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

Internal Control Evaluations

Fiscal Year 2019 Guidance

Summary of Key Dates and Deliverables

FY 2019 Key Dates	Deliverables
January 15 – February 22	OCFO setup A-123 FMA modules for each organization. Entities validate the data migration from the FMA Tools to FMA modules are accurate and complete.
Cognizant Field Office Determine (Feb 11-22)	Major contractors provide Risk Profile to cognizant Field Office.
March 1	Planned Go-Live for A-123 Application.
March 1	Field Offices upload Risk Profile, with consideration of the Major/Integrated Contractors to the Internal Controls iPortal Space, and to the cognizant HQ Office.
March 15	All HQ Offices upload Risk Profile, with consideration of reporting Field Offices as applicable, to the Internal Controls iPortal Space and to the respective Under Secretaries, if applicable.
April 5	Under Secretaries provide Risk Profile to the CFO based on the input of the reporting offices.
April 19	Departmental Elements provide Interim Internal Control Status using the A-123 Application.
May 10	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review in mid-May.
June 30	Organizations performing FMA evaluations complete testing of controls that require testing in the current year.
July 26	Field Offices provide FMA Module and EA Module using the A-123 Application. **Note:** Due to A-123 Application workflow, reporting organizations should provide adequate time for review and approval. Field Offices provide draft Assurance Memoranda using iPortal.
August 2	Field Offices upload the Assurance Memoranda to the Internal Controls iPortal Space.
August 16	Headquarters Offices and Power Marketing Administrations (PMA) provide FMA Module and EA Module using the A-123 Application. **Note:** Due to A-123 Application workflow, reporting organizations should provide adequate time for review and approval. Headquarters Offices and PMAs provide draft Assurance Memoranda using iPortal.
August 23	Headquarters Offices and PMAs reporting to Under Secretaries must provide Assurance Memoranda to the respective Under Secretaries for review.
August 30	Under Secretaries, Headquarters Offices and Power Marketing Administrations upload the Assurance Memoranda to the Internal Controls iPortal Space.
October 1	Organizations that resolve or identify a significant deficiency or material weakness, after June 28, 2019, but no later than September 30, 2019, that is not included in a signed Assurance Memoranda, must notify the CFO and update the Assurance Memoranda.

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 controls 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 standards in the *Standards for Internal Control in the Federal Government* (Green Book), and OMB established guidelines for evaluation in OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

This guidance establishes DOE Internal Control Program requirements for evaluating and reporting on internal controls and preparation of a DOE Risk Profile in accordance with OMB Circular A-123. Each organizational element is responsible for establishing, maintaining, and evaluating systems of internal controls in compliance with this guidance.

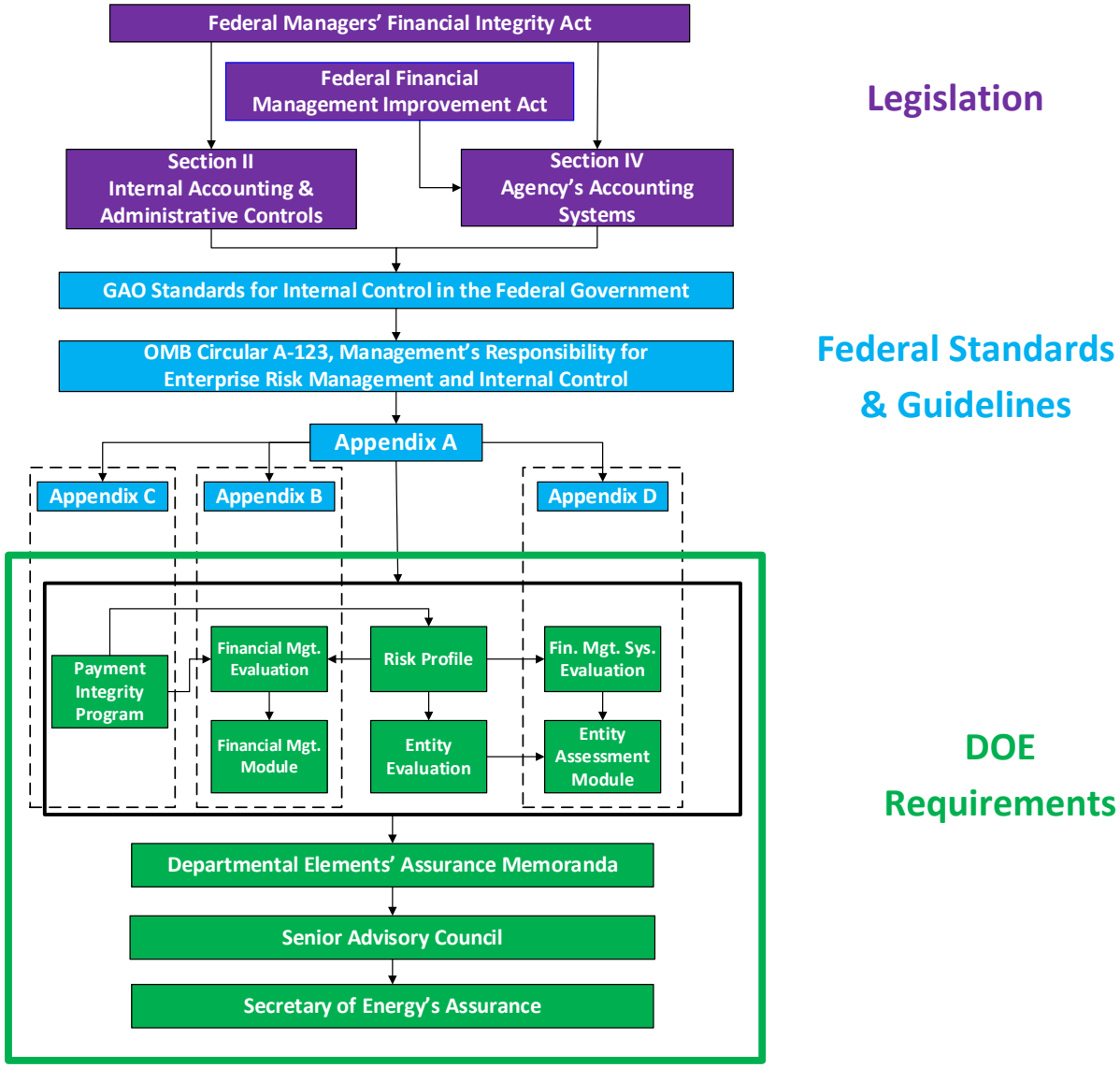
FMFIA requires each agency to:

- 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; material weaknesses, if any; and whether the agency's financial management systems are in compliance with FFMIA.[1]

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).

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

Figure 1: DOE Internal Controls Evaluation Framework



B. OMB Circular A-123

In FY 2019, DOE will comply 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 and 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 an updated 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 reduce burdens on 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 were required 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. Appendix A requires agencies to develop a Data Quality Plan that will identify and implement controls that will mitigate risks, which may interfere with data integrity. The Data Quality Plan will cover milestones and decisions pertaining to:

- Organizational structure and key processes providing internal controls for spend reporting;
- Management's responsibility to supply quality data to meet the reporting objectives of the Digital Accountability and Transparency Act (DATA); and,
- Identification of high-risk reported data and the test plans for the controls to mitigate the associated high-risks. Data should be linked through the inclusion of award identifiers in DOE's financial system and reported with plain English award descriptions.

The updated Appendix A, other than the requirement for a Data Quality Plan, does not have any new requirements beyond the existing OMB Circular A-123. Currently, DOE is developing a Data Quality Plan and will inform organizations on the Data Quality Plan status and required actions at a future date.

On June 26, 2018, OMB also released an updated Appendix C, *Requirements for Payment Integrity Improvement*, to OMB Circular A-123. The primary goal of Appendix C is to transform the improper payment compliance framework to a more unified, comprehensive, and less burdensome set of requirements. Improper payments consist of intentional fraud and abuse, unintentional payment errors, and instances where the documentation for a payment is not sufficient enough for the reviewer to determine whether a payment is proper. Organizations will receive separate and detailed guidance for DOE's Improper Payment Program no later than June 2019.

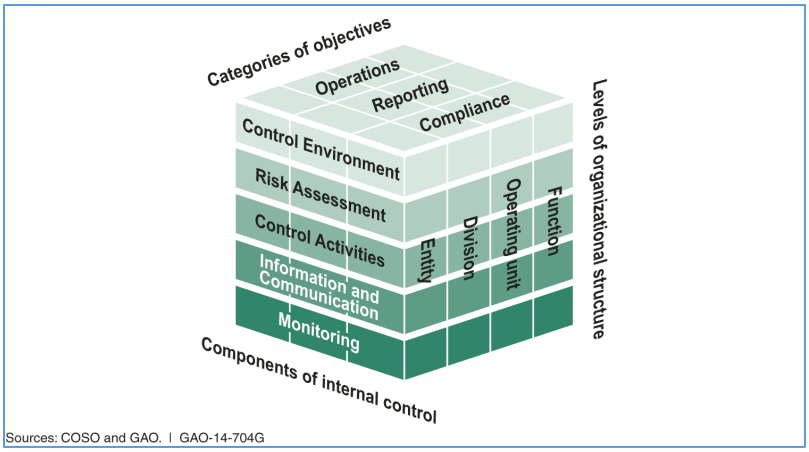
C. GAO Standards for Internal Control

The GAO *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 all three categories of objectives and the organizational structure.

D. Managing Fraud Risks

OMB Circular A-123 states that managers are responsible for determining the extent to which the leading practices in the 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. Managers may also use the Treasury's *Program Integrity: Antifraud Playbook* to assist with this effort. Activities evaluated for fraud risk typically relate to payroll, beneficiary payments, grants, large contracts, information technology and security, asset safeguards, and purchase, travel and fleet cards.

In FY 2019, DOE will continue to place emphasis on fraud prevention in the Financial Management Assessment (FMA) and Entity Assessment (EA) modules within the A-123 Application to further increase fraud prevention activities across the Department. Organizations must continue to identify the top financial and non-financial fraud risks in both the FY 2019 Risk Profile and the **Entity Objectives Evaluation** tab of the EA module in the *Fraud Prevention* entity control category. When evaluating fraud, organizations should assess fraud risk from the transaction-level to the entity-level. For example, when performing FMA evaluations, organizations that have identified control deficiencies related to fraud risks in the FMA module should consider that deficiency when assessing principle eight, *Assess Fraud Risk*, and the Fraud Prevention entity objective within the **Internal Control Evaluation** and **Entity Objective Evaluation** tabs in the EA module. Similarly, organizations that identify fraud-related issues in the assessment of the Contractor/Subcontractor entity objective should consider these issues when addressing the Contractor Oversight focus area risks in the FMA module.

E. Key Internal Control and Risk Profile Requirements

This guidance provides the FY 2019 Internal Control and Risk Profile requirements for:

- Risk Profiles (Excel Workbook);
- Financial Management Assessment (FMA) Evaluations (FMA Module);
- Entity Assessment Evaluations (Entity Assessment (EA) Module);
- Financial Management Systems (FMS) Evaluations (FMS Tab in the EA Module);
- Interim Internal Controls Status Memoranda (Interim Internal Controls Status 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 always check with respective Field and Headquarter Offices to determine if a deliverable is required to either of the cognizant organizations. A brief synopsis for organizations at each level within a reporting hierarchy is provided:

- Departmental Elements 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 must complete the five additional entity objectives in the EA Module. The small Departmental Elements are identified in Table 1 by an asterisk;
- Site Offices[3] are not required to provide evaluations to the OCFO and should check with the cognizant Field and Headquarters Offices to determine if a deliverable is required to either cognizant organization; and,
- Major/Integrated Contractors are required to provide a Risk Profile to the cognizant Field Office and are not required to provide the Risk Profile to the OCFO.

4 NEW in FY 2019

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	✓	✓	✓	✓	✓	✓
	Chief Financial Officer	✓	✓	✓	✓	✓	✓
	Chief Information Officer	✓	✓	✓	✓	✓	✓
	Congressional and Intergovernmental Affairs*		✓		✓	✓	✓
	Cybersecurity, Energy Security & Emergency Response	✓	✓	✓	✓	✓	✓
	Economic Impact and Diversity*		✓		✓	✓	✓
	Electricity Delivery and Energy Reliability	✓	✓	✓	✓	✓	✓
	Energy Efficiency and Renewable Energy	✓	✓	✓	✓	✓	✓

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

[3] Livermore, Los Alamos, Nevada, NNSA Production, Sandia, Ames, Argonne, Brookhaven, Fermi, Berkeley, Princeton, Oak Ridge, Pacific Northwest, Thomas Jefferson, SLAC

[4] NEW Internal Control deliverables to OCFO are identified for each organization emphasizing Major/Integrated Contractors and Site Offices 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
Headquarters Offices	Energy Information Administration*		✓		✓	✓	✓
	Office of Policy*		✓		✓	✓	✓
	Enterprise Assessments*		✓		✓	✓	✓
	Environment, Health,Safety and Security	✓	✓	✓	✓	✓	✓
	Environmental Management	✓	✓	✓	✓	✓	✓
	Fossil Energy	✓	✓	✓	✓	✓	✓
	General Counsel*		✓		✓	✓	✓
	Hearing and Appeals*		✓		✓	✓	✓
	Human Capital Officer	✓	✓	✓	✓	✓	✓
	Indian Energy Policy & Programs*		✓		✓	✓	✓
	Inspector General		✓			✓	✓
	Intelligence and Counterintelligence*		✓		✓	✓	✓
	Legacy Management	✓	✓	✓	✓	✓	✓
	Loan Programs Office	✓	✓	✓	✓	✓	✓
	Management	✓	✓	✓	✓	✓	✓
	National Nuclear Security Administration	✓	✓	✓	✓	✓	✓
	Nuclear Energy	✓	✓	✓	✓	✓	✓
	International Affairs*		✓		✓	✓	✓
	Project Management Oversight and Assessment	✓	✓	✓	✓	✓	✓
	Public Affairs*		✓		✓	✓	✓
	Science	✓	✓	✓	✓	✓	✓
	Small and Disadvantaged Business Utilization*		✓		✓	✓	✓
	Technology Transitions*		✓		✓	✓	✓
	Federal Energy Regulatory Commission**						✓
Power Marketing Administrations	Bonneville Power Administration	✓	✓	✓	✓	✓	✓
	Southeastern Power Administration	✓	✓	✓	✓	✓	✓
	Southwestern Power Administration	✓	✓	✓	✓	✓	✓
	Western Area Power Administration	✓	✓	✓	✓	✓	✓
Field/Operation Offices	Chicago Office	✓	✓	✓	✓	✓	✓
	EM Consolidated Business Center	✓	✓	✓	✓	✓	✓
	Golden Field Office	✓	✓	✓	✓	✓	✓
	Idaho Operations Office	✓	✓	✓	✓	✓	✓
	National Energy Technology Laboratory	✓	✓	✓	✓	✓	✓
	NNSA Complex	✓	✓	✓	✓	✓	✓
	Naval Reactors Laboratory Field Office	✓	✓	✓	✓	✓	✓
	Oak Ridge Office	✓	✓	✓	✓	✓	✓
	Oak Ridge Environmental Management	✓	✓	✓	✓	✓	✓
	Richland Operations Office	✓	✓	✓	✓	✓	✓
	Savannah River Operations Office	✓	✓	✓	✓	✓	✓
	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	✓	✓	✓			

* Single asterisks in Table 1 identifies the small Departmental Elements

** Double asterisks in Table 1 identifies independent organizations

F. 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 CFO 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 2019 Key Dates	Deliverables
January 15 – February 22	OCFO setup A-123 FMA modules for each organization. Entities validate the data migration from the FMA Tools to FMA modules are accurate and complete.
Cognizant Field Office Determine (Feb 11-22)	Major contractors provide Risk Profile to cognizant Field Office.
March 1	Planned Go-Live for A-123 Application.
March 1	Field Offices upload the Risk Profile, with consideration of the Major/Integrated Contractors to the Internal Controls iPortal Space, and to the cognizant HQ Office.
March 15	All HQ Offices upload Risk Profile, with consideration of reporting Field Offices as applicable, to the Internal Controls iPortal Space and to the respective Under Secretaries, if applicable.
April 5	Under Secretaries provide Risk Profile to the CFO based on the input of the reporting offices.
April 19	Departmental Elements provide Interim Internal Control Status using the A-123 Application.
May 10	Department completes DOE Risk Profile as required by OMB in preparation for the Annual Strategic Review in mid-May.
June 30	Organizations performing FMA evaluations complete testing of controls that require testing in the current year.
July 26	Field Offices provide FMA Module and EA Module using the A-123 Application. **Note:** Due to A-123 Application workflow, reporting organizations should provide adequate time for review and approval. Field Offices provide draft Assurance Memoranda using iPortal.
August 2	Field Offices upload the Assurance Memoranda to the Internal Controls iPortal Space.
August 16	Headquarters Offices and Power Marketing Administrations (PMA) provide FMA Module and EA Module using the A-123 Application. **Note:** Due to A-123 Application workflow, reporting organizations should provide adequate time for review and approval. Headquarters Offices and PMAs provide draft Assurance Memoranda using iPortal.
August 23	Headquarters Offices and PMAs reporting to Under Secretaries must provide Assurance Memoranda to the respective Under Secretaries for review.
August 30	Under Secretaries, Headquarters Offices and Power Marketing Administrations upload the Assurance Memoranda to the Internal Controls iPortal Space.
October 1	Organizations that resolve or identify a significant deficiency or material weakness, after June 28, 2019, but no later than September 30, 2019, that is not included in a signed Assurance Memoranda, must notify the CFO and update the Assurance Memoranda.

Entities 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	Electronic Delivery & Upload to iPortal	Major/Integrated Contractors to: Field Office Field Office to: Lead Program Secretarial Office and OCFO Headquarters to: Appropriate Under Secretary and OCFO Under Secretary to: OCFO
EA, FMA, FMS Evaluations and Interim Internal Control Status	APEX	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, senior managers, or auditors.

Examples include:

- Process flows and descriptions;
- Test documentation more detailed than what is included in the FMA and EA reporting modules; and,
- Evidence collected during testing.

Organizations must have vigorous and robust procedures to test the effectiveness of the controls using sampling, re-performance, observation, and inspection. These key procedures as referenced by OMB Circular A-123, Appendix A, *Implementation Guide,* should be cited in the FMA and EA modules where applicable:

- **Sampling**: is statistical (arithmetical and objective scientific analysis of confidence level and sample size) or non-statistical (judgmental) testing of a representative selection of a population to make assumptions about the effectiveness of a control.
- **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.

- **Observation**: is the 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.
- **Inspection/Examination**: is scrutiny of specific business processes and documents through consideration and analysis for approval signatures, stamps, reviews, etc., that indicate the effectiveness of controls.

Adequate controls testing must be documented. Examples of insufficient test procedures result descriptions or narrative that should be avoided include:

- **Walkthroughs;**
- **Limited Discussions;**
- **Reviews of organization charts**; and,
- **Talking to 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.

III. Risk Profile

OMB Circular A-123 requires each agency to prepare an annual prioritized and ranked Risk Profile by June 3, 2019, as part of the annual Strategic Review with OMB in May, identifying 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.

To meet this OMB requirement, 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 OCFO via the iPortal and also 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 10 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, 2019.

In accordance with OMB requirements, 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.

Please note that to the extent additional internal controls are necessary to manage or mitigate risks identified in Risk Profiles, the controls must be established and tested as part of FY 2019 internal control testing and attested to in the FY 2019 assurance statement.

Risk Profile, FMA and EA Module Reporting

Risk Profile financial risks require documentation and evaluation, including the establishment and testing of controls when applicable, in the **FMA Module.**

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** (e.g., internal control risks assessed as part of the **Internal Control Evaluation** tab; and risks that relate to an entity objective in the **Entity Objective Evaluation** tab category would be assessed there).

Fraud Considerations in the Risk Profile

In FY 2019, 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. Regardless of the residual risk rating, the top financial and non-financial fraud risks require identification and inclusion in the FY 2019 Risk Profile.

The Risk Profile must include an evaluation of fraud risks. Sites should use a risk-based approach to identify any material fraud risks. If an organizations identifies material fraud risks, then the entity must design and implement internal controls, and test the operating effectiveness of the controls, to mitigate the identified risks. At a minimum, entities must consider:

- Types of fraud that can occur within the entity (fraudulent financial reporting, misappropriation of assets, corruption);
- Presence of fraud risk factors (incentive or opportunity);
- Sufficiency of the entity's responses to identified fraud risks;
- Potential for management override; and,
- Presence of sufficient segregation of duties.

IV. Financial Management Assessment (FMA) Evaluation

The FMA Module is the central repository for documenting the evaluation of the relevant financial business processes, sub-processes, and risks facing each reporting entity, as well as the key controls for each process that are relied upon to mitigate the risks. Reporting entities are not required to provide supplemental documentation to support the FMA Evaluation. Reporting entities, must reference in the **Documentation Location** section of the **Assessment** tab 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. Such documents may include process mapping, risk analyses, test plans, and test results. Also, beginning in FY 2019, organizations 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 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.

A. Requirements for FY 2019

5 NEW in FY 2019

In FY 2019, 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

[5] NEW in FY 2019 Major changes are the updates to the Acquisition-related risks and the conversion of corporate controls to local controls.

upgrades, process changes, audit findings, external events, or other changes that occurred over the past year impact the risk assessment ratings. If so, entities must mark the appropriate area in the **Assessment** tab, and test the controls related to those risks. Please note that the annual risk re-evaluation could result in a determination that certain risk exposure ratings are lower because of program changes, including fewer transactions or lower dollar amounts. Also, entities should pay careful attention to the revised Acquisition-related corporate risk statements in the FMA Module when performing risk assessments. **There are 50 new, revised, and deleted Acquisition-related risks in FY 2019. In FY 2020, the risks identified for deletion as a corporate risk will no longer reside in the FMA Module, so if any of these risks are applicable to an organization, the entity should convert the corporate risk into a local risk. For detailed instructions, please see Appendix E, *Acquisition-related Risk Statements***.

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 control to determine if the one control is sufficient to mitigate the risk(s) from occurring or if additional controls should be developed to mitigate high rated risk(s) from occurring.
3. *Assess local controls that were previously corporate controls* – As part of the conversion to the A-123 Application, all corporate controls, with the exception of the IT-related corporate controls, were converted to local controls. For FMA Tools that contained multiple instances of the same corporate control with distinctly different data (i.e., different testing results or documentation locations), a unique local control was created for each instance. In FY 2019, entities must assess these new local controls (which were formerly corporate controls in the FMA Tool) to validate the appropriate control is still in place. If the control is due for testing in FY 2019, the local control must be tested with the results documented in the FMA module.
4. *Evaluate risks and test controls for the processes/sub-processes identified in Table 4* - If an organization did not select the processes/sub-processes listed in Table 4 in prior year FMA data, the processes/sub-processes will be included in the FMA Module in the **Assessment** tab as part of the data migration process to the A-123 Application. If the corporate risks for these required business sub-processes do not apply, please 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	✓	✓	✓

Process	Sub-process	Applicability		
		HQ	Field	IC
Travel Administration	Travel Authorization	✓	✓	✓
	Voucher Processing	✓	✓	✓
	Travel Closeout	✓	✓	✓
	Travel Card Program Management	✓	✓	✓
Payroll Administration	Time and Attendance Processing	✓	✓	✓
	Leave Processing	✓	✓	✓

5. *Fraud Consideration in the FMA Review* - Effective fraud risk management monitors that taxpayer dollars and government services serve the intended purposes.

   In the FMA Evaluations, sites will consider the potential for fraud when identifying, analyzing, and responding to risks. Entities will design and implement controls to mitigate assessed fraud risks and validate the controls are operating effectively. **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.** In accordance with the GAO Fraud Framework, at a minimum, entities must consider:

   - Types of fraud that can occur in the entity (e.g., fraudulent financial reporting, misappropriation of assets, corruption);
   - Presence of fraud risk factors (e.g., pressure/incentive, opportunity, and attitude/rationalization);
   - Sufficiency of the entity responses to identified fraud risks;
   - Potential for management override; and,
   - Presence of sufficient segregation of duties

6. *Complete Current Year Test Requirements* – Entities must test all applicable controls identified as **yes** or **overdue** in the *In Scope for Current Year* column of the Assessment tab of the FMA Module no later than June 30, 2019. Entities must also identify in the FMA Module any **local risks** that are suspect to fraud, improper payment, or both.
7. *Complete Focus Area Testing and Actions* – Organizations must complete testing and other required actions to address the FY 2019 focus area risks and document the actions taken in the Assessment tab of the FMA Module. The DOE and NNSA focus areas **will remain the same** for FY 2019. Section B, Focus Area Guidance, provides additional information on focus areas and assessment requirements.
8. *Develop Corrective Action Plans As Applicable* - A Corrective Action Plan (CAP) is required for each remediation area identified in testing. In the A-123 Application, any 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 as well as the 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 required to summarize significant CAP information in the **Action Tracking** tab of the FMA Module. Entities are responsible for maintaining the CAPs and are not required to provide CAP documentation unless requested by the OCFO. Also, a CAP template is located on the Internal Controls iPortal space under the Resources tab.

9. *Upload Relevant and Appropriate Supporting Documentation* – Beginning in FY 2020, organizations will be responsible for u**ploading requested documentation** to the A-123 application to support the internal control assessments and evaluations.

B. Focus Area Guidance

The Department annually identifies Focus Areas for the FMA evaluation process based on repeat audit findings or areas of high risk that require additional management evaluation. The Focus Area processes and risks are identified in Table 5.

The DOE and NNSA focus areas will remain the same for FY 2019. The Acquisition-related corporate risk statements that are part of the FY 2019 Focus Areas will also remain the same; and, organizations will continue to test the controls that are mitigating the existing risks unless the organization decides to begin testing newly identified controls, if any, for the new risks. For the 29 FMA Focus Area risks, the controls require evaluation and testing by all entities in FY 2019 unless the organization has tested the controls within the **last 12 month period**, which is July 1, 2017 – June 30, 2018. For risks that have a low or moderate exposure 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 not any audit findings or deficiencies during the controls testing.

If these requirements are met, the organization will enter the 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**.

Table 5: FY 2019 Focus Areas

FY 2019 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)
• Receipt of Good and Services-Received goods/services do not match invoice (CR2117)
• Contract Closeout-Improper/untimely closeout (CR2119)
• 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 /soil & ground water remediation. (CR6105)
• Non-EM Liabilities-Untimely updates to Long-term stewardship (CR6106)
• Non-EM Liabilities-Improper accounting of surplus materials. (CR6107)
• Non-EM Liabilities-Improper accounting of non-EM Environmental Liabilities (CR6108)
• Policy Execution-Environmental policies and procedures not up to date (CR6109)
• Policy Execution-Environmental policies/procedures not communicated (CR6110)
• Policy Execution-Roles and responsibilities not known (CR6111)
• Policy Execution –Staff has inadequate skills/knowledge (CR6112)
• Active Facilities-Incorrect Active Facility Data Collection Systems (AFDCS) data (CR6113)
• Active Facilities-Best estimates for AFDCS not used (CR6114)
• Active Facilities-Omitted or duplicate facilities (CR6115)
• Active Facilities- Facility surveys/contamination swipes/etc. not considered (CR6116)
• Active Facilities-Leased facilities inappropriately considered (CR6117)
Contractor Oversight
• Performance- Contractor/Subcontractor progress improperly assessed (CR6404)
• Performance-Contractor/Subcontractor performance and billing not monitored (CR6405)
Improper Payments
• SPC: Payment Disbursing-Incorrect implementation of OMB requirements (CR6601)

C. Consideration of Cognizant Site Reporting

In conducting and reporting on FMA evaluations, all Headquarters Offices with Field organizations must consider the results of the Field organizations' evaluations as part of the evaluation. Likewise, Field sites with Major/Integrated Contractors, must consider the results of the contractor evaluations as part of the evaluation.

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 and operating effectively to mitigate risk and validate mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulation.

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. Non-Financial Internal Controls Evaluation

In addition to requiring an assessment of financial controls, Section II of FMFIA requires an assessment of non-financial controls to assure the effectiveness and efficiency and compliance with laws and regulations. The Green Book has five components, 17 principles and 48 attributes to guide the Entity Assessment Evaluation. As required last year, all entities, as shown in Table 1, Listing of Required Internal Control Evaluations by Organization, are 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. There are eight tabs in the EA Module related to the Internal Control Evaluations. The second tab, **Internal Control Evaluation**, requires an evaluation of each entity's internal controls against the Green Book's five components and 17 principles. Any issues found in the evaluation are identified and rated as to seriousness on a scale of 1 (least serious) to 3 (most serious). Issues rated **2** or **3** require a Corrective Action Plan, and these issues automatically populate in the **Action Tracking** tab and require additional 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?**

In addition to the 17 Internal Control principles, entities required to perform FMS evaluations in accordance with Section IV of FMFIA will have eight FMS goals pre-populated in the FMS Evaluation tab of the EA Module.

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 10 entity objective categories identified in the EA Module that need evaluation by all 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
- Segregation of Duties
- Environmental

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

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

The results of the entity objectives evaluations are reported in two EA tabs. The results of the evaluation for the ten (or fifteen 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, any issues found 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. Any issues identified with a rating of **2** or **3** require a CAP. Any issues identified in the **Entity Objectives Evaluation** tab will create an entry in the **Action Tracking** tab. In the **Action Tracking** tab, entities will complete the CAP information required for each issue.

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. When addressing this internal control principle and the 10 (15 for identified organizations) entity objectives, organizations should be guided by the GAO Fraud Framework. At a minimum, entities must consider:

- Types of fraud that can occur in the entity (e.g., fraudulent financial reporting, misappropriation of assets, corruption);
- Presence of fraud risk factors (e.g., incentive or opportunity);
- Sufficiency of the entity responses to identified fraud risks;
- Potential for management override; and,
- Presence of sufficient segregation of duties.

To sustain the increased fraud prevention activities across the Department, additional emphasis will remain in this area in the EA Module. In the **Entity Objective Evaluation** tab, organizations must evaluate the fraud-related entity objectives. In addition, entities must also 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 2019 Risk Profile.

E. Consideration of Cognizant Site Reporting

In conducting and reporting on entity assessment evaluations, all Headquarters Offices with Field organizations must consider the results of the Field organization evaluations as part of the evaluation. Likewise, Field organizations with Major/Integrated Contractors, must consider the results of the contractor evaluations as part of the evaluation. 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.

VI. Financial Management Systems (FMS) Evaluation

Organizations identified as owners of a FMS included in Table 6, DOE Financial Management Systems, **and users** of a FMS must perform a 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 2019.

Table 6: 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

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.

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 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.

FMS owners and users must evaluate the design and efficacy of system controls to determine to what degree each system meets the financial management goals:

1. Record and account for federal funds, assets, liabilities, revenues, expenditures, and costs in a consistent, complete, and accurate manner.
2. Provide timely and reliable federal financial management information of appropriate form and content to agency program managers for managing current Departmental programs and activities.
3. Provide timely and reliable federal financial management information of appropriate form and content for continuing use by external stakeholders, including the President, Congress, and the public.
4. Provide timely and reliable federal financial management information of appropriate form and content that can be linked to strategic goals and performance information.
5. Provide internal control to restrict federal obligations and outlays to those authorized by law and within the amount available.
6. Perform federal financial management operations effectively within resources available.
7. Minimize waste, loss, unauthorized use, or misappropriation of federal funds, property, and, other assets within resources available.
8. Reduce federal financial management system security risks to an acceptable level.

FMS Evaluation in the FMA Module

For FY 2019, the Information Technology (IT) controls within the FMA Module includes updated controls 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.

6

NEW in FY 2019

Table 7: FY 2019 IT Corporate Controls Update

CNO	Control Description	Status
CC0153	AC-1 Access Control Policy	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.
CC0176	CA-4 Security Certification	The corporate control is no longer a separate control and OCFO will delete it from the A-123 Application in 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 will delete it from the A-123 Application in FY 2020. Per NIST SP 800-53, Rev 4, CC0174 encompasses this corporate control.

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

CC0219	PL-5 Privacy Impact Assessment	The corporate control is no longer a separate control and OCFO will delete from the A-123 Application in FY 2020. Per NIST SP 800-53, Rev 4, CC0174 encompasses this corporate control. Per NIST SP 800-53, Rev 4, the control has been incorporated into Appendix J, AR-2 (Privacy Impact and Risk Assessment)
CC0259	SI-9 Information Input Restrictions	The corporate control is no longer a separate control and OCFO will delete from the A-123 Application in FY 2020. Per NIST SP 800-53, Rev 4, CC0174 encompasses this corporate control.
New	AC-5 Separation of Duties	This is a new corporate control in accordance with NIST SP 800-53, Rev 4.
New	AC-6 Least Privilege	This is a new corporate control in accordance with NIST SP 800-53, Rev 4.

Entities with financial systems will select the **Information Technology** sub-processes applicable to the site, evaluate the appropriate risks, and add 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.

FMS Evaluation in the EA Module

The **FMS** tab in the EA Module provides a uniform Department-wide mechanism for documenting the FMS Evaluation. For each of the Financial Management System Goals listed in the **FMS** tab, entities will record a basis of evaluation. Please note that the Financial Management Goals are the same as the eight criteria on which entities should base the assessments. For each of the eight goals, the evaluation summary should briefly describe the evaluation performed and the outcome. If an organization performs a physical examination of documents, include the titles of the documents in this description.

In implementing the physical examination of documentation test technique, managers should consider a variety of existing information that is available. Examples of such sources of information are:

- Results of external audits, including financial statement audits and findings;
- Day-to-day knowledge;
- Management reviews, including, but not limited to, computer security reviews and summary management reviews;
- Department's 5-Year Systems Development Plan;
- Problems identified through on-going initiatives;
- System change requests;
- Problem(s) identified by user groups or councils;
- Prior Summary Financial Management System reviews; and,
- Prior year FMS Evaluations.

7 

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-

[7] FMS Worksheet has been added as a tab within the EA Module of the A-123 Application.

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 any 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. Any issues identified in the **FMS** tab will create a line in the **Action Tracking** tab. Then, the user will need to complete the needed information required for each issue. Any issues identified with a rating of **2** or **3** will require a CAP. If there is already an existing CAP for an FMS issue, please indicate this and identify the existing CAP name and number in the EA Module.

Please note, managers must use professional judgement 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.

VII. Classifying Deficiencies

In accordance with OMB Circular A-123 guidance, DOE is adopting 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 whether 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 8, 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 8: 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

Deficiency Title	Definition	Applicable to	Reported in Assurance Memorandum
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. 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 ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving Entity objectives. A **No** response on either Line 46 or 47 in the **EAT IC Summary Evaluation** tab requires a Material Weakness to be reported: • Are all components operating together in an integrated manner? or • Is the overall system of internal control effective?	FMA, EA	Yes
Non-Conformance	Exists when financial systems do not substantially comply with federal financial management system requirements OR where local control deficiencies impact financial systems ability to comply. The EA Module defines the criteria against which conformance is evaluated and captures identified non-conformances.	FMS (in the EA Module)	Yes
Scope Limitation	Exists when the Entity has identified potentially significant deficiencies in the scope of the internal controls evaluations conducted, which would warrant disclosure to ensure 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 if applicable, FMS Evaluation, as well as any 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. In addition, in the FY 2019 Assurance Memorandum, organizations will report any instances of non-conformance of FMS that indicate lack of compliance with Federal FMS requirements or control deficiencies that impact FMS abilities to comply.

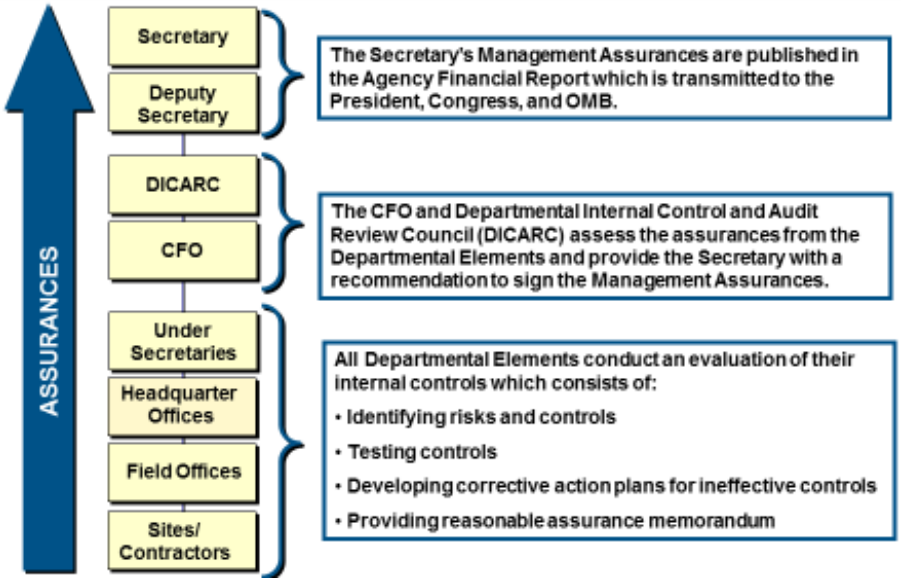
To align and comply with M-13-21, *Implementation of the Government Charge Card Abuse Prevention Act* and OMB Circular A-123, assurances have been added in the Assurance Memorandum in reference to the implementation of safeguards and internal controls for inappropriate charge card practices for purchase cards, travel cards, and centrally billed accounts 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 CFO immediately of any resolved or new significant deficiencies or material weaknesses not later than October 1, 2019, per Table 2, DOE Internal Controls and Risk Profile Process Important Dates.

Figure 3 presents the DOE annual assurance process. Assurance flows from all major/integrated contractors to the respective Departmental element, and from the Departmental element (Field and Headquarters Offices) to the Under Secretaries. The CFO and DICARC assess the assurances from the Under Secretaries and provide the Secretary with the recommendation to sign the DOE Management Assurances.

Figure 3: 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. Power Marketing

Administrations (PMA) should use the large Headquarters Office template in FY 2019. For FY 2019, the revised Assurance Memoranda merges the Operations and Compliance sections with the Reporting section. Also, heads of organizations will provide assurances on the identification of risks and testing of controls that involve Risk Profiles and Charge Card activities.

The Assurance Memorandum consists of two sections:

1. Main Body – Contains the actual assurance statements and executive summaries of any 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 2019, 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**. In addition, 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 2019 Internal Controls Guidance

Internal Control A-123 Application: In FY 2019, DOE will launch a web-based Internal Controls A-123 Application. The A-123 Application will have four modules. The modules are Entity Assessment, Financial Management Assessment, Interim Internal Controls Status, and Risk Profile (future phase). The A-123 Application will have user-friendly characteristics, data edits and validation checks, and a structured, automated workflow to support FMA and EA module reviews, approvals, and input. To facilitate a smooth transition from the FMA Tool to the A-123 Application, organizations that participate in DOE's FMA Program will receive an FMA flat file for FY 2019. The FMA flat file reflects the latest FMA Tool provided by organizations in FY 2018. [8] NEW in FY 2019

Financial Management System (FMS) Tab: In FY 2018, FMS owners and users performed FMS evaluations. The FMS worksheet assisted users through the evaluation process and the results were reported in the Entity Assessment Tool. In FY 2019, the FMS worksheet is incorporated in the FMS Evaluation Tab within the Entity Assessment Module of the A-123 Application. Similar to FY 2018, the FMS evaluations are required for both FMS owners and users.

Enterprise Risk Management (ERM): In September 2018, the Secretary designated a new Chief Risk Officer (CRO) for DOE under the Office of the Chief Financial Officer (OCFO). As the Department continues to build an ERM structure, the OCFO will draft a risk scorecard for each Departmental Element. The CRO will brief Senior DOE Leadership on the status of each Departmental Element's risk scorecard. In addition, this year's Risk Profile template will include a numeric rating scale and quantitative calculations to facilitate risk ratings, which will enhance organizations' risk prioritization. For further details, see Appendix A*, Risk Profile Template*

Acquisition-Related Risks: Acquisition-related risks and controls were updated and revised. Organizations should review the updated corporate risk statements and determine if these risks are applicable. For applicable risks, organizations should perform risk assessments and identify local controls to mitigate the new risks. A cross-walk for the updated Acquisition-related corporate risks is located in Appendix E, *Revised Acquisition-related Risk Statements*.

Corporate Controls: DOE will **minimize the use of corporate controls and only have IT-related corporate controls**, to mitigate risks. In the A-123 Application, corporate controls are now local controls for organizations that use the FMA module. When identifying and updating new local controls in the FMA module, organizations should revise the control description, frequency and other data fields in the FMA module to reflect the organization's specific activities. In addition, **the current IT corporate controls reflect the latest version of NIST SP 800-53, Rev 4.** For details, see Table 7: *FY 2019 IT Corporate Controls Update.*

Interim Internal Control Status: Beginning in FY 2018, reporting organizations provided an Interim Internal Control Status Memorandum at mid-year. As a result, in FY 2019 OCFO will no longer conduct mid-year conference calls regarding status updates during the months of April and May with FMFIA points of contacts unless an issue has been identified from an organization's Interim Internal Control Status. For FY 2019 and future reporting, the A-123 Application has incorporated the Interim Internal Control Status (IICS) report within the IICS module.

---

[8] NEW in FY 2019 Major changes are the deployment of the A-123 Application, updates on the Acquisition-related Risks and Assurance Memoranda, and the conversion of corporate controls to local controls.

Assurance Memoranda: The format for Appendix D, *Assurance Memoranda Templates* has changed to merge Operations, Reporting, and Compliance into one section. The Assurance Memoranda also includes additional assurances for the implementation of safeguards and internal controls for inappropriate charge card practices as well as assurances that processes are in place to identify risks and controls to mitigate identified risks. Under Secretaries will provide Assurance Memoranda in FY 2019 and each Under Secretary's Office must identify an Internal Control Point-of-Contact that is responsible for this action. For details, see Appendix D, *Assurance Memoranda Templates*.

Change	Location
• Updated *OMB Circular A-123*	Section I, Page 2
• Updated *Figure 1: DOE Internal Controls Evaluation Framework*	Section I, Page 2
• Updated *Managing Fraud Risks*	Section I, Page 4
• Updated *New in FY 2019*	Section I, Page 5
• Updated *Table 1: Listing of Required Internal Control and Risk Profile Evaluations by Organization*	Section I, Page 6
• Updated *Table 2: DOE Internal Controls and Risk Profile Process Important Dates*	Section I, Page 8
• Updated *Table 3: Reporting Documentation Transmittal Methods*	Section I, Page 9
• Updated *Requirements for FY 2019*	Section IV, Page 12
• Updated *Non-Financial Internal Controls Evaluation*	Section V, Page 16
• Updated *Entity Objectives Evaluation*	Section V, Page 17
• Added *Table 7: FY 2019 IT Corporate Controls Update*	Section V, Page 20
• Updated *FMS Evaluation in the EA Module*	Section VI, Page 21
• Updated *Annual Assurance Memorandum*	Section VIII, Page 23
• Updated *Risk Profile Template Guidance*	Appendix A
• To Be Published *A-123 Application User Guide*	Appendix B/C
• Updated *Assurance Memoranda Template*	Appendix D
• Added *Acquisition-related Risks*	Appendix E
• Updated *Financial Management System Evaluations*	Appendix F
• Updated *Glossary of Key Terms*	Appendix G