U.S. DEPARTMENT OF ENERGY

Internal Control Evaluations

Fiscal Year 2016 Guidance

March 4, 2016

Table of Contents

I. Introduction

A. Background

The *Federal Managers' Financial Integrity Act* (FMFIA), requires each agency to establish and maintain internal control systems that allow:

- obligations and costs to be recorded in compliance with applicable laws;
- funds, property, and other assets to be safeguarded; and
- revenues and expenditures applicable to agency operations to be properly recorded and accounted for to permit the preparation of accounts, reliable financial information and statistical reports, and to maintain accountability over the assets.

Section II of FMFIA explains management's role and responsibility in the assessment of accounting and administrative controls, including the evaluation of systems of internal accounting and administrative control to determine such systems' compliance with the requirements of internal controls. On the basis of this evaluation, the Department of Energy (DOE) Secretary annually attests to the Department's controls, established in accordance with standards prescribed by the Governmental Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*.

The Office of Management and Budget (OMB) issued Circular A-123 to provide guidance for agencies to implement internal control programs. Circular A-123 defines internal control as the steps an agency takes to provide reasonable assurance that the agency's objectives are achieved through: (1) effective and efficient operations, (2) reliable reporting, and (3) compliance with applicable laws and regulations. The safeguarding of assets is a subset of all of these objectives. Internal controls should be designed to provide reasonable assurance to prevent or detect unauthorized acquisition, use, and disposition of assets, as well as preventing or detecting fraud, waste, abuse, errors and omissions.

DOE Order 413.1B, *Internal Control Program* requires "heads of Departmental elements . . . [to] evaluate and annually report on the adequacy of their organization's internal controls, including internal controls over financial reporting and if applicable, financial management systems." This guidance provides the methodology that reporting entities, including contractors with management and operating contracts that include the contract clause located in *Title 48 CFR 970.5204-2*, *Laws, Regulations, and DOE Directives* are required to follow.

B. New for FY 2016

This year's guidance includes updates and requirements identified in the 2014 *GAO Standards for Internal Control in the Federal Government* (Green Book) and in the final draft of *OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*. In addition, there are updates to the Financial Management Assurance (FMA) tool and the Entity Assessment Tool (EAT).

Green Book

The Green Book, revised in 2014, is the foundation for OMB Circular A-123 and defines standards through components and principles of internal control that are integral to an entity's internal control system. The standards, components, and principles are discussed in Section III.

OMB Circular A-123

The draft OMB Circular A-123 provides updated guidance to improve accountability and effectiveness of Federal mission-support operations through implementation of Enterprise Risk Management practices and by establishing, maintaining, and assessing internal control. Highlights of the changes included in the Circular are discussed in Section IV.

Financial Management Assessment (FMA) Tool and Entity Assessment Tool Updates

The updated FMA tool allows offices to identify and manage fraud risks as required in the revised OMB guidance. The revised Entity Assessment Tool (EAT) reflects the hierarchical structure of internal controls as identified in the latest Green Book. The new Attributes *Supplement* and *Risk Template* worksheets will assist organizations with their entity assessments. The EAT allows Departmental elements to document the effectiveness of each entity level component, which will assist management in determining the overall assessment of its organization's system of internal control.

C. Purpose

DOE must establish and maintain effective internal controls and financial management systems, must establish an internal control program, and must annually evaluate internal controls and report on the status of any identified material weaknesses to FMFIA, Green Book, and OMB Circular A-123 requirements. To support Departmental reporting, heads of Departmental elements are required to report on the status of their organizations' internal controls, including significant deficiencies (previously reportable conditions) and progress made in correcting prior significant deficiencies. Departmental elements and integrated contractors are required to perform one or more of the following internal controls assessments:

- Financial Management Assurance (FMA) Evaluation;
- Entity Evaluation; and
- Financial Management Systems (FMS) Evaluation.

As discussed in Section XI, *FMS Evaluation,* the FMS evaluation is required of certain Departmental elements as prescribed by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and OMB Circular A-123, Appendix D. Table 1, *Listing of Required Internal Control Evaluations by Departmental Element*, provides a list of required assessments for each Departmental element.

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

Departmental Element		FMA Evaluation	Entity Evaluation	FMS
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*	✓	✓	
	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*	✓	✓	
HEADQUARTERS OFFICES	Energy Information Administration	✓	✓	
	Energy Policy and Systems Analysis	✓	✓	
	Enterprise Assessments	✓		
	Environment, Health, Safety and Security	✓	✓	
	Environmental Management*	✓	✓	✓
	Federal Energy Regulatory Commission		✓	✓
	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	✓	✓	
	Public Affairs	✓	✓	
	Science*	✓	✓	
	Small and Disadvantaged Business Utilization	✓	✓	

** Departmental elements responsible for including internal control evaluations results of Integrated Contractors.*

In addition, all Departmental elements are required to maintain written policies and procedures for implementing the internal control 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 labs for quality and accuracy.

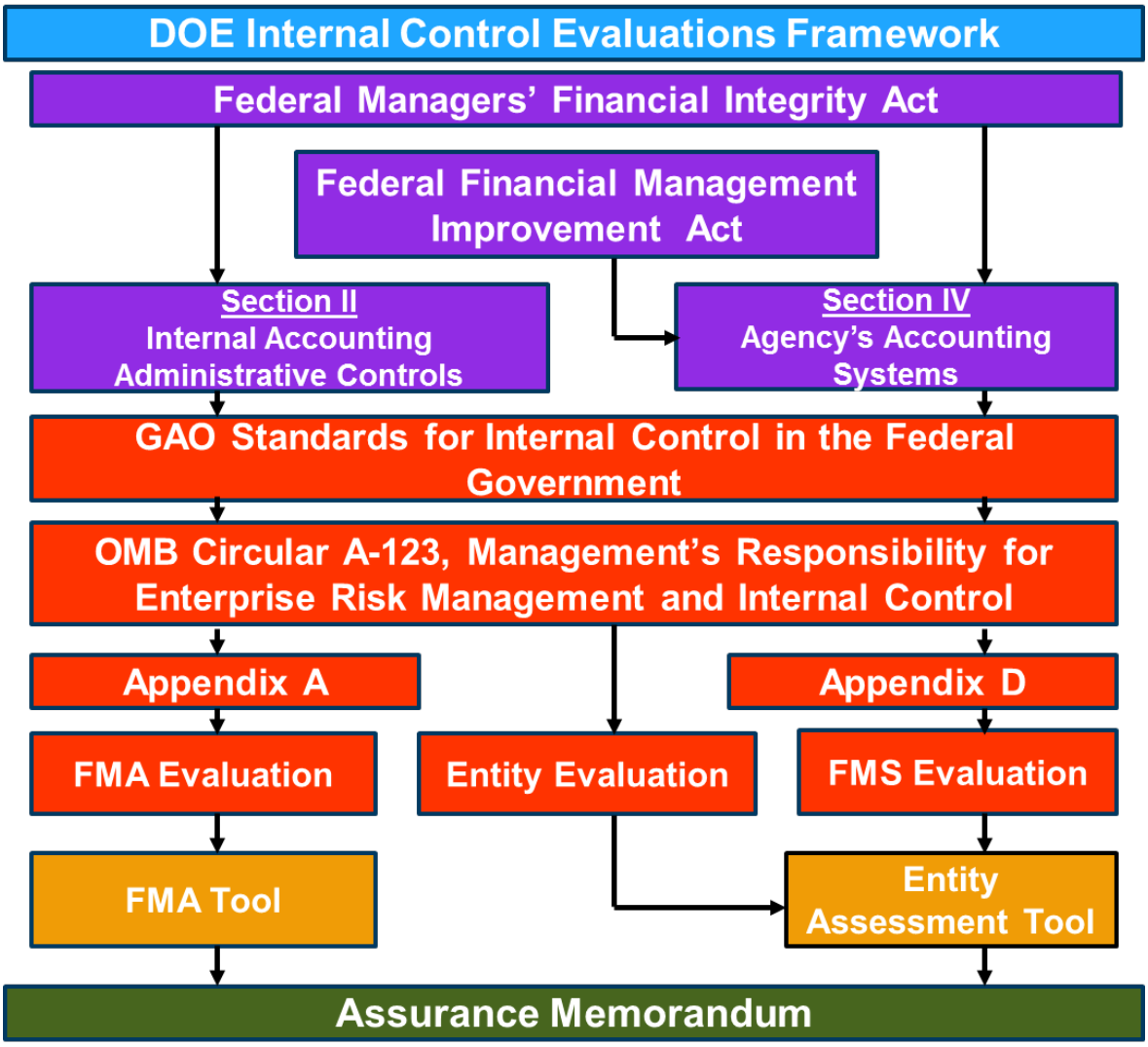
Each Departmental element must perform a QA validation before the submission of quality assurance results to the Office of Financial Policy and Internal Controls (CF-12). Each departmental element is responsible for ensuring that risk assessments, test plans, sample sizes, and documentation of final results are compliant with DOE guidance. Departmental elements should establish and document their QA process and results. The QA process includes an assessment of the contractor internal control procedures and results by the responsible Field Chief Financial Officer.

At the conclusion of the evaluation process, each Departmental element will summarize the results of its internal control evaluations in its annual Assurance Memorandum. Through the Assurance Memorandum, the head of each Departmental element provides reasonable assurance that financial and entity internal controls are working effectively and efficiently, internal and external reporting is accurate, and operations are managed in a manner consistent with applicable laws and regulations. Exceptions to such an assurance are reported as significant deficiencies, material weaknesses, material non-conformances, or scope limitations.

All Field offices must submit their Assurance Memoranda to the appropriate Program Office. Headquarters offices must consider information submitted by their Field offices in developing their Assurance Memoranda. The Assurance Memoranda should be addressed to the Secretary, and submitted to Office of Financial Policy and Internal Controls (CF-12). Field office and Headquarters office consideration of lower level assurances includes determining if a significant deficiency or material weakness reported at the lower level is significant enough to be reported for the higher level organization as a whole. CFO, in conjunction with the Departmental Internal Control and Audit Review Council (DICARC), assesses the assurances made by all the Departmental elements and provides the Secretary with a recommendation to sign the agency's Statement of Assurance. The DOE Statement of Assurance is published in the Department's Agency Financial Report and transmitted to the President, Congress, and OMB.

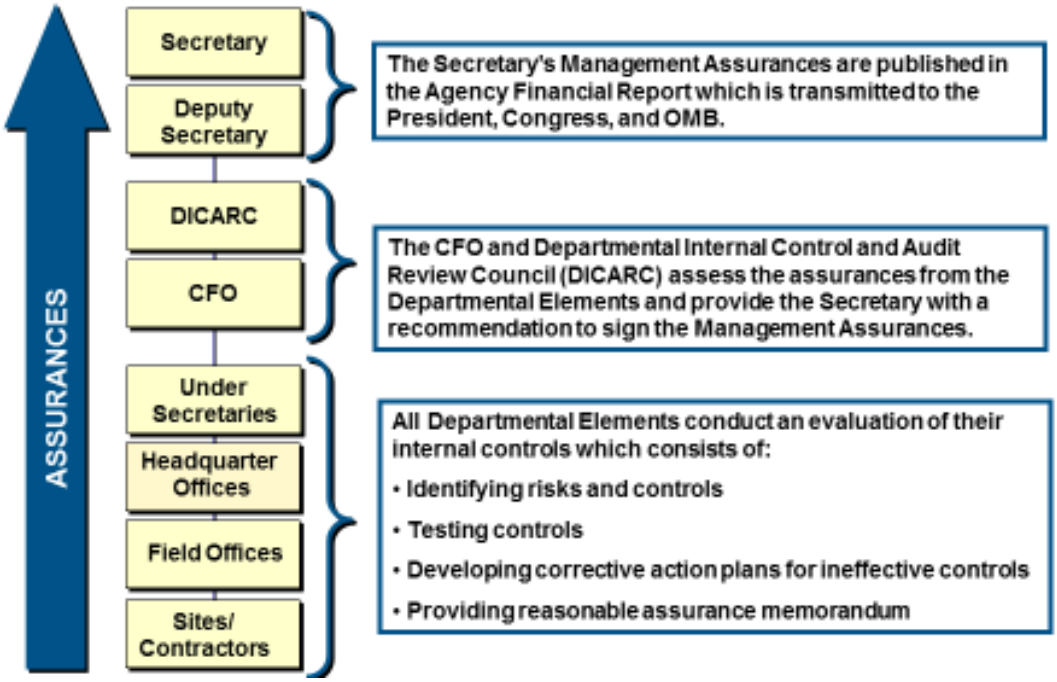
The framework for the DOE Internal Control Evaluation process for each Departmental element, with its legal and regulatory underpinnings, is summarized in Figure 1.

Figure 1: DOE Internal Control Evaluations Framework



The Secretary's Statement of Assurance is supported by assurances from each Departmental Elements as shown in Figure 2.

Figure 2: DOE Assurance Memorandum Process



D. Benefits of Performing Internal Control Evaluations

The evaluation of internal controls can provide significant benefits through risk mitigation, increasing the likelihood of the accomplishment of organizational goals while avoiding unnecessary costs and delays. Thus, an internal control evaluation can show how well risk mitigation strategies are working and which strategies may need improvement. Ultimately, internal control evaluations serve as a tool to gauge the performance of a mission-based area.

II. Important Dates

Table 2 lists deadlines in the Internal Control Evaluations process, including due dates for quarterly and annual reporting requirements. Management quality assurance reviews and testing must be completed before the submission of the quarterly FMA tool and EAT annual report.

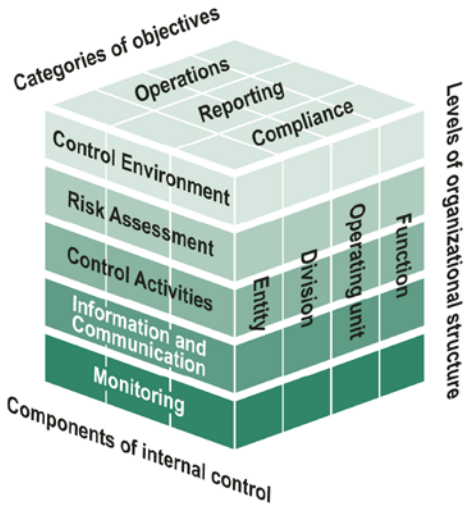
Table 2: DOE Internal Control Evaluations Process Important Dates

Date	Description
April 15, 2016	Upload second quarter FMA tool and FMA Quality Assurance Report to Internal Controls iPortal Space.
April 15, 2016	Entity status update (teleconference) to discuss known preliminary issues in high risk areas or focus areas.
June 30, 2016	Departmental elements performing FMA evaluations complete testing of controls for all High Combined risks identified in the current year assessment scope of the FMA tool, along with controls for all other risks in cycle to be tested in the current year. (See Table 5, *FMA Evaluation Test Cycles,* for requirements)
June 30, 2016	Departmental elements performing FMA evaluations complete corrective actions and re-testing of all controls in remediation.
July 15, 2016	Field offices and Power Marketing Administrations upload third quarter FMA tool, FMA Quality Assurance Report and Entity Assessment Tool to Internal Controls iPortal Space.
August 3, 2016	Field offices and Power Marketing Administrations upload Assurance Memorandum to Internal Controls iPortal Space.
August 15, 2016	Headquarters offices upload FMA and Entity Assessment Tools to Internal Controls iPortal Space.
August 19, 2016	Upload fourth quarter FMA tool and FMA Quality Assurance Report, if warranted. Required only for offices with on-going/incomplete testing on June 30.
September 2, 2016	Headquarters offices upload signed copies of the Assurance Memorandum to Internal Controls iPortal Space.
October 3, 2016	Organizations that resolve or identify a material weakness after June 30, 2016 but by September 30, 2016, that is not included in an assurance statement, must notify CFO and update the assurance statement.

III. GAO Standards for Internal Control in the Federal Government

GAO's *Standards for Internal Control in the Federal Government* outlines a framework for federal agencies to follow in establishing their internal control programs. As shown in Figure 3, GAO identifies five components that "define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency's operations: programmatic, financial, and compliance."

Figure 3: Components, Objectives, and Organizational Structure of Internal Control



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

The five components of internal control are:

Control Environment - The foundation for an internal control system that provides the discipline and structure to help an entity achieve its objectives.

Risk Assessment - Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.

Control Activities - The actions established through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information systems.

Information and Communication - The quality of information used to support the internal control system.

Monitoring - Activities established and operated to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.

These five components represent the highest level of the hierarchy of standards for internal control in the federal government and must operate together in an integrated manner for an internal control system to be effective. There are 17 principles that support the effective design, implementation, and operation of the associated components and represent requirements necessary to establish an effective internal control system.

The five components and the associated 17 principles are shown below:

Table 3: Internal Control Components and Principles

Components	**Principles**
Control Environment	1. Demonstrate Commitment to Integrity and Ethical Values 2. Exercise Oversight Responsibility 3. Establish Structure, Responsibility, and Authority 4. Demonstrate Commitment to Competence 5. Enforce Accountability
Risk Assessment	6. Define Objectives and Risk Tolerances 7. Identify, Analyze, and Respond to Risk 8. Assess Fraud Risk 9. Analyze and Respond to Change
Control Activities	10. Design Control Activities 11. Design Activities for Information Systems 12. Implement Control Activities
Information and Communication	13. Use Quality Information 14. Communicate Internally 15. Communicate Externally
Monitoring	16. Perform Monitoring Activities 17. Remediate Deficiencies

IV. OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Controls

The revised Office of Management and Budget Circular A-123 is effective for FY 2016. Appendix A of the Circular is slated to be updated in FY 2016, with implementation taking place in FY 2017. Below are a few highlights of the changes:

1. Title Change – The A-123 title is now *Management's Responsibility for Enterprise Risk Management and Internal Control* and introduces Enterprise Risk Management guidance, eliminates areas of duplication and balances the emphasis on operations, compliance, and reporting. Departmental elements with external reporting requirements will need to conduct testing on report data and ensure there is a formal management review process for external reports or other externally reported information.

2. Green Book Implementation – This guidance implements the updated *GAO Standards for Internal Control in the Federal Government* and incorporates GAO requirements in the internal controls program.

3. Risk Reporting – The management of risk has to be reviewed and reported annually. The FMA tool has been updated to facilitate the review process. In FY 2017, DOE must submit a risk profile summary with its annual assurance statement.

4. Fraud Risks – DOE must establish internal controls to manage the risk of fraud and include its evaluation and mitigation of fraud risk in the DOE risk profile summary.

5. Root-Cause Analysis – Emphasis on performing a root-cause analysis of deficiencies to ensure corrective action plans address the cause of the problem and not just the symptoms. Provides guidance on activities for corrective actions and plan development for material weaknesses.

6. Reporting Requirements – the term "reportable condition" has been replaced with "significant deficiency." The list of deficiencies has been updated in *Table 10: Definitions of Control of Control Issues.*

V. Focus Areas

The Department identifies annual focus areas for the FMA evaluation process based on repeat audit findings/issues and areas of high risk that represent areas of emphasis that require additional management assessment. Additional focus area guidance is contained in Section IX.E, *FMA Focus Area Guidance*, and Section X, *Entity Evaluation*.

VI. Importance of Risk Assessment in Internal Control Evaluations

Accurate assessments of both financial and non-financial risks are required to perform effective internal control evaluations. Management uses risk assessments to identify which areas pose the highest threat to mission achievement if controls are not in place and functioning properly. Thorough risk assessments should be performed throughout the fiscal year for both financial and non-financial risks.

A. The Risk Assessment Process

Risks are assessed in a three-step process: (1) risk identification, (2) risk rating and (3) risk ranking. Risk assessment is iterative, and should be performed at regular intervals, or incorporated into existing processes, such as a recurring program or project reviews.

1. Risk Identification

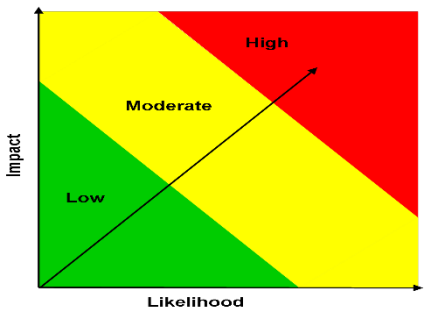
An organization must define its mission-based objectives before conducting a risk assessment and then identify the primary risks facing each objective. Risks also can be identified by considering one or more of the following: key business processes and sub-processes; cross-cutting functions, such as budgeting, human resources, information management, or contract management; or risks pertaining to specific organizational units. Financial and non-financial risks and internal and external factors must be considered during the process. Once identified, risks should be stated in an "if, then" or "cause and effect" format. For example:

- Human Resources - *If* the program does not have a sufficient number of qualified staff and managers available to effectively manage, oversee, and close out its projects, *then* project or program objectives will not be met.
- Contractor Oversight - *If* federal staff is unable to manage issues with contractor or awardee performance, such as performance or quality shortcomings, cost or schedule overruns, or non-compliance with laws and regulations, *then* waste, or abuse of government funds may occur and program objectives will not be met.
- Acquisition or Procurement - *If* a system is not in place to ensure competitiveness and fairness in contractor or awardee selection, *then* conflicts of interest may result.
- Budget Execution - *If* the organization does not follow established policies and procedures for budget execution, *then* government funds may be wasted, anti-deficiency violations may occur, and information regarding obligations, disbursements, and outlays may be inaccurate.
- Safeguards and Security - *If* security procedures are not fully documented, supported by training for the appropriate personnel, and followed, *then* non-compliance with security requirements could occur and DOE property could be damaged or stolen or employee or public safety could be at risk.

2. Risk Rating

To rate risks, management determines the likelihood of occurrence and the impact a risk would have on the organization if it were to occur. Likelihood and impact are typically considered on a Low to Moderate to High scale as shown in Figure 4.

Figure 4: Risk Matrix



Likelihood: The measure of the relative potential that the risk might occur given the operating environment.

Impact: The measure of the magnitude and nature of the effect the risk might cause given the operating environment.

Initially, the likelihood and impact should be established assuming no controls are in place. This is referred to as the inherent or "exposure risk" rating. Following the establishment of controls, risks are again rated, with consideration to the control environment. This latter risk rating should carry the greatest weight, as it reflects the "real-life" operating environment. At a minimum, an annual reassessment of risk ratings should be performed.

3. Risk Ranking

Ranking risks prioritizes management attention to and decisions on the control environment. Risk rankings can be driven by measures of management concern (e.g., dollars exposed; potential reputational damage; anticipated cost to remediate an event; immediacy of the timeframe in which the risk could occur). When ranking risks, management should first consider risks that were rated "high" or "moderate". Risks that management ranks highest are typically the risks that it will mitigate first.

B. Determining a Risk Response

To determine the risk response, management identify its level of risk tolerance when determining what actions it will take to manage those risks that pose the greatest threat to achieving organizational objectives. For example, if management establishes a performance objective of 100%, is it willing to accept a result of 90%? Once its level of risk tolerance is set, management can choose its response – to accept, avoid, reduce, or share, a risk.

Establishing controls to manage risk is a common risk response. Typically, controls are put in place when the choice is to reduce or share a risk. Controls also may be implemented to avoid risk. Controls provide only reasonable assurance – not absolute assurance – that risks will be mitigated. The risk that remains, or residual risk, should be within the risk tolerance acceptable to management.

Using Controls to Manage Risk

The determination of risk drives two major factors in the internal control process: (1) the placement of controls and (2) the prioritization of controls testing. The design and placement of controls is determined by the nature and severity of the risks identified in each process. Those controls must then be assessed to ensure they are functioning properly and effectively. Areas where risk is deemed highest may require strengthening of controls or additional controls. If an area of high risk has insufficient controls to adequately mitigate the risk, management should consider redesigning or adding controls. Managers must balance the cost of implementing additional controls with the risk mitigation benefit provided by the control. There may be areas in the high risk category that are inherently risky, and additional controls may not provide greater risk mitigation.

Integration of Risk Assessments in Internal Control Evaluations

Risk assessments should be part of each Departmental element's process for developing internal controls and conducting the FMA Evaluation, Entity Evaluation, and FMS Evaluation. While the FMA tool provides a direct and standardized approach for conducting risk assessments for the FMA Evaluation, a variety of approaches and templates can be used to conduct similar risk assessments as part of the Entity and FMS Evaluations.

The results of risk assessments are not submitted with the Assurance Memorandum. Documentation of the financial and non-financial risk assessments for each Departmental element should be maintained locally but is not required to be submitted to CFO, except as part of the documentation required for the FMA tool, as discussed in Section IX.A, *FMA Tool*.

Risk Assessments Inform Controls Assessments

Once a risk assessment is performed, management must conduct a controls assessment to evaluate its financial and non-financial internal controls to assure that the control activities being used are effective.

A control assessment is a review of the processes and controls associated with a specific or set of risk(s) to evaluate their effectiveness.

Not all controls are tested every year except in instances of previously reported significant deficiencies and material weaknesses. Risk assessments help to determine the frequency with which controls are tested. Controls in areas that have the highest risk should be tested more often than controls in areas that pose lower risk. In a three-year test cycle, for example, controls in high risk areas should be tested annually, while those in moderate risk areas are tested biannually, and those in low risk areas are tested once every three years. See required test cycle for FMA Evaluations in Section IX.B, Table 5, *FMA Evaluation Test Cycles.* Previously reported significant deficiencies and material weaknesses should be tested each year until the controls are no longer deficient.

VII. Evaluating Control Assessment Results

The results of control testing should support management's judgment whether a control is functioning adequately. Exceptions noted in the testing of internal controls could indicate ineffective controls. Management must consider the extent of a deficiency in such cases. Deficiencies can range from a *control deficiency* (e.g., missing initials indicating a supervisor's review on 1 of 26 time cards sampled) to a *significant deficiency* (e.g., multiple segregation of duties issues were identified but not corrected timely) that results in some loss of resources, to a *material weakness* (e.g., only 2 of the monthly security patches were applied for the year) that results in a major loss of resources or breaches in security. A control deficiency is an internal control deficiency that creates minimal exposure for management and is generally considered an anomaly. However, the consolidation of similar control deficiencies across an organization could result in a significant deficiency or material weakness. For example, if multiple offices in an organization had a similar procurement weakness that were individually determined to be a control deficiency when viewed collectively they could be a significant deficiency or material weakness. When exceptions are noted, management should assess whether the sample size should be expanded to validate whether an exception that appears to be a single deficiency, is indeed an anomaly.

Regardless of the acceptable threshold established by management and the number of exceptions noted in testing internal controls, management needs to assess the exposure that ***any*** exception creates to determine the results. For example, with high-risk processes, one exception could have a significant impact on the organization, and therefore, needs to be assessed to determine if one failure should be reported as a material weakness.

The following sections discuss the DOE controls assessment processes.

VIII. Internal Control Evaluations Overview

There are five steps in performing the assessment of the effectiveness of internal controls:

- Step 1: Planning;
- Step 2: Evaluating Internal Control at the Entity Level;
- Step 3: Evaluating Internal Control at the Process Level;
- Step 4: Testing Control Design and Operating Effectiveness at the Transactional Level; and
- Step 5: Concluding, Remediation, and Reporting.

Management's quality assurance program and related validation must include these steps.

Step 1: Planning

Before beginning an evaluation, each reporting entity should review the processes and sub-processes applicable to its functions. Detailed steps for the processes, how they interact, and the controls in place

to mitigate known risks in the processes, should be diagrammed in a process map. Changes in processes should be identified, and the process map updated. In addition to updating process maps, reporting entities should review current controls in place in the processes to determine if their design is adequate to address the risks they are mitigating. Audit findings and audit issues identified in previous years regardless of where the finding was found should be considered when developing focus areas. Sample test plan and results templates are on the Internal Controls iPortal space under the Resources tab.

Step 2: Evaluating Internal Control at the Entity Level
The process to execute this step is described in Section X, *Entity Evaluation*.

Step 3: Evaluating Internal Control at the Process Level
The processes to execute these steps are described in Section IX.

Step 4: Testing Control Design and Operating Effectiveness at the Transactional Level
The processes to execute these steps are described below in Section IX. This includes performing quality control on the content input into the FMA tool by running the Quality Assurance Tool (QA tool).

Step 5: Concluding, Remediation, and Reporting
The processes for executing this step are described in Section IX.D, *General Documentation Requirements*, and Section XIII, *Glossary*.

Documentation
Documentation occurs in each of the above steps outlined above, from documenting the evaluation methodology in the planning step to documenting key processes and test results in the evaluation and testing steps. Documentation is required to demonstrate the design, implementation, and operating effectiveness of an entity's internal control system. Management should determine the appropriate level of documentation to support the assessment and ensure that documentation requirements in section OV4.08 of the Green Book are met. The new EAT identifies the required documentation.

IX. Financial Management Assurance (FMA) Evaluation

The FMA tool is the central repository for documenting the relevant 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 prepare supplemental documentation to support the FMA Evaluation. However, reporting entities should note in the FMA tool (Column BL of the Assessment tab) the existing documents, e.g., process maps that support identification of the controls and verification of the applicability of the standard process, sub-process, and corporate risks to the site.

A. Financial Management Assurance (FMA) Tool

All reporting entities that are required to perform an FMA Evaluation as documented in Table 1, *Listing of Required Internal Control Evaluations by Departmental Element*, should complete the following steps:

1. Localize the FMA tool by selecting the relevant Departmental element.
2. All standard processes and sub-processes, those pre-populated in the FMA tool, applicable to the reporting entity should be selected in the FMA tool.
3. The FMA tool automatically populates all corporate risks associated with the sub-processes selected in step 2. Add any local risks specific to the reporting entity into the FMA tool.

   For the selected standard processes and sub-processes, corporate risks should be evaluated for applicability and those that are not applicable should be annotated by selecting "NR" (not

relevant), in the Exposure column. In the FMA tool, reporting entities are required to document the rationale for risks assessed with an exposure rating of "NR."

4. In the Risk Assessment section, an exposure risk assessment for each identified risk should be conducted, assuming no controls are in place, and the appropriate rating (i.e., NR, Low, Moderate, or High) should be entered. Exposure risk ratings are based on the likelihood of the risk occurring and the impact on the entity if the risk does occur, in the absence of controls. A heat map explaining the determination of exposure risk can be found in Section XIII, *Glossary*.

   Re-evaluate all prior exposure ratings against the risk factors in the tool. Risk factors are changes that may affect the exposure risk or effectiveness of the existing controls in mitigating the risk. These include system changes, process changes, organization changes, and other changes (e.g., IG or GAO audits).

5. Assess the control risk, also known as dual-purpose testing, for each risk identified in the tool. The control risk is a calculated field in the tool based on Risk Occurrence and Control Set Execution.

Table 4: Control Risk Ratings

Risk Occurrence	Control Set Execution
Determined during dual-purpose testing or through observation during normal business operations. Ask: did the risk occur during normal business operation in the current testing year? **1 =** No occurrence. **2 =** Risk occurred within acceptable threshold. **3 =** Risk occurred outside the acceptable threshold	Rating based on assessment of testing results of all individual controls within a control set. **1 =** Passed with no failures. **2 =** Passed with failures within acceptable threshold. **3 =** Failed.

6. A graph combining risk occurrence ratings and control set execution ratings to determine the control risk is in Section XIII, *Glossary*. Sample scenarios for rating risk occurrence and control set execution are available on the Internal Controls iPortal space under the Resources tab.

7. Based on the risk exposure rating and the control risk rating, the combined risk rating for each identified risk is automatically calculated. A graph showing how combined risk ratings are determined is in Section XIII, *Glossary*.

8. Controls must be identified for any risks meeting the minimum evaluation standard in the combined risk category. Controls for risks with a combined risk rating of High must be tested each year. Controls with a combined risk rating of Moderate must be tested at least every two years. Controls with a combined risk rating of Low must be tested at least every three years. All controls in business processes and sub-processes must be placed on a minimum three-year testing cycle. If controls have not been previously tested in the past two years, they must be tested in the current year.

9. Complete summary information for each Corrective Action Plan (CAP) required as a result of testing in the CAP Tracking Tab.

11. Run the FMA Quality Assurance (QA) Tool to ensure that all fields have been completed properly. The resulting QA report must be submitted along with the FMA tool. Management for

each Departmental element should resolve QA tool exceptions before submission of QA tool results to CF-12. The QA tool 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 should establish and document their QA process and results.

B. Scope of Evaluations

Below is a table of the risk-based test cycles that govern the scope of the FMA Evaluation. Note that the combined risk rating is calculated based on the exposure risk rating and the control risk rating.

Table 5: FMA Evaluation Test Cycles

Risk Ratings			Test Cycle
Exposure Risk + Control Risk = Combined Risk			
High	High	**High**	**Annual**
High	Moderate		
High	No rating		
High	Low	**Moderate**	**At least every 2 years**
Moderate	High		
Moderate	Moderate		
Moderate	No rating		
Moderate	Low	**Low**	**At least every 3 years**
Low	High		
Low	Moderate		
Low	Low		
Low	No rating		
Reporting entities are accountable for ensuring ALL risks are managed and related controls are identified and functioning, using the most effective and efficient methods deemed reasonable. FMA testing is required at least every 3 years for ALL controls in all business processes and sub-processes, including for those risks with a Low Exposure rating and no previous control risk rating. If controls have not been previously tested within the past two years, they must be tested in the current year.			

Risk Factors: Risks should be re-assessed annually. Each Departmental element should consider whether risk factors, such as organizational restructurings, system changes or upgrades, process changes, audit findings, or other changes would impact its risk ratings. If so, the controls related to those risks should be evaluated in the current year. In the FMA tool, new or changing risk factors modify the Combined Risk to "UNK" (unknown) and require further analysis or retesting in the current year.

In FY 2016, Departmental elements must perform the steps outlined below.

1. Follow the risk-based test cycles described in Table 5 and complete testing of all controls for processes that have risks with a combined risk rating of High as identified in the current year assessment scope by the FMA tool, no later than June 30, 2016. Complete testing of controls for processes that have risks with a combined risk rating of Moderate that were not tested in the previous year (as per the two-year testing cycle described above in Table 5). Complete testing of controls for processes that have risks with a combined risk rating of Low and were not tested in the previous two years (as per the three-year testing cycle described in Table 5).
2. Complete testing of any controls for processes that have risks with an exposure risk rating of High, Medium, or Low that have not been previously tested. If no control testing has been

performed, and hence no control risk rating identified, the combined risk will default to the exposure risk rating. See Table 5 for required testing cycle.

3. Complete corrective actions and re-testing of all controls in remediation (i.e., those controls that exceed established test failure thresholds) by June 30, 2016, which might have a negative impact on the Assurance Memorandum (i.e., cause a qualification of the Assurance Memorandum) if not corrected by that date. A CAP should be developed for each area of remediation. The CAP should be a detailed, step-by-step plan with associated milestones. Each CAP should also contain the signatures of the authorized individual approving the plan and the individual confirming completion of the plan. Circular A-123 emphasizes identification of the root cause in the CAP. Departmental elements should report the root cause in the FMA tool and EAT.

   A CAP should contain the following 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, etc.);
   - accountable individual; and
   - status.

   Significant information is summarized in the CAP-Tracking tab of the FMA tool. Departmental elements maintain the CAPs and are not required to submit them unless requested by CFO.

4. Complete required actions to address all FY16 focus areas and document the actions taken in the focus area tab of the FMA tool. Annually, the OCFO identifies focus areas for its FMA Evaluation areas of emphasis. These focus areas must be tested in the assessment year if exposure risk is rated moderate or high. Section IX.E, *FMA Focus Area Guidance*, provides additional information on focus areas and requirements for assessing these areas.

5. If during testing, best practices are identified for improved control effectiveness, efficiency, or monitoring, note them in the Assessment Tab of the FMA tool as "efficiency opportunities." These best practices will be shared with other Departmental elements to improve controls.

C. Testing Requirements

There are a variety of different techniques to test internal controls, including:

- Interviews, either in-person or through questionnaires. In general, it is considered a best practice to gather information from interviews, corroborated with a secondary type of evidence.
- Direct observation of performance of the control.
- Physical examination or inspection of documents.
- Transaction testing and re-performance, the latter most commonly used when testing automated controls.

Organizations may use a variety of evaluation activities and consider a range of information to identify the appropriate techniques to test internal controls, including:

- Departmental Management Priorities;[1]
- Consideration of IG and GAO audit report results required in all cases;
- Review of prior-year Assurance Memoranda and EAT and FMA tool submissions;
- Review and analysis of existing "Assurance System" reports or results;
- Consideration of contractor and Field office internal control evaluation reporting provided to the appropriate Office before year-end reporting;
- Review and analysis of performance reporting results;
- Consideration of the results of other internal or external assessments;
- Conduct management meetings or interviews with critical staff regarding key control areas;
- Review of management reports (e.g., safety manager reports, infrastructure status reports); and
- Review and analysis of other relevant and reliable information.

Reporting entities must use dual-purpose testing where applicable. Dual-purpose testing evaluates both control execution (i.e., did the control work as intended) and risk occurrence (i.e., is there evidence that the stated risk occurred). Dual-purpose testing ensures controls are effective in risk mitigation, thereby reinforcing the site's control design effectiveness decision. Test plans should include dual-purpose testing, recognizing that in some cases control execution and risk occurrence are tested simultaneously.

In testing control activities, reporting entities should use the following guidelines to select test samples:

- Use professional judgment in determining appropriate sample sizes for testing.
- Sample sizes should be selected considering:
  - combined risk rating;
  - sample universe; and
  - control attributes (e.g., frequency, mode, type, etc.).
- Reporting entities should use the OMB and CFO Council Guide sample size guidelines in Figure 5. Deviation from the sample guidelines should be documented in the work papers.

Figure 5: Sample Sizes

After considering the complexity of a control, the following are examples of sample sizes based on the frequency of the performance of the control:

performed annually – sample size = 1	performed weekly – sample size = 10
performed quarterly – sample size = 2	performed daily – sample size = 30
performed monthly – sample size = 3	recurring – sample size = 45

In addition, whether the control is manual or automated should also be considered. Ultimately, management should use its best judgment to determine how extensively a key control will be tested.

[1] Complete summaries of the Management Priorities can be found in the FY 2015 Agency Financial Report: http://energy.gov/sites/prod/files/2015/11/f27/DOE_FY2015_AFR.pdf.

D. General Documentation Requirements

In addition to the control/process documentation requirements described in Section VIII, *Step 1: Planning*, offices must document the following activities to support internal/external review or audit:

- Exposure Risk Assessment – **Must be rated** in the FMA tool. Reporting entities **must** provide a rationale for all risks rated as "NR" and "Low" in the Exposure column. Reporting entities **should** record the justifications for those risks rated as "Moderate" or "High" Exposure to support a more effective re-evaluation of exposure on an on-going basis.
- Testing Activities – Test plans and results **must be documented** in a formal test plan containing the key elements outlined in Table 6 below. Testing results **must be updated** in the FMA tool.

Table 6: Key Test Plan and Results Elements

Description of objective	Sample size
Type of test	Timeframes of execution
Procedures of the test being performed	Resources assigned
Acceptable error thresholds	Date executed
Explanation of the extensiveness of tests	Who performed the test
Universe from which sample size was selected	Approver
Document the results of the testing and any recommendations as well as electronic or physical evidence	The scores (1,2, or 3) given to each individual control and scores given to each control set
Note: Provide enough detail in the test plan and results so the test could be replicated with the same results.	

- Remediation Activities – CAPs **must be maintained** and be available to support reviews or audits for remediation activities identified in the FMA tool. The FMA tool **must also be updated** to summarize key remediation information required in the Assessment tab, including a root-cause analysis. In addition, a summary of current and previously reported open significant deficiencies and material weaknesses should be included in the Assurance Memorandum. Section XII, *Annual Assurance Memorandum*, provides Assurance Memorandum instructions.
- Best Practices – Reporting entities should use the FMA Evaluation process to identify future improvements in efficiency, effectiveness, or monitoring. Reporting entities also may use the Efficiency column in the FMA tool to note best practices and document the best practice for future use. Reporting entities are encouraged to share best practices with CFO to facilitate DOE-wide implementation. There are no requirements for adopting efficiency changes.

E. FMA Focus Area Guidance

In FY 2016 there are 28 FMA focus areas for the following business processes:

1. Acquisition Management
2. Project Cost Management
3. Property Management
4. Cost Management
5. Improper Payments
6. Environmental Liabilities
7. Information Technologies

The focus areas are managed through the "Focus Area" tab in the FMA tool that includes all corporate risks, with focus area risks highlighted with a "Y" in the "Focus Area" Column. For each focus area risk, the "Description/Action Required" column provides information on what actions are required in FY16**.**

When a focus area is selected in the "Focus Area" tab through an import tool provided by the FMA Program Manager, the "Corp Request" column in the "Assessment" tab is highlighted with a yellow "Y," and the area appears in the current year scope. Reporting entities should take the actions indicated. Once actions are completed, the site should use the drop down to place a "Y" in the "Local Action Complete" column of the Focus Area tab. Then, the site should provide a brief description of the actions taken. When done, the "Corp Request" column in the "Assessment" Tab changes to an "A" to indicate a focus area site action was taken.

At every reporting entity, action should be taken if the exposure rating for focus area risks is either High or Moderate. If a focus area is rated as Low Exposure in the FMA tool, check the "Y" under "Local Action Complete" column and insert a rationale in the "Action Taken" column. Focus areas with a Low exposure rating are not required to be tested in the current year; however, these processes and sub-processes must be tested on at least a three-year cycle. An "NR" rating applies if there is no activity related to that focus area risk and should be validated as part of quality assurance activities.

Control vs. Process Documentation: Note that some actions require only that controls be documented in the FMA tool, while others require processes or other activities be documented, (e.g., roles and responsibilities or a communications strategy). Required actions must be performed. In cases where processes must be documented, the site should prepare supplemental process narratives or flows, and maintain the documentation on an on-going basis.

Process Documentation: Required process or other documentation should be maintained locally. This documentation is critical for supporting the FY16 financial statement audit. In addition, the process documentation for the focus areas may be requested for quality assurance and peer review purposes.

X. Entity Evaluation

All Departmental elements are required to perform an evaluation, as shown in Table 1, of the internal controls in place for non-financial functions, administrative, operational, and programmatic, referred to throughout this guidance as entity functions. An Entity Evaluation is a structured self-evaluation designed to provide reasonable assurance that non-financial control systems are in place and working effectively to mitigate risk and ensure mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulations. This assessment may use a variety of techniques to provide the required level of assurance. Headquarters elements with cognizance over Field reporting elements will need to consider the status of issues at both the Field and Headquarters level. The results of the Entity Evaluation will be reported in the Departmental element's annual Assurance Memorandum to the Secretary, who in turn will report DOE results to the President, Congress, and OMB through the Statement of Assurance.

Section II of FMFIA requires an assessment of non-financial controls to assure effectiveness and efficiency and compliance with laws and regulations. The revised Green Book has 17 principles and 155 attributes to guide each Departmental element's performance of the Entity Evaluation.

Identifying Non-Financial Controls

Assessments of entity-level, or non-financial controls are also performed by each Departmental element and documentation must be retained locally. The EAT documents the outcome of local assessments of non-financial controls. When performing entity-level controls assessments, Departmental elements should consider the following types of controls:

- **Managerial** – reviews and checks that occur regularly as part of the oversight process, such as periodic project or program reviews;
- **Program and Operational** – discrete activities related to program performance and effectiveness and efficiency of operations, such as mandatory training or cascading of organizational objectives through individual performance plans;
- **Accounting** – activities that ensure safeguarding of assets, such as inventory management or physical security over valuable property (e.g., physical access controls, locks, guards); and
- **Administrative –** activities related to the authorization of transactions or events that ensure compliance with existing policies and procedures, such as approval or certification actions, or establishment of role and responsibility controls in information management systems.
- **Service Organizations** – management has oversight of the internal control activities of service organizations, including but not limited to roles and responsibilities, risk assessment activities, controls assessments, and corrective action monitoring.

A. Four-Step Evaluation Process

The Entity Evaluation process has four steps.

1. Perform the Evaluation

The entity assessment evaluates the Departmental element's controls against the five GAO Components for Internal Control. Departmental elements may perform the entity assessment using a variety of techniques; however, two basic tenets must be followed in any assessment. First, all assessments must touch on every significant aspect of the Departmental element. Second, all assessments should consider the five GAO components for Internal Control, as previously described in Section III of this document and included in the new EAT.

Testing

The breadth and depth of controls testing should be determined by the Departmental element's assessment of entity-level risks. Those areas where risks are Moderate or High should have controls tested more often than those areas where risks are determined to be Low. The nature and extent of activities employed in conducting an Entity Evaluation is at the discretion of each Departmental element. Controls identified during the assessment must be tested in order to determine if they:

- accomplish their objectives as designed;
- are necessary and sufficient to accomplish their intended objectives; and
- function appropriately.

2. Prepare and Track Corrective Actions

A CAP should be created and tracked internally for any control deficiencies identified through the internal controls assessment process. If management determines that any of these issues are of high enough materiality to warrant being reported as a significant deficiency or material weakness in the Assurance Memorandum, a CAP Summary describing the status of remediation activities must be submitted with the Assurance Memorandum. CAP Summaries should be prepared using the "HQ Assurance Memo Template" or "Field Assurance Memo Template" provided in conjunction with this Guidance. Additional instructions for filling out the CAP Summary are provided in Section XII, *Annual Assurance Memorandum*. CAPs for significant deficiencies and material weaknesses should be prepared and tracked locally. In addition, summary information for the CAP should be maintained in the EAT, including documenting the root-cause analysis.

3. Document the Evaluation

Provide the EAT to your program's FMFIA point of contact to document your Entity Evaluation in advance of the Assurance Memorandum to serve as documentation for the FMFIA Entity Evaluation.

The EAT documents:

- the evaluation summary for standardized key control areas;
- the evaluation of each component - Management should summarize its determination of whether each component is present and functioning (Effective, Effective with internal control deficiencies, or Ineffective);
- any principle that management has determined not relevant in the accomplishment of its objectives and the addressing of related risks will be supported by a rationale in the *User Field* column. The rationale will include how, in the absence of the identified principle, the associated component will be designed, implemented, and operated effectively;
- results of the review;
- impact assessments for control deficiencies identified; and
- other critical information.

Reporting entities are required to keep copies of key documents used in the evaluation in a central location. Location of the documents is noted in the EAT (Column T), and documents must be available if requested during controls assessments or quality assurance reviews. FMFIA points of contact should maintain copies of documents that are not readily available or were prepared solely for the purpose of supporting the FMFIA process (e.g., FMFIA meeting minutes, special reviews performed for FMFIA purposes). Documentation beyond the EAT and the Assurance Memorandum should be maintained locally unless requested by review teams.

The EAT must document the results of the Entity Evaluation process. Management reviews the EAT before submission, to ensure that risk assessments, testing plans, sample sizes, and final results are compliant with DOE guidance. Departmental elements should document their QA process and results.

4. Report the Results

Results of the Entity Evaluation are reported in the annual Assurance Memorandum. To determine what to report in the Assurance Memorandum, review the issues rated as a "1" or "2" in the EAT. These issues are control deficiencies. Deficiencies rated as "2" may rise to the level of a significant deficiency, if in management's judgment, they represent significant weaknesses in the design or operation of controls that could adversely affect the organization's ability to meet its internal control objectives. See Table 6 below for a description of "1" or "2" ratings in the EAT.

Table 7: EAT Issue Ratings

Ratings		Description
1	Effective with internal control deficiencies	A principle or component with an "Effective with internal control deficiencies" rating has a potentially negative impact, but will not prevent the organization from meeting mission or mission-support objectives.
2	Ineffective	A principle or component with an "Ineffective" rating has a negative impact and will prevent the organization from meeting mission or mission-support objectives. An "Ineffective" rating is a significant deficiency or material weakness depending upon the severity of the control issue.

All significant deficiencies must be reported in the Departmental element's Assurance Memorandum and must provide a CAP Summary. In addition, all control deficiencies must be documented in the EAT.

Section XII provides instructions on the Assurance Memorandum. A macro-enabled template for the Assurance Memorandum is a separate electronic attachment to this guidance. There are two Assurance Memorandum templates – one for Field offices and one for Headquarters offices.

XI. Financial Management Systems (FMS) Evaluation

The FMS Evaluation must be performed annually by Departmental elements with financial management systems included in the DOE Financial Management System Inventory to support Section IV of FMFIA and the *Federal Financial Management Improvement Act* (FFMIA). Departmental elements listed as system owners in Table 8 should perform the FMS Evaluation and follow the same four-step process used for the Entity Evaluation in Section X.

Table 8: DOE Financial Management Systems and Mixed Systems

Financial Management System and Mixed Systems	System Owner(s)
Power Marketing Administration Systems	**BPA, WAPA, SWPA, & SEPA**
Standard Accounting and Reporting System (STARS)	**CF-40**
Federal Energy Regulatory Commission Systems	**FERC**
Funds Distribution System (FDS)	**CF-40**
Electronic Work for Others	**ORNL**
Active Facilities Database	**CF-11**
Departmental Inventory Management System (DIMS)	**NNSA-NA-73**
Integrated Planning, Accountability and Budgeting System (IPABS)	**EM-62**
Facilities Information Management System (FIMS)	**MA-50**
Strategic Integrated Procurement Enterprise System (STRIPES)	**CF-40**
Funds Controls and Distribution System (FCDS)	**NNSA NA-MB-1**
Budget Execution and Reporting System (BEARS)	**OR**
Vendor Inquiry Payment Electronic Reporting System (VIPERS)	**OR**
Financial Accounting Support System (FAST)	**OR**
iBenefits	**CF-40**

XII. Annual Assurance Memorandum

Each Departmental element is required to report and submit an annual Assurance Memorandum, which captures the results of their annual FMA Evaluation, Entity Evaluation, and FMS Evaluation. The Assurance Memorandum provides reasonable assurance that internal controls are working effectively and efficiently, and that operations are maintained in a manner consistent with applicable laws and regulations. The Assurance Memorandum identifies any significant deficiencies which might qualify that assurance, as defined in Section C, *Determining Issues to Be Reported*, and will be accompanied by a summary of the corrective action plans developed to address each issues.

To identify any potential significant deficiencies during the internal control evaluations process, CFO will host a mid-year update with each reporting entity. The Office of Financial Policy and Internal Controls will conduct individual calls with FMFIA points of contact for each reporting entity in mid-April. These calls allow each reporting entity to share any control deficiencies identified to date in the evaluation process that may be reported as a significant deficiency or material weaknesses in the entity's Assurance Memorandum, if the issue may not be fully remediated by the end of the fiscal year.

Organizational assurance statements include an assessment of the effectiveness of the agency's internal control over financial reporting as of June 30. However, organizations must update 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 should 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 should be updated to include the subsequently identified significant deficiency or material weakness.

Organizations should notify CFO (CF-12) immediately of any resolved or new significant deficiency or material weaknesses to be updated, but not later than October 3, 2016, per Table 2.

A. Reporting Documentation and Transmittal Methods

Each Departmental element will provide an Assurance Memorandum and other documents or files depending on the extent of required evaluations. Certain documents have different transmittal methods. Table 9 provides instructions for transmitting required documentation.

Table 9: Reporting Documentation Transmittal Methods

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 appropriate program office.
	Signed PDF	Electronic Delivery & Upload to iPortal	Headquarters Assurance Memorandum addressed to The Secretary through appropriate Under Secretary
Entity Assessment Tool (EAT)	Excel File / Tool	Upload to iPortal	Internal Controls Space on iPortal
FMA Tool & FMA QA Results	Excel File / Tool	Upload to iPortal	Internal Controls Space on iPortal – Please note that the federal staff field locations will be responsible for uploading files for its contractors.

B. Format for the Assurance Memorandum

The Assurance Memorandum consists of two sections:

1. The Main Body – Contains the 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 material non-conformance reported in the Assurance Memorandum. Describes the remediation activities already taken place or those that will be implemented in the next fiscal year. The CAP Summary is segregated into: (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 that have been closed in FY 2016, the CAP Summary should also include a statement noting the closure of the CAP.

Responsibility for assurances that internal controls are effective and efficient, produce reliable financial reports, and are compliant with all applicable laws and regulations, lies with the head of each Departmental element. For all entities, the **Assurance Memorandum must be signed by the head of the Departmental element**, and for all Headquarters-level entities the Assurance Memorandum must be signed by the head of the Departmental element and the appropriate Under Secretary, if applicable.

C. Determining Issues to be Reported

Control deficiencies meeting certain criteria must be reported in the Assurance Memorandum. Table 10 provides the issues to be reported in each section of the Assurance Memorandum, a definition for each issue, and which issues should be reported in the Assurance Memorandum with corrective action plans.

Table 10: Definitions of Control Issues

Control Issue Type	Definition	Reported in Assurance Memorandum?
Financial Management Assurance Evaluation		
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.	Yes
Material Weakness*	A significant deficiency in which management determines to be significant enough to report outside of its organization (e.g., merits the attention of the Office of the Secretary) as a material weakness.	Yes
Entity Evaluation		
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.	Yes
Material Weakness*	A significant deficiency in which management determines to be significant enough to report outside of its organization (e.g., merits the attention of the Office of the Secretary) as a material weakness.	Yes
Financial Management Systems Evaluation		
Material 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 Tool defines the criteria against which conformance is evaluated and captures identified non-conformances.	Yes
All Evaluations		
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. Control deficiencies are only reportable if they meet the definition of a Significant Deficiency or Material Weakness.	No
Scope Limitation	Exists when the Entity has identified potentially significant deficiencies in the scope of the internal control evaluations conducted, which would warrant disclosure to ensure limitations are understood. Scope limitations may be determined by the entity or may be required by the CFO in certain circumstances.	Yes

* ***Material weaknesses resolved or identified before September 30, 2016, must be reported in the original or an assurance memorandum update.***

Considerations for Determining Material Weakness

As noted in Table 10, the consideration of a material weakness begins with a significant deficiency or combination of significant deficiencies. Significant deficiencies are the result of a control deficiency, or combination of control deficiencies. Management's judgment of 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. Management's judgment regarding financial control deficiencies is guided by the dollar amounts involved which lend themselves to quantitative analysis to determine if the potential impact on the local organization is 'material.' An entity control deficiency requires qualitative management 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 department. Following are considerations when determining an entity material weakness and documentation supporting the consideration must be developed for each material weakness:

1. **Control Deficiency.** There are three types of control deficiencies: design deficiency, implementation deficiency, and operating deficiency. The control deficiency, or combination of control deficiencies, causing the significant deficiency or material weakness must be identified so management can judge the potential likelihood of a control failure and its impact. Identification of deficiencies can be the result of scheduled control testing, other special internal reviews, IG/GAO audit findings, or unexpected performance failures. Additional analysis may be required to identify the root cause of the control deficiency when it is identified outside normal testing. An audit finding or significant performance failure may identify the lack of a needed control rather than the failure of an existing control. An adverse outcome or performance failure that results from an adverse budget/funding decision does not indicate a control deficiency. Performance expectations should be adjusted to reflect budget/funding decisions.

2. **Timing of Implementation, Remediation, or Mitigation.** Once the control deficiency is identified, management must identify the corrective actions necessary to implement a new control, correct an improperly functioning control, or identify other actions or controls, which can reduce the likelihood or adverse impact of the deficient control. The corrective actions should be documented in a CAP which includes a timeline of the corrective actions. Significant deficiencies for which corrective actions have been completed and tested, or which have been significantly mitigated by completed corrective actions, may not warrant being identified as a material weakness when in the organization Assurance Memorandum.

3. **Report Outside of the Departmental Element**. A material weakness is a significant deficiency which the head of the Departmental element determines to be significant enough to report outside of their department. Considerations should include the likelihood and magnitude of an impact on other organizational elements, the DOE as a whole, or organizations outside of the DOE; the need for higher-level support and oversight from outside the element; and the likelihood of outside interest (governmental or private) and/or adverse press.

XIII. Glossary

Assurance Memorandum — Annual statement of assurance over the status of internal controls made by each Departmental element. For required Assurance Memorandum content, see Section XII, *Annual Assurance Memorandum*.

Basis of Evaluation — The key information or activities performed to provide support for assurances that the control objectives and considerations were addressed.

The Basis of Evaluation must be a documented activity. Examples include: reports, bi-annual workforce planning survey results, other reports, memos, reviews, assessments, evaluations, or plans, emails, meeting minutes, agendas, certificates, newsletters, bulletin boards, documented signatures.

Combined Risk Assessment — The residual risk considering the control environment and a measure of the end risk to DOE. For FMA evaluations, this is a quantitative measure of residual risk. For Entity evaluations, please refer to the definition for "residual risk."

In the FMA tool, the combined risk is a calculated field based on exposure risk and control risk, as well as the presence of risk factors. If no control testing has been performed, the combined risk defaults to the risk exposure risk rating. If a risk factor is indicated in the current year (e.g., system change, process change), then the combined risk defaults to "unknown" (UNK), until controls are tested and the control risk is identified. Once control risk is identified, the Combined Risk will automatically calculate.

H – High risk, poor risk mitigation.
M – Moderate risk.
L – Low risk, effective risk mitigation

The diagram demonstrates the calculation of **High**, **Moderate**, and **Low** combined risk ratings.

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

Control Deficiency — A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel in the normal course of performing their assigned functions, to achieve control objectives and address related risks. There are three types:
Design Deficiency – A deficiency in design exists when (1) a control necessary to meet a control objective is missing or (2) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met.

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

Operating Deficiency – Exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

Control Execution

A rating resulting from individual control testing. As defined in the FMA tool:

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

Entity control tests may apply these ratings, or other ratings developed by each organization.

Control Objective

Identifies the key objectives to be achieved by the internal control in each area, as well as control issues that should be considered when performing the evaluation and the goal to be achieved to ameliorate, minimize, manage, or mitigate risks. Each objective considers the nature of the activity, the organization's mission, and the cost and benefits of each control in determining desired control objectives.

Control Risk Assessment

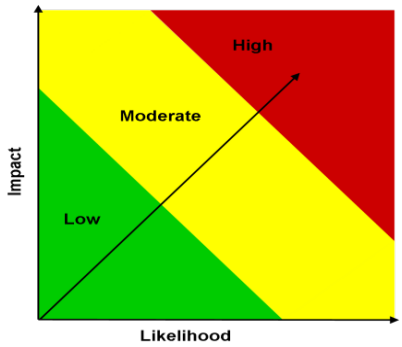
A measure of the risk considering the effectiveness of the controls to mitigate that risk and the risk occurrence. In the FMA tool, control risk is a calculated field based on Risk Occurrence and Control Set Execution. The diagram below demonstrates the calculation of **High**, **Moderate**, and **Low**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

Risk Occurrence				
	3	**High**	**High**	**High**
	2	**Moderate**	**Moderate**	**High**
	1	**Low**	**Moderate**	**Moderate**
		1	2	3
		Control Set Execution		

Control Set Execution: Rating based on assessment of testing results of all individual controls within a control set.
1 - Passed with no failures;
2 - Passed with failures within acceptable threshold; or
3 - Failed.

Risk Occurrence: Determined during dual-purpose testing or through observation during normal business operations. Ask, did the risk occur during normal business operation within the current testing year?
1 - No risk occurrence;
2 - Risk occurred within acceptable threshold; or
3 - Risk occurred outside the acceptable threshold.

	Example scenarios for rating risk occurrence and control set execution are available on the Internal Controls iPortal space under the Resources tab.
Corporate Risk	A risk that is pre-populated into the FMA tool to facilitate the FMA Evaluation. The FMA tool also allows each Departmental element to add any additional locally-identified risks to the tool.
Corrective Action Plan (CAP)	A plan to correct an internal control deficiency. A CAP must be prepared and tracked for all control deficiencies identified during the internal control evaluations process. A CAP Summary for significant deficiencies identified in the Memorandum of Assurance must be submitted with the memorandum.
Departmental Element	Refers to DOE Headquarters mission and mission support offices and field and operation offices, and all DOE Agencies.
Dual-purpose Testing	A testing mechanism designed to evaluate both control execution (i.e., did the control operate as intended) and risk occurrence (i.e., is there evidence that the stated risk occurred). Dual-purpose testing provides a mechanism for ensuring controls are actually effective in risk mitigation, thereby reinforcing the control design effectiveness decision.
Entity	Related to the organizational level and pertaining primarily to non-financial functions or controls (i.e., administrative, operational, or programmatic).
Entity Assessment Tool (EAT)	The primary system for documenting and reporting the results of evaluations and testing of entity and financial management systems risks and controls.
Entity Evaluation	Detailed evaluation of an organization's key administrative, operational, or programmatic activities, to determine whether adequate control techniques exist and are implemented to achieve cost-effective compliance with FMFIA.
Exposure Risk Assessment	A combined measure of the likelihood and impact to DOE should the risk occur (regardless of the strength of the controls to mitigate the risk, given the general environment). In the FMA tool, this is a professional judgment rating of **H**(igh), **M**(oderate), **L**(ow), or **NR** (not relevant). The NR rating is for corporately defined risks that may not impact your location. No assessment is required with a rating of NR; however a short rationale will need to be provided. **General environment:** Environment that assumes no mitigating controls are in place. **Likelihood:** The measure of the relative potential that the risk might occur given the general environment. **Impact:** The measure of the magnitude and nature of the effect the risk might cause given the general environment.



Federal Managers' Financial Integrity Act (FMFIA)

DOE Order 413.1b, *Internal Control Program* requires the Department to establish and maintain an internal control program to evaluate internal controls and report the status of major problems up through the chain of command to the President and Congress. To support Departmental reporting, Heads of Departmental elements, including the National Nuclear Security Administration (NNSA), are required to report on the status of their organization's internal controls, including reportable problems identified and progress made in correcting prior reportable problems.

FMFIA provides for:

- Evaluation of an agency's internal controls in accordance with GAO standards.
- Annual reporting by the head of each executive agency to the President.
- Identification of material weaknesses and the plans for correcting them.
- Agencies to provide for internal control assessments on an on-going basis.

Financial Management Assurance (FMA) Evaluation

An evaluation of internal controls over financial reporting that tests these controls to ensure effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Financial Management Assurance (FMA) Tool

The primary system for documenting and reporting the results of evaluations and testing of financial management reporting risks and controls.

FMA Quality Assurance (QA) Tool and Report

A macro-enabled Excel tool that is run in a standard reporting package distributed by CF-12 to Departmental FMA contacts. The QA Tool, creates a report with the results of the review. The QA Tool highlights potential data anomalies for management review and includes an area for comments in the Table of Contents, for management to discuss the results.

Financial Management Systems

OMB Circular A-123, Appendix D*, Compliance with the Federal Financial Management Improvement Act of 1996,* defines a "financial management system" as including "an agency's overall financial operation, reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions. It includes 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." The financial system encompasses processes and records that: • Identify and record all valid transactions; • Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting; • Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements; and • Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period."
Financial Management Systems (FMS) Evaluation	In accordance with the FMFIA, Departmental elements with financial management systems included in the Department's FMS Inventory are required to conduct an FMS Evaluation as part of their annual internal controls review process.
Focus Area	***In the FMA Evaluation:*** areas which require additional assessment. Risks identified in focus areas in the FMA Tool will default to "Y" in the "Corporate Request" (Corp. Req) column of the Assessment Tab worksheet.
High Combined Risk	A risk in the FMA tool that is determined to have: 1. Moderate control risk rating and high exposure risk rating; OR 2. High control risk rating and high exposure risk rating.
Impact Assessment	An evaluation of the impact of a breakdown in a particular control identified in the EAT. This evaluation includes a description of the general breakdown in the control, the program(s) and sub-program(s) affected by the breakdown, and the nature and significance of the impact. The impact assessment is documented using the Impact Assessment Tab in the EAT.
Internal Control	An integrated component of management that provides reasonable assurance that the following objectives are being achieved: • Effectiveness and efficiency of operations. • Reliability of reporting. • Compliance with applicable laws and regulations.
Key Control	A control or set of controls that address the relevant assertions for a material activity (e.g., financial statement line item) or significant risk. At the point that management is ready to test controls, and in order to focus test work, management must identify the key controls in place.
Material Non-conformance	Exists when *financial systems* do not substantially comply with federal financial management system requirements OR where local control deficiencies impact financial systems' ability to comply. EAT defines the conformance criteria and captures identified non-conformances.

Material Weakness

A significant deficiency which management determines to be significant enough to report outside its organization (e.g., merits the attention of the Office of the Secretary) as a material weakness. There are four types:

Material Weakness in Internal Control Over Operations – It could include, but is not limited to, conditions that:

- Impact the operating effectiveness of Entity Level Controls;
- Impair fulfillment of essential operations or mission;
- Deprive the public of needed services; and
- Significantly weaken established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest.

Material Weakness in Internal Control Over Reporting – It is a significant deficiency which the organization's management determines significant enough to impact internal or external decision-making and report outside the organization as a material weakness.

Material Weakness in Internal Control Over External Financial Reporting – It is a significant deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Material Weakness in Internal Control Over Compliance – It is a condition where management is unable to provide reasonable assurance that it is in compliance with laws and regulation that could have a material effect on its Federal programs or operations (compliance requirements).

Minimum Evaluation Standard

The basis by which testing cycles for the FMA Evaluation are determined. The minimum evaluation standard for FY16 is based on the combined risk rating of risks identified both corporate risks automatically populated by the FMA tool and local risks identified by the individual Departmental element for each standard process and sub-process. Controls for processes that have risks with a combined risk rating of High must be tested each year. Controls for a process that have risks with a combined risk rating of Moderate must be tested at least once every two years. Controls for processes that have risks with a combined risk rating of Low must be tested at least once every three years.

ALL controls in all business processes and sub-processes must be on a three-year testing cycle, including processes with a Low exposure rating and no control risk rating. If controls have not been tested in the past two years, they must be tested in the current year.

Mitigate

To put controls in place that would ensure the probability or impact of a given risk is as low as possible.

Mixed System

OMB Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, defines as a "hybrid of financial and non-financial portions of the overall financial management system."

OMB Circular A-123, including Appendix A	Prescribes guidelines for evaluating, improving, and reporting on internal controls. Appendix A requires annual assurance statement on Internal Controls Over Financial Reporting.
Reasonable Assurance	Judgment by management based upon available information that the systems of internal controls are operating as intended under FMFIA.
Remediation Activity	An action put in place that would address the correction of a controls deficiency identified through an internal controls assessment.
Residual Risk	The risk that remains after a risk response is executed.
Risk Assessment	A review of the susceptibility of a program or function to the occurrence of waste, loss, or unauthorized use, or misappropriation. The potential for risks to an organization may be internal or external, or both.
Risk Factor	Identification of changes that may affect the exposure risk or effectiveness of existing controls in mitigating the risk. Risk factors include system, process, organization, or other changes (e.g., IG or GAO audits). In the FMA tool, the identification of risk factors changes the combined risk assessment to "UNK" (unknown) and requires analysis and retesting.
Risk Response	A determination by management on how a risk should be managed, considering the potential impact of the risk and the likelihood of occurrence, as well as the cost associated with mitigating the risk. <u>Types of risk responses:</u> ***Acceptance*** – No action is taken to respond to the risk based on the insignificance of the risk or the risk is knowingly assumed to seize an opportunity. ***Avoidance*** – Action is taken to stop the operational process, or the part of the operational process causing the risk. ***Reduce*** – Action is taken to reduce the likelihood or magnitude of the risk. ***Share*** – Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.
Risk Tolerance	The level of variation in performance that management is willing to accept, relative to achieving its objectives. Management should establish its risk tolerance level before the placement of controls.
Scope Limitation	Exists when the Entity has identified potentially significant deficiencies in the scope of the internal control evaluations, which would warrant disclosure to ensure limitations are understood. Scope limitations may be determined by the entity or may be required by CFO in certain circumstances.

Significant Deficiency	A deficiency or a combination of deficiencies in internal control less severe than a material weakness yet important enough to merit attention by those charged with governance.
Standard Process	Pre-populated FMA tool process required to be tested in the FMA Evaluation.
Standard Sub-process	A component of a standard process, also pre-populated in the FMA tool.
Statement of Assurance	Annual statement required by FMFIA and included in the DOE Agency Financial Report that represents the Secretary's informed judgment as to the overall adequacy and effectiveness of DOE internal controls. It reports the results of evaluations made on DOE entity, financial, and financial management systems controls, including any identified material weaknesses or material non-conformances and corrective action progress made on existing material weaknesses and material non-conformances.
Testing Activity	Procedure to determine if internal control systems work in accordance with internal control objectives.