

U.S. DEPARTMENT OF ENERGY

Internal Control Evaluations

Fiscal Year 2018 Guidance



December 2017

Summary of Changes in FY 2018 Internal Controls Guidance

Change	Location
<ul style="list-style-type: none"> • Added <i>Managing Fraud Risks</i> 	Section I, Page 2
<ul style="list-style-type: none"> • Updated <i>New in FY 2018</i> 	Section I, Page 3
<ul style="list-style-type: none"> • Updated <i>Table 1: Listing of Required Internal Control and Risk Profile Evaluations by Departmental Element</i> 	Section I, Page 4
<ul style="list-style-type: none"> • Updated <i>Table 2: DOE Internal Controls and Risk Profile Process Important Dates</i> 	Section I, Page 6
<ul style="list-style-type: none"> • Updated Documentation Requirements 	Section II, Page 7
<ul style="list-style-type: none"> • Deleted FY 2017 FMA Evaluation and FMA Tool Suite Changes 	Section IV, Page 8
<ul style="list-style-type: none"> • Updated <i>Table 4: Sub-Processes for FMA Review and Testing</i> 	Section IV, Page 10
<ul style="list-style-type: none"> • Updated <i>Focus Area Guidance</i> 	Section IV, Page 11
<ul style="list-style-type: none"> • Updated <i>FY 2018 EAT Changes</i> 	Section V, Page 13
<ul style="list-style-type: none"> • Updated <i>Entity Objectives Evaluation</i> 	Section V, Page 14
<ul style="list-style-type: none"> • Updated <i>Fraud Consideration in the Entity Review</i> 	Section V, Page 15
<ul style="list-style-type: none"> • Updated <i>Table 7: Deficiency Classifications</i> 	Section VII, Page 18
<ul style="list-style-type: none"> • Added Interim Assurance Status Memorandum 	Appendix E
<ul style="list-style-type: none"> • Added Financial Management System Worksheet 	Appendix F
<ul style="list-style-type: none"> • Added Glossary 	Appendix G

Table of Contents

I. Introduction	1
A. Purpose and Background	1
B. OMB Circular A-123	1
C. GAO Standards for Internal Control	2
<i>Figure 1: The Components, Objectives, and Organizational Structure of Internal Control</i>	2
D. Managing Fraud Risks	2
E. New in FY 2018	3
F. Key Internal Control and Risk Profile Requirements	3
<i>Table 1: Listing of Required Internal Control and Risk Profile Evaluations by Departmental Element</i> ..	4
<i>Figure 2: DOE Internal Controls Evaluation Framework</i>	5
G. Important Dates and Transmittal Methods	6
<i>Table 2: DOE Internal Controls and Risk Profile Process Important Dates</i>	6
<i>Table 3: Reporting Documentation Transmittal Methods</i>	6
II. Documentation Requirements	7
III. Risk Profile	8
IV. Financial Management Assurance (FMA) Evaluation	9
A. Requirements for FY 2018	9
<i>Table 4: Sub-Processes for FMA Review and Testing</i>	10
B. Focus Area Guidance	11
<i>Table 5: FY 2018 Focus Areas</i>	11
C. Consideration of Cognizant Site Reporting	12
V. Entity Evaluation	13
A. Purpose	13
B. FY 2018 Entity Assessment Tool (EAT) Changes	13
C. Non-Financial Internal Controls Evaluation	13
D. Entity Objectives Evaluation	14
E. Fraud Considerations in the Entity Review	14
F. Consideration of Cognizant Site Reporting	15
VI. Financial Management Systems (FMS) Evaluation	15
<i>Table 6: DOE Financial Management Systems</i>	15
FMS Evaluation in the FMA Tool	16
FMS Evaluation in the EAT	16

VII. Classifying Deficiencies	17
<i>Table 7: Deficiency Classifications</i>	18
VIII. Annual Assurance Memorandum	19
<i>Figure 3: DOE Assurance Process</i>	19
A. Reporting Documentation and Transmittal Methods	20
B. Format for the Assurance Memorandum	20
C. Determining Issues to be Reported	20

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 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 the updated OMB 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 Circular A-123

In FY 2018, DOE will continue to follow OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, which provides guidance for internal control and risk management requirements and established 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 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

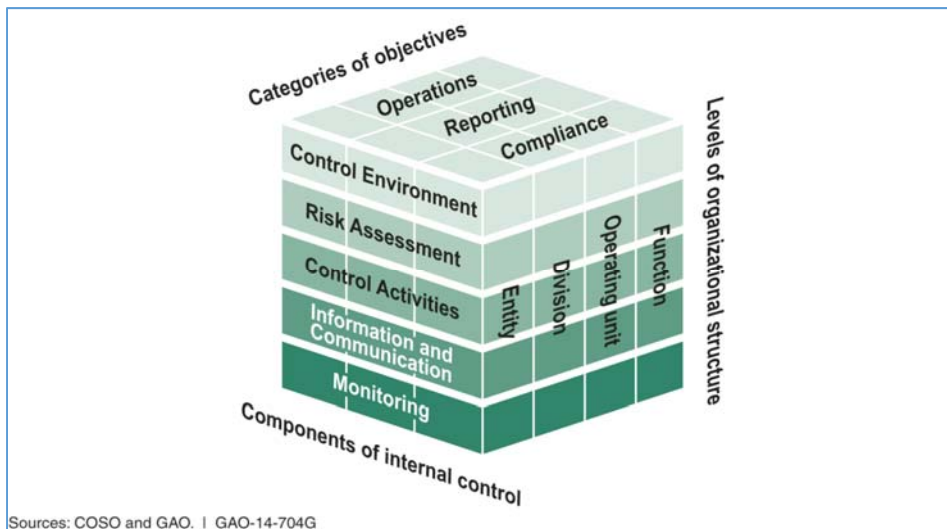
- Report annually on overall adequacy and effectiveness of DOE internal controls related to operations, reporting, and compliance, and compliance of financial management systems with government-wide requirements.

C. GAO 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 establishes standards for internal control which are defined through components and principles. Internal control in an organization 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 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 1: The Components, Objectives, and Organizational Structure of Internal Control



Sources: COSO and GAO. | GAO-14-704G

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. 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 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 its Fraud 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. New in FY 2018

Internal Control: The FY 2018 Internal Control Evaluation requirements are similar to FY 2017. The Entity Evaluation and accompanying Entity Assessment Tool (EAT) continues to focus evaluations at the component and principle level as well as evaluations of 10 entity objectives. However, *Workforce Planning* and *Project Cost Management* entity objectives have been removed because they may be addressed in the Internal Control principles, and two new entity objectives have been added, *Fraud Prevention* and *Contractor/Subcontractor Oversight* to emphasize fraud prevention activities.

Also new this year, several smaller headquarters elements (smaller staff, budget and risk) will no longer be required to document their evaluation results in the Financial Management Assurance (FMA) tool. These offices will instead document their internal control evaluation results within the EAT and therefore must evaluate five additional entity objectives within the EAT in place of the FMA tool - *Funds Management, Acquisition Management, Payables Management, Travel Administration, and Payroll Administration*. These five new additional entity objectives will only appear in the EATs for identified smaller headquarters elements. Additional information on the EAT is provided in [Section V](#) and Appendix C.

Fraud: In FY 2018, additional emphasis has been placed on fraud prevention in the EAT and FMA Tool to further increase fraud prevention activities across the Department. Departmental elements must identify their top financial and non-financial fraud risks in both their FY 2018 Risk Profile and the **Entity Objectives Evaluation** worksheet of the EAT in the new *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 that are related to fraud risks in its FMA Tool should consider that deficiency when assessing principle 8 and the Fraud Prevention entity objective within the **Internal Control Evaluation** and **Entity Objective Evaluation** worksheets in the EAT. Similarly, organizations that identify fraud-related issues in their assessment of the Contractor/Subcontractor entity objective should consider these issues when addressing the Contractor Oversight focus area risks in the FMA Tool.

In addition, the following changes are implemented in FY 2018:

- In the FMA Tool, focus area risks reflect increased emphasis across the Department in the *Acquisition Management* and *Contractor Oversight* business processes. Focus area risks that have experienced improvement across the Department are no longer included as focus areas.
- Departmental elements are no longer required to provide an interim FMA submission. However, in lieu of a FMA submission, Departmental elements are required to provide an interim assurance status memorandum (Appendix E).
- Performance of Financial Management Systems (FMS) evaluations in the EAT have been expanded to include additional entities. Impacted entities will receive an EAT populated with the eight FMS goals. Entities have also been provided a *FMS Evaluation Worksheet* (Appendix F), which will assist Departmental elements in conducting their risk assessment and evaluations to determine compliance with the Federal Financial Management Improvement Act (FFMIA).
- In the Risk Profile, all Departmental elements must also identify their top financial and non-financial fraud risks in FY 2018. These two new fraud risk statements must be included in your entity's Risk Profile submission along with other identified significant risks. Regardless of the residual risk rating, the top financial and non-financial fraud risks must be identified and included in the FY 2018 Risk Profile submission.

F. Key Internal Control and Risk Profile Requirements

This guidance provides the FY 2018 internal control and Risk Profile requirements including:

- Risk Profiles;
- Financial Management Assurance (FMA) Evaluations, including the FMA Tool;
- Entity Evaluations, including the Entity Assessment Tool (EAT);
- Financial Management Systems (FMS) Evaluations; and
- Assurance Memoranda.

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	Chicago Office*	✓	✓	✓	✓
	EM Consolidated Business Center*	✓	✓	✓	✓
	Golden Field Office*	✓	✓	✓	✓
	Idaho Operations Office*	✓	✓	✓	✓
	National Energy Technology Laboratory	✓	✓	✓	✓
	NNSA Albuquerque Complex*	✓	✓	✓	✓
	Oak Ridge Office*	✓	✓	✓	✓
	Oak Ridge Environmental Management*	✓	✓	✓	✓
	Richland Operations Office*	✓	✓	✓	✓
	Savannah River Operations Office*	✓	✓	✓	✓
	Strategic Petroleum Reserve Project Management Office*	✓	✓	✓	✓
POWER MARKETING ADMINISTRATIONS	Bonneville Power Administration	✓	✓	✓	✓
	Southeastern Power Administration	✓	✓	✓	✓
	Southwestern Power Administration	✓	✓	✓	✓
	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**		✓		✓	

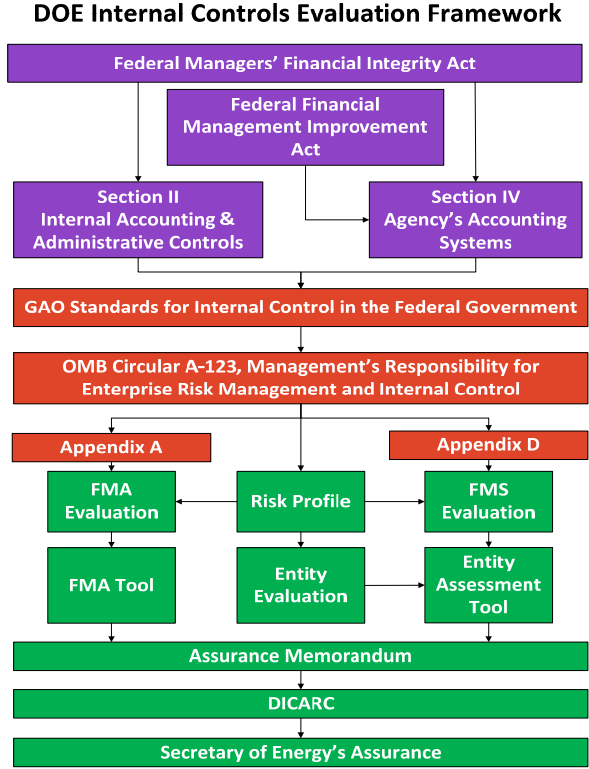
Departmental Element	FMA Evaluation	Entity Evaluation	FMS	Risk Profile
Legacy Management	✓	✓	✓	✓
Loan Programs Office	✓	✓	✓	✓
Management	✓	✓	✓	✓
National Nuclear Security Administration*	✓	✓	✓	✓
Nuclear Energy*	✓	✓	✓	✓
International Affairs**		✓		✓
Project Management Oversight and Assessment	✓	✓	✓	✓
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 evaluation (FMA, EAT, and Risk Profiles) results of major contractors.

** Departmental elements must complete the 5 additional entity objectives in the EAT.

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



G. 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.
March 16, 2018	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 30, 2018	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 13, 2018	Departmental elements upload Interim Assurance Status (Appendix E) to Internal Controls iPortal Space.
April 27, 2018	Under Secretaries submit Risk Profile to the CFO based on the submission of the reporting offices under their purview.
April 14, 2018 – May 15, 2018	Office of Finance & Accounting (OFA) conducts status update (teleconference) to discuss any known preliminary issues in high risk areas or focus areas.
June 4, 2018	Department completes DOE Risk Profile as required by OMB.
June 29, 2018	Departmental elements performing FMA evaluations complete testing of controls that are required to be tested in the current year.
July 13, 2018	Field Offices upload to the Internal Controls iPortal Space: <ol style="list-style-type: none"> 1. Final FMA Tool 2. FMA Quality Assurance Report 3. Entity Assessment Tool
August 3, 2018	Field Offices upload their Assurance Memoranda to the Internal Controls iPortal Space.
August 14, 2018	Headquarters Offices and Power Marketing Administrations upload to the Internal Controls iPortal Space: <ol style="list-style-type: none"> 1. Final FMA Tool 2. FMA Quality Assurance Report 3. Entity Assessment Tool
August 31, 2018	Headquarters Offices and Power Marketing Administrations upload their Assurance Memoranda to the Internal Controls iPortal Space.
October 2, 2018	Organizations that resolve or identify a significant deficiency or material weakness, after June 29, 2018, but no later than September 30, 2018, 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
Interim Assurance Status	PDF	Upload to iPortal	Internal Controls Space on iPortal

Document	Format	Method	Recipient(s)
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 and PMAs 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 evaluation process described in this guidance. The level and nature of documentation 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 documentation that is needed. 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 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.

Departmental elements must have vigorous and robust procedures to test the effectiveness of their controls using sampling, re-performance, observation, and inspection. These key procedures should be cited in the EAT and FMA Tool 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 that were originally 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.

The following are examples of test procedures result descriptions that are insufficient to ensure adequate tests are applied: “Walkthroughs”; “Some discussions”; “Reviews of organization charts”; and “Talking to some people, performing some 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 allow an understanding of the test and results.

III. Risk Profile

OMB Circular A-123 requires each agency to prepare an annual prioritized Risk Profile by June 4, 2018, 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, potential outcomes, and prioritizes the results of the analysis.

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

Each Headquarters Office, PMA, 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 4, 2018.

Risk Profiles will be formally updated and prepared on an annual basis in accordance with OMB requirements. 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 2018 internal control testing and included in the FY 2018 assurance statement.

Risk Profile, FMA and EAT Reporting

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

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 **EAT** (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 2018, all Departmental elements must also identify their top financial and non-financial fraud risks in their Risk Profile. These two new fraud risk statements must be included in your entity's Risk Profile submission along with other identified significant risks. Regardless of the residual risk rating, the top financial and non-financial fraud risk need to be identified and included in the FY 2018 Risk Profile submission.

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 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 Assurance (FMA) Evaluation

The FMA Tool 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 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 business process, sub-process, and corporate risks to the entity. Such documents may include process mapping, risk analyses, test plans, and test results.

A. Requirements for FY 2018

In FY 2018, Departmental elements must perform, at a minimum, the following actions:

1. *Re-assess its risks and adjust Risk Exposure Ratings in the FMA Tool* - 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 assessment ratings. If so, entities must mark the appropriate column in the **Assessment** tab (AJ – AN), 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 can be lowered because of program changes, including fewer transactions or lower dollar amounts.
2. *Evaluate risks and test controls for the processes/sub-processes identified below in Table 4* - If these processes/sub-processes have not already been selected by your organization, they must be added to the FMA Tool in the **Assessment** tab, using the **Manage** icon at the top, **Manage Framework, Add Sub-Process**. If the corporate risks for these required business sub-processes do not apply, please provide a brief rationale in **Column AV** in the **Assessment** tab. Before concluding a corporate risk is not relevant to your Departmental element, the risk should be considered at the local or organizational level. If needed, create a local risk for your organization and complete the evaluation and testing of controls associated with the local risk. Departmental Elements are responsible for the risks, and the controls to manage these risks, related to their 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	X	X	
	Budget Generation	X	X	X (CR1204)
	Funds Distribution	X	X	
	Budget Execution	X	X	X
Acquisition Management	Requisitioning	X	X	X
	Receipt of Goods and Services	X	X	X
	Contract Solicitation, Award and Adjustment	X	X	X
	Contract Closeout	X	X	X
	Purchase Card Program Management	X	X	X
Payables Management	Invoice Approval	X	X	X
Travel Administration	Travel Authorization	X	X	X
	Voucher Processing	X	X	X
	Travel Closeout	X	X	X
	Travel Card Program Management	X	X	X
Payroll Administration	Time and Attendance Processing	X	X	X
	Leave Processing	X	X	X

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 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. *Complete Current Year Test Requirements* - Departmental elements must test all applicable controls indicated by an “X” in **Column G, Current Year Controls**, of the FMA Tool no later than June 29, 2018. Entities must also test all controls that are overdue for testing indicated by the red cell color in **Columns G and H**, and identify in the FMA Tool any of its local risks that are suspect to fraud.
 5. *Complete Focus Area Testing and Actions* – Departmental elements must complete testing and other required actions to address the FY 2018 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. *Develop Corrective Action Plans As Applicable* - A Corrective Action Plan (CAP) must be 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, along with other necessary CAP information, in the **Action Tracking** tab of the 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;
- remediation target (e.g., training, system, organization);
- accountable individual; and
- status of the CAP.

Significant CAP information is summarized in the **Action Tracking** tab of the FMA Tool.

Departmental elements are responsible for maintaining their CAPs and are not required to submit CAP documentation unless requested by the OCFO.

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 and Complete other QA Actions* – Departmental elements must run the FMA QA report to ensure all fields are properly completed and submit along with the FMA Tool. Each Departmental element will resolve QA Report exceptions before QA Report submission to the 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 must establish and document their QA process and results. For more information on the QA Report, see the FMA Tool User Guide, Appendix B.

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. For the 29 FMA Focus Area risks, the controls must be evaluated and tested by all Departmental elements in FY 2018 unless the organization has tested the controls within the “last 12 month period”, which is July 1, 2016 – June 30, 2017. For risks that have a low or moderate exposure risk rating, if the controls have been tested within the last 12 month period, then the focus area risk may be assessed by verifying that:

1. The business process has not changed, and
2. There were not any deficiencies during the controls testing.

If the above requirements have been met, the following verbiage will be entered into the Action Taken column 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 assessment was performed on MM/DD/YYYY.” However, if the controls have not been tested within the last 12 month period, then the controls mitigating the focus areas risk will need to be tested **regardless of the risk rating or test cycle**. The Focus Area processes and risks include:

Table 5: FY 2018 Focus Areas

FY 2018 Focus Areas
<p>Acquisition Management</p> <ul style="list-style-type: none"> • 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)

FY 2018 Focus Areas

- 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 incorrect assessed (CR6404)
- Performance-Contractor/Subcontractor performance and billing not monitored (CR6405)

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 2018, as well as an explanation why a particular area was selected.

C. 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 elements' 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 internal 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 2018 Entity Assessment Tool (EAT) Changes

The following changes have been made to the Entity Objectives Evaluation worksheet of the EAT:

- Added new *Fraud Prevention* and *Contractor/Subcontractor Oversight* entity control sub-categories.
- Removed the *Workforce Planning* and *Project Cost Management* entity control sub-categories.
- Added five additional entity objectives, which are *Funds Management*, *Acquisition Management*, *Payables Management*, *Travel Administration*, and *Payroll Administration* to the EAT. These five entity objectives will be completed only by identified organizations (**See Table 1**). If an organization was not previously identified, the five additional entity objectives will not appear in their EAT.

C. 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 their effectiveness and efficiency and compliance with laws and regulations. The Green Book has five components, 17 principles and 48 attributes to guide the Entity Evaluation. As required last year, all Departmental elements, as shown in [Table 1, Listing of Required Internal Control Evaluations by Departmental Element](#), are required to perform an entity evaluation of the internal controls for "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 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 **IC 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. Most categories are populated based on information provided in the **Internal Control Evaluation** tab and 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 please refer to Appendix C, EAT User Guide.

In addition to the 17 Internal Control principles, the EAT will be pre-populated with additional control objectives for those Departmental elements responsible for performing an FMS Evaluation in accordance with Section IV of FMFIA. 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 the Entity 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 ensure the objective is met. There are 10 entity objective categories identified in the EAT that need evaluation by all Departmental elements:

- 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

Reminder: Workforce planning and Project Cost Management have been removed and should be addressed within the **Internal Control Evaluation** tab.

In addition to the entity objectives that are listed above, Departmental elements that have been previously notified and that are identified 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 EAT tabs. The results of the evaluation for the ten (or fifteen for the Departmental elements indicated in Table 1) 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, entities will complete the CAP information required for each issue.

E. 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 further increase fraud prevention activities across the Department, additional emphasis has been placed in this area in the EAT. In the **Entity Objective Evaluation** worksheet, Departmental elements must evaluate the fraud-related entity objectives. In addition, Departmental elements must also identify their top financial and non-financial fraud risks. The top fraud risks identified in a Departmental element’s EAT should be consistent with the fraud risks included in its FY 2018 Risk Profile submission.

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

Departmental elements 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.

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 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. Additionally, 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 should be considered when assessing whether the 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 their 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 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 “NR” must include an accompanying explanation in **Column AV**. Controls mitigating the selected risks will be tested based on the testing cycle shown in the Scope Columns (**Columns G-J**).

FMS Evaluation in the EAT

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, entities will 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 an assessment should be based. For each of the eight goals, the evaluation summary should briefly describe the evaluation performed and the outcome. If a physical examination of documents was performed, 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 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.

Designated Departmental entities and major contractors should use the *FMS Evaluation Worksheet, Appendix F*, to assist with their evaluation in the EAT. The *FMS Evaluation Worksheet* will guide Departmental elements with the evaluation of their organization's achievement of the eight financial management goals by using compliance indicators to assess their risk of non-compliance with the FFMIA on a rating scale from 1 (lowest risk) to 3 (highest risk). For each goal, the risk level rating and the sources used should be documented in the *Internal Controls Evaluation worksheet* along with a summary of the evaluation results for each financial management goal. Departmental elements should also use the *FMS Evaluation Worksheet, Appendix F*, to identify the sources, such as IG/GAO Audits or A-123 Internal Reviews that are used to provide the basis for their organization's assessment. After entities have determined the risk level rating for each goal, the sum of the risk level ratings should be used by entities to determine their 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, any deficiencies or 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 will require a CAP. If there is already an existing CAP for an FMS issue, please indicate this and refer to the existing CAP name and number in Column N, Remediation Strategy, in the Action Tracking tab of the EAT.

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 if they are identified 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 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, should be documented by the entity.

NOTE: Control deficiencies (including significant deficiencies and material weaknesses) must be distinguished from funding and resource issues. Funding levels are not control deficiencies, and therefore, funding and budgetary limitations should not be reported as a significant deficiency or material weakness in the Assurance Memorandum.

Table 7: 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	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>A “No” response on either Line 46 or 47 in the EAT IC Summary Evaluation tab requires a Material Weakness to be reported:</p> <ul style="list-style-type: none"> • Are all components operating together in an integrated manner? or • Is the overall system of internal control effective? 	FMA, EAT	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 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, and if applicable, 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 Departmental element's internal controls. The Assurance Memorandum must identify significant deficiencies or material weaknesses which might qualify that assurance, as defined in [Section VIII.C, Determining Issues to Be Reported](#), and will be accompanied by a summary of the corrective action plans developed to address such issues. Additionally, 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 should be reported in the FY 2018 Assurance Memorandum.

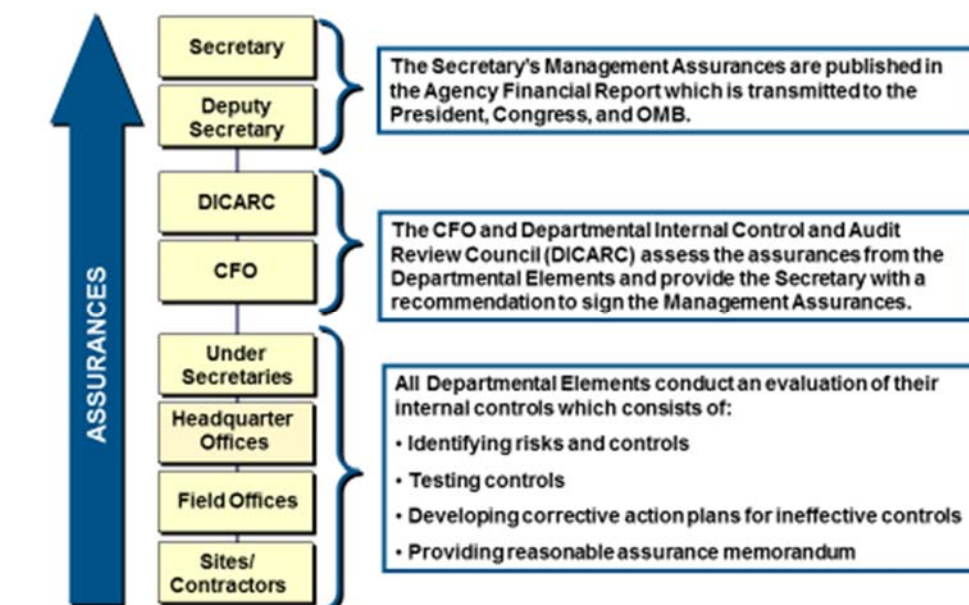
CFO will conduct status updates in mid-April through May with FMFIA points of contact for each reporting entity to identify potential significant deficiencies or material weaknesses identified early during the internal controls evaluation process that may be reported in the entity's Assurance Memorandum.

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 their Assurance 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 2, 2018, 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. Power Marketing Administrations (PMA) should use the Headquarters Office template in FY 2018.

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 that remediate deficiencies reported in previous years and now closed in FY 2018, 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**. Additionally, for all Headquarters-level entities that report to an Under Secretary, the Assurance Memorandum must also 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 7, 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 a corrective action plan.