U.S. DEPARTMENT OF ENERGY

Internal Control Evaluations

Fiscal Year 2015 Guidance

February 12, 2015

Table of Contents

I. Introduction

A. Background

In 1982, Congress enacted the *Federal Managers' Financial Integrity Act* (FMFIA), which 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 and 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 that evaluation the Department of energy (DOE) Secretary annually attests to the Department's controls, established in accordance with standards prescribed by the Comptroller General, which is accomplished through the Governmental Accountability Office's *Standards for Internal Control in the Federal Government*.

Following the publication of the initial GAO Standards, the Office of Management and Budget (OMB) issued Circular A-123 to provide specific guidance for agencies to follow in implementing internal control programs. In 1995, OMB revised Circular A-123 to require internal controls to support the purpose of the newly enacted *Government Performance and Results Act of 1993*, namely the improvement of program effectiveness and accountability. This revision required agencies to transmit a single annual Statement of Assurance from the head of the agency to the President, Congress, and OMB, stating whether there is reasonable assurance that the agency's controls are achieving intended objectives.

The Public Company Accounting Reform and Investor Protection Act of 2002 (also known as Section 404 of the *Sarbanes-Oxley Act*) requires the management of public companies to assess and report on their companies' internal controls over financial reporting. In 2004, OMB revised Circular A-123 to hold federal managers to the same standards. Appendix A of revised OMB Circular A-123 requires federal managers to specifically assess and report on the agency's internal controls over financial reporting.

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 financial 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.

Internal controls should be designed to provide reasonable assurance for safeguarding assets, and preventing or detecting fraud, waste, abuse, errors and omissions.

In October 2008, the DOE issued DOE Order 413.1B, *Internal Control Program*. Incorporating the requirements set out in the above-mentioned laws and regulations, this order 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 is intended to provide the specific methodology that reporting entities (including certain contractors) should follow to meet the requirements specified in Order 413.1B. Contractors required to follow this guidance are contractors with management and operating contracts that include the contract clause at DEAR 970.5204-2, *Laws, Regulations, and DOE Directives*.

B. New for FY 2015

Changes to this year's guidance include an expanded discussion related to Focus Areas; clarification that Field Office and Headquarters Office consideration of lower level assurances includes determining if reportable conditions or material weaknesses reported at the lower levels are significant enough to be reported for the higher level organization as a whole; and additional guidance on evaluations of reportable conditions as potential material weaknesses. Finally, the guidance now includes a reminder that organizations are responsible to update assurance statements when material weaknesses are resolved or identified by September 30th but after the assurance statement is issued. These changes are discussed in detail in the applicable sections of the guidance.

FMA Tool Update

The FY 2015 FMA tool includes updates to the standard (Corporate) risk statements and controls. Broadly, the changes can be classified as financial related and IT related (Network and Information Systems Security). The revisions clarify the purpose of the risk statements to ensure common understanding and consistent application of the statements in testing internal controls. Although the revisions reduced the number of risk statements by 12, there are 40 new statements, 16 in financial-related areas and 24 in information technology (IT). The changes do not represent new risks or require the addition of controls for any organization. Management of each organization is responsible for maintaining a properly functioning system of internal controls. Therefore, identifying actual organizational risks and appropriate controls to be included in the customized local tool, remains a matter of local management judgment. The standard risks and controls provide a consistent core population of risks and controls, not an expectation that local management will include them in the local risk inventory. After reviewing the revised standard risk statements and controls, if management remains satisfied with the risks and controls already identified, no changes to the existing risks, controls, testing, and assurance processes are required. Additional effort is required only if review of the new statements and controls results in management identifying an applicable risk or control not previously recognized.

This year, the FMA tools and training were provided before issuance of the final guidance to solicit comments and minimize delays in management review of the updated risks and controls. This final guidance and the FMA Tool were revised based on comments from multiple organizations and supersede the previous draft guidance and previous version of the FMA Tool.

The two groups of changes are described below.

Financial-Related Changes. The financial-related changes were based on the review of the existing risk statements and controls in multiple areas, including accounting, budget, property management, grant management, and procurement, by program office subject matter experts (SMEs) in the respective areas. The SMEs revised risk statements and controls to reflect updated guidance and program standards.

IT-Related Changes. The IT risk statements and controls were significantly revised to reflect requirements in DOE Order 205.1B, *Department of Energy Cyber Security Program*, consistent with the National Institute of Standards and Technology (NIST) cyber requirements and processes. The new IT statements are structured to test compliance with the DOE order and NIST standards and to align with a parallel effort to address IT findings identified in both internal reviews and external audits.

C. Purpose

DOE management is responsible for establishing and maintaining effective internal controls and financial management systems that meet the objectives of FMFIA and revised OMB Circular A-123, which provides guidance for the execution of FMFIA. In accordance with FMFIA requirements and DOE Order

413.1B, DOE management is responsible for establishing an internal control program and annually evaluating internal controls and reporting on the status of any identified material weaknesses up through the chain of command to the President, Congress, and OMB. To support Departmental reporting, heads of Departmental elements are required to report on the status of their organizations' internal controls, including reportable conditions identified and progress made in correcting prior reportable conditions.

In order to comply with the requirements of FMFIA and OMB Circular A-123, all Departmental elements (inclusive of all integrated contractors) are required to perform one or more of the following types of internal controls assessments:

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

See Table 8, *Listing of Required Internal Control Evaluations by Departmental Element*, of this guidance for a full listing of required assessments for each Departmental element.

The FMS Evaluation is required of select Departmental elements under the requirements as prescribed by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and OMB Circular A-123, Appendix D, which provides guidance for compliance with FFMIA. Circular A-123, Appendix D went into effect October 1, 2013 and rescinds all previously issued versions of Circular A-127. Further detail regarding reporting for Departmental financial management systems under the requirements of Appendix D can be found in Section X, *FMS Evaluation*.

In addition, all Departmental elements are required to maintain written policies and procedures for implementing the internal controls evaluations process described in this guidance. These policies and procedures must include a quality assurance (QA) program to be conducted by DOE field offices on submissions by their respective labs for quality and accuracy of the content.

Management for each Departmental element should perform a QA validation before the submission of quality assurance results to the Office of Financial Risk, Policy, and Controls (CF-50). Senior management is responsible for ensuring that risk assessments, testing 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.

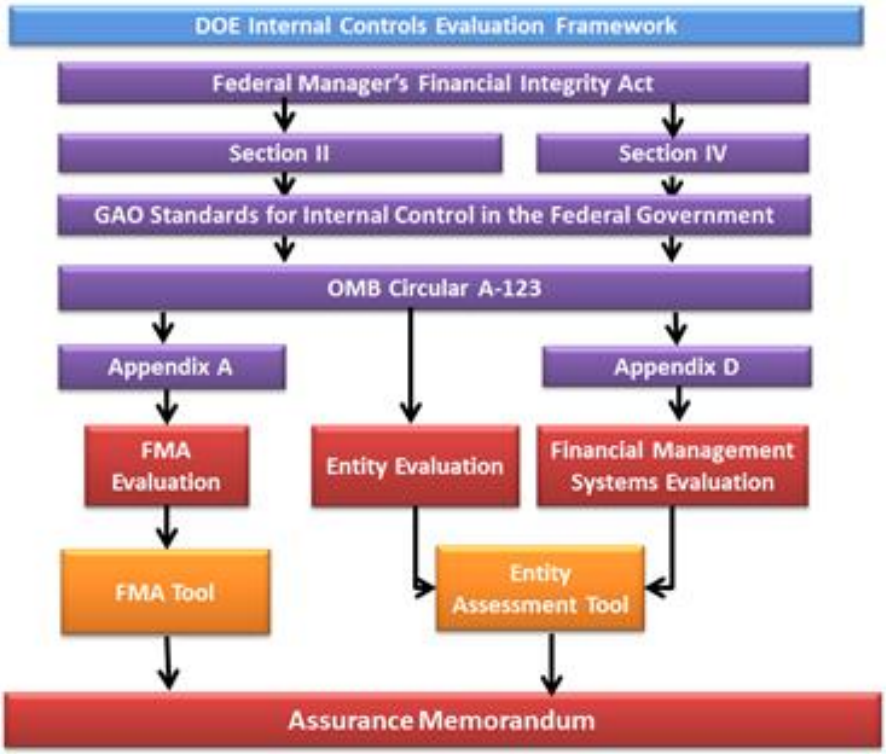
At the conclusion of the evaluation process, each Departmental element will summarize the results of their internal controls evaluations in their annual Assurance Memorandum. Through the Assurance Memorandum, the head of each Departmental element provides reasonable assurance that financial and entity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

All field offices submit their Assurance Memoranda to the appropriate Lead Program Secretarial Office, with copies to the Cognizant Secretarial Office. Headquarters offices, considering any information submitted by their field offices, submit their Assurance Memoranda, addressed to the Secretary, to the Office of the Chief Financial Officer (OCFO). Field Office and Headquarters Office consideration of lower level assurances includes determining if a reportable condition or material weakness reported at the

lower level is significant enough to be reported for the higher level organization as a whole. OCFO, in conjunction with the Departmental Internal Control and Audit Review Council (DICARC), assesses the assurances made from all the Departmental elements and provides the Secretary with a recommendation to sign the agency's Statement of Assurance. The final Statement of Assurance from the Department is then published in the Agency Financial Report and transmitted to the President, Congress, and OMB.

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

Figure 1: DOE Internal Controls Evaluation Framework



D. Benefits of Performing Internal Controls Evaluations

Ongoing evaluation of internal controls can provide significant benefits to all Departmental elements. Controls are designed to help mitigate risks. Thus, a controls assessment can show how well risk mitigation strategies are working and which strategies may need to be modified and improved. Ultimately, controls assessments serve as a tool that management can use to gauge the performance of a mission-based area. They can be tailored to show a macro perspective of an entire Departmental element as a whole or drill down into specific functions and processes. Performing controls assessments allows managers to gain insight into the effectiveness of their programs and can lead to substantive improvements and best practices in meeting mission objectives.

II. Important Dates

Table 1 below lists important dates in the Internal Controls Evaluation process. This includes deadlines for quarterly and annual reporting requirements. Management quality assurance reviews need to be completed prior to the submission of the quarterly FMA Tool and EAT annual report.

Table 1: DOE Internal Controls Assessment Process Important Dates

Date	Description
April 15, 2015	Upload second quarter FMA Tool and FMA Quality Assurance Report to Internal Controls iPortal Space.
April 15, 2015	Entity status update (teleconference) to discuss any known preliminary issues in high risk areas or focus areas.
June 30, 2015	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 2, *FMA Evaluation Test Cycles,* for requirements)
June 30, 2015	Departmental elements performing FMA evaluations complete corrective actions and re-testing of all controls in remediation, which may have a negative impact on the Statement of Assurance.
July 15, 2015	Upload third quarter FMA Tool and FMA Quality Assurance Report to Internal Controls iPortal Space.
July 15, 2015	Field offices and Power Marketing Administrations upload Entity Assessment Tool to Internal Controls iPortal Space.
August 3, 2015	Field offices and Power Marketing Administrations upload Assurance Memorandum to Internal Controls iPortal Space.
August 14, 2015	Headquarters offices upload Entity Assessment Tool to Internal Controls iPortal Space.
September 1, 2015	Headquarters offices upload signed copies of the Assurance Memorandum to Internal Controls iPortal Space.
October 1, 2015	Organizations that resolve or identify a material weakness, after June 30, 2015 but by September 30, 2015, that is not included in a submitted assurance statement, must notify the OCFO and update the assurance statement.

III. GAO Standards for Internal Control in the Federal Government

In 1999, GAO issued revised Standards for Internal Control in the Federal Government. This document outlines a framework for federal agencies to follow in establishing their internal control programs. In this framework, GAO identifies five standards 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."[1]

The five components representing the highest level of the hierarchy of standards of internal control are described below.

1. Control Environment

The control environment consists of the organizational structure and culture created by management and sustained by employees that provides organizational support for effective internal control. The assessment should include obtaining a sufficient knowledge of the control environment to understand management's attitude, awareness, and actions concerning the control environment. The assessment should consider the collective effect on the control environment, since management's strengths and weaknesses can have a pervasive effect on internal control. Specific elements of the control environment that should be considered include:

[1] *Standards for Internal Control in the Federal Government*, Government Accountability Office, GAO-14-704G.

- integrity and ethical standards;
- commitment to competence;
- management philosophy and operating style;
- organizational structure;
- assignment of authority and responsibility; and
- human resources policies and practices.

2. Risk Assessment

Risk assessment is the process by which management identifies internal and external risks that may prevent the Departmental element from meeting its mission objectives. The assessment should determine how management identifies risks, estimates the significance of risks, assesses the existence of risks in the current environment, and relates them to operations. The assessment should include obtaining sufficient knowledge of the agency's process on how management considers risks relevant to mission objectives and decides about actions to address those risks. The results of this assessment at the Departmental element-level will drive the extent of testing and review performed of internal controls. Some significant circumstances or events that can affect risk include:

- complexity or magnitude of programs and operations;
- extent of manual processes or applications;
- changes in operating environment;
- new personnel or significant personnel changes;
- new or revamped information systems;
- significant new or changed programs or operations;
- new technology; or
- new or amended laws or regulations.

3. Control Activities

Control activities are the mechanisms that help ensure that management directives are carried out, mission objectives are met, and risks are effectively mitigated. The assessment should include obtaining an understanding of the control activities applicable at the Departmental element-level, such as:

- policies and procedures;
- management objectives (clearly written and communicated throughout the agency);
- planning and reporting systems;
- analytical review and analysis;
- segregation of duties;
- safeguarding of assets; and
- physical and access controls.

4. Information and Communication

Relevant, reliable, and timely information should be communicated within the organization to relevant personnel at all levels and externally to outside stakeholders. The assessment should include obtaining an understanding of the information system(s) relevant to performance of mission objectives. Such an understanding should include:

- the type and sufficiency of reporting produced;
- the manner in which information systems development is managed;
- disaster recovery;
- communication of employees' control-related duties and responsibilities; and
- how incoming external communication is handled.

5. Monitoring

The effectiveness of internal controls should be monitored during the normal course of business. The assessment should include obtaining an understanding of the major types of activities the Departmental element uses to monitor internal controls, including the source of the information related to those activities and how those activities are used to initiate corrective actions. Several examples include:

- self-assessments by managers;
- periodic reviews, reconciliations, or comparisons of data;
- evaluation by the IG or external auditor; and
- direct testing.

These five components must operate together in an integrated manner for an internal control system to be effective.

IV. Focus Areas

The Department annually identifies focus areas for the Financial Management Assurance (FMA) evaluation and Entity Evaluation processes. The focus areas are derived from repeat audit findings or areas of high risk within the Department, and therefore, represent areas of emphasis that require additional management assessment. Additional focus area guidance is contained in Section VIII.E, *FMA Focus Area Guidance*, and Section IX, *Entity Evaluation*.

V. Importance of Risk Assessment in Internal Controls Evaluations

Accurate assessments of both financial and non-financial risks are integral to performing effective internal controls evaluations. Management should use risk assessments to identify which areas in the organization pose the highest threat to mission achievement if controls are not in place and functioning properly. In the passage below, GAO describes the responsibility of management to assess risk as part of maintaining adequate internal control.

> Internal control should provide for an assessment of the risks the agency faces from both internal and external sources. Once risks have been identified, they should be analyzed for their possible effect. Management then has to formulate an approach for risk management and decide upon the internal control activities required to mitigate those risks and achieve the internal control objectives of efficient and effective operations, reliable financial reporting, and compliance with laws and regulations.[2]

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 recurring program or project reviews.

1. Risk Identification

An organization must define its mission-based objectives before conducting a risk assessment. Following this, the organization can identify the primary risks facing each of those objectives. In

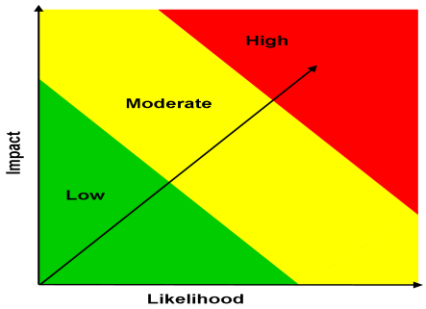
[2] *Internal Control Management and Evaluation Tool*, Government Accountability Office, GAO-01-008G, 2001.

addition, risks 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. Both financial and non-financial risks must be considered during the process. The organization should also consider both internal and external factors. Once identified, risks should be stated in an "if, then" or "cause and effect" format. The following are examples of common risks within DOE.

- 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

In rating 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 below:



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 organization's "real-life" operating environment. At a minimum, an annual reassessment of risk ratings should be performed.

3. Risk Ranking

Ranking risks helps to prioritize management's attention to and decisions on the control environment. Risk rankings can be driven by measures of management concern (e.g., the dollars exposed; potential reputational damage; the anticipated cost to remediate an event, if the risk were to occur; the immediacy of the timeframe in which the risk could occur, etc.). In other words, if a risk were to impact near-term mission objectives, then management may prioritize that risk in its rankings.

When ranking risks, management should first consider those risks that were rated "high" or "moderate", in the context of these additional measures of concern. Those risks that management ranks highest are typically the risks that management will choose to mitigate first.

B. Determining a Risk Response

After risks are assessed, management can then determine its risk response. Management should have a clear concept of 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 preferred risk response – to accept, avoid, reduce, share, or transfer a risk. In selecting its risk response, management should give consideration to the current operating environment, including what existing processes can be leveraged to manage certain risks.

Establishing controls to manage risk is a common risk response. Typically, controls are put into place when the choice is to reduce or share a risk. Controls also may be implemented to avoid a risk. Management should keep in mind that controls can provide only reasonable assurance – not absolute assurance – that the risks will be mitigated. The risk that remains, or residual risk, should be within levels 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 a strengthening of existing controls or additional controls to be put in place. If, in the evaluation process, one finds that an area of high risk has insufficient controls to adequately mitigate the risk, management should consider redesigning the existing controls. Alternatively, management can consider implementing additional controls. When determining the need for additional controls in high risk areas, managers must balance the cost of implementing an additional control with the benefit that control will bring in terms of added risk mitigation. There will be some areas in the high risk category that are inherently risky. The placement of additional controls may not result in greater mitigation in such instances.

Integration of Risk Assessments in Internal Controls 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. While it is expected that a determination of risk plays a key role

in the internal controls evaluation process for each Departmental element, the results of those risk assessments are not required to be submitted with the Assurance Memorandum.

Documentation of the financial and non-financial risk assessments for each Departmental element should be maintained locally and is not part of the required documentation to be submitted to the Office of the Chief Financial Officer, except as part of the documentation required for the FMA Tool, as discussed in Section VIII.A, *FMA Tool*.

Risk Assessments Inform Controls Assessments

Once a risk assessment is performed, management must assess and evaluate its financial and non-financial internal controls to assure that the control activities being used are effective and updated when necessary, by conducting a controls assessment. A control assessment is a formal review of the processes and controls associated with a specific, or set of, risk(s) to evaluate their effectiveness. A control assessment is a component of the overall internal controls evaluation process.

Generally speaking, sound business practices would dictate that 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 only tested once every three years. See required test cycle for FMA Evaluations in Section VIII.B, Table 2, *FMA Evaluation Test Cycles.* Previously reported significant deficiencies and material weaknesses should be tested each year until the controls are no longer deficient.

VI. Evaluating Control Assessment Results

As discussed in the CFO Council Guide, test results evaluation section, test results should support management's judgment whether a control is functioning adequately. Exceptions noted in the testing of properly designed internal controls could indicate ineffectiveness. Management must consider the extent of a deficiency in such cases. Deficiencies can range from a *simple deficiency* (e.g., missing initials indicating a supervisor's review on 1 of 26 reconciliations sampled) to a *significant deficiency* (e.g., only 8 monthly reconciliations were performed for the year) that results in some loss of resources, to a *material weakness* (e.g., reconciliation of several key accounts were not performed throughout the year) that results in a major loss of resources or breaches in security. A simple deficiency is an internal control deficiency that creates minimal exposure for management and is generally considered an anomaly. A significant deficiency usually indicates a history of internal control deficiencies that, when consolidated, equate to a reportable condition 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 simple 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 for the organization 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 specific controls assessment processes applied at the Department.

VII. Internal Control Evaluations Overview

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

- 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 Transaction Level; and
- Step 5: Concluding, Remediation, and Reporting.

Management's quality assurance program and related validation should encompass all of the above steps.

Step 1: Planning

Before beginning an evaluation, a certain amount of planning is required. Each reporting entity should review all of the processes and sub-processes applicable to their functions. Detailed steps for these processes and how they interact, as well as the controls put in place to mitigate known risks within those processes, should be diagrammed in a process map. Changes in any processes should be identified and the process map should be updated. In addition to updating the process maps, reporting entities should review all of the current controls in place within these processes to determine if their design is still adequate to address the risks they are mitigating. Example test plan and results templates are available 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 IX, *Entity Evaluation*, of this guidance.

Step 3: Evaluating Internal Control at the Process Level, and

The processes to execute these steps are described below in Section VIII.

Step 4: Testing Control Design and Operating Effectiveness at the Transactional Level

The processes to execute these steps are described below in Section VIII. 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 VIII.D, *General Documentation Requirements*, and Section XII, *Glossary*, of this guidance.

Documentation occurs within each of the basic steps outlined above, whether documenting the evaluation methodology during the planning step or documenting key processes and test results during the evaluation and testing steps.

VIII. Financial Management Assurance (FMA) Evaluation

The FMA Tool serves as the primary 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 specifically to support the FMA Evaluation. However, reporting entities should reference in the FMA Tool the existing documents that support the identification of the controls and verification of the applicability of the standard process, sub-process, and corporate risks to the site. Such documents can take the form of process mapping.

A. Financial Management Assurance (FMA) Tool

Specifically, the following should be completed by all reporting entities that are required to perform an FMA Evaluation (see Table 8, *Listing of Required Internal Control Evaluations by Departmental Element*, for a detailed list):

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.
4. 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", or not relevant, in the Exposure column.

   Within the FMA Tool, reporting entities are required to document the rationale for risks assessed to have an exposure rating of "NR".
5. In the Risk Assessment section of the tool, an exposure risk assessment for each identified risk should be conducted, assuming no controls are in place, and the appropriate rating (i.e., not relevant (NR), Low, Moderate, or High) should be input in the tool. Exposure risk ratings are based on the likelihood of the risk occurring and the impact on the reporting 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 XII, *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, other changes (e.g., audit, IG, GAO, etc.).
6. 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.

   - **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 occurrence.
     - **2 =** Risk occurred within acceptable threshold.
     - **3 =** Risk occurred outside the acceptable threshold.

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

   - A graph combining risk occurrence ratings and control set execution ratings to determine the control risk can be found in Section XII, *Glossary*. Example 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 can be found in Section XII, *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 within all business processes and sub-processes must be placed on a three-year testing cycle, including those processes that have risks with a Low Exposure rating and no control risk rating. If controls have not been previously tested within the past two years, they will need to 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.

10. 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 the submission of QA Tool results to CF-50. 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 2: FMA Evaluation Test Cycles

Risk Ratings			Test Cycle
Exposure Risk + Control Risk = Combined Risk			
High	High	**High**	**Annual (every year)**
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 that ALL risks are managed and that related controls are identified and functioning, using the most effective and efficient methods deemed reasonable. Specific testing for FMA is required on a cycle of at least every 3 years for ALL controls within 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 will need to 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 "UKN" (unknown) and require further analysis or retesting in the current year.

In FY 2015, Departmental elements are expected to perform the steps outlined below.

1. Follow the risk-based test cycles described in Table 2 above 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, 2015. 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 2). 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 above in Table 2).
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 2 above 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, 2015, 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. A CAP template is provided on the Internal Controls iPortal space under the Resources tab.

While there is not a prescribed format for a CAP, it should contain the key elements listed below:

- 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.

The significant information should be summarized in the CAP-Tracking tab of the FMA Tool. Departmental elements will maintain the CAPs and will not be required to submit the CAPs unless requested by the OCFO.

4. Complete required actions to address all FY15 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 within the assessment year (if exposure risk is rated moderate or high). Section VIII.E, *FMA Focus Area Guidance*, provides additional information on focus areas and specific requirements for assessing these areas.

5. If, during the course of testing, any best practices are identified for improved control effectiveness, efficiency, or monitoring, they should be denoted in the Assessment Tab of the FMA Tool as "efficiency opportunities." Departmental elements are encouraged to document those best practices and share them with the appropriate Departmental element, where applicable. These best practices will be shared with other Departmental elements, in order to facilitate control improvements agency-wide.

C. Testing Requirements

There are a variety of different techniques available to test internal controls. Below are just a few that may be considered in conducting tests of internal controls.

- Interviews, which can be either in-person or through the use of questionnaires. In general, it is considered a best practice to have information gathered from interviews, corroborated with a secondary type of evidence. However, this may not always be possible.
- Direct observation of performance of the control.
- Physical examination or inspection of documents.
- Transaction testing and re-performance, the latter being most commonly used when testing automated controls.

Organizations may employ a variety of evaluation activities and consider a wide-range of reliable existing information to effectively identify the appropriate techniques to be used to test internal controls. Examples of typical activities and considerations include, but are not limited to:

- Departmental Management Priorities;[3]
- Consideration of the results of Inspector General (IG) and GAO audit reports (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 controls evaluation reporting (provided to Lead Program Secretarial Offices and Cognizant Secretarial Offices prior to year-end reporting);
- Review and analysis of performance reporting results;
- Consideration of the results of other internal or external assessments;
- Conduct of management meetings or interviews with critical staff regarding key control areas;
- Review of relevant management reports (e.g., safety manager reports, infrastructure status reports, etc.); and
- Review and analysis of other relevant and reliable information.

Reporting entities must use dual-purpose testing where applicable. Dual-purpose testing is 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 is important because it provides a mechanism for ensuring that controls are actually effective in risk mitigation, thereby reinforcing the site's control design effectiveness decision. Test plans should clearly convey this type of 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 guidelines outlined below when selecting testing samples.

- Use professional judgment in determining appropriate sample sizes for testing.
- Sample sizes should be selected considering the:
  - combined risk rating;
  - sample universe; and
  - control attributes (e.g., frequency, mode, type, etc.).
- Reporting entities should at a minimum use the OMB and CFO Council Guide sample size guidelines presented in Figure 2 below. If there is deviation from the sample guidelines the rationale should be documented in the workpapers.

[3] Complete summaries of the Management Priorities can be found in the FY 2014 Agency Financial Report: http://www.energy.gov/sites/prod/files/2014/11/f19/DOE_FY2014_AFR.pdf.

Figure 2: 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.

D. General Documentation Requirements

In addition to the control and process documentation requirements, as described in Section VII, *Step 1: Planning*, reporting entities must also ensure the following activities are documented to support internal and 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" 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 3 below. Testing results **must be updated** in the FMA Tool.

Table 3: Key Test Plan 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	Approver
Universe from which sample size was selected	Who performed the test

- Remediation Activities – CAPs **must be maintained** and be readily available to support reviews or audits for all remediation activities identified in the FMA Tool. The FMA Tool **must also be updated** to summarize key remediation information required in the Assessment tab. In addition, a summary of all current and previously reported open reportable conditions and material weaknesses should be included in the Assurance Memorandum. Please see Section XI, *Annual Assurance Memorandum*, for explicit instructions on completing the Assurance Memorandum.
- Best Practices – Reporting entities should leverage the FMA Evaluation process to identify future improvements in efficiency, effectiveness, or monitoring. In addition, reporting entities may use the Efficiency column in the FMA Tool to note the potential best practice and briefly document the nature of the best practice for future use. Reporting entities are encouraged to share best practices with the OCFO in order to facilitate implementation of possible improvements agency-wide. Such activities should be pursued as time and resources permit; however, there are no specific requirements for adopting efficiency changes.

E. FMA Focus Area Guidance

In FY 2015 there are 37 FMA focus areas for the following business processes:

1. Acquisition management
2. Project cost management
3. Property management
4. Environmental liabilities, and
5. Information technologies

The focus areas are managed through the "Focus Area" tab in the FMA Tool. This tab includes all corporate risks, with focus area risks highlighted with a "Y" in the "Focus Area" Column. In addition, for each focus area risk, the "Description/Action Required" column provides information on what actions are to be taken in FY 2015, as well as some insight into why a particular area was selected**.**

When a focus area is selected in the "Focus Area" tab (this is done 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 shows up in the current year scope. Reporting entities should review and take the appropriate actions as 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. Once this is done, the "Corp Request" column in the "Assessment" Tab will change to an "A" to indicate a focus area existed and site action was taken.

At every reporting entity, focus area actions should be taken if the exposure rating for these 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 need to be tested on at least a three-year testing cycle. An "NR" rating may also be given if there is no activity related to that focus area risk. This risk rating 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 specifically state that processes or other specific activities be documented, (e.g., roles and responsibilities or a communications strategy, etc.). Please be sure that the specific required actions are performed. In cases where processes are requested to be documented, the site should prepare supplemental process narratives or flows, and maintain that documentation in a current status on an on-going basis.

Process Documentation: Process or other documentation required should be maintained locally. This documentation is critical for supporting the FY 2015 financial statement audit conducted by DOE's external auditor. In addition, the process documentation for the focus areas will likely be requested for quality assurance and peer review purposes.

IX. Entity Evaluation

As in prior years, all Departmental elements are required to perform an evaluation, as shown in Table 8, of the internal controls in place for non-financial functions (administrative, operational, and programmatic), collectively 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 incorporate a variety of techniques to provide the required level of assurance. Headquarters elements with cognizance over Field reporting elements will need to take into account 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 synthesized results for the entire agency to the President, Congress, and OMB through the Statement of Assurance.

Section II of FMFIA requires an assessment of non-financial controls to assure their effectiveness and efficiency and their compliance with laws and regulations. There are several principles that can help guide each Departmental element's performance of the Entity Evaluation.

1. The purpose of internal controls evaluations is to test the effectiveness of controls already in place and identify gaps in internal controls.
2. Internal controls must be tested to determine if the controls are functioning effectively and performing their designated objectives.
3. The results of internal controls evaluations must be documented and retained to support the conclusions reached.
4. The results of internal controls evaluations provide the basis for the Department's Statement of Assurance, which is published in DOE's Agency Financial Report.
5. The monitoring of internal controls is an on-going process. Assessments of internal controls are not limited to an annual exercise and may be conducted multiple times per year, especially in areas that have high inherent risk or are central to mission fulfillment. Therefore testing should not be held up pending the issuance of annual guidance. While the head of the Departmental element is responsible for the direction and oversight of internal controls evaluations, the evaluations can be performed by other in-house or contractor personnel.
6. If significant control deficiencies or indications of potential weaknesses are identified, these issues must be reported.

Entity Focus Area Guidance

There are 11 non-financial focus areas identified in the Entity Assessment Tool (EAT) with a "Y" in the "Focus Area" column in the "Entity Evaluation" tab. The focus areas are as follows:

- Control Environment (Workforce Planning);
- Risk Assessment (Risk Management Process, Technological Capabilities, Infrastructure Status, Systems and IT Posture, Safety and Health Posture, Security Posture);
- Control Activities (Project Cost Management, Planning, Programming, Budget and Evaluation) and
- Monitor Performance (Audit Resolution and Follow-up).

All focus areas should be addressed by management by considering and reviewing each area based on the control objectives and considerations stated in the EAT. Management should also ensure that assessments are conducted and that established corrective actions have been completed and tested. The "Basis of Evaluation" section of the EAT should reflect the results of controls assessments for each Focus Area, if applicable.

Entity-level Risk Assessments

Risk assessments should be performed before beginning the entity control assessments. Entity-level risk assessments are performed by each Departmental element and documentation on these assessments must be retained locally.

As discussed in Section V, *Importance of Risk Assessment in Internal Controls Evaluations*, entity-level risks should be assessed at least annually, and should focus on the key non-financial risks that would impact the organization's ability to meet its mission objectives. Risks should be identified, rated, and ranked, according to areas of management concern. Several examples of non-financial risks are provided in Section V.

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, which is submitted to CF-50, 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, etc.); 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.

A. Four-Step Evaluation Process

The Entity Evaluation process has four steps.

1. Perform the Evaluation: Each Departmental element will be responsible for performing an Entity Evaluation to assess the effectiveness of its most critical entity internal controls for ensuring that mission objectives are met effectively, efficiently, and in compliance with applicable laws and regulations. Departmental elements should leverage existing resources and assurance activities to perform this assessment.
2. Prepare and Track Corrective Actions: CAPs should be developed and tracked through completion for any control deficiencies identified. Once a corrective action is completed it must be tested for effectiveness.
3. Document the Evaluation: Each Departmental element will document the Entity Evaluation using the EAT, which will be provided to all FMFIA points of contact to guide and substantiate the assessment and remediation process.
4. Report the Results: The results of the Entity Evaluation will be reported in an annual Assurance Memorandum.

1. Perform the Evaluation

The Entity Evaluation evaluates the Departmental element's controls against the five GAO Standards for Internal Control. The five standards are broken down into 22 key control areas that must be evaluated.

Departmental elements may elect to perform the Entity Evaluation using a variety of techniques; however, two basic tenets must be followed in any assessment. First, all assessments must touch on

every aspect of the Departmental element. Second, all assessments should consider the five GAO Standards for Internal Control, as previously described in Section III of this document.

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.

In addition, reporting entities should consider establishing sample sizes and failure thresholds for each control being tested. It is important to determine in a test plan how many instances of a control activity will be tested and of those instances, how many failures of individual instances of the control activity constitute a failure of the entire control. Specific guidance on performing control tests, including guidance on sample sizes, is provided in Section VIII.C, *Testing Requirements*.

Leveraging Existing Assurance Activities

FMFIA requires management to monitor the status of internal controls on an on-going basis and design control systems to address key risks. As such, Departmental elements should seek to leverage the results of existing assurance systems, such as the Contractor Assurance System, and other information, to the extent possible, to help evaluate the current status of controls. Where existing information and activities are not sufficient to validate the current status of controls, programs should identify and take additional steps to verify the status of the controls to ensure there is adequate support for the program's certifications in the annual Assurance Memorandum.

Departmental elements should perform additional evaluation and validation activities where relevant and reliable information is not available to be leveraged.

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 reportable condition 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 XI, *Annual Assurance Memorandum*. CAPs for reportable conditions and material weaknesses should be prepared and tracked locally. In addition, summary information for the CAP should be maintained in the EAT. Please refer to the EAT User Guide for detailed instructions on how to document CAPs in the EAT.

3. Document the Evaluation

The EAT will be provided to your program's specific FMFIA point of contact to document critical information regarding your Entity Evaluation in a common format to support corporate consolidation and analysis. The completed EAT will be submitted in advance of the Assurance Memorandum and will serve as the primary source of documentation for the FMFIA Entity Evaluation.

The EAT will document the most critical supporting information including:

- the basis of evaluation for standardized key control areas;
- the results of the review;
- impact assessments for significant issues identified; and
- other critical information.

As such, it will not be necessary to maintain additional extensive documentation to support the assessment, assuming a thorough job is done in completing the EAT.

Reporting entities will not be required to keep copies of key documents leveraged for the evaluation in a central location. However, the location of the documents can be noted in the EAT and documents must be readily available if requested during controls assessments or quality assurance reviews by Headquarters CFO staff, peer review teams, or internal and external auditors. 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, etc.). Documentation beyond the EAT and the Assurance Memorandum should be maintained locally unless requested by the CFO, Inspector General, or peer review teams.

It is management's responsibility to ensure that the EAT comprehensively documents the results of the Entity Evaluation process. Management should perform a quality assurance review on the EAT before submission, to ensure that risk assessments, testing plans, sample sizes, and final results are compliant with DOE guidance. Departmental elements should establish and document their QA process and results.

4. Report the Results

Results of the Entity Evaluation should be reported in the annual Assurance Memorandum. To determine what to report in the Assurance Memorandum, review all of the issues rated as a "1", "2", or "3" in the EAT. These issues are known as control deficiencies. Those deficiencies rated as a "2" or a "3" may rise to the level of a reportable condition 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 4 below for a description of "1", "2", or "3" ratings in the EAT.

Table 4: EAT Issue Ratings

Ratings		Description
1	**Non-Significant Issue**	An issue which **would not** have a "Significant" current or potential future negative impact on meeting mission or mission support objectives, operating in a safe and secure manner, or meeting major internal or external commitments, but represents an issue management would like to address and periodically review.
2	**Potential Significant Issue**	An issue with a "Significant" negative impact on meeting mission or mission support objectives, operating in a safe and secure manner; or meeting major internal or external commitments, that are **potential future issues** (i.e., likely impacts **a year or more away**) trending towards negative impacts, trending and unacceptable risk levels, or will negatively influence outcomes if not addressed.

Ratings		Description
3	**Immediate Significant Issue**	An issue with a "Significant" negative impact on meeting mission or mission support objectives, operating in a safe and secure manner; or meeting major internal or external commitments, that are **currently negatively** influencing outcomes or which will most likely have a **negative impact within the next year** if not addressed. This would also include issues which have resulted in the entity **managing** an activity **at an unacceptable level of risk**.

Please note that all reportable conditions must be reported in the Departmental element's Assurance Memorandum and must have a CAP Summary attached. In addition, all control deficiencies must be documented in the EAT.

Please see Section XI of this guidance for detailed instructions on how to compose and address the Assurance Memorandum. A macro-enabled template for the Assurance Memorandum is also available as a separate electronic attachment to this guidance. Please note that there are two Assurance Memorandum templates – one for field offices and one for headquarters offices. Please make sure to use the appropriate template.

X. 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. This will support core requirements of Section IV of FMFIA and the *Federal Financial Management Improvement Act* (FFMIA). Only Departmental elements listed as system owners should perform the FMS Evaluation.

Effective in FY14, the requirements governing agency financial systems are now contained in OMB Circular A-123, Appendix D. The requirements under OMB Circular A-127 were explicitly rescinded. Appendix D to Circular A-123 replaces A-127's "check-the-box" compliance approach with more of an outcome-based approach focusing on financial management, business, and information needs. The previous Conformance Criteria have been updated accordingly with Financial Management Goal areas, as described below. The updated Financial Management Goals articulate what the Department wants to achieve to advance its mission and address relevant problems, needs, and challenges. Achievement of these Goals should be assessed to determine whether the Department is in compliance with FFMIA.

OMB Circular A-123, Appendix D,[4] defines a financial management system broadly 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."

[4] OMB M-13-23, Appendix D to Circular No. A-123, *Compliance with the Federal Financial Management Improvement Act of 1996,* Sept. 20, 2013 (interim final version), supersedes OMB Circular A-127.

Table 5 on the following page provides the applicable DOE financial systems inventory and system owners.

Table 5: DOE Financial Management Systems

Financial Management System	System Owner(s)
Power Marketing Administration Systems	**BPA, WAPA, SWPA, & SEPA**
iManage 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-10**
Departmental Inventory Management System (DIMS)	**NNSA-NA-73**
Integrated Planning, Accountability and Budgeting System (IPABS)	**EM-62**
Facilities Information Management System (FIMS)	**MA-50**
iManage 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**
Vendor Invoice Approval System (VIAS)	**OR**
iBenefits	**CF-40**

In accordance with the FFMIA guidelines, system owners should determine whether the financial systems in Table 5 above conform to federal financial management systems requirements. FFMIA was intended to advance federal financial management by ensuring that federal financial management systems can and do provide reliable, consistent disclosure of financial data and that they do so on a basis that is uniform across the federal government from year-to-year, consistently using generally-accepted accounting principles.

A. FMS Evaluation Process

The FMS Evaluation process generally follows the same four-step process used for the Entity Evaluation, described in Section IX of this guidance. These four steps are:

1. Perform the Assessment;
2. Prepare and Track CAPs;
3. Document the Assessment; and
4. Report the Results.

1. Perform the Assessment

FFMIA requires agencies to have financial management systems that substantially comply with the federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the U.S. Standard General Ledger (USSGL) at the transaction level. Financial management systems shall have general and application controls in place in order to support management decisions by providing timely and reliable data.

To meet these requirements, those Departmental elements that are designated as owners of the financial management systems listed in Table 5 above must design and perform tests of those systems. These tests should be designed to evaluate the degree to which 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 stakeholders external to the Department, 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. Minimize federal financial management system security risks to an acceptable level.

There are three common test techniques that can be implemented to perform the necessary tests required for an FMS Evaluation:

1. Direct observation of performance of the control.
2. Physical examination or inspection of documents.
3. Transaction testing and re-performance, the latter being most commonly used when testing automated controls.

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

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

In some cases, a review of these types of documents could comprise the entirety of a test for a specific criterion. However, given the automated nature of the systems being tested, in many if not most cases, transaction testing will also be required. Regardless of the test techniques implemented, the design of each test should be documented in writing.

When designing tests for specific controls, sample sizes should be determined in the test plan. In general, when applying statistical sampling, the following factors should be taken into account: (1) desired confidence level, (2) importance or significance of the control being tested, and (3) ensuring that the selected sample size is representative of the population. These considerations will drive the determination of sample size for each control being tested.

2. Prepare and Track Corrective Actions

If system testing reveal that the system does not adequately conform to a particular criterion, a CAP should be developed to address the non-conformance and resolve it, thus bringing the system back into conformance. This CAP should be documented on the Action Tracking tab of the EAT. However, the Departmental element is still responsible for tracking the CAP and ensuring that the milestones it sets out for correction of the non-conformance are met.

If any of the non-conformances identified in the Entity Evaluation tab are determined to rise to the level of a material non-conformance, a detailed CAP must be developed and tracked locally. A CAP Summary should be submitted with the annual 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 completing the CAP Summary are provided in Section XI, *Annual Assurance Memorandum*.

3. Document the Assessment

The Entity Evaluation tab of the EAT provides a uniform Department-wide mechanism for documenting the FMS Evaluation. For each of the Financial Management Goals listed on the "Systems Evaluation" tab, a basis of evaluation must be recorded. Please note that the Financial Management Goals are exactly the same as the eight criteria listed above on which test design should be based.

For each of the eight goal areas, the basis of evaluation should briefly describe the type of test performed, its general design, and its outcome. If a physical examination of documents was performed, the titles of the documents should be included in this description.

4. Report the Results

Results of the FMS Evaluation should be reported in the annual Assurance Memorandum. All material non-conformances that are revealed as a result of system testing must be reported in the Assurance Memorandum. A summary of remediation activities for each material non-conformance should be included in the CAP Summary and attached to the Assurance Memorandum.

Please see Section XI of this guidance for detailed instructions on how to compose and address the Assurance Memorandum.

XI. 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 will further identify any significant control 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 such issues.

To facilitate early communication of any significant control deficiencies identified during the internal controls evaluation process, the OCFO will be hosting a mid-year status update with each reporting entity. Staff from the Office of Financial Risk, Policy & Controls will participate in individual conference calls with FMFIA points of contact for each reporting entity in mid-April. These calls will be an

opportunity for each reporting entity to share any control deficiencies identified to date in the evaluation process that may be reported as reportable conditions or material weaknesses in the entity's Assurance Memorandum, if it is anticipated that the issue may not be fully remediated by the end of the fiscal year.

Organizational assurance statements include an assessment of the effectiveness of the agency's internal control over financial reporting as of June 30. However, organizations remain responsible to provide an update to the statements when a material weakness is resolved or identified after June 30, as follows:

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

Organizations should notify the OCFO immediately of any resolved or new material weaknesses to be updated, but no later than October 1, 2015.

A. Reporting Documentation and Transmittal Methods

Each Departmental element will provide an Assurance Memorandum and selected other documents or files depending on the extent of evaluations required. In addition, certain documents will have different transmittal methods. Table 6 below provides specific instructions for transmitting required documentation.

Table 6: 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: Lead Program Secretarial Office with copies to the Cognizant Secretarial Office(s).
	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

A separate electronic macro-enabled attachment to this guidance provides the required templates for preparing the Assurance Memorandum. There are two templates, one for field offices and one for headquarters offices. Please ensure that the appropriate template is used.

The Assurance Memorandum consists of two main sections.

1. The Main Body – Contains the actual assurance statements and executive summaries of any reportable control deficiencies.

2. The CAP Summary – Provides a listing of action plans for each reportable condition, material weakness, or material non-conformance reported in the Assurance Memorandum. The CAP Summary should briefly describe the remediation activities that have 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 2015, the CAP Summary should also 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 financial reports, and are compliant with all applicable laws and regulations, lies with the head of each Departmental element. As such, 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 as well as the appropriate Under Secretary.

C. Determining Issues to be Reported

In the Assurance Memorandum, control deficiencies that meet certain criteria must be reported. In a typical control assessment, control deficiencies may be identified; however, only certain issues need to be specifically discussed and referenced in the Assurance Memorandum. Table 7 below provides a description of the types of issues to be reported for each section of the Assurance Memorandum, a definition for each issue type, and an indication of which issue types should be reported in the Assurance Memorandum (with corrective action plans).

Table 7: Definitions of Control Issues

Control Issue Type	Definition	Reported in Assurance Memorandum?
Financial Management Assurance Evaluation		
Reportable Condition	A control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential, will not be prevented or detected.	Yes
Material Weakness*	Reportable condition, or combination of reportable conditions that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.	Yes
Entity Evaluation		
Reportable Condition	A control deficiency, or combination of control deficiencies, that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal controls that could adversely affect the organization's ability to meet its internal control objectives.	Yes

Control Issue Type	Definition	Reported in Assurance Memorandum?
Material Weakness*	Reportable conditions which the head of the Departmental element determines to be significant enough to report outside of their department.	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 specific control objectives are not being met. This could be due to a deficiency in the design or operations of controls and may result in risk occurrence. Control deficiencies are only reportable if they meet the definition of a Reportable Condition or Material Weakness.	No
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.	Yes

* ***Material weaknesses resolved or identified prior to September 30, 2015, must be reported in the original or an assurance memorandum update.***

Considerations for Determining Material Weakness

As noted in Table 7 above, the consideration of a material weakness begins with a reportable condition (or combination of reportable conditions). Reportable conditions in turn 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 reportable condition or material weakness. Management's judgment is generally more straightforward regarding financial control deficiencies because the dollar amounts involved lend themselves to quantitative analysis to determine the potential impact on the financial statements is 'material.' An entity reportable control deficiency requires qualitative management judgment that a significant internal control weakness that could adversely affect the organization's ability to meet its internal control objectives, and an entity material weakness is a "reportable condition 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 should be developed for each identified material weakness:

1. Control Deficiency. The specific control deficiency, or combination of control deficiencies, causing the material weakness must be specifically identified to ensure 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, outside audit (IG/GAO) findings, or unexpected performance failures. Additional review and analysis may be required

to identify root cause control deficiencies when a control deficiency identified by other than normal testing. An audit finding or significant performance failure may identify the total lack of a needed control rather than the failure of an existing control. Note that an adverse outcome or performance failure that results from an adverse budget/funding decision does not indicate a control deficiency. Management controls and performance expectations should be adjusted to reflect budget/funding decisions.

2. Timing of Implementation, Remediation, or Mitigation. Once the control deficiency is identified and understood, 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 compiled into a CAP which includes a detailed timeline of the corrective actions. Reportable conditions for which corrective actions have been completed and tested, or which have been significantly mitigated by the corrective actions already accomplished, may not warrant being identified as a material weakness when the organization Assurance Memorandum is issued.
3. Report Outside of the Departmental Element. A material weakness is a reportable condition 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.

The information gathered and the decisions made related to the above considerations should be documented.

Table 8: 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	✓	✓	
	Rocky Mountain Oilfield Testing Center/Naval Petroleum Reserve-3		✓	
	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*	✓	✓	
	Energy Information Administration		✓	

	Departmental Element	FMA Evaluation	Entity Evaluation	FMS
	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*

XII. Glossary

Assurance Memorandum

Annual statement of assurance over the status of internal controls made by each Departmental element.

For further details regarding the required content of the Assurance Memorandum, please see Section XI, *Annual Assurance Memorandum*.

Basis of Evaluation

Represents the key information or activities leveraged or performed to provide reliable support for assurances that the control objectives and considerations have been addressed.

The Basis of Evaluation must be a tangible and documented activity to be valid. Examples include: transaction testing, safety managers' reports, annual infrastructure 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, etc.

Combined Risk Assessment

The residual risk considering the control environment. 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 will default to the risk exposure risk rating. If a risk factor is indicated to be present in the current year (e.g., system change, process change, etc.), then the combined risk will default 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 below 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

Control deficiencies exist when the design or operation of a control does not

allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A design deficiency exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met. An operation deficiency exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled 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 specific types of control issues that should be considered when performing the evaluation.

Specific end to be achieved to ameliorate, minimize, manage, or mitigate risks. Each objective takes into consideration the nature of the activity, the organization's mission, and the cost and benefits of each control technique in determining desired control objectives.

The positive things agency managers want to have happen or the negative things managers want to prevent from happening.

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.

Apply the ratings in the following table:

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 testing results of all

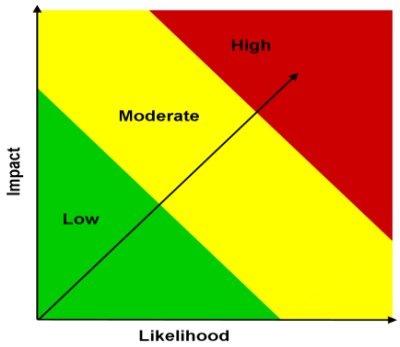
	individual controls within a control set. **1 -** Passed with no failures; **2 -** Passed with failures within acceptable threshold; or **3 -** Failed. **Risk Occurrence:** Determined during dual-purpose testing or through observation during normal business operations. Ask, did the risk occur during 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 of action to correct an internal control deficiency. A CAP must be prepared and tracked for all control deficiencies identified during the internal controls evaluation process. A CAP Summary for reportable conditions identified in the Memorandum of Assurance must be submitted along with the memorandum.
Departmental Element	Refers to Department of Energy headquarters mission and mission support offices and field and operation offices, and all DOE Agencies. This includes all contractors.
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. Pertaining primarily to functions or controls that are non-financial in nature (i.e., administrative, operational, or programmatic).
Entity Assessment Tool (EAT)	The primary system for documenting and reporting on 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 on the results of evaluations and testing of financial management reporting risks and controls.

FMA Quality Assurance

A macro-enabled Excel tool that is run from within a standard reporting

(QA) Tool and Report

package distributed by CF-50 to Departmental FMA contacts. After running the QA Tool, a report is created that houses the results of the review. The QA Tool highlights potential data anomalies for management review, and also 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."

OMB Circular A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, defines a "financial system" as "an information system or set of applications that comprise the accounting portion of the financial management system that maintains all summary or detailed transactions resulting from budgetary and proprietary financial activity.

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 of emphasis which require additional assessment within the year. Risks identified in focus areas within the FMA Tool will default to "Y" in the "Corporate Request" (Corp. Req) column of the Assessment Tab worksheet.

In the Entity Evaluation

The 11 cross-cutting control areas represent high risk control activities for ensuring an agency meets its core mission objectives. When issues are identified in these control areas, a more detailed impact assessment will be required to support corporate consolidation and reporting.

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 an organization's management that provides reasonable assurance that the following objectives are being achieved. • Effectiveness and efficiency of operations. • Reliability of financial and program 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, etc.) 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. The EAT defines the criteria against which conformance is evaluated and captures identified non-conformances.
Material Weakness	**Non-Financial reporting**- Reportable conditions which the head of the Departmental element determines to be significant enough to report outside the agency. **Financial reporting** - Reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.
Minimum Evaluation Standard	The basis by which testing cycles for the FMA Evaluation are determined. The minimum evaluation standard for FY 2015 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 within all business processes and sub-processes must be placed on a three-year testing cycle, including those processes that have risks with a

	Low exposure rating and no control risk rating. If controls have not been previously tested within the past two years, they will need to 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 a "mixed system" as a "hybrid of financial and non-financial portions of the overall financial management system."
OMB Circular A-123, including Appendix A	OMB Circular A-123 prescribes the guidelines for evaluating, improving, and reporting on internal controls. Appendix A requires an annual assurance statement on Internal Controls Over Financial Reporting (ICOFR).
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.
Reportable Condition	**Non-Financial reporting** – A control deficiency, or combination of control deficiencies, that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives. **Financial reporting** - A control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected.
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. The possibility of suffering harm or loss.
Risk Factor	Refers to the identification of changes that may affect the exposure risk or effectiveness of the existing controls in mitigating the risk. Risk factors include system changes, process changes, organization changes, and other changes (e.g., audit, IG, GAO, etc.). In the FMA Tool, the identification of risk factors changes the combined risk assessment in the FMA Tool to "UNK" (unknown) and requires analysis and retesting.

Risk Response	A determination by management on how a risk should be managed. Management must take into consideration the potential impact of the risk and the likelihood of occurrence, as well as the cost associated with mitigating the risk. Types of risk responses: ***Accept*** – No action is taken to affect risk likelihood or impact. ***Avoid*** – Exiting the activities that give rise to risk. This may involve changing project scope, using an alternate technology, selecting a different vendor or product, or canceling an initiative. ***Reduce*** – Action is taken to reduce risk likelihood or impact, or both, to mitigate a risk to an acceptable level. Typically performed through the placement of controls or other risk management activities. ***Share*** – Reducing the likelihood or impact of a risk by sharing a portion of the risk with another organization. This may include forming partnerships with other organizations that have a "stake" in the success of a mission objective. ***Transfer*** – Changing ownership of a risk from one organization to another; typically done through written acknowledgment.
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 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.
Standard Process	A process that is pre-populated in the FMA Tool and is required to be tested during the FMA Evaluation.
Standard Sub-process	A component of a standard process, also pre-populated in the FMA Tool.
Statement of Assurance	An annual statement required by the *Federal Managers' Financial Integrity Act* (FMFIA) that represents the Secretary's informed judgment as to the overall adequacy and effectiveness of internal controls within the Department. The statement reports the results of evaluations made on the Department's entity, financial, and financial management systems controls, including any material weaknesses or material non-conformances identified during the fiscal year. Also, updates of corrective action progress made on existing material weaknesses and material non-conformances are included in the statement. The annual Statement of Assurance is included in the Department's Agency Financial Report. This statement is generally based on the fiscal year period from October through September.
Testing Activity	A procedure to determine whether internal control systems are working in accordance with internal control objectives.