U.S. DEPARTMENT OF ENERGY

Internal Control Evaluations

Fiscal Year 2017 Guidance

December 2016

Summary of Changes in FY 2017 Internal Controls Guidance

Change	Location
• The FY 2017 guidance is restructured to provide the core requirements in the body of the guidance and moves supporting guidance to user guides and other appendices.	NA
• The introduction discusses overall Enterprise Risk Management in accordance with OMB Circular A-123 revisions.	Section I, Page 1
• The new A-123 requirement to develop a Risk Profile is added.	Section I, Page 3 Section III, Page 7 Appendix A
• The List of *Required Internal Control Evaluations by Departmental Element* is updated and clarified.	Section I, Page 3
• FY 2017 due dates are established.	Section I, Page 5
• Updated FMA Tool includes minor changes and establishes minimum business processes that must be addressed.	Section IV, Page 8 Appendix B
• Updated Focus Area Guidance includes the requirement to test all Focus Area risks, regardless of Exposure Rating or test cycle.	Section IV, Page 10
• Updated Entity Assessment Tool (EAT) directions to simplify and clarify requirements.	Section V, Page 11 Appendix C
• The classification of issues in the EAT and FMS assessment is changed from a 2-category to a 3-category rating system.	EAT, Section V, Pages 12 and 13 FMS, Section VI, Page 15
• Minimum fraud considerations during the entity review and role of the GAO's *Fraud Risk Management Framework* (GAO-15-593SP) are highlighted.	FMA Section V, Page 9 EAT, Section V, Page 13
• Developed and provided Risk Profile Guidance in Appendix A.	Appendix A
• Updated FMA Tool User's Guide is included as Appendix B.	Appendix B
• Updated EAT User's Guide is included as Appendix C.	Appendix C
• Assurance Memorandum formats are included as Appendix D.	Appendix D

Table of Contents

I. Introduction 1

A. Purpose and Background 1

B. OMB Guidance 1

C. GAO Green Book 2

Figure 1: The Components, Objectives, and Organizational Structure of Internal Control 2

D. New in FY 2017 2

E. Key Internal Control and Risk Profile Requirements 3

Table 1: Listing of Required Internal Control and Risk Profile Evaluations by Departmental Element . 3

Figure 2: DOE Internal Controls Evaluation Framework 5

F. Important Dates and Transmittal Methods 5

Table 2: DOE Internal Controls and Risk Profile Process Important Dates 5

Table 3: Reporting Documentation Transmittal Methods 6

II. Documentation Requirements 7

III. Risk Profile 7

IV. Financial Management Assurance (FMA) Evaluation 8

A. FY 2017 FMA Evaluation and FMA Tool Suite Changes 8

B. Requirements for FY 2017 8

Table 4: Sub-Processes for FMA Review and Testing 9

C. Focus Area Guidance 10

D. Consideration of Cognizant Site Reporting 11

V. Entity Evaluation 11

A. Purpose 11

B. FY 2017 EAT Changes 12

C. Non-Financial Internal Control Evaluation 12

D. Entity Objectives Evaluation 13

E. Fraud Considerations in the Entity Review 13

F. Consideration of Cognizant Site Reporting 13

VI. Financial Management Systems (FMS) Evaluation 13

Table 5: DOE Financial Management Systems 14

FMS Evaluation in the FMA Tool 15

FMS Evaluation in the EAT Tool 15

VII. Classifying Deficiencies 16

Table 6: Deficiency Classifications 16
VIII. Annual Assurance Memorandum 17
Figure 3: DOE Assurance Process 18
A. Reporting Documentation and Transmittal Methods 18
B. Format for the Assurance Memorandum 18
C. Determining Issues to be Reported 19

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 its *Standards of Internal Control in the Federal Government* (the 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 the updated Circular A-123. Each organizational element is responsible for establishing, maintaining, and evaluating its system 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 its internal control systems. Internal control systems should allow: 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 ensure reliable financial reporting and to maintain accountability over the assets;
- Evaluate their financial management systems to determine if they comply 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 its internal controls related to operations, reporting, and compliance; materials weaknesses, if any; and whether the agency's financial management systems are in compliance with FFMIA.

B. OMB Guidance

In July 2016, OMB issued Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* that updated guidance for existing internal control and risk management requirements and established the requirement to produce an agency risk profile as part of implementation of an Enterprise Risk Management (ERM) capability coordinated with strategic planning and review and internal control processes.

OMB Circular A-123 requires DOE to:

- Integrate risk management and internal control functions;
- Implement 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;
- Build risk identification capabilities into the framework to identify new/emerging risks or changes in existing risks;
- Develop a Risk Profile, including fraud risk evaluation, coordinated with annual strategic reviews;
- Establish and maintain internal controls to achieve objectives related to operations, reporting and compliance;
- Evaluate effectiveness of DOE internal controls in accordance with the GAO Green Book; and

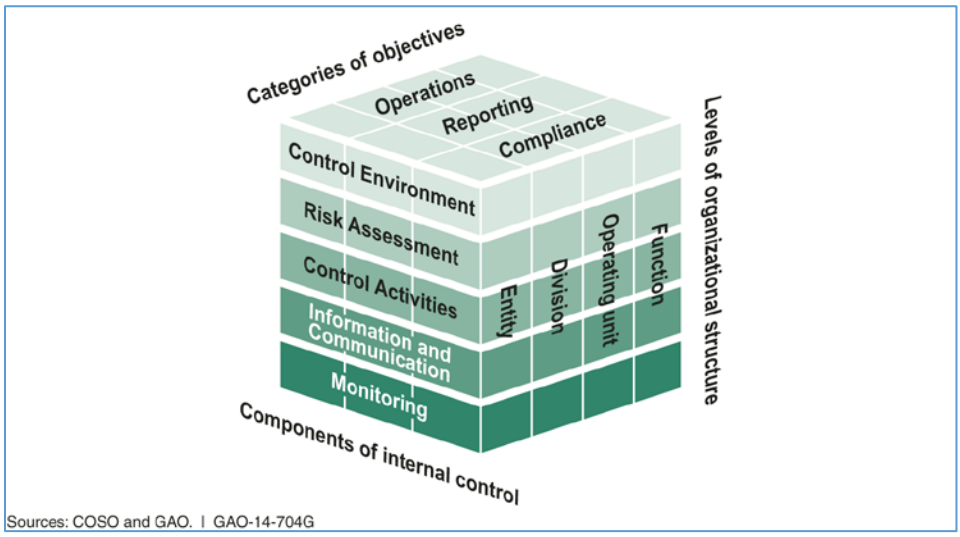
- Report annually on overall adequacy and effectiveness of DOE internal controls related to operations, reporting, and compliance, and compliance of financial management systems with government-wide requirements.

C. GAO Green Book

The GAO Green Book provides criteria for designing, implementing and operating an effective internal control system and establishes standards for internal control which are defined through components and principles. Internal control is a continuous component of an organization's operations that provides reasonable, not absolute, assurance that the organization's objectives related to operations, reporting, and compliance will be achieved.

Using the standards and guidance provided in the Green Book, an organization can design, implement and operate internal controls to achieve its objectives related to operations, reporting and compliance. The five components of internal control are: control environment, risk environment, control activities, information and communication, and monitoring. There are 17 principles which describe the requirements of the components of internal control.

Figure 1: The Components, Objectives, and Organizational Structure of Internal Control



The three categories into which an entity's objectives can be classified are represented by the columns labeled on top of the cube. The five components of internal control are represented by the rows. The organizational structure is represented by the third dimension of the cube. Each component of internal control applies to all three categories of objectives and the organizational structure.

D. New in FY 2017

Internal Control: The FY 2017 Internal Control Evaluation requirements are similar to FY 2016. The Entity Evaluation and accompanying Entity Assessment Tool (EAT) is simplified to focus evaluations only on the component and principle level as compared to reporting at the Attribute level in FY 2016. Also, the Entity Evaluation reintroduces evaluation of 10 entity objectives, including Infrastructure Status, Physical Security, and Safety & Health Posture. Additional information on the EAT is provided in Section V and Appendix C.

ERM Capability: DOE is continuing to implement an ERM capability that includes both internal control and risk management activities. 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.

Risk Profile: OMB Circular A-123 requires agencies to submit a prioritized agency Risk Profile on June 2, 2017. To meet this requirement, all Departmental elements and Under Secretaries are required to submit a prioritized Risk Profile. Headquarters elements and Under Secretaries should include no more than 10 prioritized risks which include consideration of all Risk Profiles submitted by lower level elements. Please 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 2017 internal control testing and included in the FY 2017 assurance statement. Financial risks should be included in the FMA review and reported in the FMA Tool. Non-financial risks are evaluated as part of the Entity Assessment process and reported in the EAT. Non-financial risks should be addressed in the appropriate section of the EAT (e.g., internal control risks assessed as part of the **Internal Control Evaluation** tab; risks that relate to one of the 10 **Entity Objective Evaluation** tab categories would be assessed there). **Note:** the Risk Profile must include an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate identified material fraud risks as appropriate.

Managing Fraud Risks: The revised Circular A-123 states that managers are responsible for determining the extent to which the leading practices in the GAO framework, *Fraud Risk Management Framework* (Framework), are relevant to their 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 Framework. Managers should adhere to these leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. 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.

E. Key Internal Control and Risk Profile Requirements

This guidance provides the FY 2017 internal control and Risk Profile requirements including:

- Risk Profile (new requirement)
- Financial Management Assurance (FMA) Evaluation, including the FMA Tool;
- Entity Evaluation, including the Entity Assessment Tool (EAT);
- Financial Management Systems (FMS) Evaluation; and
- Assurance Memorandum.

Table 1 provides the Internal Control and Risk Profile requirements for each Departmental element.

Table 1: Listing of Required Internal Control and Risk Profile Evaluations by Departmental Element

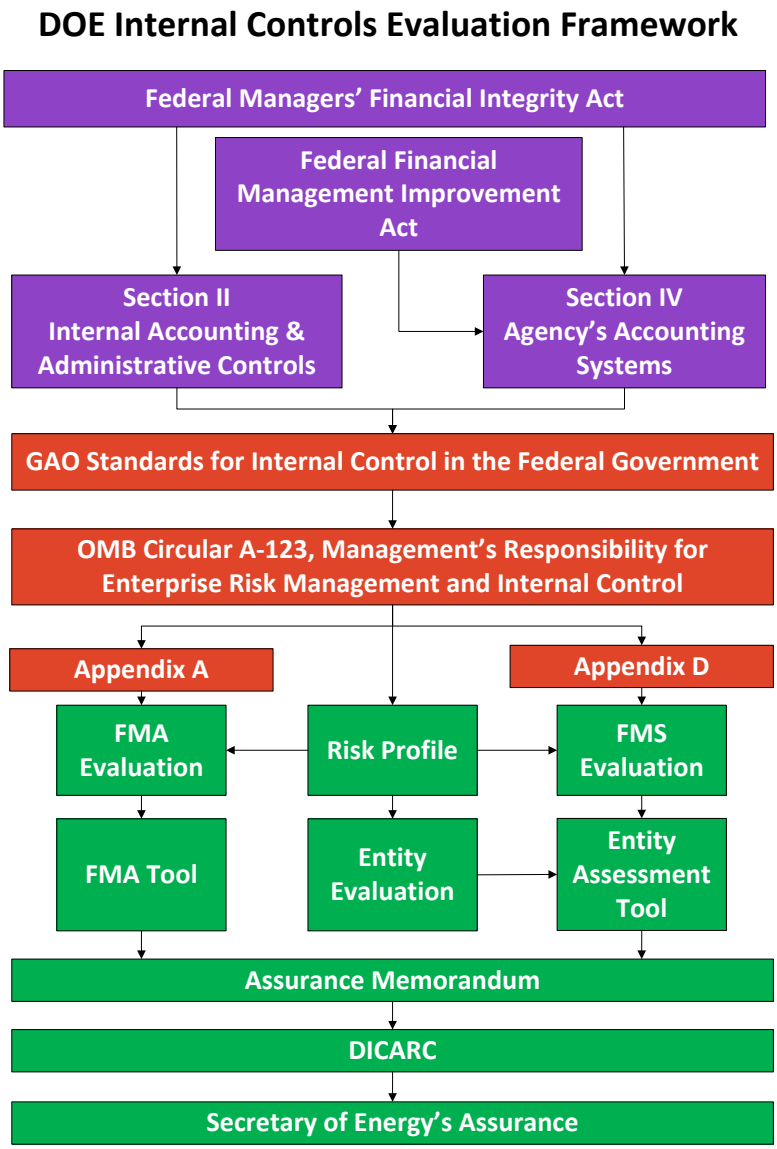
Departmental Element		FMA Evaluation	Entity Evaluation	FMS	Risk Profile
FIELD OFFICES	Bonneville Power Administration	✓	✓	✓	✓
	Chicago Office*	✓	✓		✓
	Consolidated Business Center*	✓	✓		✓
	Golden Field Office*	✓	✓		✓
	Idaho Operations Office*	✓	✓		✓
	National Energy Technology Laboratory	✓	✓		✓
	Oak Ridge Office*	✓	✓	✓	✓
	Richland Operations Office*	✓	✓		✓
	Savannah River Operations Office*	✓	✓		✓
	Southeastern Power Administration	✓	✓	✓	✓
	Southwestern Power Administration	✓	✓	✓	✓
	Strategic Petroleum Reserve Project Management Office*	✓	✓		✓

Departmental Element		FMA Evaluation	Entity Evaluation	FMS	Risk Profile
	Western Area Power Administration	✓	✓	✓	✓
HEADQUARTERS OFFICES	Advanced Research Project Agency–Energy	✓	✓		✓
	Chief Financial Officer	✓	✓	✓	✓
	Chief Information Officer	✓	✓		✓
	Congressional and Intergovernmental Affairs	✓	✓		✓
	Economic Impact and Diversity	✓	✓		✓
	Electricity Delivery and Energy Reliability	✓	✓		✓
	Energy Efficiency and Renewable Energy*	✓	✓		✓
	Energy Information Administration	✓	✓		✓
	Energy Policy and Systems Analysis	✓	✓		✓
	Enterprise Assessments	✓	✓		✓
	Environment, Health, Safety and Security	✓	✓		✓
	Environmental Management*	✓	✓	✓	✓
	Fossil Energy	✓	✓		✓
	General Counsel	✓	✓		✓
	Hearings 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	✓	✓		✓
Independent Agency	FERC	✓	✓	✓	
	(FERC is not required to submit DOE Tools; however, it does conduct evaluations as required by OMB Circular A-123 and reports the results of these evaluations in the FERC Annual Assurance Memo to the Secretary of Energy.)				

** Departmental elements responsible for considering internal control evaluations (FMA, EAT, and Risk Profiles) results of major contractors.*

Figure 2 presents the DOE framework for internal control evaluations. The DOE activities (shown in green) are conducted to meet statutory requirements (shown in purple) and Federal Government guidance (shown in red).

Figure 2: DOE Internal Controls Evaluation Framework



F. Important Dates and Transmittal Methods

Table 2 provides Internal Control Evaluation deadlines. Management quality assurance reviews must be completed before all required submissions.

Table 2: DOE Internal Controls and Risk Profile Process Important Dates

Date	Description
TBD by Cognizant Field Office	Major contractors submit Risk Profile to cognizant Field Office.
TBD by Cognizant HQ Office	Field Offices upload Risk Profile, with consideration of the major contractors under their purview, to the Internal Controls iPortal Space, and to their cognizant HQ Office.
March 31, 2017	All HQ Offices upload Risk Profile, with consideration of their reporting Field Offices as applicable, to the Internal Controls iPortal Space and to their respective Under Secretaries, if applicable.
April 14, 2017	Departmental elements upload interim FMA Tool and FMA Quality Assurance Report to Internal Controls iPortal Space.

Date	Description
April 28, 2017	Under Secretaries submit Risk Profile to the CFO based on the submission of the reporting offices under their purview.
May 15, 2017	Office of Finance & Accounting (OFA) conducts status update (teleconference) to discuss any known preliminary issues in high risk areas or focus areas.
June 2, 2017	Department submits DOE Risk Profile to OMB.
June 30, 2017	Departmental elements performing FMA evaluations complete testing of controls that are required to be tested in the current year.
July 14, 2017	Field Offices and Power Marketing Administrations upload to the Internal Controls iPortal Space: 1. Final FMA Tool 2. FMA Quality Assurance Report 3. Entity Assessment Tool
August 4, 2017	Field Offices and Power Marketing Administrations upload to the Internal Controls iPortal Space: 1. Assurance Memorandum 2. Risk Profile
August 15, 2017	Headquarters Offices upload FMA and Entity Assessment Tools to Internal Controls iPortal Space: 1. Final FMA Tool 2. FMA Quality Assurance Report 3. Entity Assessment Tool
September 1, 2017	Headquarters Offices upload to the Internal Controls iPortal Space: 1. Assurance Memorandum 2. Risk Profile
October 3, 2017	Organizations that resolve or identify a material weakness, after June 30, 2017, but no later than September 30, 2017, that is not included in a submitted assurance statement, must notify the CFO and update the assurance statement.

Table 3 provides instructions for transmitting required documentation.

Table 3: Reporting Documentation Transmittal Methods

Document	Format	Method	Recipient(s)
Risk Profile Template	Excel File	Electronic Delivery & Upload to iPortal	Field Office to: Lead Program Secretarial Office Headquarters to: Appropriate Under Secretary Internal Controls Space on iPortal
FMA Tool and FMA QA Report	Excel File / Tool	Upload to iPortal	Internal Controls Space on iPortal
Entity Assessment Tool (EAT)	Excel File / Tool	Upload to iPortal	Internal Controls Space on iPortal
Assurance Memorandum (Including Corrective Action Plan Summary)	Signed PDF	Electronic Delivery & Upload to iPortal	Field Office Assurance Memorandum addressed To: Lead Program Secretarial Office with copies to the Cognizant Secretarial Office(s). Internal Controls Space on iPortal
	Signed PDF	Electronic Delivery & Upload to iPortal	Headquarters Assurance Memorandum addressed To: The Secretary Through: Appropriate Under Secretary Internal Controls Space on iPortal

Please note that the Federal staff field locations will be responsible for uploading files for its contractors.

II. Documentation Requirements

All Departmental elements are required to maintain written policies and procedures for implementing the internal controls evaluations process described in this guidance. These policies and procedures must include a quality assurance (QA) program conducted by DOE field offices on submissions by their respective major contractors to ensure quality and accuracy. Documentation supporting internal control evaluations and results must be maintained and provided if requested by CFO, senior managers, or auditors.

Examples include:

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

III. Risk Profile

OMB Circular A-123 requires each agency to submit a prioritized Risk Profile on June 2, 2017, identifying the most significant risks to achieving agency strategic objectives and the appropriate options for addressing the significant risks. These risks are to be analyzed 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 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.

To meet this OMB requirement, major contractors must submit a Risk Profile in accordance with the guidance in Appendix A, Risk Profile Template, identifying their most significant risks, to their cognizant Field Office. Field Offices, taking into consideration the major contractors under their purview, must submit a Risk Profile identifying their most significant risks, to the CFO via the iPortal and to the responsible HQ Office in accordance with due dates established by their cognizant HQ Office.

Each Headquarters Office and Under Secretary must prepare a Risk Profile identifying no more than 10 of its most significant risks. Each lower-level organizational element will produce its Risk Profile and submit it to its 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 to be submitted to OMB on June 2, 2017.

Risk Profiles will be formally updated and submitted on an annual basis.

Appendix A, Risk Profile Template, provides the Risk Profile template and detailed instructions for developing the Risk Profile.

<u>Risk Profile FMA and EAT Reporting</u>

Risk Profile financial risks must be documented and evaluated, including establishment and testing of controls when applicable, in the **FMA Tool.**

Risk Profile non-financial risks are evaluated, including establishment and testing of controls when applicable, as part of the Entity Assessment process and reported in the appropriate section of the EAT (e.g., internal control risks assessed as part of the **Internal Control Evaluation** tab; risks that relate to one of the 10 **Entity Objective Evaluation** tab categories would be assessed there).

Fraud Considerations in the 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 material fraud risks are identified, then the entity must design and implement internal controls, and testing of those controls, to mitigate those risks. At a minimum, entities must consider:

- types of fraud that can occur within the entity (fraudulent financial reporting, misappropriation of assets, corruption, etc.);
- presence of fraud risk factors (pressure/incentive, opportunity, and attitude/rationalization);
- sufficiency of the entity's responses to identified fraud risks;
- potential for management override; and
- presence of sufficient segregation of duties.

IV. Financial Management Assurance (FMA) Evaluation

The FMA Tool is the central repository for documenting the evaluation of the relevant financial processes, sub-processes, and risks facing each reporting entity, as well as the key controls for each process that are relied upon to mitigate risks. Reporting entities are not required to submit supplemental documentation to support the FMA Evaluation. Reporting entities, however, must reference in Column BL of the Assessment tab the documents that support the identification of the controls and verification of the applicability of the standard process, sub-process, and corporate risks to the site. Such documents may include process mapping, risk analyses, test plans, test results.

A. FY 2017 FMA Evaluation and FMA Tool Suite Changes

FMA Evaluation: Focus Area risks are now required to be evaluated and tested regardless of Risk Exposure rating or test cycle.

There were several minor changes to the FMA Tool, including:

- Revised Inventory Management process risk statements.
- Updated designations for **Type of Risk** in **Column Q** of the **Assessment** tab to identify Corporate Risks that also include the potential for fraud (F) and improper payments (I), or both (A).
- Updated material in the FAQ tab.

There were also two minor changes made to the URT Tool's Quality Assurance Report, including:

- Revised QA Report, Tab 5, **Ctl Ratings**, to include controls that were not tested.
- Revised QA Report, Tab 8, **FY Scope Table**, to include a **Comments** column, where sites will explain why certain controls that were in scope for this year, were not tested.

B. Requirements for FY 2017

In FY 2017, Departmental elements must perform, at a minimum, the following steps:

1. Re-assess risks and adjust Risk Exposure Ratings in the FMA Tool accordingly. Each Departmental element 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 impact its risk ratings. If so, mark the appropriate column in the **Assessment** tab (AJ – AN), and test the controls related to those risks. Note: the annual risk re-evaluation could result in determination that certain risk exposure ratings can be lowered because of program changes, including fewer transactions or lower dollar amounts.

2. To ensure consistency, all Departmental elements must evaluate risks and test controls for the processes/sub-processes identified below in Table 4. If those processes/sub-processes have not already been selected by your organization, they must be added to the FMA Tool in the **Assessment** tab, **Manage** icon at the top, **Manage Framework**, **Add Sub-Process**. If specific risks do not apply, please provide a brief rationale in **Column AV** in the **Assessment** tab. For more information, see the FMA Tool User Guide, Appendix B.

Table 4: Sub-Processes for FMA Review and Testing

Process	Sub-process
Funds Distribution	Budget Formulation
	Budget Generation
	Funds Distribution
	Funds 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

3. **Fraud Consideration in the FMA Review:** Effective fraud risk management ensures that taxpayer dollars and government services serve their intended purposes.

   In their FMA Evaluations, sites will consider the potential for fraud when identifying, analyzing, and responding to risks. Additionally, entities will design and implement controls to mitigate assessed fraud risks and ensure the controls are operating effectively. In accordance with the GAO *Fraud Risk Management 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.

4. Test all applicable controls indicated by an "X" in **Column G, Current Year Controls**, of the FMA Tool no later than June 30, 2017. Also test all controls that are overdue for testing indicated by the red cell color in **Columns G and H**.
5. Complete testing and other required actions to address the FY17 focus area risks and document the actions taken in the Focus Area tab of the FMA Tool. Section C, Focus Area Guidance, below, provides additional information on focus areas and assessment requirements.
6. A Corrective Action Plan (CAP) must developed for each remediation area identified in testing. 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. Departmental elements must report the root cause in the **Action Tracking** tab FMA Tool in **Column O**.

At a minimum, a CAP will contain the following key elements:

- summary of the control deficiency;
- summary of remediation activities;
- process or sub-processes affected;
- date identified;
- exposure and combined risk assessment;
- remediation target (e.g., training, system, organization);
- accountable individual; and
- status.

Significant CAP information is summarized in the **Action Tracking** tab of the FMA Tool. Departmental elements maintain the CAPs and are not required to submit CAP documentation unless requested by CFO.

For more information on CAPs, see the FMA Tool User Guide, Appendix B. Also, a CAP template is provided on the Internal Controls iPortal space under the Resources tab.

7. Run the FMA Quality Assurance (QA) Report to ensure all fields are completed properly. The resulting QA Report must be submitted with the FMA Tool. Each Departmental element will resolve QA Report exceptions before QA Report submission to CFO. The QA Report is only a portion of the QA program and senior management is also responsible for ensuring that risk assessments, test plans, sample sizes, and final results comply with DOE guidance. Departmental elements establish and document their QA process and results.

   For more information on the QA Report, see the FMA Tool User Guide, Appendix B.

C. 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.

There are no changes to the FY 2017 Focus Areas. There are 28 FMA Focus Area risks for the following business processes that must be evaluated and tested by all Departmental elements in FY 2017 **regardless of the risk rating or test cycle**. The Focus Area processes and risks include:

FY 2017 Focus Areas
Cost Management
• Cost Accrual-Variance with actuals (CR1411)
Acquisition Management
• Contract Solicitation, Award, and Adjustment-Competitive process not followed (CR2106)
• Contract Solicitation, Award, and Adjustment-Small Business (CR2108)
• Contract Solicitation, Award, and Adjustment-Inadequate Cost Analysis (CR2115)
• Contract Closeout-Improper/untimely closeout (CR2119)
• Contract Closeout- Improper/untimely Deobligations (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)

FY 2017 Focus Areas
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 remed. (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)
Improper Payments • SPC: Payment Disbursing-Incorrect implementation of OMB requirements (CR6601)

The Focus Areas are managed through the **Focus Area** tab in the FMA Tool. This tab includes all Corporate Risks that have been designated as Focus Area risks that are applicable to each site. In addition, for each Focus Area risk, the **Description/Actions Required** column provides information on what actions are to be taken in FY 2017, as well as an explanation why a particular area was selected**.**

D. Consideration of Cognizant Site Reporting

In conducting and reporting on FMA evaluations, all Headquarters Offices with Field organizations must consider the results of their Field element evaluations as part of their evaluation. Likewise, Field sites with major contractors, must consider the results of the contractor evaluations as part of their evaluation.

V. Entity Evaluation

A. Purpose

The purpose of the Entity Evaluation is to conduct structured self-evaluations to provide reasonable assurance that non-financial control systems are designed and implemented and operating effectively to mitigate risk and ensure mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulation.

There are two major goals in the Entity Evaluation. The first is to assess the status of your entity's internal controls. The second is to evaluate each of your entity's objectives (functions, missions, activities) to determine if there are issues that need to be addressed to help ensure objectives are met.

B. FY 2017 EAT Changes

EAT changes include:

- Simplified Internal Control evaluation that is now conducted at the Principle level rather than the Attribute level.
- Renamed Entity Evaluation tab to **Internal Control Evaluation** tab.
- Added **Designed and Implemented** column to the **Internal Control Evaluation** tab with entry choices of "Yes" or "No."
- Renamed Summary Evaluation tab to **IC Summary Evaluation** which is primarily populated from input provided in the **Internal Control Evaluation** tab.
- Renamed Action Tracking tab to **IC Action Tracking**.
- Removed Impact Assessment tab.
- Added an **Entity Objectives Evaluation** tab.
- Added an **EO Action Tracking** tab.
- Renamed Attributes Supplement tab to **IC Attributes** which lists Green Book Attributes for reference.
- Removed Template Instructions, Risk Profile Template, Risk Profile Definitions, and Risk Profile Ratings Matrix tabs.
- Changed issue rating system from a two-category system to a three-category system.

C. Non-Financial Internal Control Evaluation

In addition to requiring an assessment of financial controls, Section II of FMFIA requires an assessment of non-financial controls to assure their effectiveness and efficiency and compliance with laws and regulations. The revised Green Book has 5 components, 17 principles and 48 attributes to guide the Entity Evaluation. As required last year, all Departmental elements, as shown in Table 1, DOE Internal Controls Evaluation Framework, are required to perform an entity evaluation of the internal controls for non-financial "entity" functions (administrative, operational, and programmatic).

The results of the evaluations are reported in the EAT. There are three tabs in the EAT related to the Internal Control Evaluations. The first tab, **Internal Control Evaluation**, requires an evaluation of your entity's internal control against the Green Book's 5 components and 17 principles. Any issues found in the evaluation are identified and rated as to seriousness on a scale of 1 (least serious)-3 (most serious). Issues rated 2 or 3 require a Corrective Action Plan, and these issues automatically populate in the **IC Action Tracking** tab and require additional information. There is also an **IC Summary Evaluation** tab. This tab summarizes the results of the evaluation reported in the **Internal Control Evaluation** tab and is automatically populated in most categories based on information provided in the **Internal Control Evaluation** tab. There are only two lines on the **IC Summary Evaluation** tab that require user input:

- Excel Line 46 "Are all components operating together in an integrated manner?
- Excel Line 47 "Is the overall system of internal control effective?

For further guidance refer to the EAT User Guide, Section IV.C.

In addition to the 17 Internal Control principles, the EAT will generate additional control objectives for those Departmental elements responsible for performing an FMS Evaluation in accordance with Section IV of FMFIA. This automatic generation will happen if the user indicates responsibility for an FMS Evaluation during the initial setup of the EAT as described in the EAT User Guide, Appendix C. Section D below provides further FMS guidance. (Refer to Table 1, Listing of Required Internal Control Evaluations by Departmental Element, to determine if this requirement applies to your organization.) Details for completing the FMS Evaluation can be found in Section VI and in Appendix C, EAT User Guide.

D. Entity Objectives Evaluation

The second aspect of Entity Evaluation is evaluation of each objective (e.g., functions, missions) in your entity to determine if there are issues that need to be addressed to help ensure the objective is met. This is similar to the EAT evaluation done in FY 2015 and prior years. There are 10 entity objective categories identified in the EAT that need evaluation:

- Workforce Planning
- Systems & IT Posture
- Safety & Health (S&H) Posture
- Security Posture
- Physical Security
- Continuity of Operations
- Segregation of Duties
- Infrastructure Status
- Establishment of Activity-Level Objectives (Entity Missions)
- Environmental

The results of the entity objectives evaluations are reported in two EAT tabs. The results of the evaluation for the ten categories listed above 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 a line in the **EO Action Tracking** tab. In the **EO Action Tracking** tab, complete the information required for each issue.

E. Fraud Considerations in the Entity Review

The GAO *Standards for Internal Control* Principle 8 addresses fraud as an aspect of internal control. Specifically, the entity must consider the potential for fraud when identifying, analyzing, and responding to risks. When addressing this internal control Principle and the 10 entity objectives, organizations should be guided by the GAO *Fraud Risk Management 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.

F. Consideration of Cognizant Site Reporting

In conducting and reporting on entity evaluations, all Headquarters Offices with Field organizations must consider the results of their Field element evaluations as part of their evaluation. Likewise, Field sites with major contractors, must consider the results of the contractor evaluations as part of their evaluation.

VI. Financial Management Systems (FMS) Evaluation

This section is only applicable to those Departmental elements with financial management systems as shown below in Table 5, DOE Financial Management Systems.

Departmental elements with financial management systems in the DOE Financial Management System Inventory must perform the FMS Evaluation to support core requirements of Section IV of FMFIA and the *Federal Financial Management Improvement Act* (FFMIA).

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 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."

Table 5: 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**

In accordance with the FFMIA and OMB Circular A-123, Appendix D guidelines, system owners should determine whether their financial and mixed systems conform to federal financial management systems requirements.

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

1. Consistently, completely, and accurately record and account for federal funds, assets, liabilities, revenues, expenditures, and costs.
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 Tool

Departmental elements with financial systems will select the **Information Technology** sub-processes applicable to their site, evaluate the appropriate risks, and add and test controls. Risks that are rated as "Low Exposure" or "NR" will include an explanation in **Column AV**. Controls mitigating the selected risks will be tested based on the testing cycle shown in the **Scope Columns G through J**.

FMS Evaluation in the EAT Tool

The **Internal Control Evaluation** tab in the EAT provides a uniform Department-wide mechanism for documenting the FMS Evaluation. For each of the Financial Management System Goals listed in the **Internal Control Evaluation** tab, record a basis of evaluation in **Column G, Evaluation Summary**. Please note that the Financial Management Goals are the same as the eight criteria listed above on which test design will be based. For each of the eight Goals, the evaluation summary should briefly describe any type of test or evaluation performed, its general design, and its outcome. If a physical examination of documents was performed, include the titles of the documents in this description.

In implementing the physical examination of documents test technique, managers should consider a variety of existing information at their disposal. 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.

Just as for the evaluation of internal controls, any issues found in the FMS Evaluation will be reported and given 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 severe. Any issues identified in the **Internal Control Evaluation** tab will create a line in the **IC Action Tracking** tab. The user will then, within the **IC Action Tracking** tab, need to complete the needed information required for each issue. Any issues identified with a rating of 2 or 3 require a CAP.

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.

Webinar(s) will be held to provide further details on FMS Evaluations.

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 if they are identified in the organizational Assurance Memorandum as a significant deficiency or material weakness. An entity reportable control deficiency requires qualitative judgment that a significant deficiency exists that could adversely affect the organization's ability to meet its internal control objectives, and an entity material weakness is a significant deficiency which the head of the Departmental element determines to be significant enough to report outside of their organization. The information gathered and the decisions made related to the above considerations will be documented.

Table 6: 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 allow management or personnel, in the normal course of performing their 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, EAT, FMS	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, EAT	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.	FMA, EAT	Yes

Deficiency Title	Definition	Applicable to	Reported in Assurance Memorandum
	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 EAT defines the criteria against which conformance is evaluated and captures identified non-conformances.	FMS	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, EAT, FMS	Yes

VIII. Annual Assurance Memorandum

Each Departmental element is required to submit an annual Assurance Memorandum that documents the results of its annual FMA Evaluation, Entity Evaluation, or FMS Evaluation, as well as any other reviews conducted. The Assurance Memorandum provides a status of the overall adequacy of and effectiveness and efficiency of the element's internal controls. The Assurance Memorandum must identify significant deficiencies or material weaknesses which might qualify that assurance, as defined in Section VII.C, Determining Issues to Be Reported, and will be accompanied by a summary of the corrective action plans developed to address such issues.

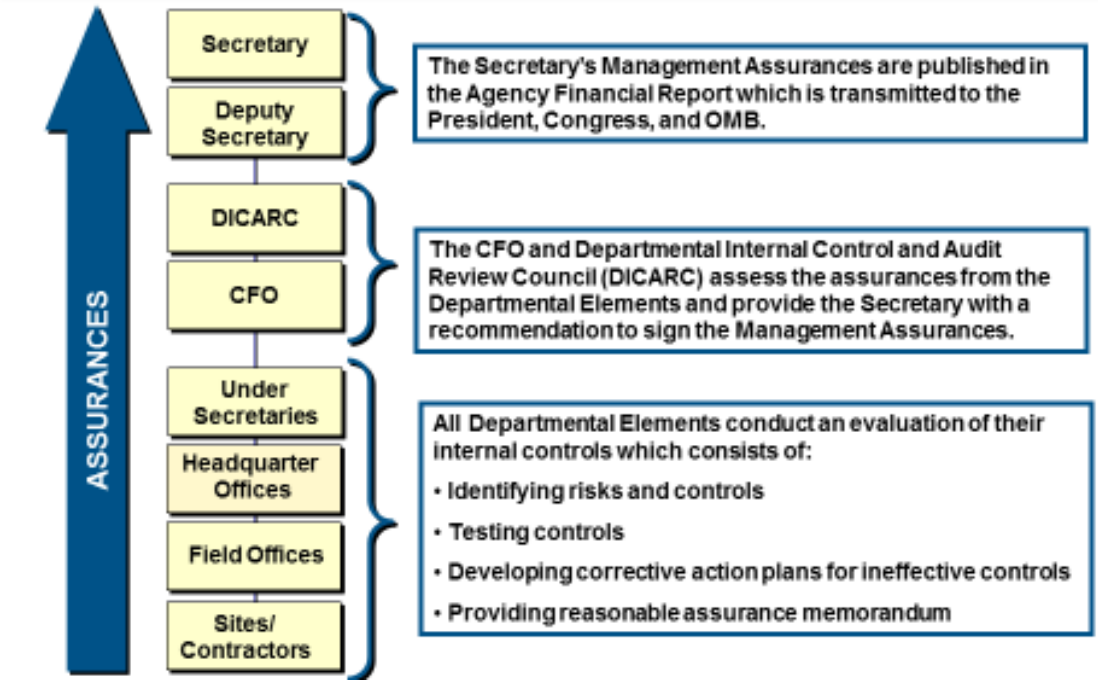
CFO will conduct a mid-year update in mid-May with FMFIA points of contact for each reporting entity to identify potential significant deficiencies or material weaknesses identified during the internal controls evaluation process that may be reported in the entity's Assurance Memorandum, if it is anticipated that the issue may not be fully remediated by the end of the fiscal year.

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

- If a significant deficiency or material weakness is discovered by June 30, but corrected by September 30, a statement will be included identifying the significant deficiency or material weakness, the corrective action taken, and that it has been resolved by September 30.
- If a significant deficiency or material weakness is discovered after June 30, but before September 30, the statement identifying the significant deficiency or material weaknesses will be updated to include the subsequently identified significant deficiency or material weakness.

Organizations will notify CFO immediately of any resolved or new significant deficiencies or material weaknesses not later than October 3, 2017, per Table 2, DOE Internal Controls and ERM Process Important Dates.

Figure 3: DOE Assurance Process



A. Reporting Documentation and Transmittal Methods

Each Departmental element must provide an Assurance Memorandum and other documents or files as required in Table 3, Reporting Documentation Transmittal Methods.

B. Format for the Assurance Memorandum

Appendix D provides separate templates for Field Offices and for Headquarters Offices to use in preparation of the Assurance Memorandum.

The Assurance Memorandum consists of two sections:

1. The Main Body – Contains the actual assurance statement and executive summaries of any significant deficiencies or material weakness.
2. The CAP Summary – Lists action plans 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 those that will be implemented in the next fiscal year.

   The CAP Summary includes:

   (a) New Issues and Action Plans; and
   (b) Action Plans from prior-year reporting (may be open or closed). For action plans remediating deficiencies reported in previous years closed in FY 2017, 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 Departmental element. Therefore, the **Assurance Memorandum must be signed by the head of the Departmental element**, and for all

Headquarters-level entities that report to an Under Secretary, the Assurance Memorandum also must be signed by the respective Under Secretary.

C. Determining Issues to be Reported

Control deficiencies that meet certain criteria must be reported in the Assurance Memorandum. Table 6, Deficiency Classifications provides a description of the issues to be reported for each section of the Assurance Memorandum, a definition for each issue, and an indication of which issues will be reported in the Assurance Memorandum with corrective action plan.