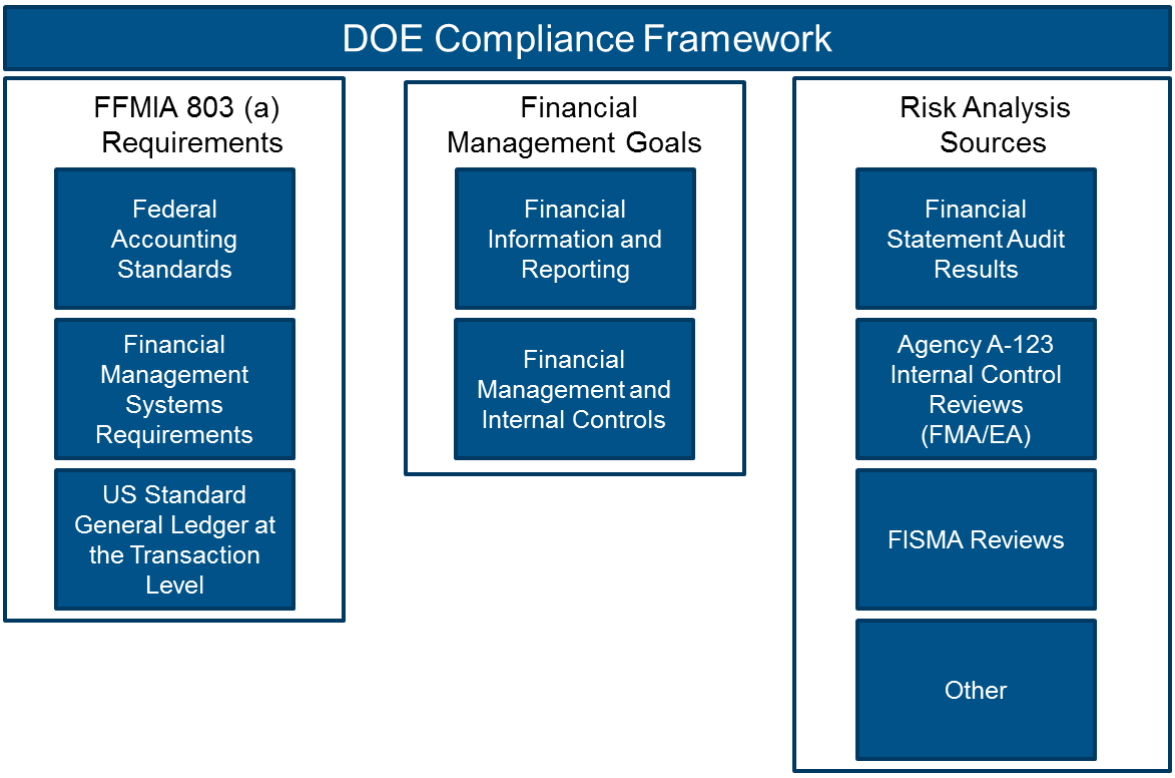
Owners and users of financial management systems will perform financial management system evaluations. Headquarter's organizations, Field/Site Offices, and Major/Integrated Contractors use and/or provide information into one or more of the Department's financial management systems. If an entity's system (including integrated and major contractor systems) feed into a DOE financial management system, then those systems are subject to an FMS Evaluation for FY 2020. 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

The Department of Energy's (DOE) compliance framework (Figure 1) is based on the compliance framework published in OMB Circular A-123, Appendix D. DOE's compliance framework consists of 3 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) that have been identified for each goal. An entity's FMS evaluation should capture the results of its evaluation for all applicable systems – a separate FMS evaluation for each FMS system is not necessary.

Figure 1: DOE Compliance Framework



Submission Requirements

As depicted in the FY 2019 *DOE Evaluations Guidance*, Table 1, Headquarters and Field Offices and Major/Integrated Contractors are responsible for completing a financial management system evaluation. Beginning in FY 2019, organizations will record the results of financial management system evaluations in the Financial Management System Evaluation Tab of the Entity Assessment Module of the A-123 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) has been designed to assist organizations perform assessments on financial management systems. An explanation of each area as they appear in the A-123 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.

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)		

Figure 3: Financial Management System Evaluation Worksheet

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

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, *Annual Assurance Memorandum*.

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.

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		

Control Deficiency

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. 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 follows:

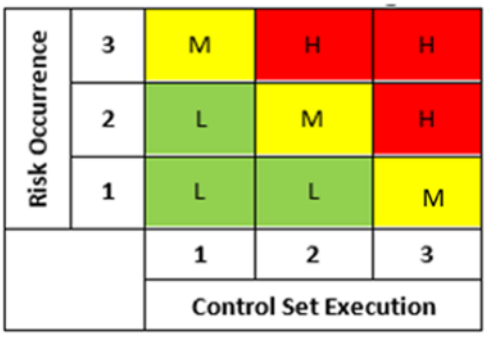
1 – Passed with no failures.
2 – Passed with failures within acceptable threshold.
3 – Failed.

Control Objective

Identifies the key objectives to be achieved by the internal control in each area, as well as 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

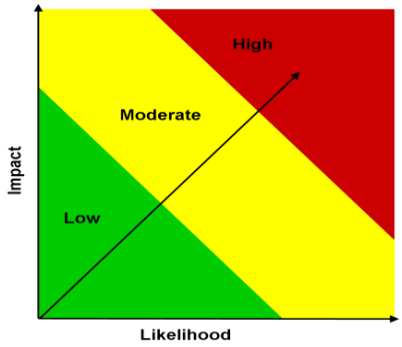
A measure of the risk considering the effectiveness of the controls to mitigate that risk and the risk occurrence. In the FMA Module, control risk is calculated based on the **Control Set Execution** and **Risk Occurrence scores**. The diagram demonstrates the calculation of High, Moderate, and Low control 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.
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 primary system for documenting and reporting the results of evaluations of entity and financial management system risks and controls.
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.
Enterprise Risk Management	Enterprise Risk Management (ERM) is 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.
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; however 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 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 financial reporting that tests these controls to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Financial Management Assessment (FMA) Module	The DOE primary system for documenting and reporting the results of evaluations and testing of financial management reporting risks and controls.
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.
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.
Inquiry	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 signatures, stamps, reviews, etc. 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.
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 which management determines to be significant enough to report outside its organization (e.g., merits the attention of the Office of the Secretary) 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 weaken 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 which the organization's management determines significant enough to impact internal or external decision-making and report outside the organization 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 is unable to provide reasonable assurance that it is in compliance with laws and regulation that could have a material effect on Federal programs or operations (compliance requirements).
Major/Integrated Contractors	DOE contractors with responsibility for the management and/or operation of a Department-owned or leased facility.
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 have 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."
OMB Circular A-123	Prescribes guidelines for evaluating, improving, and reporting on internal controls.
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, managing travel and purchase cards.
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.
Observation	Viewing of a specific business process in action, and in particular the control elements associated with the process, so as to test the effectiveness of an internal control.
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, as well as any 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 risk that remains after a risk response is executed.

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., IG or GAO audits). 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.
Risk Response	**Types of risk responses**: *Acceptance* – No action is taken to respond to the risk based on the insignificance of the risk or the risk is knowingly assumed to seize an opportunity. *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 magnitude of the risk. *Share* – Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses. *Transfer* – Action to transfer the responsibility for ownership and handling the risk to an organization other than the one 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.
Scope Limitation	Exists when an entity has identified potentially significant deficiencies in the scope of the internal control evaluations, which would warrant disclosure to ensure limitations are understood. Scope limitations may be determined by the entity or may be required by the OCFO in certain circumstances.
Significant Deficiency	A deficiency or a combination of deficiencies in internal control 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 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 any 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.

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 only applicable to DOE reporting organizations identified in Table 1 as an owner and lead office responsible for a Management Priority in FY 2020.

Management Priorities represent the most important strategic management issues facing the Department and are reviewed and identified by DOE's senior management council, the Departmental Internal Control and Audit Review Council (DICARC). The DICARC considers the results and any significant deficiencies and/or material weaknesses reported in 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 reporting 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 2020, 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. The lead responsible office of the Management Priority will be responsible for updating the narrative with an enterprise perspective and approving each priority update prior to delivering to the OCFO. Table 1 lists DOE's FY 2020 Management Priorities and the lead responsible offices.

Table 1: FY 2020 Management Priorities

Management Priorities in FY 2020	Lead Responsible Office
Contract & Major Project Management	MA
Security	AU
Environmental Cleanup	EM
Nuclear Waste Disposal	NE/GC
Cybersecurity	CIO
Infrastructure	MA
Human Capital Management	HC
Safety	AU

C. Management Priorities Update Process

In the third quarter of FY 2020, the OCFO will provide the lead responsible offices with Management Priorities published in the FY 2019 AFR. The lead responsible office will update this narrative (using tracked changes) based on significant activities and results performed in FY 2020. In the fourth quarter, OCFO will provide each lead responsible office with relevant significant deficiencies and/or material weaknesses reported by Departmental Elements throughout DOE for potential consideration and incorporation into updates for Management Priorities. Each lead responsible office will consider the enterprise reported results and provide a fourth quarter Management Priorities update (using tracked changes) to the OCFO. Table 2 provides a summary of the Management Priorities key dates and deliverables for FY 2020.

Table 2: FY 2020 Management Priorities Key Dates and Deliverables

FY 2020 Key Dates	Deliverables
June 15	OCFO provides the lead responsible offices Management Priorities from the DOE FY 2019 AFR in required update templates.
June 29	Lead responsible offices provides OCFO with Management Priorities update templates based on FY 2020 significant enterprise activities performed and planned.
September 22	Lead responsible offices update 3rd quarter Management Priorities with year-end updates and relevant Field and Headquarter Offices reported deficiencies/weaknesses.
October - TBD	OCFO will provide Management Priorities updates to the DICARC in early October for review. **Note:** Following DICARC recommendation, the final Management Priorities are incorporated into the AFR and proceed through Exec Sec Concurrence Process.

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 2020 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 2020 DOE AFR and will serve as the starting point for the FY 2021 update process.

Appendix I: Corporate Risk Worksheet Guidance

The Corporate Risk worksheet is used to assist reporting organizations to help determine which corporate risks are applicable to their respective organizations within the Financial Management Assessment (FMA) Module.

Corporate Risk Table

The **Corporate Risk Table** contains the data structure of the Corporate Framework embedded in the FMA Module. This information is presented for each corporate risk by cycle, process, and risk number (RNO). The Corporate Risk Table is presented in Table 1 with information about the table discussed in the Corporate Risk worksheet section.

Table 1: Corporate Risk Table Numbering System Legend

Cycle	Process	Example RNO
Budget to Close (B2C)	General Ledger Management	CR11XX
	Funds Management	CR12XX
	Fund Balance with Treasury	CR13XX
	Cost Management	CR14XX
	Financial Assistance	CR15XX
	Loan Administration	CR16XX
Procure to Pay (P2P)	Acquisition Management	CR21XX
	Inventory Management	CR22XX
	Payable Management	CR23XX
	Travel Administration	CR24XX
Quote to Cash (Q2C)	Revenue Recognition	CR31XX
	Receivable Management	CR32XX
Projects to Assets (P2A)	Project Cost Management	CR41XX
	Property Management	CR42XX
Enterprise Resource Management (ERM)	Payroll Administration	CR51XX
	Benefits Administration	CR52XX
Special Purpose (SPC)	Environmental Liabilities	CR61XX
	ES&H Liabilities	CR62XX
	Other Management Estimates	CR63XX
	Contractor Oversight	CR64XX
	Information Technology	CR65XX
	Improper Payments	CR66XX

Corporate Risk Worksheet

The **Corporate Risk Worksheet** depicts the corporate risks by cycle, process, sub-process, risk number (RNO) and risk statement. The Corporate Risk Worksheet is adopted from the A-123 Management of Entity Risk and Internal Control Application (AMERICA). OCFO has updated some Acquisition related risks with revisions shown in red in the worksheet.

The Corporate Risk Worksheet is presented in Figure 1 followed by instructions explaining each column. The worksheet and instructions will be provided in Excel for organizations' use in assessing each Corporate Risk that is applicable.

Cycle Name (Column B): This column is used to distinguish the Corporate Risk cycles. Below is a listing of each potential Corporate Risk cycle and a brief description of each corporate risk cycle category.

- **Budget to Close (B2C) -** cycle comprises financial and/or accounting processes used to manage financial data and resources such as: *General Ledger Management*; *Funds Management*; *Funds 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. **B2C** Corporate Risk Cycle will begin with CR**1**XXX.

- **Procure to Pay (P2P) -** 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 Request for Proposals (RFP), maintaining and selecting vendors, awarding contracts, maintaining obligations, receiving and managing goods or services, approving and paying invoices, tracking funds, monitoring continuing resolutions, managing travel and purchase cards. **P2P** Corporate Risk Cycle will begin with CR**2**XXX.

- **Quote to Cash (Q2C) –** 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, as well as any other expected revenues through to managing accounts receivable and receiving cash. **Q2C** Corporate Risk Cycle will begin with CR**3**XXX.

- **Project to Assets (P2A) –** 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. **P2A** Corporate Risk Cycle will begin with CR**4**XXX.

- **Enterprise Risk Management (ERM) -** cycle comprises the processes related to the management of human capital, in particular, the management of payroll. The cycle consists of *Payroll Administration.* Specific areas that fall within this process cycle include the maintenance and administration of payroll data necessary to calculate payroll and the appropriate distribution of labor costs. **ERM** Corporate Risk Cycle will begin with CR**5**XXX. **Please note:** This definition is <u>only</u> applicable to the FMA Module.

- **Special Purpose (SPC) –** cycle comprises processes which are unique and cannot be categorized under other process cycles. These processes require significant attention due to their impact on the financial statements and scope of responsibility. The cycle also include the *EM Liability* process. **SPC** Corporate Risk Cycle will begin with CR**6**XXX.

Process (Column C): This column identifies the business process that resides within the respective corporate risk cycle. The business process is indicated by the second digit in the RNO Number for instance CRX**1**XX.

Sub-Process (Column D): This column identifies the business sub-process. The last two numbers is the order the risk statement is added to the business process.

FY 2020 RNO (Column E): This column identifies the corporate risk number for each corporate risk for instance **CRXXXX. Corporate Risk Example**: CR1201 would be in reference to the Budget to Close (B2C) cycle (cycle 1) and the process "Funds Management" (the second process in the B2C cycle). The remaining two numbers reflect the order in which the risk was added to a given process.

FY 2020 Corporate Risk Statement (Column F): A risk statement that is pre-populated into the FMA module to facilitate the FMA evaluation. A corporate risk statement is a risk that is applicable to two or more reporting organizations.

The Corporate Risk worksheet includes columns G – I, which identifies the applicability of the corporate risk statements to reporting organizations at each level. If an entity believes a risk is applicable but the risk is marked as not applicable in the table, organizations may choose to add and test that risk, if appropriate. Applicability is divided into three groups as follows:

- HQ = DOE Headquarter Offices
- Field = DOE Field Offices
- IC = DOE Major/Integrated Contractors

Applicability HQ (Column G): This column identifies corporate risks that are applicable to Headquarters Offices.

Applicability Field (Column H): This column identifies corporate risks that are applicable to Field Offices.

Applicability IC (Column I): This column identifies corporate risks that are applicable to Major/Integrated Contractors.

Improper Payments (Column J): This column is used to indicate which risks may have improper payments implications.

- The purpose of the column is used to show organizations which risk impact improper payment.
- Each risk is marked with a Y, N, or NA to indicate Improper Payment applicability
    - Y = Yes, the risk may have controls that mitigate improper payments
    - N = No, the risk does not have controls that mitigate improper payments
    - NA = Not Applicable, the risk is unrelated to improper payments

Guidance and Comments (Column K): This column is used to provide supplementary information to provide context to the risk statements.