U.S. DEPARTMENT OF ENERGY

Enterprise Risk Management

Fiscal Year 2024
Guidance

[This Page Intentionally Left Blank]

Department of Energy
Washington, DC 20585

December 28, 2023

MEMORANDUM FOR DISTRIBUTION

FROM: KARIN DASUKI Karin Dasuki Digitally signed by Karin Dasuki Date: 2023.12.28 14:53:54 -05'00'
DIRECTOR, OFFICE OF FINANCE AND ACCOUNTING

SUBJECT: Department of Energy FY 2024 Enterprise Risk Management Guidance

The attached Department of Energy (DOE) FY 2024 Enterprise Risk Management (ERM) Guidance provides DOE's framework for ERM as required by the Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. This ERM guidance includes risk management, internal controls and a fraud risk framework that meets the requirements of the Government Accountability Office (GAO) *A Framework for Managing Fraud Risks in Federal Programs*.

DOE's ERM and Internal Control Program continues to execute initiatives to reduce burdens on reporting organizations while maintaining effective internal controls for the Department. The initiatives are:

- Continuing the implementation of a Departmental Fraud Risk Framework to mitigate and reduce potential fraud activities by establishing risk tolerances, and continuing to establish a data analytics program that leverages existing business practices; and
- Continuing the synchronization of the Department's Risk Profile to the Planning, Programming, Budgeting, and Execution processes to better align funding to needed resources during Budget Formulation.

Heads of Departmental Elements (Field and Headquarters) and Under Secretaries are responsible for maintaining an ERM Program that includes evaluating internal controls and reporting the evaluation results to the Secretary in annual Assurance Memoranda. These Assurance Memoranda report on the overall adequacy and effectiveness of internal controls, identify any material weaknesses or significant deficiencies and assert financial management systems compliance with government-wide requirements. These individual organizational assurances are compiled to support the Secretary's annual assurances in DOE's annual Agency Financial Report (AFR).

Signed Assurance Memoranda are due from Field Elements on **September 4, 2024,** Headquarters Offices and Power Marketing Administrations on **September 17, 2024,** and each Under Secretary on **September 24, 2024**. If there is an issue preventing a timely Assurance Memorandum, organizations must provide the reason(s) for the delay and advance notice of any potential significant deficiencies or material weaknesses to the monitored Internal Controls and Fraud Risk Management Division mailbox. A summary of all key dates and deliverables is provided in **Table 2** *Consolidated Summary of DOE ERM Important FY 2024 Dates*, found on **page 14**.

If you have any questions about this guidance, please contact the monitored mailbox at CFO-ICFRMD@hq.doe.gov.

DISTRIBUTION LIST:

S-1 Chief of Staff
S-2 Chief of Staff
Under Secretary for Science and Innovation
Under Secretary for Infrastructure
Under Secretary for Nuclear Security/Administrator for National Nuclear Security Administration
Assistant Secretary for Congressional and Intergovernmental Affairs
Director, Office of Cybersecurity, Energy Security & Emergency Response
Assistant Secretary for Electricity
Acting Assistant Secretary for Energy Efficiency and Renewable Energy
Acting Assistant Secretary for Environmental Management
Assistant Secretary for Fossil Energy and Carbon Management
Assistant Secretary for Nuclear Energy
Assistant Secretary, International Affairs
Director, Office of Environment, Health, Safety & Security
Acting Executive Director, Office of Policy
Chief Human Capital Officer
Chief Information Officer
General Counsel
Inspector General
Executive Director, Loan Programs Office
Director, Joint Office of Energy and Transportation
Director, Office of Advanced Research Projects Agency-Energy
Acting Director, Office of Clean Energy Demonstrations
Director, Office of Energy Justice and Equity
Director, Office of Enterprise Assessments
Director, Office of Federal Energy Management Programs
Director, Grid Deployment Office
Director, Office of Hearings and Appeals
Director, Office of Indian Energy Policy and Programs
Director, Office of Intelligence and Counterintelligence
Director, Office of Legacy Management
Director, Office of Management
Director, Office of Manufacturing and Energy Supply Chains
Director, Office of Project Management
Director, Office of Public Affairs
Director, Office of Science
Director, Office of State and Community Energy Programs
Director, Office of Small and Disadvantaged Business Utilization
Director and Chief Commercialization Officer, Office of Technology Transitions
Power Marketing Administration Liaison Office

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose and Background

Enterprise Risk Management (ERM) requirements are codified in the Office of Management and Budget (OMB) Circular A-123 (Circular A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control*. After OMB published OMB Circular A-123 in 2016, the Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) published the *Playbook: Enterprise Risk Management for the U.S. Federal Government* (Playbook) to assist Federal agencies with addressing the additional ERM requirements in OMB Circular A-123, including making improved decisions by having a holistic view of risks and their interdependencies.

1.2 OMB Circular A-123

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* provides guidance for ERM and internal control requirements. OMB Circular A-123 establishes the requirement for agencies to establish an ERM framework. An agency's ERM framework includes the following elements:

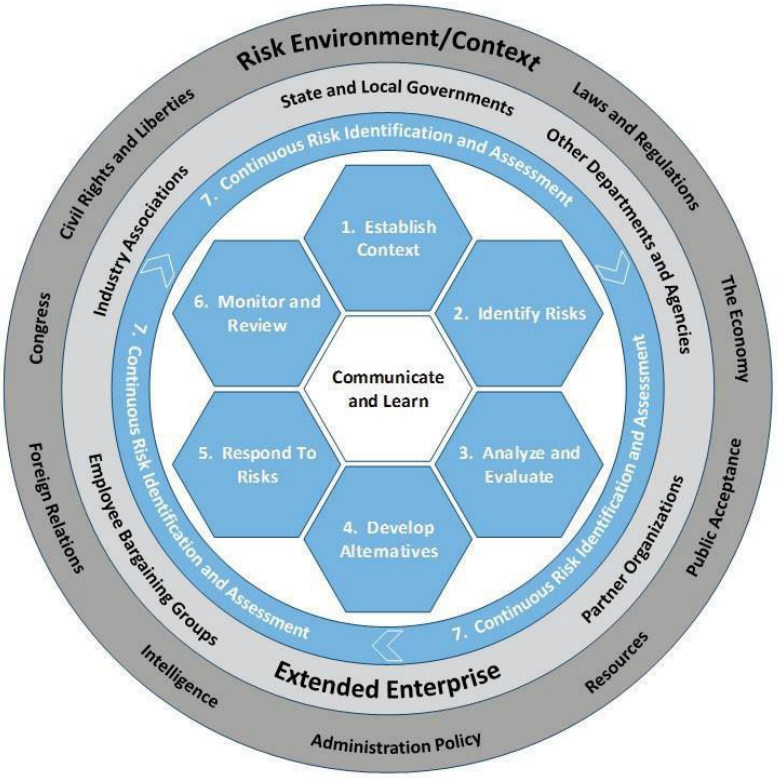
- **Risk Appetite:** Amount of risk an organization is willing to accept in pursuit of its mission and vision. It is established by the organization's most senior-level leadership and serves as the guidepost to set strategy and select objectives;
- **Risk Tolerance:** Acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program-, objective-, or component-level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite; and
- **A Portfolio View of Risk:** Provides insight into all areas of organizational exposure to risk (such as reputational, programmatic performance, financial, Information Technology [IT], acquisitions, human capital, etc.), thus increasing the chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment.

The Department of Energy (DOE) uses the ERM model, as depicted in OMB Circular A-123, which includes:

1) Establishing the context by understanding the internal and external environments of the organization;
2) Initial risk identification that uses a systematic approach to recognizing the potential for undesired outcomes;
3) Analyzing and evaluating the risks to include the probability and impact;
4) Developing alternative risk responses that are guided by the organization's risk appetite;
5) Responding to risks by deciding and executing the best course of action for the appropriate response strategy;
6) Monitoring the performance to determine whether the executed response strategy achieved the goals and objectives; and
7) Conducting continuous risk identification, which is an ongoing process.

An illustrative example of the model is identified in ***Figure 1***.

Figure 1: Illustrative Example of an ERM Model



Source: Playbook: Enterprise Risk Management for the U.S. Federal Government (CFOC)

2 DOE's Enterprise Risk Management Framework

As DOE's ERM Framework matures, risk management, budget formulation, and performance management will become an integrated, seamless, and coordinated effort. DOE's ERM Framework consists of horizontal and vertical interdependencies, beginning with the governance structure. The Departmental Internal Control and Assessment Review Council (DICARC)/Senior Risk Management Council (SRMC) is the governance body, formally chartered by the Secretary, that provides oversight for DOE's ERM and Internal Control Program. The DICARC/SRMC is chaired by the Deputy Chief Financial Officer (DCFO). The DICARC/SRMC members consist of Senior Executive Service (SES) personnel representing various HQ Offices throughout DOE. There is a subset of the DICARC/SRMC called the Senior Assessment Team (SAT) that is responsible for overseeing DOE's anti-fraud strategy. The SAT is chaired by the Chief Risk Officer (CRO).

Figure 2: DOE ERM Framework

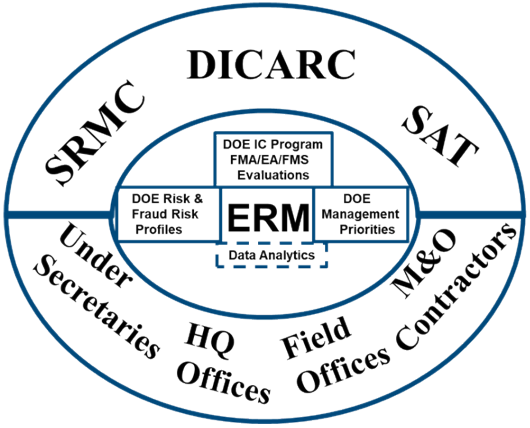
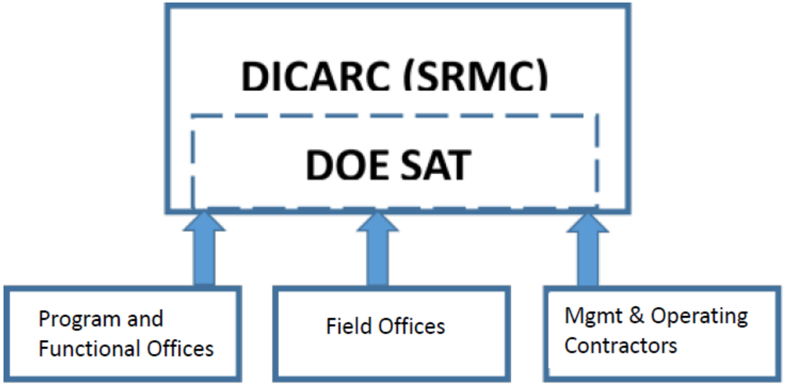
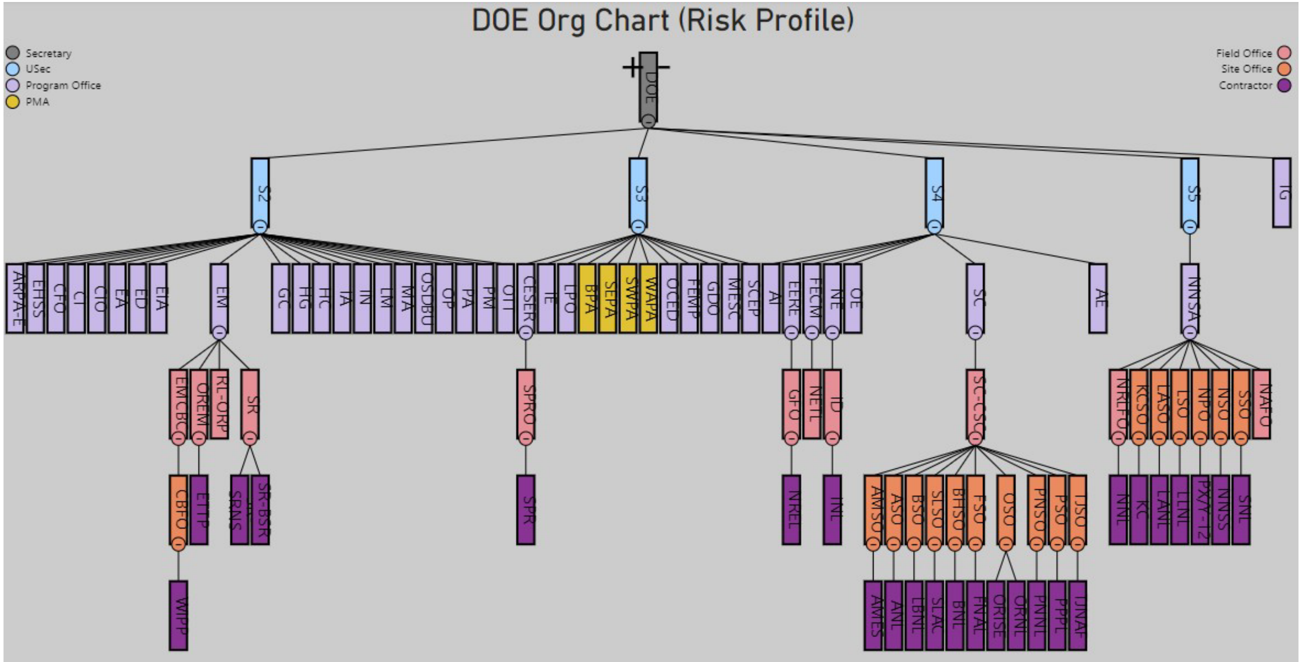

DICARC
SRMC
SAT
DOE IC Program FMA/EA/FMS Evaluations
DOE Risk & Fraud Risk Profiles
ERM
DOE Management Priorities
Data Analytics
Under Secretaries
HQ Offices
Field Offices
M&O Contractors

Figure 3: DICARC/SRMC and the SAT



The DICARC/SRMC provides oversight of DOE's ERM activities. As part of DOE's ERM activities, risk profiles are prepared by organizations at each reporting level (Management and Operating [M&O] Contractor, Field Offices, HQ Offices, and Under Secretary Offices) across the Department with risks being submitted to the next higher-level organization for consideration in the development of the next higher-level organization's risk profile.

Figure 4: Depiction of How the Risk Profile Rolls Up Using the DOE Org Chart[1]



Organization's risks should always consider DOE's risk appetite and risk tolerances. Risk tolerances are linked to risk categories and DOE's Management Priorities (See ***Table 18***), which are the greatest concerns of senior leadership across the Department, and will allow DOE to accomplish its strategic objectives with proper risk mitigation. DOE's strategic objectives support the Department's goals in the accomplishment of its mission.

Table 1: FYs 2022-2026 DOE Goals and Strategic Objectives

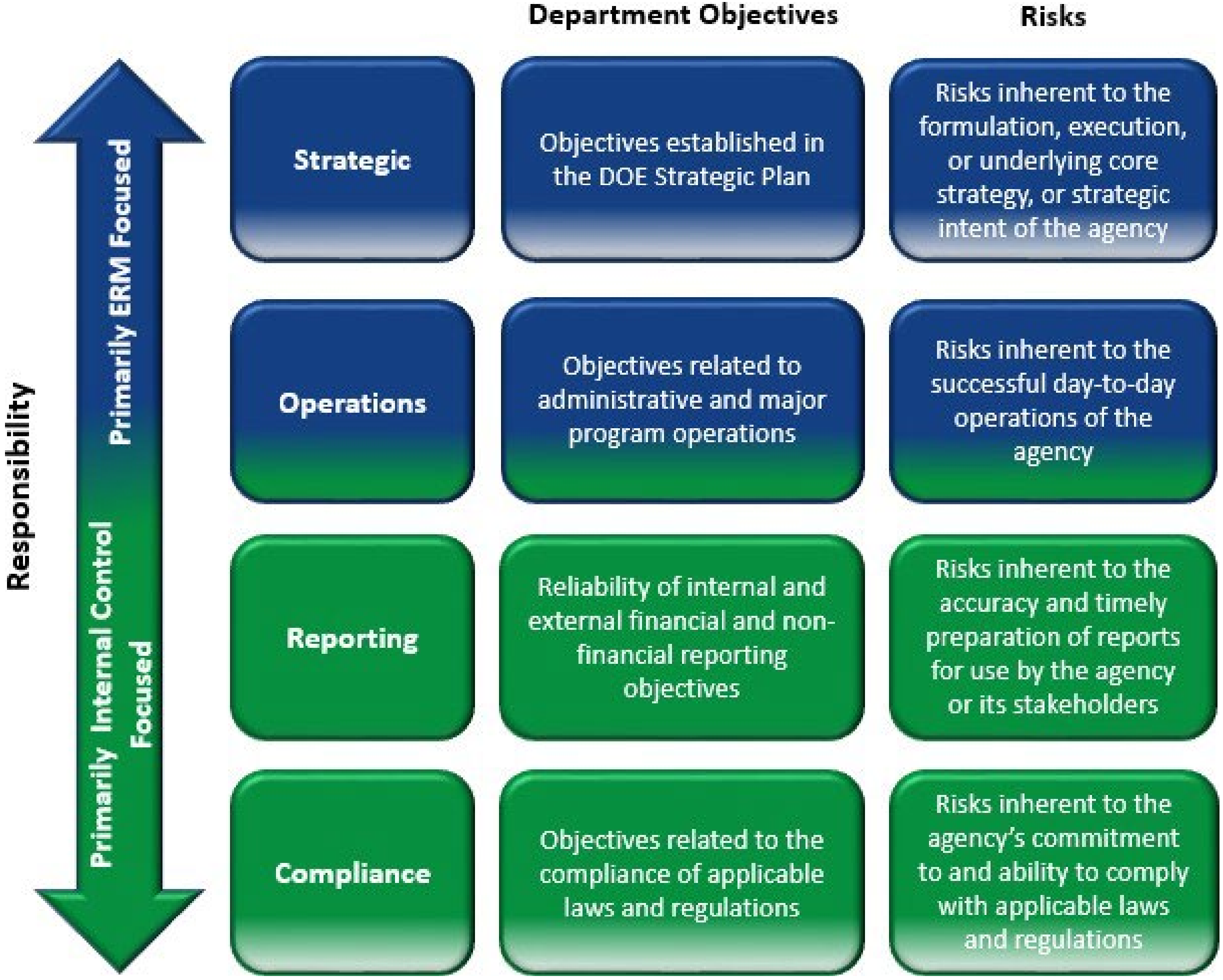
Goal 1: Drive U.S. Energy Innovation and Deployment on a Path to Net-Zero Emissions by 2050
Strategic Objective 1: Drive innovation of cost-efficient and affordable clean technologies and solutions through Research, Development, Demonstration, and Deployment (RDD&D) and Carbon Management
Strategic Objective 2: Accelerate deployment of clean technologies at scale and pace
Strategic Objective 3: Engage internationally to achieve global decarbonization and energy security while expanding markets for U.S. clean energy goods and services
Strategic Objective 4: Catalyze clean energy solutions for job creation and economic growth, including with a robust place-based focus
Goal 2: Strengthen the Nation's Energy Security, Resiliency, Affordability, and Reliability
Strategic Objective 5: Develop and deploy innovative solutions to harden energy infrastructure against physical threats, including climate change
Strategic Objective 6: Advance adoption of solutions to prevent and respond to cyber vulnerabilities and incidents
Strategic Objective 7: Secure the supply chain for a robust clean energy transition
Strategic Objective 8: Support an effective emergency response capability in the Federal Government for responding to critical energy events
Strategic Objective 9: Implement consolidated interim storage for the Nation's spent nuclear waste

[1] DOE Organization chart includes newly established offices that are in the process of getting incorporated into the Internal Control and ERM Program.

Goal 3: Advance Science Discovery and National Laboratory Innovation
Strategic Objective 10: Advance basic scientific understanding and identify new methods and tools to further discovery
Strategic Objective 11: Lead globally in key innovation and national security areas, including clean energy technologies, Artificial Intelligence (AI), quantum information sciences, microelectronics, advanced computing, particle accelerator technologies, and next generation biology and biosecurity
Strategic Objective 12: Commercialize innovations to improve the lives of Americans and the world
Goal 4: Ensure America's Nuclear Security by Harnessing Unparalleled Science and Technology Capabilities
Strategic Objective 13: Design, deliver, and maintain a safe, secure, reliable, and effective nuclear stockpile in support of the Nation's integrated deterrent
Strategic Objective 14: Forge and deliver cutting-edge solutions to shape and enable future arms control and nonproliferation regimes, increase strategic stability, counter nuclear terrorism, disrupt emerging threats, and advance the safe, secure, and peaceful use of nuclear energy
Strategic Objective 15: Harness the atom to safely, reliably, and affordably power a global fleet that enables unrivaled responsiveness, endurance, stealth, and warfighting capability
Goal 5: Promote Equity and Energy Justice
Strategic Objective 16: Advance equity in DOE's procurement, funding, Research and Development (R&D), and D&D processes and activities
Strategic Objective 17: Increase access to affordable, sustainable, and reliable energy for disadvantaged communities
Strategic Objective 18: Ensure 40 percent of the overall benefits of relevant Federal investments are delivered to disadvantaged communities
Strategic Objective 19: Support economic development, including through clean economy opportunities for workers in communities and industries in transition
Strategic Objective 20: Enhance engagement and energy economic development opportunities in Tribal communities
Strategic Objective 21: Support diversity and equity among researchers, projects, entrepreneurs, and the National Laboratories
Goal 6: Advance Clean-Up of Radioactive and Chemical Waste
Strategic Objective 22: Support environmental remediation
Goal 7: Operational Excellence
Strategic Objective 23: Attract, manage, train, and retain the best Federal workforce to meet future mission needs
Strategic Objective 24: Use taxpayer funds efficiently and improve visibility into how funds are being used
Strategic Objective 25: Monitor Departmental performance to ensure that program activities are executed in a safe and secure manner, consistent with Departmental direction

When assessing risks, leaders and their organizations should consider the various types of external and internal risks that may influence DOE's accomplishment of its goals, objectives, and mission. The risks should be grouped into categories to provide a meaningful understanding of the potential impact on DOE's strategic objectives, which influences the goals and mission accomplishment. DOE's risk categories include the Department's Management Priorities, along with other internal and external influences. In addition, leaders and their organizations should consider relationships between risk types and the Department's objectives.

Figure 5: Portfolio View of the Relationship Between Objectives and Risk



	Department Objectives	Risks
Strategic	Objectives established in the DOE Strategic Plan	Risks inherent to the formulation, execution, or underlying core strategy, or strategic intent of the agency
Operations	Objectives related to administrative and major program operations	Risks inherent to the successful day-to-day operations of the agency
Reporting	Reliability of internal and external financial and non-financial reporting objectives	Risks inherent to the accuracy and timely preparation of reports for use by the agency or its stakeholders
Compliance	Objectives related to the compliance of applicable laws and regulations	Risks inherent to the agency's commitment to and ability to comply with applicable laws and regulations

Source: SSA Integrity Act Handbook, Chapter 3: Enterprise Risk Management

Table 2: Consolidated Summary of DOE ERM Important FY 2024 Dates

Key Dates	Deliverables
December 15	A-123 Management of Enterprise Risk & Internal Controls Application (AMERICA) open for documenting Fiscal Year (FY) 2024 internal control testing and evaluation results.
December 28	The Office of the Chief Financial Officer (OCFO) publishes FY 2024 ERM Guidance to include the Data Analytics Survey Template.
January 18	Reporting organization's provide primary IT Point of Contact's (POC) name, e-mail address, and phone number to the Internal Controls and Fraud Risk Management Division's (ICFRMD) shared mailbox at CFO-ICFRMD@hq.doe.gov.
February 6	HQ Offices and Power Marketing Administrations (PMA) **will provide their Risk Profile, both in excel and signed PDF versions,** with consideration of reporting from Field Offices, Site Offices, and M&O Contractors, as applicable. Risk Profiles will be submitted to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov. Reporting organizations should follow cognizant organizations subsequent timelines to assure Risk Profiles are provided to DOE on time. **Note:** *All reporting organizations will provide a risk profile so risk tolerances may be assessed in FY 2024*.
February 22	Reporting organizations will provide completed Data Analytics Survey Template to the ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov.
March 5	Under Secretaries **will provide their Risk Profile, both in excel and signed PDF versions,** to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov based on input of their reporting offices.
March 12	Reporting organizations (M&O Contractors, Site Offices, Field Offices, PMAs, and HQ Offices) provide Interim Internal Control Status (IICS) using the AMERICA Application.
April 1 – 30	AMERICA semi-annual user access reviews are conducted by OCFO and reporting organizations.
April 2	OCFO provides the FY 2024 Assurance Memoranda Template to reporting organizations.
April 18	OCFO completes DOE Risk Profile and Fraud Risk Profile as required by OMB and GAO's Fraud Risk Framework in preparation for the Annual Strategic Review and the FY 2026 Budget Formulation Process.
May 14	OCFO provides the lead coordinating offices with Management Priorities in required templates for FY 2024 update. **Note:** *Applicable to Management Priority Lead Coordinating Offices Only.*
June 18	Lead coordinating offices provide OCFO with mid-year updates on Management Priorities using provided templates based on FY 2024 planned and performed enterprise activities. **Note:** *Applicable to Management Priority Lead Coordinating Offices Only.*
July 11	M&O Contractors and Field Offices provide FMA Module and Entity Assessment (EA) Module using the AMERICA Application. Reporting organizations should follow subsequent timelines published by cognizant organizations to assure FMA and EA Modules are provided to DOE on time.
July 30	HQ Offices and PMAs provide FMA Module and EA Module using the AMERICA Application.
August 6	OCFO provides eDOCS information to HQ Offices and PMAs.
August 13	Field Offices provide a draft Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov, considering and incorporating Site Offices and M&O Contractors. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Draft".**
September 4	Field Offices provide signed Assurance Memoranda to the ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Signed".**
	HQ Offices and PMAs provide draft Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Draft".**

Key Dates	Deliverables
September 5	Lead coordinating offices provide OCFO with Management Priorities year-end updates. **Note:** *Applicable to Management Priority Lead Coordinating Offices Only.*
September 17	HQ Offices and PMAs provide signed Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov and eDOCS. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Signed."**
September 24	Deputy Secretary and Under Secretaries provide signed Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov.
September 26	AMERICA close-out for FY 2024.
October 1 – 31	AMERICA semi-annual user access reviews are conducted by OCFO and reporting organizations.
October 1	Organizations that resolve or identify a significant deficiency or material weakness, after June 30, 2024, and no later than September 30, 2024, that is not included in a signed Assurance Memoranda, must notify the OCFO and update the Assurance Memoranda.
October – TBD	OCFO will provide Management Priorities updates to the DICARC in early October for review. **Note:** *Applicable to Management Priorities Lead Coordinating Offices Only. Per DICARC recommendation, the final Management Priorities are incorporated into the AFR and proceed through Exec Sec Concurrence Process.*

3 Risk Profile and Fraud Considerations in the Risk Profile

3.1 Purpose and Background

DOE prepares a consolidated agency risk profile annually. The consolidated risk profile takes into consideration reporting organizations' risk profiles and their FMA and EA submissions from the Department's A-123 Application (AMERICA). Likewise, on an annual basis, DOE requires each Under Secretary and HQ Offices to prepare and submit a risk profile that takes into consideration the risk profiles from Field Offices, Integrated M&O Contractors, and Integrated non-M&O Contractors.

In FY 2024, DOE continues to comply with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* which provides guidance for internal control and risk management requirements. OMB Circular A-123 also establishes the requirement to produce an agency Risk Profile as part of the implementation of an ERM capability coordinated with strategic planning, strategic review, and internal control processes.

OMB Circular A-123 requires:

- Integration of risk management and internal control functions;
- Implementation of an ERM capability in coordination with the strategic planning and strategic review process required by the *Government Performance and Results Act Modernization Act* (GPRAMA) and the internal control processes required by the *Federal Mangers Financial Integrity Act* (FMFIA);
- Incorporation of risk identification capabilities into the framework to identify new/emerging risks or changes in existing risks; and
- Development of a Risk Profile, including fraud risk evaluation, coordinated with annual strategic reviews.

The DOE Risk Profile identifies the most significant risks faced by the Department in meeting strategic objectives and communicates the strategy for addressing those significant risks. Significant risks are captured from detailed financial and non-financial risks reported through AMERICA to provide an entity-wide view of all risks. Risks are analyzed in relation to the achievement of objectives in the following areas:

- **Strategic**: DOE strategic goals and objectives;
- **Operations**: Effective and efficient use of DOE resources in administrative and major program operations, including financial and fraud objectives covered in annual internal control testing;
- **Compliance**: DOE compliance with applicable laws and regulations; and
- **Reporting**: Reliability of DOE internal and external financial or non-financial reporting.

Risk consideration is a key element during budget formulation and vital to an organization's planning process. As such, risk management professionals should be part of every organization's leadership effort for planning future years' budget. At the Department-level, resource planning is a joint effort that is guided by the Chief Financial Officer (CFO) and CRO. Using this approach, the Department's risk posture is reflected in DOE's budget, addresses budget needs for key controls to mitigate the most important risks, and reflects the priorities and risk appetite of the Department's leadership. The Department's risk profile is also used to shape discussions between DOE and OMB in supporting budget justifications. Leadership should also consider risks during budget execution with discussions on funding to improve performance while responding to emerging risks.

For FY 2024, the DICARC and SAT, which are comprised of senior level executives across DOE identified the amount of deviation that DOE is willing to allow in the accomplishment of its objectives, which is known as the risk tolerance. In general terms, risk tolerance is the level or amount of variance in performance that DOE is willing to accept as it executes its mission.

NEW
in FY 2024

Risk tolerances are linked to the risk categories in the Department's Risk Profile Template. Reporting organizations should assess their residual risk score to the Agency's Risk Tolerance. By doing so, reporting organizations can make a better and more informed decision about risks on their risk profile and assess how well they are doing to mitigate a risk. The organization will be able to determine if additional resources are needed to mitigate a risk, if the current resources are sufficient, if funding is needed to resource additional controls, or if a risk needs to be ranked higher on their risk profile as a greater concern.

NEW
in FY 2024

3.2 Risk Profile Deliverable Requirements

The Risk Profile requires both identification and analysis of risks, **including fraud risks**. Risk identification offers a structured and systematic approach to recognizing where the potential for undesired outcomes can arise. Risk analysis and evaluation considers the causes, sources, probability of risk occurring, potential outcomes, and prioritizes the results of the analysis. Reporting organizations' risk profiles must identify the risks, **including fraud risks**, to achieve agency strategic objectives and the appropriate options for addressing the risks. Organizations should analyze the risks in relation to the achievement of the strategic goals and objectives presented in the DOE Strategic Plan, as well as internal control objectives related to operations, compliance, and reporting.

In FY 2024, reporting organizations will continue to identify the top financial and non-financial fraud risks in the Risk Profile. These ongoing fraud risks must be included in each entity's Risk Profile deliverable, along with other identified risks. Reporting organization's fraud risks that are identified in their Risk Profile and AMERICA will be considered in the Department's Fraud Risk Register as part of DOE's strategy to identify and mitigate potential fraud risk occurrences. DOE's Fraud Risk Register is vital in preparing and maintaining a relevant DOE Fraud Risk Profile.

The Risk Profile deliverable must be reviewed and approved by the reporting organization's management. Management pertains to the Department Head who may also delegate authority to sign the organization's Risk Profile. The Risk Profile template includes a signature box at the top where the entity's management should document the approver name, title, and signature.

In FY 2024, all reporting organizations will provide a risk profile so risk tolerances may be gauged and HQ Risk POCs will also provide a Risk Profile Crosscut as part of the risk profile deliverable. The Risk Profile Crosscut is an explanation on how your organization's risks were considered in the FY 2025 budget formulation process or how your organization's risks will be considered in the FY 2026 budget formulation process. The Risk Profile Crosscut is located on the second tab of the risk profile template and requires coordination with reporting organizations Budget POCs and management to complete. **Risk profiles are NOT submitted through the A-123 Application, AMERICA.** Both the PDF and Excel Risk Profile documents will be sent to the ICFRMD's e-mail address at CFO-ICFRMD@hq.doe.gov.

NEW
in FY 2024

Integrated Contractors, **including both M&O and integrated non-M&O Contractors**, are required to identify and analyze their risks, including fraud risks, and provide a Risk Profile using the **FY 2024 Risk Profile template** to the cognizant[2] Field Office. Field Offices, taking into consideration the Integrated Contractors, **including both M&O and integrated non-M&O Contractors**, are required to identify and analyze the risks, including fraud risks, and provide a Risk Profile using the **FY 2024 Risk Profile template** to the cognizant HQ Office. Each HQ Office, PMA, and Under Secretary are required to prepare a Risk Profile **using the FY 2024 Risk Profile template** to identify their top risks, including fraud risks, in accordance with the due dates in ***Table 3***. **Risk Profiles will be returned to reporting organizations that do not use the FY 2024 Risk Profile** *template* **or HQ Risk POCs that do not complete the Risk Profile Crosscut that is located on the second tab.**

The Risk Profiles from each Under Secretary, as well as each HQ element not reporting to an Under Secretary, will be consolidated into a prioritized DOE Risk Profile and used during the Department's FY 2026 budget formulation process and as part of the annual Strategic Review with OMB in May. The risks identified as fraud-related in the Risk Profile will also be considered for DOE's Fraud Risk Profile.

Table 3: DOE Risk Profile Important FY 2024 Dates

Key Dates	Deliverables
February 6	HQ Offices and PMA **will provide their Risk Profile, both in Excel and signed PDF versions,** with consideration of reporting from Field Offices, Site Offices, and M&O Contractors, as applicable. Risk Profiles will be submitted to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov. Reporting organizations should follow cognizant organizations subsequent timelines to assure Risk Profiles are provided to DOE on time. **Note:** *All reporting organizations will provide a risk profile so risk tolerances may be assessed in FY 2024.*
March 5	Under Secretaries **will provide their Risk Profile, both in excel and signed PDF versions,** to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov based on input of their reporting offices.
April 18	OCFO completes DOE Risk Profile and Fraud Risk Profile, as required by OMB and GAO's Fraud Risk Framework in preparation for the Annual Strategic Review and the FY 2026 Budget Formulation Process.

3.3 Emerging Risks in the Realm of Artificial Intelligence

Major advances in the realm of AI holds extraordinary potential for both promise and peril. *Executive Order*[3] *on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* was released on October 30, 2023, and establishes new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition, advances American leadership around the world, and more.

NEW
in FY 2024

The Executive Order (EO) directly requires Federal agencies to issue standards and guidance and to use their existing authorities to police the use of AI. It also devotes Federal resources towards AI-related

[2] Cognizant Field Office and Program Offices will establish due dates and process for all M&O Contractors' Risk Profile.

[3] Executive Order: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
Fact Sheet: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

education, training, and research, including the further development of Privacy Enhancing Technologies (PET), such as differential privacy and synthetic data generation.

The EO directed DOE to address AI systems' threats to critical infrastructure, as well as chemical, biological, radiological, nuclear, and cybersecurity risks. On top of safety and security, AI can also pose threat to commerce, fair competition, and advancing equity and civil rights.

Reporting organizations should recognize AI threats and consider the National Institute of Standards and Technology's (NIST) *AI Risk Management Framework*[4] when conducting risk assessment and assembling the Risk Profile.

3.4 Risk Profile, FMA, and EA Module Reporting

To the extent additional internal controls are necessary to manage or mitigate risks identified in Risk Profiles, the controls must be established and evaluated as part of annual internal control testing and attested to in the annual assurance statement. If a control existed in last year's Risk Profile deliverable and was tested, then the reporting organization may treat it in the same manner as a focus area exemption.

Reporting organizations should indicate where each reported risk is evaluated using the Current Evaluation Category column (Column M). Risk Profile financial risks must be documented and evaluated, including the establishment and testing of controls when applicable, in the **FMA Module** in AMERICA. Risk Profile non-financial risks are evaluated, including the establishment and testing of controls when applicable, as part of the EA process and reported in the appropriate section of the **EA Module** in AMERICA. Internal control risks are assessed and reported in the **Internal Control Evaluation** tab and the entity objective risks are assessed and reported in the **Entity Objective Evaluation** tab.

Entities should continue to provide further detail of where risks are being evaluated within the EA or FMA Modules using the Current Evaluation Details column (Column O). For example, if the current evaluation category is "Internal Control Evaluation," indicate which of the 17 Principles the risk is evaluated. If the current evaluation category selected is "Entity Objectives Evaluation," then identify the specific entity objective. For the FMA Module, if the current evaluation category is "FMA Evaluation," then identify the sub-process where the controls are located that mitigate the risk.

3.5 Instructions for Risk Profile Template

The Risk Profile Template involves the identification and analysis of risk. Risk identification offers a structured and systematic approach to recognizing where the potential for undesired outcomes can arise. Risk analysis and evaluation considers the causes, sources, probability of risk occurring, the potential outcomes, and prioritizes the results of the analysis.

When identifying and analyzing your organization's risks, consider these questions:

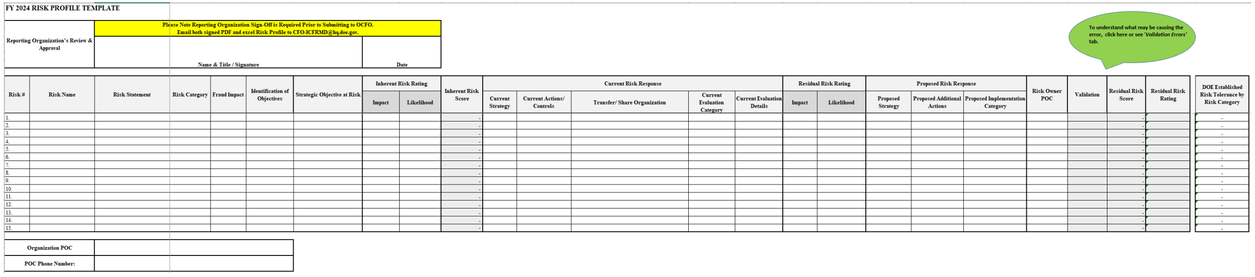
- What are the organization's goals and objectives that support the DOE Strategic Plan?
- What events could happen that would prevent the organization from achieving its goals and

[4] NIST's Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023
nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

objectives aligned with the DOE Strategic Plan?
- What events could impede effective or efficient use of resources for Departmental operations?
- What events could affect reliability, accuracy, or timeliness of reporting?
- What events could prevent the organization from achieving compliance with statutory, Congressional, OMB, or other requirements?
- What are the corresponding impacts of these risks and what is the severity of this impact?
- What is the likelihood that this event will occur?
- What are the most significant risks?
- What are the fraud risks?
- Which risks require a response?
- What actions will you take to address these risks? What actions could you take in the future to address these risks?
- Did the actions taken to address a risk have an effect? Is there any remaining residual risk? If so, then what is the severity of impact and likelihood of occurrence of this risk?
- Who is accountable for the actions to address the risk?

After risks are identified, management must determine a risk response. In determining a risk response, management should consider risk tolerance, placement of controls, and other mitigating actions. Risk tolerance is particularly important as management has significant discretion in setting risk tolerance levels and should assess the organization's risk tolerance based on DOE's risk tolerance. Should the organization's risk tolerance differ from the Department's risk tolerance, the organization may provide context in the Current Risk Response fields of the Risk Profile Template. The GAO's *Standards for Internal Control in the Federal Government* (Green Book) defines risk tolerance as the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerance levels will significantly impact management's risk response decisions and should always be considered. The Risk Profile *template* is presented in ***Figure 6***, followed by instructions explaining how to complete each column in the FY 2024 Risk Profile. The *template* and instructions will be provided in Excel for your organization's use in completing the Risk Profile.

Figure 6: Risk Profile Template



FY 2024 RISK PROFILE TEMPLATE

Please Note Reporting Organization Sign-Off is Required Prior to Submitting to OCFO.
Email both signed PDF and excel Risk Profile to CFO-ICFRMD@hq.doe.gov.

Reporting Organization's Review & Approval	Name & Title / Signature	Date

To understand what may be causing the error, click here or see '*Validation Errors*' tab.

Risk #	Risk Name	Risk Statement	Risk Category	Fraud Impact	Identification of Objectives	Strategic Objective at Risk	Inherent Risk Rating		Inherent Risk Score	Current Risk Response					Residual Risk Rating		Proposed Risk Response			Risk Owner POC	Validation	Residual Risk Score	Residual Risk Rating	DOE Established Risk Tolerance by Risk Category
							Impact	Likelihood		Current Strategy	Current Actions/ Controls	Transfer/ Share Organization	Current Evaluation Category	Current Evaluation Details	Impact	Likelihood	Proposed Strategy	Proposed Additional Actions	Proposed Implementation Category					
1.									-													-		-
2.									-													-		-
3.									-													-		-
4.									-													-		-
5.									-													-		-
6.									-													-		-
7.									-													-		-
8.									-													-		-
9.									-													-		-
10.									-													-		-
11.									-													-		-
12.									-													-		-
13.									-													-		-
14.									-													-		-
15.									-													-		-

Organization POC	
POC Phone Number:	

Note: Verify that the file is "Enabled" by clicking on "File," "Enable Content," and "Enable All Content" before entering data into the template. Provide Name and Title of the Department Head approving the Risk Profile and the date when the Risk Profile was completed. Provide the POC Name and POC phone number at the bottom of the Risk Profile. After completion, the Risk Profile must be produced in PDF format with signature as well.

Risk # (Column A): This column is pre-populated with a unique number and used to assign a numerical ID to each identified risk.

Risk Name (Column B): Use this column to name the identified risk statement. This risk name can be used for easy identification of a specific risk statement across an entity.

Risk Statement (Column C): Use this column to identify risks and the impacts/ effects. Use the "if, then" sentence construction to describe the event ("if") and the impacts ("then"). List all possible impacts in the statement and do not limit the statement to a single impact to avoid understatement of the risk. For example:

- If the roof collapses at Building X, then workers may be injured, water infiltration can damage equipment, and the protected area adjacent to Building X will be more vulnerable to additional damage that could render the storage of nuclear material unsafe; and
- If we lose technical capabilities in the program's workforce, then we will not be able to complete the work on schedule and at cost.

Risk Statements are not meant to be descriptions of issues, meaning risks that have already occurred, but are potential events that could occur. Some risks may be unavoidable and beyond an organization's ability to reduce to a tolerable level. Nevertheless, the organization should identify these risks, make contingency plans, and manage risks against those plans to the best of abilities. For example, many organizations may have to accept risks that arise due to natural disasters that cannot be controlled but may have emergency response mechanisms in place to mitigate against these risks.

Risk Category (Column D): Use this column to select a risk category to describe the identified risk. The drop-down menu lists the 10 management priorities identified in the most recent Agency Financial Report (AFR) (Contract and Major Project Management; Safety and Security; Environmental Cleanup; Nuclear Waste Disposal [Commercial Waste, Defense Waste]; Nuclear Stockpile Stewardship; Cybersecurity; Infrastructure; Human Capital Management and Diversity and Inclusion; Energy Justice; and Climate Change), along with seven other common risk categories (i.e., Political, Reputational, IT Infrastructure, Grants/Loans/Financial Assistance, Continuity of Operations (COOP), and Financial Management). These management priorities along with the other listed categories serve as proxies for risk categories and will be used to aggregate risks. Select one risk category only. For instances where multiple risk categories may seem to apply, use best judgement to select the most relevant category. In addition, if the identified risk does not align with one of the listed risk categories, then choose "Other" from the drop-down menu.

Dropdown Options:

- Contract and Major Project Management;
- Safety and Security;
- Environmental Cleanup;
- Commercial Waste;
- Defense Waste;
- Nuclear Stockpile Stewardship;
- Cybersecurity;
- Physical Infrastructure;
- Human Capital Management and Diversity and Inclusion;
- Energy Justice;
- Climate Change;
- Political;
- Reputational;
- IT Infrastructure;

- Grants/Loans/Financial Assistance;
- COOP;
- Financial Management (i.e., financial statements, financial reporting, etc.); and
- Other.

Fraud Impact (Column E): Use this column to identify if the risk is a Financial-, Non-Financial-, Top Financial-, or Top Non-Financial Fraud-related risks. If a risk does not have a fraud impact, then organizations should select "N/A" from the drop-down menu. **Note**: If a fraud sub-category is not identified for each risk, then an error will occur in the validation column (Column U).

Dropdown Options:

- Financial Fraud;
- Non-Financial Fraud;
- Top Financial Fraud;
- Top Non-Financial Fraud; and
- N/A.

Identification of Objectives (Column F): Risks must be linked to achievement of one of the four objectives identified by OMB: strategic objectives (objectives established in the DOE Strategic Plan), operational objectives (administrative and major program operations), reporting objectives (reliability of internal and external financial and non-financial reporting objectives), and compliance objectives (compliance with applicable laws and regulations). Only select one objective and, for instances where multiple objectives may seem to apply, use best judgement to select the most relevant objective.

Strategic Objective at Risk - Primary (Column G): This column has a drop-down menu that will allow only one choice. Use this column to select the strategic objective from the drop-down menu that the risk affects only if the "Strategic Objectives" option was selected in the Identification of Objectives column (Column F). The drop-down menu contains the strategic objectives from the Draft DOE Strategic Plan Framework. Select one primary strategic objective only and, for instances where multiple strategic objectives may seem to apply, use best judgement to select the most relevant strategic objective. If the objective identified is anything but Strategic in the previous field, then select 'N/A - Strategic Objective was not selected as an objective in the previous field' for this column. **Note:** A validation error would occur if the requirement stated here is not fulfilled.

Dropdown Options:

- **Objective 1:** Drive innovation of cost-efficient and affordable clean technologies and solutions through RDD&D and Carbon Management;
- **Objective 2:** Accelerate deployment of clean technologies at scale and pace;
- **Objective 3:** Engage internationally to achieve global decarbonization and energy security while expanding markets for U.S. clean energy goods and services;
- **Objective 4**: Catalyze clean energy solutions for job creation and economic growth, including with a robust place-based focus;
- **Objective 5:** Develop and deploy innovative solutions to harden energy infrastructure against physical threats, including climate change;
- **Objective 6:** Advance adoption of solutions to prevent and respond to cyber vulnerabilities and incidents;
- **Objective 7:** Secure the supply chain for a robust clean energy transition;
- **Objective 8:** Support an effective emergency response capability in the Federal Government

for responding to critical energy events;

- **Objective 9:** Implement consolidated interim storage for the Nation's spent nuclear waste;
- **Objective 10:** Advance basic scientific understanding and identify new methods and tools to further discovery;
- **Objective 11:** Lead globally in key innovation and national security areas, including clean energy technologies, AI, quantum information sciences, microelectronics, advanced computing, particle accelerator technologies, and next generation biology and biosecurity;
- **Objective 12:** Commercialize innovations to improve the lives of Americans and the world;
- **Objective 13:** Design, deliver, and maintain a safe, secure, reliable, and effective nuclear stockpile in support of the Nation's integrated deterrent;
- **Objective 14:** Forge and deliver cutting-edge solutions to shape and enable future arms control and nonproliferation regimes, increase strategic stability, counter nuclear terrorism, disrupt emerging threats, and advance the safe, secure, and peaceful use of nuclear energy;
- **Objective 15:** Harness the atom to safely, reliably, and affordably power a global fleet that enables unrivaled responsiveness, endurance, stealth, and warfighting capability;
- **Objective 16:** Advance equity in DOE's procurement, funding, R&D, and D&D processes and activities;
- **Objective 17:** Increase access to affordable, sustainable, and reliable energy for disadvantaged communities;
- **Objective 18:** Ensure 40 percent of the overall benefits of relevant Federal investments are delivered to disadvantaged communities;
- **Objective 19:** Support economic development, including through clean economy opportunities for workers in communities and industries in transition;
- **Objective 20:** Enhance engagement and energy economic development opportunities in Tribal communities;
- **Objective 21:** Support diversity and equity among researchers, projects, entrepreneurs, and the National Laboratories;
- **Objective 22:** Support environmental remediation;
- **Objective 23:** Attract, manage, train, and retain the best Federal workforce to meet future mission needs;
- **Objective 24:** Use taxpayer funds efficiently and improve visibility into how funds are being used;
- **Objective 25:** Monitor Departmental performance to ensure that program activities are executed in a safe and secure manner consistent with Departmental direction; and
- **N/A –** Strategic Objective was not selected as an objective in the previous field.

Inherent Risk Rating: Inherent risk is the exposure arising from a risk before any action is taken to manage it. Because the Inherent Risk Rating is the assessment of a risk before any action to manage or mitigate the risk through the use of controls, the Inherent Risk Rating will **never be lower** than the Residual Risk Rating. Inherent risk is measured using the impact and likelihood metrics described below.

Inherent Impact (Column H): Inherent Impact refers to the measurements of the effect of an event that could result from the occurrence of the identified risk. The impact is assessed to gauge how severe the effect will be on the ability to achieve an organization's goals and objectives. Assess this by estimating the level of impact, using a scale of 1 to 5, which will happen if the risk occurs. Use informed judgment and the experience of knowledgeable individuals and groups to assist in determining the level of impact. In this assessment, consider these questions:

- Is there a threat to human life?
- Is there a threat of fraud, waste, and abuse?

Use the scale with defined parameters in ***Table 4*** to rate the impact of the risk.

Table 4: Impact Assessment

Measured Impact	Reduced Quality and Performance
1 – Very Low	The **impact is insignificant** and localized and does not affect the entity's ability to achieve one or more of its objectives or performance goals. Impact on single non-critical task/objective resulting in minor plan/work adjustment with no impact on achieving project/organizational goals/deliverables (e.g., data for a report provided late but ultimate deadline met).
2 – Low	The **impact will not significantly affect** the entity's ability to achieve one or more of its objectives or performance goals. Impact on multiple non-critical plan tasks/objectives resulting in several minor plan/work adjustments with no significant impact on achieving project/organizational goals/deliverables (e.g., data provided fails data checks and data accumulations system/process must be corrected and rerun resulting in delays).
3 – Moderate	The **impact could significantly affect** the entity's ability to achieve one or more of its objectives or performance goals. Impact on one or more critical plan tasks/objectives resulting in major plan/work adjustments with significant impact resulting in reduced achievement of project/organizational goals/deliverables (e.g., expected data unavailable and final report/product lacks expected information/analysis or results in significant delivery delay).
4 – High	The **impact could preclude or highly impair** the entity's ability to achieve one or more of its objectives or performance goals. Impact on one or more critical plan tasks/objectives resulting in major plan/work adjustments with major impact resulting in only partial achievement of project/organizational goals/deliverables (e.g., expected data unavailable and final report/product lacks critical information/analysis and/or results in significant delays).
5 – Very High	The **impact will likely preclude** the entity's ability to achieve one or more of its objectives or performance goals. Impact on one or more critical plan tasks/objectives, resulting in major plan/work adjustments with severe impact resulting in failure to achieve project/organizational goals/deliverables (e.g., expected data unavailable and final report/product not issued).

Inherent Likelihood (Column I): This is the probability that a given event will occur. Assess the likelihood (using a scale of 1 to 5) based on data (when available) or the knowledge and experience of an expert or group. Use the scale with defined parameters in ***Table 5*** to rate the likelihood of the identified risk:

Table 5: Likelihood

Likelihood	Definition
1 – Very Low	Risk event **rarely** to occur. Less than a 5% chance of occurrence.
2 – Low	Risk event **unlikely** to occur. Between a 5% – 25% chance of occurrence.
3 – Moderate	Risk event **possible** to occur. Between a 26% – 49% chance of occurrence.
4 – High	Risk event **highly likely** to occur. Between a 50% – 74% chance of occurrence.
5 – Very High	Risk event **almost certain** to occur. Greater than a 75% chance of occurrence.

Inherent Risk Score (Column J): This column automatically calculates the inherent risk score for each identified risk by multiplying the risk's inherent impact (Column H) by the inherent likelihood (Column I). A score of 25 reflects the highest possible residual risk rating (5 x 5) and a score of 1 reflects the lowest possible residual risk rating (1 x 1).

NEW in FY 2024

Current Strategy (Column K): Use this column to indicate the action currently taken to manage the identified risk. Consider these questions when preparing a risk response:

- What action or multiple actions will be taken to address this risk?
- How are these actions managing the risk?
- How long will these actions continue?

Select a current risk response from the options in the drop-down menu. (See ***Table 6***)

Table 6: Risk Responses

Response Type	Definition	Example
Accept	Take no action to respond to the risk based on insignificance of risk, requirement to complete the work, or benefits and opportunities exceed the risk.	Continue an environmental cleanup project, despite identified risks, because taking no action has unacceptable public safety and environmental impacts.
Avoid	Action is taken to stop the operational process, or the part of the operational process, causing the risk.	Supplier of a specialty part may no longer be in business when part is needed, so action is taken to modify the design specifications to use generic, widely available part.
Reduce	Take action to reduce the likelihood or impact of the risk.	Past end-of-life infrastructure needs replacement, but increased inspection and extraordinary maintenance reduces risk of catastrophic failure.
Transfer	Take action to transfer the responsibility for ownership and handling the risk to an organization other than the current entity that owns the risk.	Scope of work on a project is transferred to another organization with more expertise or experience.
Share	Take action to share the risk with another entity within the organization or with one or more external parties.	Strategic partnership formed to share high risk work with an outside organization with expertise and special facilities.

In developing the Risk Profile, management must determine those risks for which the appropriate response includes implementation of formal internal controls activities according to defined criteria, as described in Section III of OMB Circular A-123 and which conforms to the standards published by GAO in the Green Book. **Note:** To the extent internal controls are necessary to manage or mitigate risks identified in Risk Profiles, the controls must be established and tested as part of the annual internal control testing cycle and included as part of the attestation in the annual assurance memorandum.

Current Actions/Controls (Column L): This column provides a narrative explanation of how to currently apply the risk response identified in the prior column. Include any formal internal control activities that are currently in place to manage the risk. The brief narrative should also summarize the **action** taken and, as applicable, may include an explanation of the action. For example, the action to address a safety risk might involve repair of faulty equipment, so the selection “reduce” from the risk response strategy drop-down menu is appropriate and then explain in this text box how the faulty equipment was repaired to reduce the risk. Also, the narrative should explain the **controls** put in place to reduce the risk. Using the same example above, explain how regular safety inspections were implemented.

Transfer/Share Organization (Column M): If the Current Strategy is to "Transfer" or "Share," then this field should be used to identify the organization to which the risk is transferred or shared. Organizations will need to coordinate with the identified organization to which the risk ownership is transferred to or shared with to ensure that the risk is included on the identified organization’s risk profile as well. The inclusion of the risk on the identified organization’s risk profile will not only indicate that they accept the transfer or sharing of risk ownership but will also close the gap on the actions taken to respond to the risk. If the Current Strategy is other than ”Transfer” or ”Share,” then ”N/A” should be selected in this field. However, if the Current Strategy in column J is “Transfer” or “Share”, then select the organization the risk is being transferred to or the risk is being shared with. Note that if an organization does not identify the Transfer/Share Organization in this column (only for risks with a transfer or share risk response) or select ”N/A” when applicable, an error will occur in the validation column (Column V).

Current Evaluation Category (Column N): Use this column to indicate where the internal control activities to manage the risk have been evaluated. If the risk is a financial risk, and the appropriate internal controls are tested and documented in the entities' FMA Module in AMERICA, select "FMA Evaluation" from the drop-down menu. If the risk is a non-financial risk, and the controls to manage this risk are evaluated in the EA’s Entity Objective Evaluation, select this option from the drop-down menu. If the internal control activities to address the risk are evaluated in the EA’s Internal Control Evaluation, then select this choice from the available options. If formal internal control activities were not implemented to manage the risk (i.e., the current strategy is to "Accept"), then this column should be left blank.

Current Evaluation Details (Column O): This column provides text space to provide further detail of where the risk is currently evaluated. For example, if the current evaluation category is "Internal Control Evaluation”, indicate which of the 17 Principles the risk is evaluated. If the current evaluation category is "Entity Objectives Evaluation”, identify which entity objective. If the current evaluation category is "FMA Evaluation”, identify the sub-process where the controls are located that mitigate the risk.

Residual Risk Rating: Residual risk is the amount of risk that remains after action has been taken to manage it. In the earlier example about safety, after implementation of safety inspections, residual risk from the limitations of testing equipment may remain. Use the same assessment standards provided in the prior section to assess residual risk impact and likelihood on a scale of 1 to 5 (***Table 4*** and ***Table 5***, respectively). Because the Residual Risk Rating is the assessment of a risk after actions have been implemented to manage or mitigate the risk, the Residual Risk Rating will **never be higher** than the Inherent Risk Rating. However, if no actions were taken to address the inherent risk or if the Current Risk Response strategy is "Accept", then the residual risk field will be the same as the inherent risk.

Residual Impact (Column P): This column refers to the measurement of the effect of an event that could result from the occurrence of the identified residual risk. The impact is assessed to gauge how severe the effect will be. Assess this by estimating the level of impact that will happen if the event occurs based on informed judgment and experience of knowledgeable individuals and groups on a scale of 1 to 5 (using the scale in ***Table 4***). For risks where no actions were taken to address the inherent risk, then the residual risk impact field will be the same.

Residual Likelihood (Column Q): This is the probability that a given event will occur. This assessment is used to gauge how likely an event is to occur. For example, events that may happen every day have a far greater likelihood than events that may only happen once in 10 years. Assess the likelihood (using a scale of 1 to 5) based on data available or use the knowledge and experience of an expert or group using the scale in ***Table 5***. For risks where no actions were taken to address the inherent risk, then the residual risk likelihood field will be the same.

Proposed Strategy (Column R): This column indicates proposals on how to treat the residual risk like the consideration of the inherent risk discussed above. Consider these questions when preparing a proposed risk response:

- What additional actions would address this risk in addition to the initial risk mitigation actions already taken?
- Would these actions actually manage the risk?
- How long will the actions continue?

Select a proposed residual risk strategy from the options found in ***Table 6***. For risks where no actions were taken to address the inherent or residual risk, the proposed risk response (Columns R-T) may be blank.

Proposed Additional Actions (Column S): Use this column to provide a narrative explanation of how to employ the proposed risk response to the residual risk identified in the prior column. These additional actions could further reduce the exposure remaining after the initial risk mitigation actions have been taken. The amount and type of description in this column is subjective, but a summary is recommended. Proposed risk responses should use the same standards applied to the current risk response, as described above, including the identification of risks for which implementation of formal internal control activities is appropriate. This column is also to be used to explain why it is appropriate to accept the residual risk if that is the decision.

Proposed Implementation Category (Column T): Identify the management process that will be used to implement, test, and monitor proposed actions. Select one of the following three options as the relevant management process: 1) Strategic Review; 2) Budget Formulation Process; or 3) Internal Control Assessment.

Risk Owner POC (Column U): In this column, provide the name of the person accountable for implementing risk response(s) and ensuring that risk mitigation plans are developed and implemented.

For cross-cutting risks involving multiple programs across organizations, use the lead coordinator of the risk response. This person will also identify or monitor mitigating controls, if applicable.

Validation (Column V): This is an automatically calculated column and requires no input. This column will identify if a selection was not made where it is required, or if a wrong combination of selections was made. Review this column prior to finalizing to ensure the accuracy of the Risk Profile.

Table 7: Possible Validation Errors

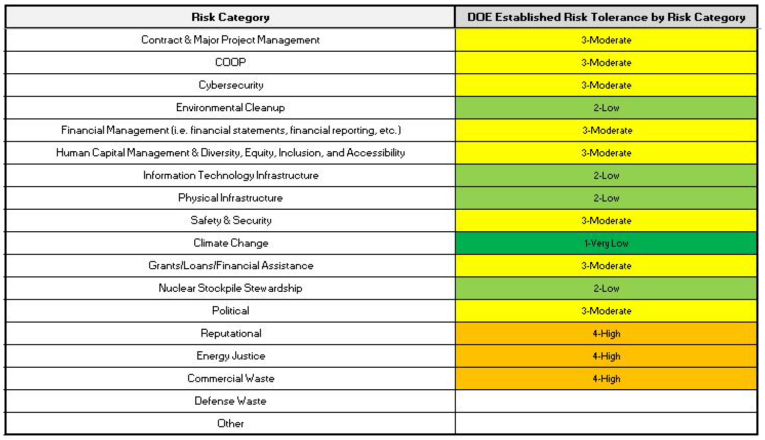
Possible Validation Errors
If a selection was not made in the *Fraud Impact* column (Column E) from the dropdown menu.
If a *Strategic Objective at Risk* (Column G) is applicable and missing.
If any of the *Operations Objectives*, *Reporting Objectives*, or *Compliance Objectives* is selected for Identification of Objectives (Column F) and "*N/A - Strategic Objective was not selected as an objective in the previous field*" is not selected for *Strategic Objective at Risk* (Column G).
If a *Strategic Objectives* is selected for Identification of Objectives (Column F) and *"N/A - Strategic Objective was not selected as an objective in the previous field*" is selected for Strategic Objective at Risk (Column G).
If *a Transfer/ Share Organization* (Column L) is applicable and missing.
If *Transfer* or *Share* is selected for *Current Strategy* (Column J) and *"N/A"* is selected for *Transfer/ Share Organization* (Column L).
If *Inherent Risk Rating* for *Impact* and *Likelihood* (Column H & I) are blank.
If the *Residual Risk Impact* and/or *Likelihood* values are greater than the *Inherent Risk Impact* and/or *Likelihood* values. For example, if the *Inherent Risk Rating* is 4 for *Impact* and 4 for *Likelihood*, and the current strategy is to reduce the risk, then selecting a *Residual Risk Impact* or *Likelihood* rating of 5 should not occur.

Residual Risk Score (Column W): This column automatically calculates the residual risk score for each identified risk by multiplying the risk's residual impact (Column P) by the residual likelihood (Column Q). A score of 25 reflects the highest possible residual risk rating (5 x 5) and a score of 1 reflects the lowest possible residual risk rating (1 x 1).

Residual Risk Rating (Column X): This column is automatically populated based on the residual risk score (Column W). The possible inputs include Very High, High, Moderate, Low, and Very Low.
DOE Established Risk Tolerance by Risk Category (Column Z): This column is automatically populated with the risk tolerance determined by the selection of the risk category (Column D). The possible inputs include Very High, High, Moderate, Low, and Very Low. If the risk category chosen does not have a risk tolerance established, this column will be blank.

NEW
in FY 2024

Table 8: DOE Risk Tolerances[5]



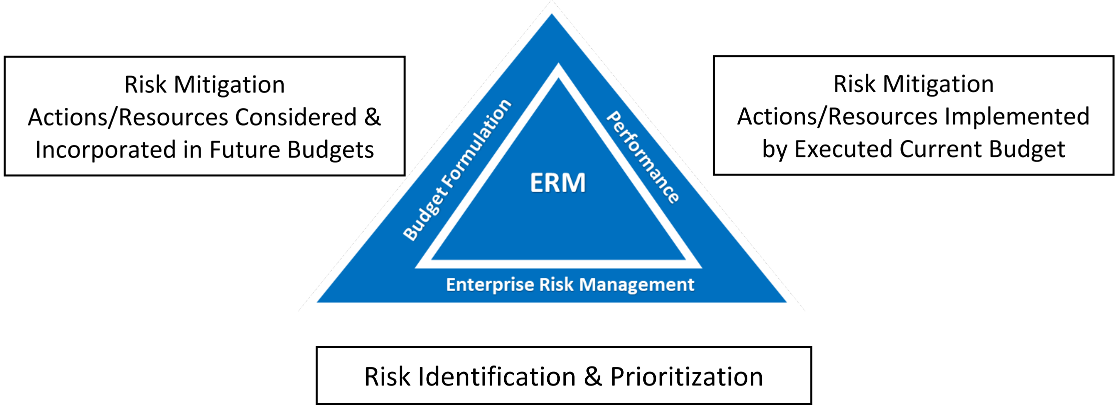
Risk Category	DOE Established Risk Tolerance by Risk Category
Contract & Major Project Management	3-Moderate
COOP	3-Moderate
Cybersecurity	3-Moderate
Environmental Cleanup	2-Low
Financial Management (i.e. financial statements, financial reporting, etc.)	3-Moderate
Human Capital Management & Diversity, Equity, Inclusion, and Accessibility	3-Moderate
Information Technology Infrastructure	2-Low
Physical Infrastructure	2-Low
Safety & Security	3-Moderate
Climate Change	1-Very Low
Grants/Loans/Financial Assistance	3-Moderate
Nuclear Stockpile Stewardship	2-Low
Political	3-Moderate
Reputational	4-High
Energy Justice	4-High
Commercial Waste	4-High
Defense Waste	
Other	

[5] Risk Tolerances for *Defense Waste* and *Other* will be assigned next fiscal year.

3.6 Risk Profile Crosscut

NEW
in FY 2024

In FY 2024, DOE will continue synchronizing risk profile and budget formulation processes. Risk consideration is a key element during budget formulation and is vital in an organization’s planning process. As such, risk management professionals should be part of every organization’s leadership effort for planning future years’ budgets. At the DOE enterprise-level, resource planning is an organizational effort that is guided by the OCFO. This approach provides oversight that the agency’s risk posture is reflected in the Department’s budget, addresses budget needs for key controls to mitigate the most important risks, and reflects the priorities and risk appetite of the Department’s leadership. It also ensures that Enterprise Risk Management, Budget Formulation, and Performance are linked when using resources. The Department’s risk profile is also used to shape discussions between DOE and OMB in supporting budget justifications. Leadership should consider risks during budget execution with discussions on funding to improve performance while responding to emerging risks.


Risk Mitigation Actions/Resources Considered & Incorporated in Future Budgets
Budget Formulation
ERM
Performance
Risk Mitigation Actions/Resources Implemented by Executed Current Budget
Enterprise Risk Management
Risk Identification & Prioritization

To demonstrate that risks are being integrated in the budget process, **there should be proper coordination and communication between the HQ Risk POC and Budget Analyst**. After the HQ Risk POC has completed the Risk Profile template, it will then be shared with the organization’s corresponding Budget Analyst to inform of their top risks. In the same workbook, the Risk Profile Crosscut tab will be completed by the Budget Analyst. Using the information from the local Risk Profile, the Budget Analyst will answer the Crosscut questions found in the template. The OCFO will review each organization’s Risk Profile Crosscut using established budget criteria to evaluate organization’s risk considerations and inclusions in budget formulation submissions.

Figure 7: FY 2024 Risk Profile Crosscut Template

FY 2024 Risk Profile Crosscut
(HQ Risk POC and Budget Representative Input)

As DOE's ERM Program matures, OCFO is requesting offices to integrate budget formulation process and link risk, budget, and performance together to ensure DOE's resources and funding requests appropriately address risks.

Please explain how your organization's risks were considered and incorporated in the previous budget formulation process or how your organization's risks will be considered and incorporated in the upcoming budget formulation process by providing responses to the questions in the below table:

Does your organization's budget request address any of the Department-wide risks as identified in the most recently published DOE Risk Profile? a. Please identify the Department-wide risk making sure to note budget estimates required to mitigate any of these risks including Bipartisan Infrastructure Legislation (IIJA) risk and similar risks with the Inflation Reduction Act (IRA). Does your organization's budget request address any organizational risks in its current risk profile? b. Please identify any specific organizational risks (not elevated/linked to DOE Risks) and related budget estimates to address and mitigate those risks in the upcoming budget request.	**Insert Response Here:** **SAMPLE RESPONSE:** ***a. Yes.*** - ***Cybersecurity - $2 million*** - ***Workforce Planning - $1 million*** ***b. Yes.*** - ***Material Shortages - $500,000*** - ***Emergency Management - $600,000***

See the link below to view the DOE Risk Profile worksheet with crosswalk tab linking to lower-level DOE Organizational risks to provide a comprehensive source of risk information across the Department for considerations in future budgets.

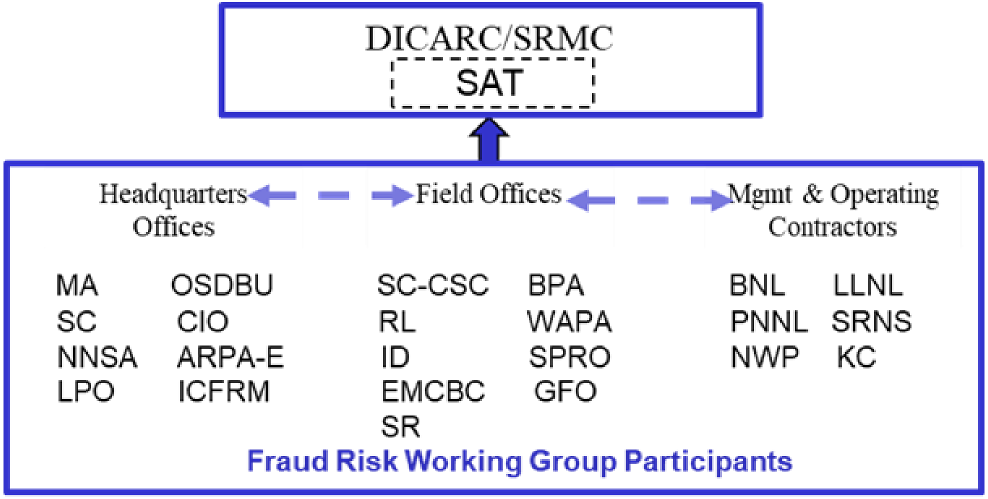
https://iportalwc.doe.gov/webcenter/content/conn/iPortalContent/path/Enterprise%20Libraries/Department_FS/Z%20-%20Other/Internal%20Controls/Crosswalk%20of%20FY2023%20DOE%20Risk%20Profile%20&%20Supporting%20DOE%20Organizational%20Risks.xlsm

4 Fraud Risk Management

DOE must continue to enhance and mature its fraud risk management efforts through effective ***Internal Controls*** and ***Data Analytics***. The passing of the ***Infrastructure Investment and Jobs Act (Infrastructure Bill), IRA, and CHIPS and Science Act*** has increased funding for DOE activities and increases the risk of fraudulent activities with taxpayer's resources.

DOE will continue implementing the plan for its Fraud Risk and Data Analytics Framework by coordinating and executing fraud risk management and mitigating activities through various working groups, with SAT such as the Data Analytics Working Group (DAWG) and Fraud Risk Working Group (FRWG). Both groups are represented by organizations at various levels throughout the Department.

Figure 8: DOE SAT as a subset of SRMC leveraging recommendations from the FRWG



In FY 2024, DOE will continue implementing its Fraud Risk and Data Analytics Framework plan with the DAWG, led by OCFO, issuing a follow-up Department-wide survey to further solidify information regarding data analytic activities that are executed within organizations throughout DOE. The refined survey results will support formalizing the Department data analytics program by leveraging existing data analytic activities. For further details, see the ***Data Analytics*** section.

4.1 Purpose and Background

Fraud poses a risk to the integrity of Federal programs and can erode public trust in government. Effective fraud risk management helps to make sure that the Department's services are fulfilling intended purposes, funds are spent effectively, and assets are safeguarded. In FY 2024, DOE continues to place emphasis on fraud prevention, detection, and mitigation to decrease fraud and to comply with the *Payment Integrity Information Act of 2019* (PIIA). PIIA indicates that the guidelines required to be established under section 3(a) of the *Fraud Reduction and Data Analytics Act* (FRDAA) shall continue to be in effect on or after the date of enactment of PIIA, which requires agencies to:

- Conduct an evaluation of fraud risks using a risk-based approach to design and implement control activities to mitigate identified fraud risks;
- Collect and analyze data from reporting mechanisms on detected fraud to monitor fraud trends and use that data and information to continuously improve fraud prevention controls; and

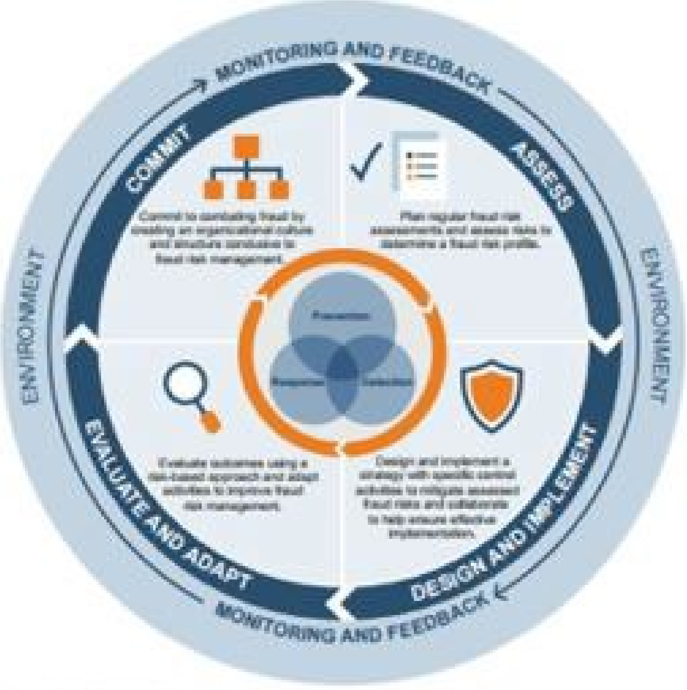
- Use the results of monitoring, evaluations, audits, and investigations to improve fraud prevention, detection, and response.

4.2 GAO Fraud Framework

To help combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks in its GAO-15-593SP, GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Framework). The Fraud Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, and highlights opportunities for Federal managers to take a more strategic, risk-based approach to managing fraud risks and developing effective antifraud controls. The Fraud Framework describes leading practices for establishing an organizational structure and culture that are conducive to fraud risk management, designing and implementing controls to prevent and detect potential fraud, and monitoring and evaluating to provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud.

DOE reporting organizations should adhere to the leading practices in the GAO Fraud Framework as part of the efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. OMB Circular A-123 establishes that managers are responsible for determining the extent to which the leading practices in the GAO Fraud Framework are relevant to the program and for tailoring the practices, as appropriate, to align with program operations. To help combat fraud and preserve integrity, Managers should adhere to the leading practices that GAO identified, as part of the efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. For details on the GAO Fraud Framework, refer to GAO-15-593SP, *A Framework for Managing Fraud Risks in Federal Programs*.

Figure 9: GAO Fraud Risk Framework and Select Leading Practices


MONITORING AND FEEDBACK
COMMIT
Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
ASSESS
Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
ENVIRONMENT
Prevention
Response
Detection
ENVIRONMENT
EVALUATE AND ADAPT
Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
DESIGN AND IMPLEMENT
Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
MONITORING AND FEEDBACK

Source: GAO-15-593SP

4.3 DOE Fraud Risk and Data Analytics Framework

In FY 2024, DOE will continue implementing a fraud risk framework over the next several years using a three-phased approach. Phase I adjusted the roles and responsibilities of the DICARC to perform additional duties as the SRMC, established the Senior Assessment Team (SAT) and identified the use of data analytics across DOE. Phase II focuses on evaluating fraud risk occurrences across DOE along with preparing and providing direction on DOE's anti-fraud strategy. Phase III will continue to mature and monitor DOE's fraud risk framework. The SAT will lead the effort for implementing DOE's Fraud Risk Framework based on recommendations from the FRWG and the DAWG, as shown in ***Figure 8***.

In response to recent legislation, ***Infrastructure Bill, IRA, and CHIPS and Science Act***, OCFO is establishing and formalizing a Department-wide data analytics program that is cross-cutting with participation from field offices to form the DAWG. To support formalizing a Department-wide data analytics program, a second survey will occur in FY 2024 to solidify results from an initial survey in FY 2023. The survey will remain focused on identifying key gaps in areas where we should establish collaborative forums to efficiently strategize an analytics approach. It will also demonstrate progress to GAO and the Office of the Inspector General (OIG) that DOE is aligning with best practices. In addition, the data analytics program will leverage Subject Matter Expert (SME) expertise throughout the Department while **not** being prescriptive on how to perform analytics because it will build on existing efforts and work.

The survey will collect an inventory of analytics activities currently performed across the Department in seven risk areas that have a high potential of fraudulent activities as prioritized by the OIG and DICARC/SRMC. Those potential risk areas include:

1) Rebates;
2) Grant/Cooperative Agreements;
3) Loans;
4) Cybersecurity (includes labs and M&O Contractors);
5) Labor charging – Federal and Contractor (includes labs and contractors);
6) Materials and Service – Contract and Project Management (includes labs and contractors); and
7) Property.

After the DAWG analyzes the data, the results will be reconciled to the Department's Fraud Risk Register to identify potential gaps.

4.4 Fraud Considerations in the Risk Profile

Management has overall responsibility for establishing internal controls to manage the risk of fraud. When developing the FY 2024 Risk Profile, organizations must consider the potential for fraud and should follow the guidance set forth by the GAO Fraud Framework and GAO Green Book.

In FY 2024, reporting organizations must continue to identify the top financial and non-financial fraud risks in the Risk Profile. These ongoing fraud risk statements must be included in each entity's Risk Profile deliverable along with other identified risks. **Organizations must identify each risk with financial or nonfinancial fraud impact by completing the *Fraud Impact* column (Column E) in the Risk Profile template.** Organizations will select from a drop-down menu, identifying whether a risk is a **financial fraud, non-financial fraud, top financial fraud, or top non-financial fraud**. If a risk does not have a financial or nonfinancial fraud implication, then organizations will select '*N/A*' from the drop-down menu selection. While financial fraud risks are often well known, there can be difficulties in identifying non-financial fraud risks. Examples of potential non-financial fraud risks are included below:

- Theft of PII or classified information;
- False claims or false statements (e.g., a contractor makes false statements to win a bid, an employee provides false statements to be hired, or a grantee provides false claims to be awarded a grant);
- Employees pressured to issue knowingly incorrect non-financial data/reports;
- Product substitution or counterfeit parts (e.g., a subcontractor fraudulently provides the wrong parts or parts of a lesser material); and
- Employee sabotage or employee vandalism.[6]

4.5 Fraud Considerations in the FMA and EA Reviews

DOE maintains an emphasis on fraud prevention in the FMA Module within AMERICA to further increase fraud prevention activities across the Department. Entities should continue to review controls to determine if a fraud and/or improper payments risk is mitigated. Any controls that mitigate a fraud and/or improper payments risk should be designated as such in the FMA Module Assessment tab by **selecting the appropriate designation from the *Fraud/Improper Payments* dropdown option for controls**. **Entities should also continue to improve data integrity by identifying from the dropdown menu whether the control is *Business, Compliance, Performance*, or *IT*.** Also, if a control is designed to mitigate a fraud and/or improper payment risk and the control fails testing, or fails related to the detection of potential fraud, the organization will promptly notify their assigned OCFO Analyst on the control failure and the remediation plan to confirm a control is designed and operating effectively to mitigate the risk. **A written notification to the assigned OCFO Analyst will occur within two weeks of the identified control test failure**.

In FY 2023, 58 corporate risks were added to the FMA Module within AMERICA. The 58 corporate risks are financial related fraud risks that are linked to the Department's Fraud Risk Register and are mapped to risks in the Department's Fraud Risk Profile. In FY 2024, reporting organizations should continue to identify relevant risks, perform risk assessments, and test controls to mitigate the newly added corporate risks.

To sustain increased fraud prevention activities across the Department, emphasis remains in this area in the EA Module. In the Entity Objective Evaluation tab, organizations must evaluate the Fraud Prevention entity objective. This evaluation is in addition to the assessment of fraud risk under the GAO Green Book Principle #8, "management should consider the potential for fraud when identifying, analyzing, and responding to risks," in the Internal Controls Evaluation tab. The Fraud Prevention entity objective has several considerations that should be evaluated by reporting organizations.

1) *Top Financial and Top Non-Financial Fraud Risks:* Organizations must identify the top financial and non-financial fraud risks. The top fraud risks identified in an entity's EA Module should be consistent with the fraud risks included in the FY 2024 Risk Profile deliverable;
2) *Fraud Risk Factors:* Entities should consider the fraud risk factors from the GAO Green Book. While the following fraud risk factors do not necessarily indicate that fraud exists, they are often present when fraud occurs;
    - Incentive/Pressure: Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud

[6] Black's Law Dictionary defines vandalism as mindless and malicious harm and injury to another's property.

- Opportunity: Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud
- Attitude/Rationalization: Individuals involved can rationalize committing fraud

3) *Fraud Mitigation Controls for Identified Fraud Risks:* Organizations should determine if controls are in place to mitigate identified fraud risks. For controls reported in the FMA Module that manage a fraud risk, organizations should assign a fraud, and/or improper payments control type;
4) *Management's Commitment to Reporting Fraud:* Entities should evaluate whether the organization is encouraging the reporting of suspected fraud to the DOE OIG in accordance with DOE Order 221.1B, "Reporting Fraud, Waste and Abuse to the Office of Inspector General;"
5) *Additional Potential Areas of Fraud Risk:* Organizations should specifically consider potential fraud risks in the following areas that are more susceptible to fraud at DOE:
   - Rebates;
   - Grant/Cooperative Agreements;
   - Loans;
   - Cybersecurity;
   - Labor charging;
   - Materials and Service; and
   - Property

Entities that complete an FMA Module should assess and evaluate the potential fraud risks in the FMA. Organizations that are not required to complete an FMA Module should list mitigating control activities in their EA Module.

4.6 Fraud Trends Across the Department

The Department continues efforts to combat and prevent fraud, waste, and abuse. One particular fraud risk that continues to emerge as a threat to the Department is Business E-Mail Compromise (BEC). BECs involve the impersonation of legitimate DOE personnel or vendors to request changes in the payment information to route Department funds to a fraudulent bank account. Fraudsters use the information available online to impersonate a legitimate Department vendor/employee, create a spoofed e-mail address similar to the legitimate vendor/employee e-mail address, and then send an e-mail to a DOE entity requesting a change in banking information.

BEC fraudulent activities continue to adversely impact the Department and Government as a whole. Reporting organizations should review the *Business E-mail Compromise Checklist* on the final page of this appendix. The checklist contains immediate actions in the event of a BEC, as well as potential controls for prevention and recognition. Reporting organizations should consider the risk of business e-mail compromise fraud and establish or enhance controls to manage the risk as warranted.

GAO has identified nine fraud scheme categories in recent audits that may impact the DOE. Reporting organizations should consider the actions they are taking to mitigate the potential risks of these fraud schemes from occurring. The fraud schemes are found in ***Table 9***.

***Table 9: GAO Contracting Fraud Schemes Categories*[7]**

Bid Rigging	Payroll Schemes	Kickback and Gratuities
Conflicts of Interests	Misrepresentation of Eligibility	Theft
Product Quality	Contract Progress Schemes	Billing Schemes

The DOE OIG also identified common fraud schemes that entities should consider:

- **Non-Deliverables:** Where a recipient fails to produce what is required from the statement of work or the grants/contract is closed out without holding the recipient/contractor accountable;
- **Bid Rigging or Collusion:** Two or more contractors/subcontractors/grantees work together and attempt to extort the Department of funds;
- **Fraud in the Inducement:** When a grantee lies about capabilities to receive agency funding;
- **Ghost Employees:** Paying Government funds to employees that do not exist;
- **Fictitious Invoices/Laundering:** Fake companies send fictitious bills to the prime contractors /grantee for reimbursement;
- **Kickbacks/Bribes/Extortion/Conflict of Interest by Federal officials in the award and administration of grants/ contracts**; and
- **Foreign Corrupt Practices on the part of U.S. or foreign officials**.

There has been a rise of vulnerability to BEC and targeted phishing on most remote and teleworkers; therefore, the following should be considered to avoid becoming a victim to these common fraud schemes when not working in the office:

- **Use DOE equipment for DOE business only:** Do not connect unauthorized devices (e.g., smartphones and USB devices) to your DOE equipment;
- **Update your work devices:** Check that your devices and software are up to date;
- **Communicate your working hours:** Establish and disclose your hours of availability for your team's awareness;
- **Observe your surroundings:** Avoid having sensitive work-related conversations in public areas;
- **Encrypt e-mail messages containing sensitive information:** Ensure your online activities are encrypted and use telework capabilities provided;
- **Avoid leaving DOE equipment unattended at any time:** Lock your screen when walking away and store your work device in a secure location;
- **Practice good phishing hygiene:** Avoid clicking on suspicious links and attachments from unsolicited e-mails; and
- **Be cautious of unfamiliar e-mails**.

4.7 Fraud Communication Requirements

DOE internal controls reporting organizations are expected to report allegations and actual instances of fraud, waste, abuse, corruption, criminal acts, or mismanagement related to DOE programs to the Department's OIG in accordance with DOE Order 221.1B. The DOE OIG is responsible for investigating any fraudulent acts involving DOE, contractors or subcontractors, or any crime affecting the programs, operations, Government funds, or employees of those entities. Entities can report suspected or actual fraud to the OIG anonymously and confidentially through the OIG Hotline[8]. **Organizations should report allegations of suspected or actual fraud promptly to the Department OIG**.

[7] The definitions are found in the Glossary.

[8] Contact OIG Hotline via e-mail: ighotline@hq.doe.gov, or phone: (202) 586-4073, toll free: (800) 541-1625, and fax: (202)-586-4902. A webform may also be filled out using the following web address: https://www.energy.gov/ig/complaint-form.

5 Internal Controls

As part of DOE's fraud risk management efforts in FY 2024, the Department's Internal Control Program will continue with a more collaborative approach to its Focus Area Risks in AMERICA by being less prescriptive and coordinating with reporting organizations. By doing so will allow more efficient use of limited resources while mitigating potential fraud risk occurrences. Reporting entities focus area risks will concentrate on each organization's highest vulnerabilities. In addition to DOE's revised approach for identifying its Focus Area Risks, reporting organizations risk assessments will continue to focus on identifying and mitigating risks related to the *Infrastructure Bill, IRA, and CHIPS and Science Act*, where applicable*.*

5.1 Purpose and Background

Internal control requirements are codified in the FMFIA. The Act requires the Comptroller General of the GAO to establish internal control standards and the Director of the OMB, to establish guidelines for agency evaluation of systems of internal control to determine such systems' compliance with the requirements. The GAO established formal standards in the Green Book, and OMB established guidelines for evaluation in OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

This guidance establishes the DOE Internal Control Program requirements for evaluating and reporting on internal controls in accordance with A-123.

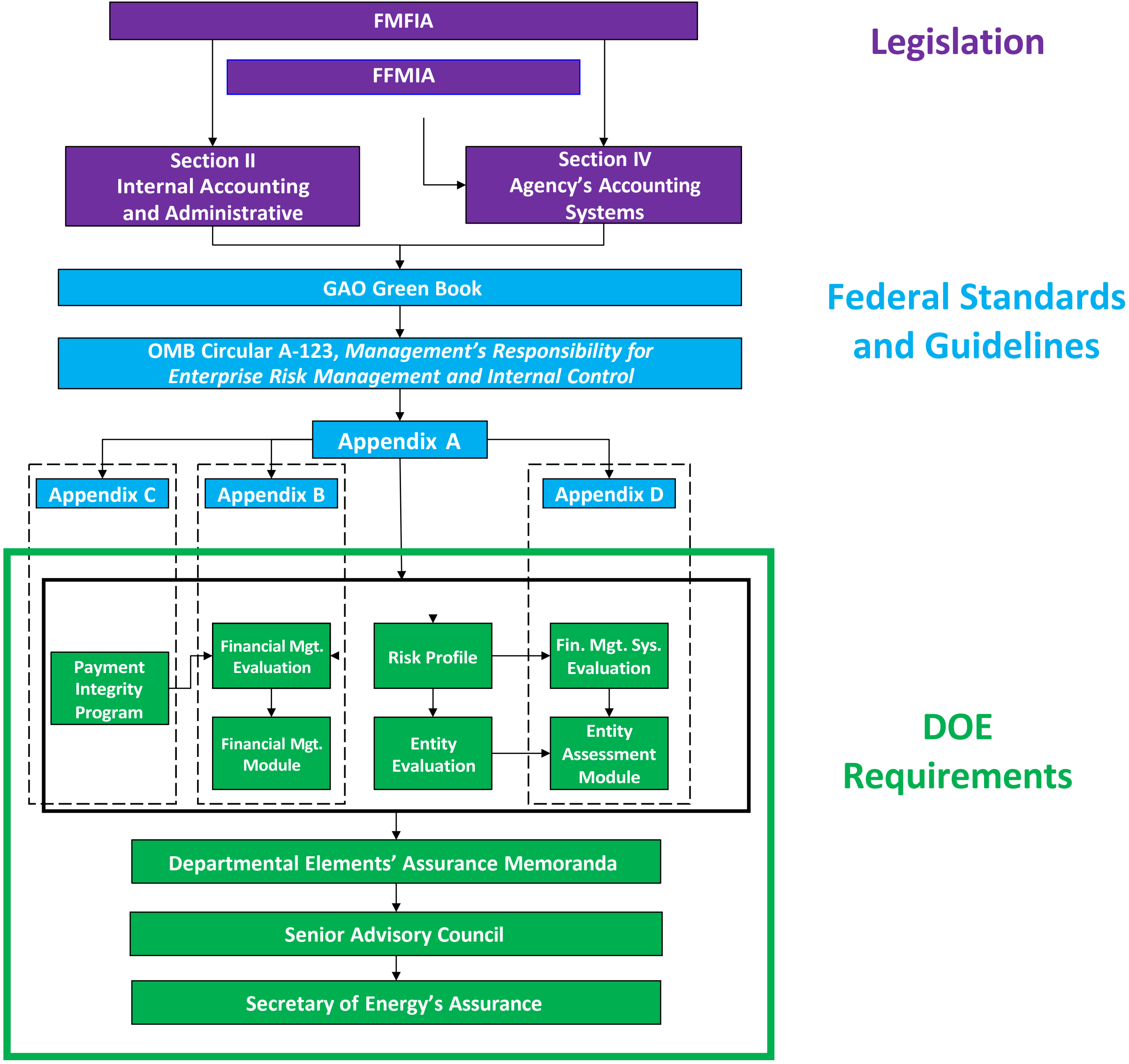
FMFIA requires each agency to:

- Establish and maintain an internal control system, and report on the overall adequacy and effectiveness of internal control systems. Internal control systems should provide: 1) obligations and costs to be recorded in compliance with applicable laws; 2) funds, property, and other assets to be safeguarded; and 3) revenues and expenditures applicable to agency operations to be properly recorded and accounted for to provide reliable financial reporting and to maintain accountability over the assets;
- Evaluate Financial Management Systems (FMS) to determine compliance with Government-wide requirements mandated by Section 803(a) of the FFMIA and to take corrective actions if systems are non-compliant; and
- Provide an annual assurance statement signed by the head of the agency reporting on the overall adequacy and effectiveness of internal controls related to operations, reporting, and compliance; identified material weaknesses; and whether the agency's FMS are in compliance with FFMIA.[9]

Figure 10 presents the DOE framework for internal control evaluations. The DOE activities (in green) meet statutory requirements (in purple) and Federal Government guidance (in blue).

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

Figure 10: DOE Framework for Internal Control Evaluations



5.2 OMB Circular A-123

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, requires the:

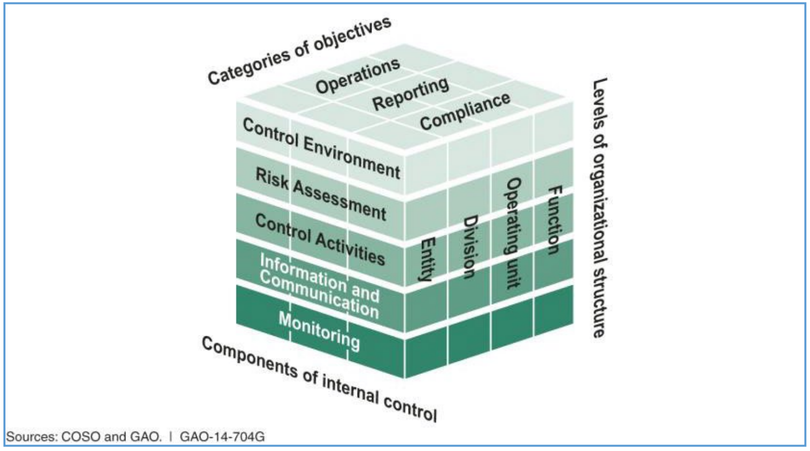
- Establishment and maintenance of internal controls to achieve objectives related to operations, reporting and compliance;
- Evaluation of the effectiveness of DOE internal controls in accordance with the GAO Green Book; and
- Annual reporting of overall adequacy and effectiveness of DOE internal controls related to operations, reporting, and compliance, and compliance of FMS with Government-wide requirements.

5.3 GAO Standards for Internal Control

GAO's Green Book provides criteria for designing, implementing, and operating an effective internal control system, and through the use of components and principles, establishes standards for internal control. Internal control in an organization provides reasonable, not absolute, assurance that the organization will achieve objectives related to operations, reporting, and compliance.

Using the standards and guidance provided in the Green Book, an organization can design, implement, and operate internal controls to achieve objectives related to operations, reporting, and compliance. The five components of internal control are: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. There are 17 principles which support the effective design, implementation, and operation of the five components and represent requirements necessary to establish an effective internal control system.

Figure 11: The Components, Objectives, and Organizational Structure of Internal Control



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

Source: GAO-14-704G

The columns labeled on the top of the cube represents the three categories of an entity's objectives. The rows represent the five components of internal control. The levels of organizational structure represent the third dimension of the cube. Each component of internal control applies to the three categories of objectives and the organizational structure.

5.4 Shifting from Low-Value to High-Value Work

DOE continues to streamline operations and incorporate flexibility for the components, complementing broader Government-wide efforts to shift resources from low-value to high-value work. Consistent with this effort, in FY 2024 reporting organizations will perform control assessments on DOE's highest rated risks, including fraud risks. In FY 2024, reporting organizations will focus on testing controls that are mitigating fraud risks and risks that have high and moderate combined risk ratings. Also, in FY 2024, OCFO will conduct a series of Lunch-n-Learns during Q2 and Q3 through the Microsoft Teams platform. The Lunch-n-Learns will focus on the basics of data analytics and business process documentation.

NEW
in FY 2024

5.5 Key Internal Control Requirements

This guidance provides the FY 2024 Internal Control requirements for:

- Financial Management Assessment Evaluations (FMA Module);
- EA Evaluations (EA Module);
- FMS Evaluations (FMS Tab within the EA Module);
- Interim IICS Module; and
- Assurance Memoranda.

Table 10 provides the DOE Internal Control requirements for each entity. While DOE does not require every organization to provide Internal Control deliverables to the OCFO, organizations should check with respective HQ Offices to determine if a deliverable is needed by the cognizant organization. A brief synopsis for organizations at each level within a reporting hierarchy are:

- Departmental Elements (HQ and Field Offices) are responsible for considering internal control evaluation results of Major/Integrated Contractors, **including both M&O and integrated non-M&O Contractors**[10];
- Small Departmental Elements are not required to perform FMA evaluations. These Elements must complete the five peripheral entity objectives in the EA Module. (Small Departmental Elements are identified in ***Table 10***);
- Site Offices[11] are not required to provide an EA deliverable to the OCFO and should check with the cognizant Field and HQ Offices to determine if an EA deliverable is required to either cognizant organization;
- Major/Integrated Contractors, **including both M&O and integrated non-M&O Contractors**, are required to provide a Risk Profile to the cognizant Field Office and are not required to provide the Risk Profile to the OCFO; and
- Reporting organizations that are required to provide Risk Profiles will refer to the ***Risk Profile and Fraud Considerations in the Risk Profile*** section.

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

[11] The site offices are Kansas City, Livermore, Los Alamos, Nevada, NNSA Production, Sandia, Ames, Argonne, Berkley, Brookhaven, Fermi, Princeton, Oak Ridge, Pacific Northwest, SLAC, and Thomas Jefferson.

Table 10: Listing of Required Internal Control Evaluations due to OCFO by Organization[12]

Departmental Elements & Reporting Organizations		FMA Evaluation	Entity Evaluation	FMS	Interim Internal Control Status	Assurance Memorandum
Deputy Secretary & Under Secretary Offices	Office of the Deputy Secretary (S2)					✓
	Office of the Under Secretary for Infrastructure (S3)					✓
	Office of the Under Secretary for Science and Innovation (S4)					✓
	Office of the Under Secretary for Nuclear Security and National Nuclear Security Administration (S5)					✓
Independent Agency	Federal Energy Regulatory Commission					✓
Headquarters Offices	Advanced Research Projects Agency-Energy	✓	✓	✓	✓	✓
	Office of the Chief Financial Officer	✓	✓	✓	✓	✓
	Office of the Chief Information Officer	✓	✓	✓	✓	✓
	Cybersecurity, Energy Security & Emergency Response	✓	✓	✓	✓	✓
	Office of Electricity	✓	✓	✓	✓	✓
	Energy Efficiency and Renewable Energy	✓	✓	✓	✓	✓
	Environment, Health,Safety and Security	✓	✓	✓	✓	✓
	Environmental Management	✓	✓	✓	✓	✓
	Fossil Energy and Carbon Management	✓	✓	✓	✓	✓
	Human Capital Officer	✓	✓	✓	✓	✓
	Inspector General		✓		✓	✓
	Joint Office of Energy and Transportation					✓
	Legacy Management	✓	✓	✓	✓	✓
	Loan Programs Office	✓	✓	✓	✓	✓
	Management	✓	✓	✓	✓	✓
	National Nuclear Security Administration	✓	✓	✓	✓	✓
	Nuclear Energy	✓	✓	✓	✓	✓
	Project Management	✓	✓	✓	✓	✓
	Science	✓	✓	✓	✓	✓
	Office of Clean Energy Demonstrations	✓	✓	✓	✓	✓
	Federal Energy Management Programs	✓	✓	✓	✓	✓
	Grid Deployment Office	✓	✓	✓	✓	✓
	Manufacturing & Energy Supply Chains	✓	✓	✓	✓	✓
	State and Community Energy Programs	✓	✓	✓	✓	✓
Small Headquarters Offices	Congressional and Intergovernmental Affairs		✓		✓	✓
	Energy Justice and Equity		✓		✓	✓
	Energy Information Administration		✓		✓	✓
	Office of Policy		✓		✓	✓
	Enterprise Assessments		✓		✓	✓
	General Counsel		✓		✓	✓
	Hearings and Appeals		✓		✓	✓
	Indian Energy Policy & Programs		✓		✓	✓
	Intelligence and Counterintelligence		✓		✓	✓
	International Affairs		✓		✓	✓
	Public Affairs		✓		✓	✓
	Office of Small and Disadvantaged Business Utilization		✓		✓	✓
	office of Technology Transitions		✓		✓	✓
Power Marketing Administrations	Bonneville Power Administration	✓	✓	✓	✓	✓
	Southeastern Power Administration	✓	✓	✓	✓	✓
	Southwestern Power Administration	✓	✓	✓	✓	✓
	Western Area Power Administration	✓	✓	✓	✓	✓
Field/Operation Offices	EM Consolidated Business Center	✓	✓	✓	✓	✓
	Golden Field Office	✓	✓	✓	✓	✓
	Idaho Operations Office	✓	✓	✓	✓	✓
	National Energy Technology Laboratory	✓	✓	✓	✓	✓
	NNSA Albuquerque Complex	✓	✓	✓	✓	✓
	Naval Reactors Laboratory Field Office	✓	✓	✓	✓	✓
	Oak Ridge Environmental Management	✓	✓	✓	✓	✓
	Richland Operations Office	✓	✓	✓	✓	✓
	Savannah River Operations Office	✓	✓	✓	✓	✓
	Science Consolidated Service Center	✓	✓	✓	✓	✓
	Strategic Petroleum Reserve Project Management Office	✓	✓	✓	✓	✓
Major/ Integrated Contractors	Kansas City National Security	✓	✓	✓	✓	
	Lawrence Livermore National Laboratory	✓	✓	✓	✓	
	Los Alamos National Laboratory	✓	✓	✓	✓	
	Nevada National Security Site	✓	✓	✓	✓	
	Pantex Plant	✓	✓	✓	✓	
	Y-12 National Security Complex	✓	✓	✓	✓	
	Sandia National Laboratory	✓	✓	✓	✓	
	Naval Nuclear Laboratory	✓	✓	✓	✓	
	Ames Laboratory	✓	✓	✓	✓	
	Argonne National Laboratory	✓	✓	✓	✓	
	Brookhaven National Laboratory	✓	✓	✓	✓	
	Fermi National Accelerator Lab	✓	✓	✓	✓	
	Lawrence Berkeley National Laboratory	✓	✓	✓	✓	
	Princeton Plasma Physics Laboratory	✓	✓	✓	✓	
	Oak Ridge National Laboratory	✓	✓	✓	✓	
	Oak Ridge Institute for Science & Education	✓	✓	✓	✓	
	Pacific Northwest National Laboratory	✓	✓	✓	✓	
	Thomas Jefferson National Accelerator Facility	✓	✓	✓	✓	
	SLAC National Accelerator Laboratory	✓	✓	✓	✓	
	National Renewable Energy Laboratory	✓	✓	✓	✓	
	Strategic Petroleum Reserve	✓	✓	✓	✓	
	Idaho National Laboratory	✓	✓	✓	✓	
	Waste Isolation Pilot Plant	✓	✓	✓	✓	
	East Tennessee Technology Park	✓	✓	✓	✓	
	Savannah River Nuclear Solutions	✓	✓	✓	✓	
	Battelle Savannah River Alliance	✓	✓	✓	✓	

***Major/Integrated Contractors are required to complete a Risk Profile and submit to their cognizant Field Office; but are not required to submit the Risk Profile to the OCFO.**

**** While Site Offices are not required to submit evaluations to OCFO, Site Offices should check with their Field and Headquarters Offices to determine if a submission is required to either cognizant organization.**

5.6 Important Dates and Transmittal Methods

Table 11: DOE Internal Controls Important FY 2024 Dates

Key Dates	Deliverables
December 15	AMERICA open for documenting FY 2024 internal control testing and evaluation results.
December 28	OCFO publishes FY 2024 ERM Guidance to include the Data Analytics Survey Template.
January 18	Reporting organization's provide primary IT POC's name, e-mail address, and phone number to the ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov.
February 22	Reporting organizations will provide the completed Data Analytics Survey Template to the ICFRMD shared mailbox at CFO-ICFRMD@hq.doe.gov.
March 12	Reporting organizations (M&O Contractors, Site Offices, Field Offices, PMAs & HQ Offices) provide IICS using the AMERICA Application.
April 1 – 30	AMERICA semi-annual user access reviews are conducted by OCFO and reporting organizations.
April 2	OCFO provides the FY 2024 Assurance Memoranda Template to reporting organizations.
July 11	M&O Contractors and Field Offices provide FMA Module and EA Module using the AMERICA Application. Reporting organizations should follow subsequent timelines published by cognizant organizations to assure FMA and EA Modules are provided to DOE on time.
July 30	HQ Offices and PMAs provide FMA Module and EA Module using the AMERICA Application.
August 6	OCFO provides eDOCS information to HQ Offices and PMAs.
August 13	Field Offices provide a draft Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov, considering and incorporating Site Offices and M&O Contractors. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Draft".**
September 4	Field Offices provide signed Assurance Memoranda to the ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Signed".**
	Headquarters (HQ) Offices and PMAs provide draft Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Draft".**
September 17	HQ Offices and PMAs provide signed Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov and eDOCS. **Subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-Signed".**
September 24	Under Secretaries provide signed Assurance Memoranda to ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov.
September 26	AMERICA close-out for FY 2024.
October 1	Organizations that resolve or identify a significant deficiency or material weakness, after June 30, 2024, and no later than September 30, 2024, that is not included in a signed Assurance Memoranda, must notify the OCFO and update the Assurance Memoranda.

Table 11 provides Internal Control Evaluation deadlines. Organizations must provide the Internal Control deliverables on time. If there is an emerging issue preventing an organization from providing a deliverable on time, then the organization will provide the specific reason(s) for the delay to include any potential significant deficiency or material weakness to the assigned OCFO analyst for the organization. Management quality assurance reviews will take place at every level prior to providing Internal Control deliverables and Risk Profiles.

Entities (Federal and contracting organizations) should provide the Internal Control Deliverables in accordance with ***Table 12***. When reporting organizations are providing draft and signed assurance memoranda, **the subject line of the e-mail should read "FY 2024 <insert org's name> Assurance Memo-**

[12] Includes newly established organizations that are in the process of getting incorporated into the Internal Control and ERM Program.

Draft" or FY 2024 <insert org's name> Assurance Memo-Signed". For example, FY 2024 CFO Assurance Memo-Draft or FY 2024 CFO Assurance Memo-Signed, whichever is appropriate.

Table 12: Reporting Documentation Transmittal Methods

Deliverable	Format	Method	Due Dates	Recipient(s)
EA, FMA, FMS Evaluations, and IICS	AMERICA	A-123 Application	See *Table 11*	Major/Integrated Contractors to: Field Office Field Office to: Lead Program Secretarial Office Lead Program Secretarial Office to: OCFO
Assurance Memorandum (Including Corrective Action Plan Summary)	Draft (Word)	E-mail to CFO-ICFRMD@hq.doe.gov	08/13/2024	Field Offices Assurance Memorandum addressed to: Lead Program Secretarial Office with copies to the Cognizant Secretarial Office(s)
	Signed PDF	E-mail to CFO-ICFRMD@hq.doe.gov	09/04/2024	
	Draft (Word)	E-mail to CFO-ICFRMD@hq.doe.gov	09/04/2024	HQ and PMAs Assurance Memorandum addressed to: The Deputy Secretary
	Signed PDF	E-mail to CFO-ICFRMD@hq.doe.gov and upload to eDOCS	09/17/2024	

5.7 Documentation Requirements

All organizations are required to maintain written policies and procedures for implementing the internal controls evaluation process described in this guidance. The level and nature of documentation may vary based on the size of the entity and the complexity of the operational processes the entity performs.

Management uses professional judgment in determining the extent of the documentation that is developed. Documentation is required to demonstrate the design, implementation, and operating effectiveness of an entity's internal control system. These policies and procedures must include a Quality Assurance (QA) program conducted by Departmental Elements on inputs from the reporting organizations to provide quality and accuracy. Documentation supporting internal control evaluations and results will remain on file with the organization and upon request, provided to the OCFO, respective Field or HQ Office, senior managers, or auditors. Documentation records should remain on file for six years.

Examples include:

- Internal and external assessments;
- Results of external audits, including financial statement audits and findings along with appropriate work papers;
- Internal audits to include working papers and/ or management reviews;
- Process flows and descriptions;
- Biennial pricing reviews;
- Test documentation more detailed than what is included in the FMA and EA Modules; and
- Evidence collected during testing.

Organizations must have appropriate and verified procedures to test the effectiveness of the controls using re-performance, observation, inquiry, and inspection. These key procedures as referenced by A-123, Appendix A, *Implementation Guide,* should be cited in the FMA and EA Modules, where applicable:

- **Re-performance** is an objective execution of procedures or controls performed as part of a test of the effectiveness of the entity's internal control (e.g., recalculating an estimate or re-performing a reconciliation);
- **Observation** is the viewing of a specific business process in action and, in particular, the control activities associated with the process, to test the effectiveness of an internal control (e.g., observing a physical inventory or watching a reconciliation occur);
- **Inquiry** is a detailed discussion with knowledgeable personnel to determine if controls are in place and functioning (e.g., do you reconcile your activity or do you review a certain report each month); and
- **Inspection/Examination** is scrutiny of specific business processes and documents through consideration and analysis for approval authorities that indicate the effectiveness of controls (e.g., looking for signatures of a reviewing official or reviewing past reconciliations).

Controls testing must be sufficient and well documented. Examples of **insufficient test** result descriptions or narratives that **should be avoided** include:

- Walkthroughs;
- Limited Discussions;
- Reviews of organization charts; and
- Talking to a limited number of people, performing inadequate testing.

These test procedures result descriptions are not adequate and detailed enough to reveal the effectiveness or weakness of internal controls. Testing procedures and results should be adequately written and have enough detail that will provide an understanding of the test and results.
When determining test procedures, the complexity and frequency of controls, including whether the controls are automated or manual, are key considerations. For example, complex controls that are manual and used on a regular basis should be tested more in-depth than less complex controls that are automated and used on a periodic basis. Sampling is used to select the appropriate number of transactions to test for each control. Sampling methods for consideration are:

- **Random:** A method of selecting a sample whereby each item in the population[13] of transactions is given an equal chance of selection regardless of the population size. Typically, sampling software or a random number generator is used to identify the items comprising the sample. Random selection is generally considered the most likely method to result in a sample that is representative of the population;
- **Judgmental:** A method of sample selection whereby the sampled items are selected based on a deliberate choice based on the profile of the population of transactions (e.g., there may be unusual patterns or higher-risk items that exist). This method provides validation that high-risk or other items of interest are included in the selected sample and reviewed as part of testing the control; and
- **Systematic:** A method of sample selection whereby a uniform interval (i.e., every *n*th item) is selected throughout the population. The appropriate interval is determined by dividing the number of items in the population by the sample size.

[13] A population includes every transaction that occurred within a given time period.

NEW in FY 2024

Sample size for tests of controls is dependent on the nature of the control (manual versus automated), the frequency of the control, control risk and whether the control is related to a financial or operational process. Financial controls are primarily designed to ensure the accuracy, reliability, and integrity of financial reporting. They focus on safeguarding assets, preventing and detecting errors or fraud, and ensuring compliance with laws and regulations. Financial controls correspond to various processes (e.g., segregation of duties, authorization and approval procedures, documentation of transactions, and periodic reconciliations). Minimum sample sizes listed in *Table 13: Suggested Sample Sizes for Financial Controls* are consistent with guidance provided by the Implementation Guide for OMB Circular A-123, Appendix A.

Table 13: Suggested Sample Sizes for Financial Controls[14]

Minimum Sample Size for Testing Manual Controls (Based on Zero Acceptable Deviations)				
Assumed Population of Control Occurrences	**Approximate Frequency of Control**	**Number of items to Test (Sample Size)**		
		Low Risk Rating	Moderate Risk Rating	High Risk Rating
1	Annual / Semi-Annual / Bi-Annual	1	1	1
4	Quarterly	2	2	2
12	Monthly	2 or 16.67%	3 or 25%	5 or 41.67%
24-52	Weekly / Biweekly	5 or 9.62%	10 or 19.23%	15 or 28.85%
53-250	Daily	20 or 8%	30 or 12%	40 or 16%
Over 250	Multiple Times Per Day	30	45	60
Note: In certain instances, sample sizes may need to be adjusted. There are times when the sample sizes should be increased and determined based on the population of occurrences instead of relying on the control frequency to provide reasonable assurance over the operating effectiveness of the control.				
Minimum Sample Size for Testing Automated Controls				
Description			**Sample Size**	
For an automated control, the number of items required to be tested is minimal.			1	

Significant operational controls concentrate on operational efficiency and effectiveness rather than financial reporting. They involve processes, procedures, and guidelines put in place to optimize operations, manage risks, enhance productivity, and achieve organizational goals. While financial controls are critical for accurate financial reporting and compliance, significant operational controls are vital for the overall functioning and success of the organization beyond financial considerations.

5.8 Financial Management Assessment (FMA) Evaluation

5.8.1 FMA Supporting Documentation

The FMA Module is the central location for documenting the evaluation of the relevant financial business processes, sub-processes, and risks facing each reporting entity, as well as the key controls and testing information for each process that are relied upon to mitigate the risks. Reporting entities should reference within the **Documentation Location** section of the **Assessment** tab in AMERICA the physical or electronic location of the documents that support the identification of the controls and verification of

[14] Implementation Guide for OMB Circular A-123, *Management's Responsibility for Internal Control, Appendix A, Internal Control over Financial Reporting*

the applicability of the business process, sub-process, corporate and local risks to the entity.

5.8.2 Requirements for FY 2024

In FY 2024, entities must perform, at a minimum, these actions:

a) **Fraud and Improper Payments Consideration**: Effective fraud risk management determines whether taxpayer dollars and Government services serve the intended purposes. Entities are responsible for reviewing the controls to determine if the controls are mitigating a fraud and/ or improper payments risk. Controls that mitigate a fraud and/ or improper payments risk should be designated as such in the Assessment tab by selecting the appropriate designation from the Fraud/ Improper Payments dropdown option for controls.

NEW
in FY 2024

In FY 2024, the *Fraud/Improper Payments/Both Fraud & IP* dropdown options have been removed from the *Control Category* field. **Local controls** which were reported as *Fraud, Improper Payments,* or *Both Fraud & IP* in the *Control Category* field at the end of FY 2023 has a "blank space" in the *Control Category* field. Organizations affected by this change will need to review and update these **local controls,** if needed. Impacted organizations will be notified in January of the local controls affected by this change and **must** identify in the FMA Module **local controls** that are subject to fraud, improper payment, or both by **selecting from the dropdown menu of the *Fraud/Improper Payments* field**. Also, if a control is designed to mitigate a fraud and/ or improper payment risk and the control fails testing, or fails related to the detection of potential fraud, the organization will notify their assigned OCFO Analyst on the control failure and the remediation plan to confirm a control is designed and operating effectively to mitigate the risk. **A written notification to the assigned OCFO Analyst will occur within two weeks of the identified control test failure**. In FY 2023, fraud risk statements from the Department's Fraud Risk Register were added as corporate risks to the FMA Module and **reporting organizations were to determine whether the fraud risks were applicable and perform risk assessments. For the fraud risk statements that are applicable, reporting organizations will continue to identify and test mitigating controls in FY 2024.**

NEW
in FY 2024

b) **New Risks and Controls Added to the FMA Module and Control Set Execution**: AMERICA will provide a one-year grace period for reporting organizations to test the controls that are mitigating new risks that are added to the FMA module. However, if there is sufficient data to conduct control testing, reporting organizations must test the controls that are mitigating risks with a high exposure risk rating in the same year the risks are added to the FMA Module or if the added risk is a corporate risk that has been identified as a focus area regardless of the risk rating. If there is no sufficient data to conduct the controls testing in the same year when a reporting organization adds a risk with a high exposure risk rating or is a focus area risk, then the reporting organization will test the controls the following year. Instances when a reporting organization does not have sufficient data to test the controls for a newly added risk, there will not be a Control Execution rating. As a result, the Control Set Execution rating should remain blank. Some scenarios may exist in AMERICA that will allow reporting organizations to receive a two-year grace period for a newly added risk and control. However, reporting organizations are required to test newly added risks and controls within one year of the risk being added to AMERICA. Also, the **reasons for controls that are due or overdue for testing, but are not tested, should be entered into Control User Field 1.** For more details, refer to the AMERICA FMA, EA, and IICS Module User Guides.

c) **Lease Risk Statements:** In FY 2024, DOE began implementing revised financial reporting standards for Federal lease accounting in accordance with the Statement of Federal Financial Accounting Standards (SFFAS) 54, *Leases*. Consequently, reporting organizations are required to recognize a lease liability and a lease asset at the beginning of a lease term unless it meets the scope exclusions or the definitions/criteria of a non-intragovernmental short-term lease, contract, or agreement that transfers ownership, or intragovernmental lease as defined in the SFFAS 54: Leases. As risk assessments are performed, reporting organizations should identify the current lease risk statements in AMERICA that are no longer applicable to their organization. In addition, **as reporting organizations implement requirements for SFFAS 54, *Leases*, considerations should be given to potential new risks and documented as a local risk statement in the Department's A-123 Application, AMERICA**. As part of year-end reviews, OCFO will determine if newly identified local lease risk statements submitted by reporting organizations should be captured as a corporate risk in future years.

NEW
in FY 2024

d) **Complete Current Year Test Requirements:** Except for risks with a low exposure risk rating, reporting organizations using the Assessment Tab of the FMA Module in AMERICA, entities must test applicable controls identified as *Yes* or *Overdue* in the *In Scope at Rollover* column and *Yes* or *Overdue* in the *In Scope Now* column no later than June 30. Entities should remain cognizant that the *In Scope Now* is a dynamic column that will update when risk assessments, control tests, and ratings are updated. When the controls in the *In Scope Now* column change to yes due to an updated risk assessment, entities should factor the testing for those controls into the testing schedule.

Entities will focus their testing on controls that are mitigating risks with high and moderate combined risk ratings as well as controls that are mitigating fraud risks. As reporting organizations focus on testing controls mitigating high, moderate, and fraud risks, it is critical that reporting organizations are conducting **proper risks assessments** on an annual basis. As part of the risk assessment, reporting organizations must consider the following risk factors at a minimum:

NEW
in FY 2024

i. Significant Changes to Financial and /or Non-Financial Systems;
ii. Significant Changes to in Business Processes;
iii. Organizational Changes and/or Restructure;
iv. Signficant High Personnel Turnover;
v. Recent Audit Findings;
vi. Significant Budget Increase or Decrease;
vii. Policy and/or Legilsative Changes; and,
viii. Other Risk Factors.

Significant changes in risk factors will vary between reporting organizations; therefore, each organization must carefully evaluate each risk factor and determine what constitutes a significant change. **Reporting organizations that do not experience significant changes in the common risk factor for four years with low exposure risk ratings will test mitigating controls in the fifth year**. Reporting organizations should consider staggering the controls testing for risks with low exposure or low combined risk rating to prevent having an overwhelming number of controls due for testing the same time.

For the low-risk areas that may appear as *In Scope Now* or *Overdue* for testing in the current year, but falls under the reporting organizations' test plan in the next five years, those controls may be tested in the future. This must be properly supported by the reporting organizations' risk assessment and well-documented in AMERICA. At the Control window, the organization can utilize the ***Control User Field 1*** to provide an explanation as to why the control was not tested in the current year. Organizations will enter "*A proper risk assessment was conducted and currently has a test plan for low-risk areas that will provide staggered testing in the next five years.*" as applicable.

e) **Develop Corrective Action Plans as Applicable:** A Corrective Action Plan (CAP) is required for each risk with a risk occurrence rating of 3 or a control set execution rating of 3. Organizations also have the option of developing formal CAPs for control tests that pass with some failures. During these instances, the organization may opt to select a control set execution rating of 2 with CAP (rather than a 2 without CAP rating), which will automatically initiate the CAP process similar to a rating of 3 within the FMA Module. In AMERICA, risks with a risk occurrence rating of 3 or control sets identified as a 2 with CAP or 3 rating will automatically initiate a CAP. The CAP is a detailed, step-by-step plan with associated milestones and contains the signatures of the authorized individual approving the plan and the individual confirming completion of the plan. OMB Circular A-123 emphasizes the need to identify the root cause when developing a CAP, prompt resolution, and internal control testing to validate the correction of the control deficiency. Entities must report the root cause, along with other necessary CAP information, in the Internal Control CAPS Details section in the Assessment tab of the FMA Module.

At a minimum, a CAP will contain these key elements:

- Issue description;
- General Description;
- Source/ Type;
- CAP Title;
- Root Cause;
- Remediation Strategy/ Criteria for Closure (e.g., training, system, organization);
- Remediation Actions Taken;
- Current status and planned completion date or actual completion date; and
- Approving Official: The first line supervisor or higher may be considered the approving official.

Open CAPs carried over from previous years need to be reviewed and updated. If the action required has been completed and the issue mitigated (risks and controls tested as well), then the CAP status can be marked completed. The corresponding CSE can then be marked down to a 1 or 2 without CAP. Entities are responsible for maintaining the CAPs and are not required to provide CAP documentation unless requested by the OCFO.

NEW
in FY 2024

f) **Infrastructure Bill, IRA, and CHIPS and Science Act:** In FY 2024, reporting organizations and their downstream organizations that receive funding from the Infrastructure Bill, IRA, or the CHIPS and Science Act must continue to ensure business process documentation is current and properly working controls are in place for financial assistance awards that will ensure:

- DOE officials that are involved in the review of financial assistance applications do not have conflicts of interest;
- Financial assistance applications are reviewed, selected, and awarded according to the

planned schedule;

- Financial assistance awards are approved by contracting officers that are certified for financial assistance;
- Financial assistance awards are issued with sufficient funding;
- Advance notification is provided to the House and Senate appropriations committee for financial assistance awards that are in excess of $1 million;
- Non-competitive financial assistance awards have the appropriate level of authority and the approval is documented;
- Monitoring of the financial assistance award is consistent with the award terms and conditions;
- Recipients submit its single audit reporting package to the Federal Audit Clearinghouse in a timely manner;
- Recipients are aware of required reporting;
- Financial assistance awards are closed out properly and in a timely manner; and
- Performance metrics are established as part of the financial assistance or program plan, and the plans are approved prior to the transfer of funds;
- **DOE base funding is not comingled with IIJA and IRA funding on any financial assistance agreements, contracts, or subcontracts.**

g) **Organizational Business Processes:** In FY 2024, HQ entities that report to the Deputy Secretary must conduct a detailed review of their organizational business processes that have risks with a Department-wide impact. For those organizational business processes with risks that have a Department-wide impact, **HQ entities that report to the Deputy Secretary must begin documenting those risks and identifying controls in AMERICA.**

NEW in FY 2024

h) **Complete Focus Area Testing and Actions:** Organizations must complete testing and other required actions to address their FY 2024 selected focus area risks and document the actions taken in the **Assessment** tab of the FMA Module. **The environmental liabilities risks are focus area risks for EM reporting organizations and non-EM reporting organizations that have relevant environmental liabilities risks.**

NEW in FY 2024

i) As part of FY 2024 IT controls testing, **reporting organizations will be required to upload into AMERICA the controls test results and the associated Plan of Action and Milestones (POA&Ms)**. The uploaded IT network security control assessment documentation will be used to confirm each organization's mitigation efforts and ensure compliance regarding the testing of federal information systems.

NEW in FY 2024

5.8.3 Focus Area Guidance

Focus area risks represents areas of emphasis for the Department and are determined by senior management concerns, GAO and OIG repeat audit findings, or areas of high risks throughout the Department. Focus Area risks require additional assessment by reporting organizations regardless of the risk rating or test cycle. For FY 2024, the Department continues taking more of a collaborative approach to the Focus Area Risks by being less prescriptive and coordinating with Field Offices and their reporting organizations. By doing so will allow more efficient use of limited resources while mitigating potential fraud risk occurrences. Field Offices and M&O Contractors can focus on controls that are mitigating higher rated risks that are pertinent to their operations and shift resources to areas that may require immediate attention.

Field Offices considerations for focus area risks for their organizations and M&O Contractors should consider the following:

- Passing of IRA, IIJA, and CHIPS legislature in FY 2022;
- Recent audit findings;
- Business processes that have the highest percentage of controls failure within the past three years; and
- Areas with potential fraud, waste, or abuse.

NEW
in FY 2024

Reporting organizations that are using other selected risks, in addition to the environmental liabilities' risks, as their focus area risks will need to go to the *Other Factors to Consider* section for each risk and change *Local Request* to "yes", which will ensure all controls mitigating those risks are reported as In *Scope This Year in AMERICA* and should be tested in FY 2024.

Reporting organizations are exempt from testing controls that are mitigating focus area risks if the controls have been tested within the past 15-month period, which is July 1, 2022 – September 30, 2023. For risks that have a low or moderate combined risk rating, and the entity has tested the controls within the last 15-month period, then the focus area assessment may verify that:

1) The business process has not changed; and
2) There were no audit findings and there were no deficiencies found during the controls testing.

If these requirements are met, then the organization will check the focus area exemption box and enter this verbiage into the Action Taken dialogue box in the **Focus Area** tab: "***The controls have been tested within the past 15-month period, the business process has remained the same, and zero deficiencies were noted during testing. The organization performed this assessment on MM/DD/YYYY***." If the organization has not tested the controls within the last 15-month period, then the controls mitigating the focus areas risk will require testing **regardless of the risk rating or test cycle**.

Table 14: DOE FY 2024 Focus Area Risks

Environmental Liabilities	
CR6101	Liability Validation-Insufficient documentation
CR6102	Liability Validation-Subsequent events not considered
CR6103	EM Liability-IPABS out of date
CR6104	EM Liability-Unapproved baselines in IPABS
CR6105	Non-EM Liabilities-Improper accounting for contaminated media/oil & ground water remediation.
CR6106	Non-EM Liabilities-Untimely updates to Long-term stewardship
CR6107	Non-EM Liabilities-Improper accounting of surplus materials.
CR6108	Non-EM Liabilities-Improper accounting of non-EM Environmental Liabilities
CR6109	Policy Execution-Environmental policies and procedures not up to date
CR6110	Policy Execution-Environmental policies/procedures not communicated
CR6111	Policy Execution-Roles and responsibilities not known
CR6112	Policy Execution –Staff has inadequate skills/knowledge
CR6113	Active Facilities-Incorrect Active Facility Data Collection Systems (AFDCS) data
CR6114	Active Facilities-Best estimates for AFDCS not used
CR6115	Active Facilities-Omitted or duplicate facilities
CR6116	Active Facilities- Facility surveys/contamination swipes/etc. not considered
CR6117	Active Facilities-Leased facilities inappropriately considered

5.8.4 FMA IT Corporate Controls

NEW
in FY 2024

In accordance with OMB and the Federal Information Security Modernization Act (FISMA), Federal agencies are required to test the Department's information systems using the NIST 800-53, Rev 5 *Security and Privacy Controls for Information Systems*, and manage associated risks of the systems. The Office of the Chief Information Officer (CIO) and OCFO have partnered to streamline the evaluation process of the IT risks and controls that are associated with the NIST SP 800-53, Revision 5 cyber and privacy requirements. To best manage IT security risks and controls, all reporting organizations will be required to report the following results and documentation into AMERICA: **IT network security controls assessment test results, and the associated Plan of Action and Milestones (POA&Ms).** In Q2 FY 2024, a CIO IT Team will begin meeting with HQ and Field organizations IT POCs to better gain an understanding of how entities are evaluating the IT risks and controls in the FMA, including a review of reporting organizations' prior year(s) test results and POA&Ms and if needed, a copy of the System Security Plan (SSP) and/or documentation confirming mitigation of specific NIST standards. **To facilitate this effort, HQ and Field entities are requested to provide their organization's primary IT POC's name, e-mail address, and phone number to the ICFRMD's shared mailbox at CFO-ICFRMD@hq.doe.gov by January 18, 2024.**

For FY 2024, the IT controls will remain corporate controls within the FMA Module and IT network security assurance language will be incorporated into all organizational assurance memorandums to confirm DOE testing and compliance of Federal information systems as supported by provided AMERICA documentation. The IT corporate controls are security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. IT corporate controls are intended to keep DOE compliant with the NIST Special Publication (SP) 800-53, Revision 5 cyber and privacy requirements. As part of this effort, AMERICA user access reviews will occur during the second and fourth quarters of each FY.

Entities with IT systems will **select the IT sub-processes** applicable to the site, evaluate the appropriate risks, and test controls. Risks rated as **not relevant** must include an accompanying explanation. Controls mitigating the selected risks receive testing based on the risk rating coupled with the last control test date.

5.9 Entity Assessment Evaluation

5.9.1 Purpose

The purpose of the EA Evaluation is to conduct structured self-evaluations to provide reasonable assurance that internal control systems are designed and implemented as well as operating effectively. Self-structured evaluations are performed to verify that risks are mitigated and to validate that mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulations.

There are three major objectives of the EA Evaluation. The first is to assess the status of an entity's internal controls. The second is to evaluate each entity's objectives (e.g., functions, missions, activities) to determine if there are issues that require attention. The third is to evaluate the design and efficacy of system controls to determine what degree an organization's system meets the eight financial management goals.

5.9.2 Internal Controls Evaluation

Section II of FMFIA requires an assessment of non-financial controls to verify the effectiveness and efficiency and compliance with laws and regulations. The Green Book has five components, 17 principles and 48 attributes to guide the EA Evaluation. As with last year, each reporting organization, as shown in ***Table 15***, is required to perform an EA evaluation of the internal controls for entity functions (e.g., administrative, operational, and programmatic).

Organizations will report the results of the evaluations in the EA Module. The **Internal Control Evaluation** tab requires an evaluation of each entity's internal controls against the Green Book's five components and 17 principles.

For FY 2024, HQ Offices will ensure they are capturing the effectiveness, timeliness, and issues for internal and external reporting as part of their assessments of GAO's Green Book Principles 13 – 17, which are:

Table 15: GAO's Green Book Principles 13-17

Component	Principle
Information and Communication	Management should use quality information to achieve the entity's Objectives
Information and Communication	Management should internally communicate the necessary quality information to achieve the entity's objectives
Information and Communication	Management should externally communicate the necessary quality information to achieve the entity's objectives
Monitoring Activities	Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results
Monitoring Activities	Management should remediate identified internal control deficiencies on a timely basis

Some areas of consideration for assessing Principles 13 – 17 are the reporting of corrective action plans in the Department's Audit Reporting and Tracking System (DARTS) and the AMERICA.

Issues found in the evaluation of the 17 Principles must be identified and rated as to the seriousness on a scale of 1 (least serious) to 3 (most serious). Issues rated **2** or **3** require a CAP, and these issues automatically populate in the **Action Tracking** tab and require further information. There is also an **IC Summary Evaluation** tab, which summarizes the results of the evaluation reported in the **Internal Control Evaluation** tab. As a result, there are **only two lines on the IC Summary Evaluation tab that require user input:**

- Are all components operating together in an integrated manner?
- Is the overall system of internal control effective?

5.9.3 Entity Objectives Evaluation

The second aspect of the EA Evaluation is an evaluation of each entity objective (e.g., functions, missions) to determine if there are issues that need to be addressed to help meet the objective. There are nine entity objective categories identified in the EA Module that need evaluation by reporting organizations:

- Fraud Prevention;
- Establishment of Entity-Wide Objectives (Entity Missions);
- Infrastructure Status;
- Systems and IT Posture;
- Safety and Health (S&H) Posture;
- Security Posture;
- Continuity of Operations;
- Contractor/ Subcontractor Oversight; and
- Environmental.

Small HQ Offices in ***Table 10*** must complete five accompanying entity objectives:

- Funds Management;
- Acquisition Management;
- Payables Management;
- Travel Administration; and
- Payroll Administration.

The results of the evaluation for the nine (or 14 for the Departmental Elements indicated in ***Table 10***) entity objective categories are reported in the **Entity Objectives Evaluation** tab. As with the evaluation of internal controls, issues identified in the entity objectives evaluation will be reported and given a rating of 1 (least serious) to 3 (most serious) depending on the seriousness of the issue. Issues identified with a rating of **2** or **3** require a CAP.

5.9.4 Financial Management Systems Evaluation

The third aspect of the EA Evaluation is to evaluate the design and efficacy of system controls to determine what degree an organization's system meets the eight financial management goals. OMB Circular A-123, Appendix D, defines an FMS 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**. FMS include hardware, applications and system software, personnel, procedures, data, and reporting functions. The FMS may fully integrate with other management information systems (i.e., mixed systems) where transactions automatically flow into an accounting general ledger. The FMS could also include manual processes to post transactions from other management systems into the accounting general ledger. OMB Circular A-123, **Appendix D provides a risk-based evaluation model that leverages the results of existing audits, evaluations, and reviews which auditors, agency management, and others already perform.** This evaluation model also includes:

1) Financial management goals common to all Federal agencies;
2) Compliance indicators associated with each financial management goal; and
3) Recommended risk or performance level that entities should consider when assessing whether financial management goals have been met.

Organizations identified in ***Table 16*** as responsible for an FMS Evaluation must evaluate the design and efficacy of system controls to determine to what degree their system meets the eight financial management goals. As indicated in ***Table 10***, most entities are required to complete an FMS Evaluation. The FMS Evaluation is a risk assessment that should be conducted toward the end of the assessment year, and it relies on the results of internal control evaluations and other assessment activities already performed. Organizations may use A-123 Internal Review evaluations, management's knowledge of operations, FISMA review results, and external financial statement/Inspector General (IG)/ GAO audits, as applicable, to determine the entity's risk of non-compliance with the eight goals. No further evaluations or testing should be necessary to perform this FMS Evaluation. If the entity's internal control evaluations and other assessments do not provide an adequate basis for the FMS evaluation, then the entity should raise the risk levels of non-compliance with the eight goals.

The **FMS** tab within the EA Module provides a uniform Department-wide mechanism for documenting the FMS Evaluation. For each of the eight FMS Goals listed in the **FMS** tab, entities will record:

- Level of risk of being non-compliant with that goal;
- Sources used in determining that risk level; and
- An evaluation summary that briefly describes any relevant assessments, evaluations, and testing performed during the assessment year – both internal and external – and the outcomes.

Guidance to assist with this determination is co-located with each rating. For each goal, entities are required to document the risk level rating and the sources used along with a summary of the evaluation results for each financial management goal in the FMS Tab in the EA Module. After entities have determined the risk level rating for each goal, the sum of the risk level ratings will automatically calculate to determine the overall FMS risk of non-compliance with FFMIA, which should support the FMS assurance in the Assurance Memorandum. Similar to the evaluation of internal controls, entities should report identified deficiencies or issues found in the FMS Evaluation and provide a rating of 1-3 depending on the seriousness of the issue. A rating of 1 being the least serious and 3 being the most serious. Issues identified in the **FMS** tab will create a line in the **Action Tracking** tab. Then, the user will need to input information required for each issue. Issues identified with a rating of **2** or **3** will require a CAP. If there is an **existing CAP** for an FMS issue, then reporting organizations must indicate and identify the existing CAP name and number in the EA Module.

Managers must use professional judgment in assessment of the FMS Goals. For example, a rating of 3 on one goal does not necessarily indicate non-conformance for the entire FMS Evaluation.

Additionally, organizations identified as owners of an FMS included in ***Table 16***, must perform an FMS Evaluation to support core requirements of Section IV of FMFIA and FFMIA. If an entity's system (including Major/Integrated Contractor systems) feed into a DOE FMS, then those systems are subject to an FMS Evaluation.

Table 16: DOE Financial Management Systems

FMS and Mixed Systems	System Owner(s)
Power Marketing Administration Systems	BPA, WAPA, SWPA, & SEPA
Standard Accounting and Reporting System (STARS)	CFO
Federal Energy Regulatory Commission Systems	FERC
Budget Formulation and Distribution System (BFADS-formerly FDS 2.0)	CFO
Electronic Work for Others	ORNL

FMS and Mixed Systems	System Owner(s)
Active Facilities Database	CFO
ABC Financials	NNSA-NA-ESH
Integrated Planning, Accountability and Budgeting System (IPABS)	EM-62
Facilities Information Management System (FIMS)	MA-50
Strategic Integrated Procurement Enterprise System (STRIPES)	CFO
Vendor Inquiry Payment Electronic Reporting System (VIPERS)	CFO
Financial Accounting Support System (FAST)	CFO
iBenefits	CFO
Budget and Reporting Codes System (BARC)	CFO

In accordance with the FFMIA and OMB Circular A-123, Appendix D, system owners and users should determine whether the financial and mixed systems conform to Federal FMS requirements. As a result, entities are required to have FMS that substantially comply with the requirements of FFMIA Section 803(a), which includes Federal FMS Requirements, Federal accounting standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the requirements of the United States Standard General Ledger (USSGL) at the transaction-level.

5.9.5 Classifying Deficiencies

In accordance with OMB Circular A-123, DOE adopted a three-level rating system for reporting deficiencies to internal control principles and to issues identified in entity objective reviews. The severity of the deficiencies determines if the entity should report it in the organizational Assurance Memorandum. An entity control deficiency requires qualitative judgment that a significant deficiency exists that could adversely affect the organization's ability to meet internal control objectives, and an entity material weakness is a significant deficiency which the head of the organization determines is significant enough to report outside of the organization. The entity should document the information gathered and the decisions made related to the considerations.

Organizations must report control deficiencies that meet certain criteria in the Assurance Memorandum. ***Table 17*** provides a description of the issues that organization should report for each section of the Assurance Memorandum, a definition for each issue, and an indication of which issues requires a CAP in the Assurance Memorandum.

Note: Organizations must distinguish control deficiencies (including significant deficiencies and material weaknesses) from funding and resource issues. Funding levels are not control deficiencies and organizations should not report funding and budgetary limitations as a significant deficiency or material weakness in the Assurance Memorandum.

Table 17: Deficiency Classifications[15]

Deficiency Title	Definition	Applicable to	Reported in Assurance Memo
Control Deficiency (Non-Significant Issue)	A control deficiency exists when the design, implementation, or operation of a control does not provide management or personnel, in the normal course of performing the assigned functions, to achieve control objectives and address related risks. A deficiency in design exists when: 1) a control necessary to meet a control objective is missing or 2) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.	FMA, EA	No
Significant Deficiency	A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.	FMA, EA	Yes
Material Weakness	A significant deficiency that the Entity Head determines to be significant enough to report outside of the Entity as a material weakness. In the context of the Green Book, non-achievement of a relevant Principle and related Component results in a material weakness. A material weakness in internal control over operations might include, and is not limited to, conditions that: • Impacts the operating effectiveness of Entity- Level Controls; • Impairs fulfillment of essential operations or mission; • Deprives the public of needed services; or • Significantly weakens established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest. A material weakness in internal control over reporting is a significant deficiency, in which the Entity Head determines significant enough to impact internal or external decision-making and reports outside of the Entity as a material weakness. A material weakness in internal control over external financial reporting is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected,	FMA, EA	Yes

[15] Deficiency Classifications are derived from OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*

Deficiency Title	Definition	Applicable to	Reported in Assurance Memo
	on a timely basis. A material weakness in internal control over compliance is a condition where management lacks a process that reasonably assures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving Entity objectives. A **No** response on either Line 46 or 47 in the **EAT IC Summary Evaluation** tab requires a Material Weakness to be reported: • Are all components operating together in an integrated manner? or • Is the overall system of internal control effective?		
Non-Conformance	Exists when financial systems do not substantially comply with Federal FMS requirements OR where local control deficiencies impact financial systems ability to comply. The EA Module defines the criteria against which conformance is evaluated and captures identified non-conformances.	FMS (in the EA Module)	Yes
Scope Limitation	Exists when the Entity has identified potentially significant deficiencies in the scope of the internal control evaluations conducted, which would warrant disclosure to assure limitations are understood. Scope limitations may be determined by the entity or may be required by the CFO in certain circumstances.	FMA and EA	Yes

5.9.6 Annual Assurance Memorandum

Each entity is required to provide an annual Assurance Memorandum that documents the results of the annual FMA Evaluation if applicable, EA Evaluation, and FMS Evaluation, if applicable, along with other reviews conducted. The Assurance Memorandum provides a status of the overall adequacy, effectiveness, and efficiency of the organization's internal controls. The Assurance Memorandum must identify significant deficiencies or material weaknesses that might qualify that assurance, as defined in ***Table 17***, and a summary of the CAPs developed to address such issues will accompany the Assurance Memorandum. Organizations will also report instances of non-compliance with Federal FMS requirements or control deficiencies that affect an organization's ability to comply with the eight financial management goals.

HQ Offices with Field organizations must consider the results of the Field organization FMA and EA evaluations. Likewise, Field organizations with Major/ Integrated Contractors, must consider the results of the contractor FMA and EA evaluations. When considering the results of various cognizant organizations, the Departmental Element should consider multiple instances of similar control deficiencies and similar significant deficiencies across the entity to determine if a significant deficiency or material weakness exists at the Departmental Element's-level.

To align and comply with OMB Circular A-123, Appendix B, *A Risk Management Framework for Government Charge Card Programs*, assurances are in the Assurance Memorandum in reference to the implementation of safeguards and internal controls for inappropriate charge card practices, as well as assurances that organizations have processes in place to identify risks and controls, and that the controls are operating effectively.

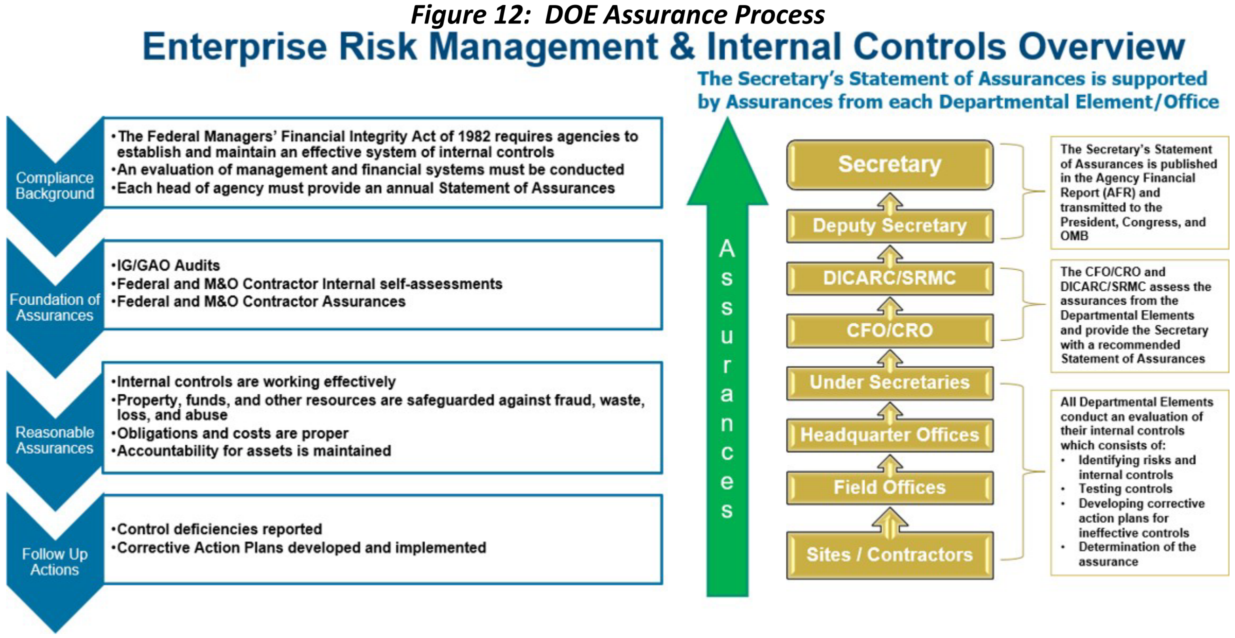
Organizational assurance statements include an evaluation of the effectiveness of internal control over operations, reporting, and compliance, as of June 30. Organizations remain responsible to provide an update to the assurance statements when a significant deficiency or material weakness is resolved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

- If an organization discovers a significant deficiency or material weakness by June 30, and implements corrective actions by September 30, then the organization will update the statement identifying the significant deficiency or material weakness, the corrective action taken, and the resolution occurred by September 30; and
- If an organization discovers a significant deficiency or material weakness after June 30, and before September 30, then the organization will update the statement identifying the significant deficiency or material weaknesses to include the subsequently identified significant deficiency or material weakness.

Organizations will notify the OCFO immediately of any resolved or new significant deficiencies or material weaknesses no later than October 1, 2024, per ***Table 11***.

Figure 12 presents the DOE annual assurance process. Assurance flows from each major/integrated contractors to the respective Departmental element, and from the Departmental element (Field and HQ Offices) to the Under Secretaries. The CFO and DICARC assess the assurances from the Under Secretaries and provide the Secretary with the recommendation to sign the DOE Management Assurances.

Figure 12: DOE Assurance Process



Enterprise Risk Management & Internal Controls Overview

The Secretary's Statement of Assurances is supported by Assurances from each Departmental Element/Office

Compliance Background
- The Federal Managers' Financial Integrity Act of 1982 requires agencies to establish and maintain an effective system of internal controls
- An evaluation of management and financial systems must be conducted
- Each head of agency must provide an annual Statement of Assurances

Foundation of Assurances
- IG/GAO Audits
- Federal and M&O Contractor Internal self-assessments
- Federal and M&O Contractor Assurances

Reasonable Assurances
- Internal controls are working effectively
- Property, funds, and other resources are safeguarded against fraud, waste, loss, and abuse
- Obligations and costs are proper
- Accountability for assets is maintained

Follow Up Actions
- Control deficiencies reported
- Corrective Action Plans developed and implemented

The Secretary's Statement of Assurances is published in the Agency Financial Report (AFR) and transmitted to the President, Congress, and OMB

The CFO/CRO and DICARC/SRMC assess the assurances from the Departmental Elements and provide the Secretary with a recommended Statement of Assurances

All Departmental Elements conduct an evaluation of their internal controls which consists of:
- Identifying risks and internal controls
- Testing controls
- Developing corrective action plans for ineffective controls
- Determination of the assurance

Templates for Field Offices, PMAs, large HQ Offices, smaller HQ Offices, and Under Secretaries to use in preparation of the Assurance Memorandum will be provided in accordance with ***Table 10***. A separate template will be provided for PMAs in FY 2024.

NEW
in FY 2024

The Assurance Memorandum consists of two portions:

1) Main Body – Contains the actual assurance statements and executive summaries of identified significant deficiencies or material weakness; and
2) Corrective Action Plan Summary – Lists CAPs for each significant deficiency, material weakness, or non-conformance reported in the Assurance Memorandum. The CAP Summary briefly describes the remediation activities that have occurred or the remediation activities the organization will implement in the next FY.

   CAP Summary includes:
   a) New Issues and CAPs; and
   b) Action Plans from prior-year reporting (may be open or closed). For CAPS that remediate deficiencies reported in previous years and now closed in FY 2024, the CAP Summary must include a statement noting the closure of the CAP.

Final responsibility for making assurances that financial, entity, and FMS internal controls are effective and efficient, produce reliable reports, and are compliant with all applicable laws and regulations lies with the head of each entity. The **head of the Departmental Element must sign the Assurance Memorandum**. During instances when the head of the Departmental Element is not available, the organization's Assurance Memorandum may be signed by the designated representative that has a Delegation of Authority Memorandum signed by the head of the Departmental Element. HQ-level entities that report to an Under Secretary will provide the Assurance Memorandum to the respective Under Secretary for signature.

DOE Order 520.1B was approved January 2021 directing the head of each Departmental Element to designate an Internal Control Action Officer that will coordinate the organization's Internal Control Program that is consistent with the DOE Internal Control Evaluations Guidance. **When an organization changes the designated Internal Control Action Officer, the updated name and contact information should be provided to the ICFRMD shared mailbox** at CFO-ICFRMD@hq.doe.gov.

6 Data Analytics

The Data Analytics section of the guidance is new for FY 2024. As the Department's Data Analytics Program matures, this guidance will be key to the Department's approach to embracing data analytics into its financial operations.

NEW
in FY 2024

In FY 2022, the OCFO formed a DAWG to leverage, integrate, and synchronize the various data analytic efforts that are being performed across the Department. The DAWG, represented by HQ and Field Office personnel across DOE, initiated an OCFO led Data Analytics Data Call Survey in Q1, FY 2023 with an initial focus on six areas that were rebates, grants/cooperative agreements, loans, cybersecurity, labor charging, and materials and services. Initial efforts in FY 2023 were grouping DOE's various data analytic activities that are conducted across the Department into a synchronized and integrated effort that will enhance the Department and its organization's ERM and Internal Control Programs. In FY 2024, a follow-up Data Analytics Survey will be conducted to refine the results of the initial Data Analytics Data Call.

6.1 Purpose

The potential use of data analytics could save the taxpayers substantial funds and improve efficiency and oversight. In March 2020, the PIIA was enacted and incorporated select provisions from the Fraud Reduction and Data Analytics Act of 2015, the Improper Payments Information Act of 2002, the Improper Payments Elimination and Recovery Act of 2010, and the Improper Payments Elimination and Recovery Improvement Act of 2012 into a single subchapter in the U.S. Code. To comply with the Payment Integrity Information Act of 2019, the Department has undertaken the development and implementation of a Fraud Risk and Data Analytics Framework (Framework). The significance of the potential use of data analytics within the Department cannot be overstated. For example, the use of data analytics would improve effective and efficient management and oversight of the significant influx of funds associated with IIJA, the CHIPS Act, and IRA.

As a response, DOE must be institutionally agile to keep pace with such developments and embrace the evolving opportunities in data analytics. The Digital Accountability and Transparency Act of 2014 (DATA Act) requires Federal agencies to report financial, procurement, and financial assistance data using Government-wide financial data standards. In May 2015, the Office of Management and Budget (OMB) and the U.S. Department of Treasury (U.S. Treasury) published 57 data definition standards, most coming from existing data standards, and required Federal agencies to report quarterly agency data in accordance with these standards, beginning in the second quarter of FY 2017, for publication on USAspending.gov. Creation of the Data Analytics Working Group for Data Management and Analytics was the first step in establishing this framework.

The Guidelines for Data Analytics is a major initiative in institutionalizing the practice and use of data analytics within DOE. These guidelines explain the concept of data analytics, outline the data analytic process, and envision development of data analytic models. Data analytics is an evolving discipline and therefore these guidelines would have to be periodically reviewed and updated.

6.2 What is Data Analytics?

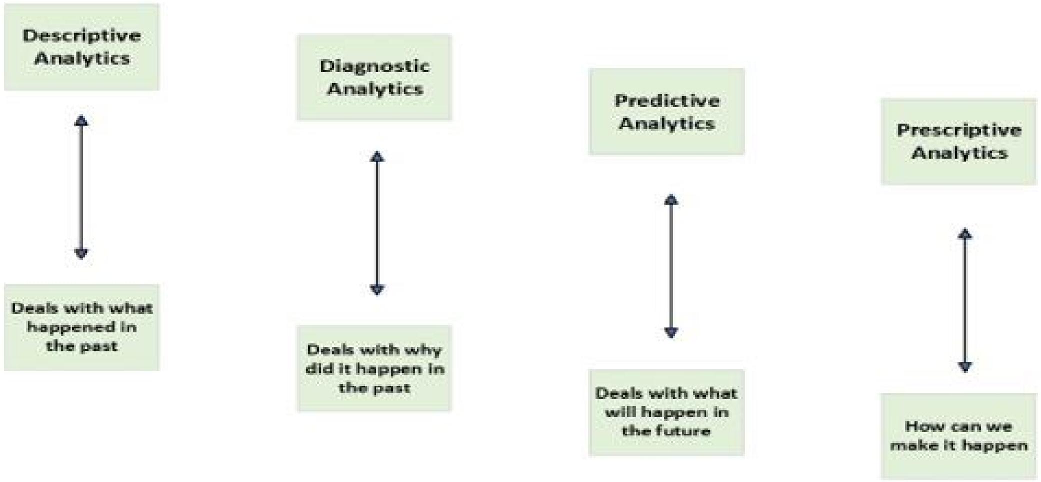
- Data analytics is the science of analyzing raw data to make conclusions about that information;
- Data analytics help a business optimize its performance, perform more efficiently, maximize

profit, or make more strategically guided decisions;

- The techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data for human consumption;
- Various approaches to data analytics include looking at what happened (i.e., descriptive analytics), why something happened (i.e., diagnostic analytics), what is going to happen (i.e., predictive analytics), or what should be done next (i.e., prescriptive analytics); and
- Data analytics relies on a variety of software tools, including spreadsheets, data visualization, reporting tools, data mining programs, and open-source languages for the greatest data manipulation.

6.3 Types of Data Analytics

Figure 13: Types of Data Analytics


Descriptive Analytics
Deals with what happened in the past
Diagnostic Analytics
Deals with why did it happen in the past
Predictive Analytics
Deals with what will happen in the future
Prescriptive Analytics
How can we make it happen

Descriptive (Business Intelligence and Data Mining): Descriptive Analytics looks at data and analyze past events for insight as to how to approach future events. It looks at past performance and understands the performance by mining historical data to understand the cause of success or failure in the past. Almost all management reporting such as sales, marketing, operations, and finance uses this type of analysis. The descriptive model quantifies relationships in data in a way that is often used to classify customers or prospects into groups. Unlike a predictive model that focuses on predicting the behavior of a single customer, Descriptive analytics identifies many different relationships between customer and product.

Common examples of Descriptive Analytics are company reports that provide historic reviews like:

- Data Queries;
- Reports;
- Descriptive Statistics; and
- Data dashboard.

Diagnostics: In this analysis, we generally use historical data over other data to answer any question or for the solution of any problem. We try to find any dependency and pattern in the historical data of the particular problem. For example, companies go for this analysis because it gives a great insight into a problem, and they also keep detailed information about their disposal otherwise data collection may turn out individual for every problem and it will be very time-consuming. Common techniques used for

Diagnostic Analytics are:

- Data discovery;
- Data mining; and
- Correlations.

Predictive (Forecasting): Predictive Analytics turn the data into valuable, actionable information. Predictive Analytics uses data to determine the probable outcome of an event or a likelihood of a situation occurring. Predictive analytics holds a variety of statistical techniques from modeling, machine learning, data mining, and game theory that analyze current and historical facts to make predictions about a future event. Techniques that are used for predictive analytics are:

- Linear Regression;
- Time Series Analysis and Forecasting;
- Data Mining;
- Predictive modeling;
- Decision Analysis and optimization; and
- Transaction profiling.

Example of Predictive Analytics: This moves to what is likely going to happen in the near term. What happened to sales the last time we had a hot summer? How many weather models predict a hot summer this year? In what year will we meet the Payment Integrity outlay threshold?

Prescriptive (Optimization and Simulation): Prescriptive Analytics automatically synthesize big data, mathematical science, business rule, and machine learning to make a prediction and then suggests a decision option to take advantage of the prediction. Prescriptive Analytics goes beyond predicting future outcomes by also suggesting action benefits from the predictions and showing the decision maker the implication of each decision option. Prescriptive Analytics not only anticipates what will happen and when to happen, but also why it will happen. Further, Prescriptive Analytics can suggest decision options on how to take advantage of a future opportunity or mitigate a future risk and illustrate the implication of each decision option. For example, Prescriptive Analytics can benefit healthcare strategic planning by using analytics to leverage operational and usage data combined with data of external factors, such as economic data, population demography, etc.

6.4 Instructions for DAWG Survey Template

The DAWG Survey Template in spreadsheet form is presented as an attachment in ***Appendix C***. The instructions explaining how to complete each column are included as a tab in the template and are also listed below. Guidance as follows for FY 2023 data:

- If results are considered analytics (refer to column R), then please copy the same results from last year's survey which has been attached. Columns have been changed so please copy to the correct cell;
- If section is NOT considered analytics, then please revise and/or update based on the new guidance below;
- If results are UNKNOWN, or new analytics are identified, then please e-mail the ICFRMD shared mailbox at CFO-ICFRMD@hq.doe.gov or attend Data Analytic Survey Office Hours to assistance in next steps; and
- If a new organization to the survey in FY 2024, then please disregard and follow instructions below.

Guidance as follows for FY 2024 data:

Note: Verify that the file is “Enabled” by clicking on “File,” “Enable Content,” “Enable All Content” before entering data into the template. Please refer to tab Template Instructions Tab within the worksheet to answer each column. Yellow columns indicate new information for FY 2024.

HQ Office (Column A): This is an open text, data entry column.
Use this column to identify your HQ Office. The drop-down menu lists all of DOE’s HQ Offices.

*This column is hidden and will be populated by the DAWG.

Field Office (Column B): This is an open text, data entry column.
Use this column to identify your Field Office. If you are not at a Field Office, then “N/A” should be selected from the drop-down menu.

*This column is hidden and will be populated by the DAWG.

Lab/Facility (Column C): This is an open text, data entry column.
Use this column to identify your Lab or Facility. If you are not at a Lab or Facility listed, then “N/A” should be selected from the drop-down menu.

*This column is hidden and will be populated by the DAWG.

Site Code (Column D): This column has a drop-down menu allowing multiple selections to be made.
Use this column to select the site code for your Reporting Organization. The drop-down menu has been populated with all DOE site codes.

Dropdown Options: Please refer to the Drop Down List Tab in the worksheet.

Analytics Performed By (Column E): This column has a drop-down menu that will allow multiple selections to be made.
Use this column to identify who is performing the analytics. Drop-down options consist of Federal Staff, M&O Contractor Staff, and Other. If “Other” is selected, then please provide details of who is performing the analytics in Column G - Data Set.

*Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process.

Automated Or Manual (Column F): This column has a drop-down menu that will allow multiple selections.
Use this column to identify if the data set is gathered manually or automated.

Data Set Description (Column G): This is an open text, data entry column.
Use this column to identify the data set used to perform the analytics. Also, if “Other” is selected in Column E provide details in this column of who is performing the analytics.

Data System Provider (Column H): This column has a drop-down menu that will allow multiple selections.
Use this column to list any systems used to assist with performing analytics. Some examples include STARS, STRIPES, SAM, or any Site-Specific System.

Dropdown Options:

- STARS;
- Site Specific Accounting System;
- STRIPES;
- Site Specific Acquisition System;
- SAM;
- USAspending;
- Concur – DOE;
- Concur - Site Specific;
- AMERICA;
- Automated Time Attendance and Production System (ATAAPS);
- DOEInfo;
- FAST;
- Infor Risk Compliance (IRC);
- Integrated Data Warehouse (IDW);
- iPortal;
- CHRIS;
- Site Specific Payroll/Time Keeping System;
- ASAP;
- Cit-Bank Card System; and
- Other.

Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process.

Tools Used (Column I): This is an open-text data entry column.
Use this column to list any tools or software used to assist with performing analytics. Some examples include Microsoft (MS) Excel and Access, Tableau, Power BI, DOE systems, or any specialty software.

Dropdown Options:

- Access;
- Excel;
- Power BI;
- Tableau;
- Microstrategy;
- Splunk;
- Encase;
- EBS;
- BurpSuite Pro;

- Axiom;
- Kronos; and
- Other.

Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process.

Org Performing Analytics (Column J): This is an open-text data entry column.
Use this column to identify the organization performing the analytics. This allows for identification of the specific office or division, within the organization, performing the analytics.

Entity Analyzed (Column K): This column has a drop-down menu that will allow multiple selections to be made.
Use this column to identify the entity or entities analyzed by the data analytics performed.

Drop-Down Options:

- Labs;
- Site Offices;
- M&O Contractors; and
- DOE.

If the Entity analyzed is a DOE Office not listed, then please select "DOE" from the drop-down list.

Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process.

Fraud Risk Category (Column L): This column has a drop-down menu that will allow multiple selections to be made.
Use this column to select the fraud risk category that best describes the analytics performed.

Dropdown Options:

- The drop-down includes the following Fraud Risk Categories;
- Rebates;
- Grants/Cooperative Agreements;
- Loans;
- Cybersecurity (includes labs and contractors);
- Labor Charging - Federal and Contractor (includes labs and contractors), and Materials and Services - Contract and Project Management (includes labs and contractors); and
- Property.

Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process. If multiple selections are made, then please add a new Row in Excel. This will allow column L and M to interact with each other.

Sub-function (Column M): This column has a drop-down menu that will allow multiple selections to be made.
Use this column to select the sub-function that applies to the Fraud Risk Category that best describes the analytics performed. This selection is based on the selection on column L.

Dropdown Options: Please refer to the Fraud Risk Table in the worksheet.

Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process.

*If multiple selections are made please add a new Row in Excel. This will allow column L and M to interact with each other.

Purpose of Analytics (Column N): This is an open text, data entry column.
Use this column to describe the purpose for why analytics are performed.

Type of Analytics (Column O): This column has a drop-down menu that will allow multiple selections to be made.
Dropdown Options:

- Predictive (Forecasting);
- Descriptive (AI/BI);
- Prescriptive; and
- Diagnostic.

i. Example of predictive analytics: This moves to what is likely going to happen in the near term. What happened to sales the last time we had a hot summer? How many weather models predict a hot summer this year? In what year will we meet the Payment Integrity outlay threshold?

ii. Examples of descriptive analytics are company reports that provide historic reviews like:
   a) Data Queries
   b) Reports
   c) Descriptive Statistics
   d) Data dashboard

iii. Examples of prescriptive analytics can benefit healthcare strategic planning by using analytics to leverage operational and usage data combined with data of external factors such as economic data, population demography, etc.

iv. Examples of diagnostic analytics: Companies go for this analysis because it gives a great insight into a problem, and they also keep detailed information about their disposal otherwise data collection may turn out individual for every problem and it will be very time-consuming. Common techniques used for Diagnostic Analytics are:
   a) Data discovery
   b) Data mining
   c) Correlations.

Description of Analytics Performed (Column P): This is an open text, data entry column.
Use this column to provide a description of the analytics performed. Please provide enough detail so an individual outside of your reporting organization can understand the analytics conducted. Also, if "Other" is stated in Column N provide details in this column on the purpose of the analytics.

Examples of Descriptions:

- **Cyber Security:** *Utilizing SPLUNK, capture vulnerability scanning data to identify remediation needs. Summarization and analysis of threat and related information if identified will be sent to HR for further investigation;*
- **Labor Charging:** *Perform labor charging analytics to detect non-compliance, trends, anomaly detection, and other prescriptive analytics to detect, deter, and mitigate fraud risk pertaining to labor charging;*
- **Grants:** *Analyses of the language and supporting documentation to ensure that there is no misuse, waste, or abuse utilizing text-based analysis in R;*
- **Loans:** *Confirm the accuracy of the requested claim against the interest and/or principal default payment amounts calculated/maintained by Loan Accounting as established in the loan documents utilizing isolation forest analytics;*
- **Materials and Services:** *Vendor/Employee Analytics using Python. Comparison trends analysis of selected vendor and employee data for improper relationships;*
- **Rebates:** *Trend analysis (e.g., root causes, improper payment rates/amounts, and payment categories) and forecasting rates and amounts. Deep dives to identify internal control weaknesses and best practices for process improvement initiatives; and*
- **Property:** *Anomaly detection utilizing Python, R, and other analytic techniques to develop an anomaly detection dashboard for unrecognized property invoices.*

Frequency (Column Q): This is an open-text data entry column.
Use this column to select the frequency of how often the analytics are performed.

Output (Column R): This is an open-text data entry column.
Use this column to describe how the results of the analytics are documented.

Summary of Results (Column S): This is an open-text data entry column.
Use this column to provide details of the results obtained from the analytics performed.

Examples:

- **Cyber Security:** *Summarization and analysis of threat and related information, if identified, will be sent to Human Resources (HR) for further investigation.*
- **Labor Charging:**
  Ex. 1. Anomalies in results are validated, positive results are initiated for fraud investigation, action is taken, as appropriate
  Ex. 2. Prescriptive analytics determined improvement of controls, results are briefed to proper leadership, improvement of controls/business process is taken. Re-run of analytics take place to determine effectiveness of controls
- **Grants:**
  Reports and spreadsheets showing that the agreements have been reviewed and all expected charges are within the agreed terms
- **Loans:**
  Validate the Lender's default claim payment request, LPO's claim amount confirmation, and supporting documentation
- **Materials and Services:**
  Results will provide potential conflicts of interest, thus prompting further investigation with major stakeholders
- **Rebates:**
  Identifying areas of improvement by site/program office focusing on root causes. Forecast future results to access our susceptibility to OMB thresholds/significant improper payments
- **Property:**
  Results of dashboard will flag any unrecognized property invoicing or checking out of inventory for further investigation.

Results Shared with (Column T): This column has a drop-down menu that will allow multiple selections to be made.
Use this column to list who the results are shared with.

Dropdown Options:

- External;
- Internal and External;
- HQ;
- Internal/M&O Contractors; and
- Internal/Recipients.

Multiple selections can be made from the drop-down menu by selecting your first item and then proceeding to reopen the drop-down menu and making the next selection until all necessary selections are made. Duplicative selections cannot occur. If a selection is made by mistake and needs removed, then either open the drop-down menu and reselect the item that you wish to remove or delete the information in the cell and restart the selection process.

7 Management Priorities[16]

7.1 Background

Management Priorities represent the most important strategic management issues facing the Department and are reviewed and identified by DOE's SRMC, DICARC. The DICARC/SRMC considers the results and any significant deficiencies and/or material weaknesses reported in the Departmental Elements' Assurance Memoranda. The DICARC/SRMC also consults and considers the DOE IG's Management Challenges and the GAO biennial High Risk Series update when assembling DOE's Management Priorities.

The Department's Management Priorities are identified in ***Table 18***. Each DOE Management Priority is assigned a Senior Executive and lead coordinating office to track progress and provide enterprise level updates for inclusion in the FY 2024 AFR. The owner or lead coordinating office for each Management Priority will provide updates to the OCFO during the Q3 and Q4 of the FY. The lead coordinating office of the Management Priority will update the narrative with an enterprise perspective and approve each priority update prior to delivering to the OCFO.

Table 18: DOE's Management Priorities and Lead Coordinating Offices[17]

Management Priorities in FY 2024	Lead Coordinating Offices
Cybersecurity	CIO
Human Capital Management and Diversity, Equity, Inclusion, and Accessibility	HC and EJE
Contractor and Major Project Management	MA
Infrastructure	MA
Nuclear Waste Disposal	NE
Safety and Security	EHSS
Nuclear Stockpile Stewardship	NNSA
Environmental Cleanup	EM
Climate Change	MA
Energy Justice	EJE

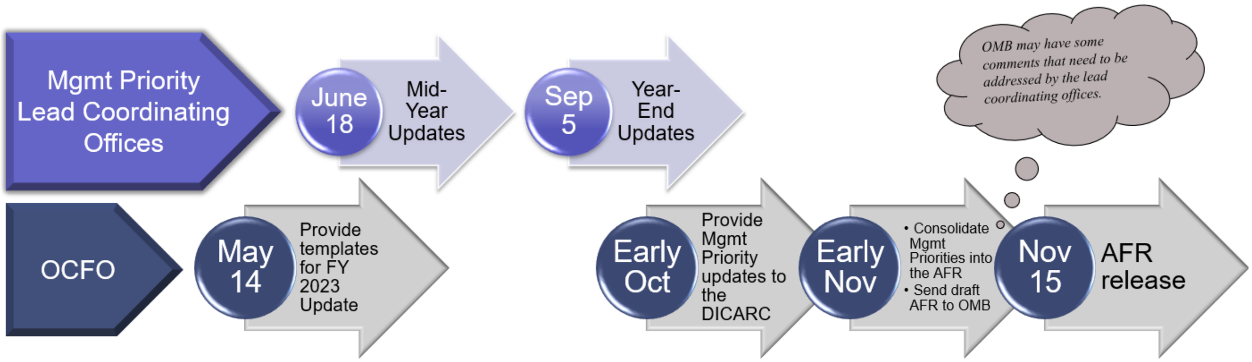
7.2 Management Priorities Update Process

In the third quarter of FY 2024, the OCFO will provide the lead coordinating offices with Management Priorities published in the previous FY AFR. The owners and lead coordinating offices will update the narrative (using tracked changes) based on significant activities and results performed in FY 2024. In Q4, OCFO will provide each lead coordinating office with relevant significant deficiencies and/or material weaknesses reported by Departmental Elements along with the top risks throughout DOE for potential consideration and incorporation into Management Priorities updates. Lead coordinating offices will consider the enterprise reported results and provide a Q4 Management Priorities update (using tracked changes) to the OCFO. ***Figure 14*** shows an illustration of the process with timelines for both the OCFO and the Management Priority lead coordinating offices.

[16] This section is applicable to Management Priority Owners and Lead Coordinating Offices only.

[17] Includ Program Office input

Figure 14: Management Priority Process with Timeline


Mgmt Priority Lead Coordinating Offices
June 18
Mid-Year Updates
Sep 5
Year-End Updates
OMB may have some comments that need to be addressed by the lead coordinating offices.
OCFO
May 14
Provide templates for FY 2023 Update
Early Oct
Provide Mgmt Priority updates to the DICARC
Early Nov
• Consolidate Mgmt Priorities into the AFR
• Send draft AFR to OMB
Nov 15
AFR release

The OCFO will provide the Management Priorities updates to the DICARC for consideration along with the OIG Management Challenges and the GAO High-Risk List. The DICARC will meet in May 2024 and determine whether to revise, edit, or maintain DOE's Management Priorities. The Management Priorities updates determined by the DICARC will be reported in the FY 2024 DOE AFR and will serve as the starting point for the next FY update process.

7.3 Guideline on Writing the Management Priority Narrative

The Management Priority narrative is composed of the *Title Header*, *Key Challenges*, and *Departmental Initiatives*. Refer to ***Table 19*** for the description of each section.

Table 19: Management Priorities Narrative Structure

Structure	Instructions
Management Priority Title Header	Management Priority Title Headers are consistent with the Management Priorities approved by the DICARC. Any newly identified management priorities need to be coordinated with the corresponding DICARC representatives.
Key Challenges	**Introduction:** Provide a narrative description of the management priority in terms of the key challenges DOE faces (e.g., what risks or vulnerabilities do the challenges present to DOE?). Summarize the specific elements and contributors of the challenges associated with the management priority. **Body:** Use bullets and sub-bullets to provide additional detail for each area under the key challenges.
Departmental Initiatives	**Introduction:** Provide a summarized description of the Department's efforts taken and on-going initiatives to improve and/or address the key challenges identified with the management priority. **Body:** Use bullets and sub-bullets to provide additional detail on specific elements or factors associated with challenges or initiatives that were completed in the current FY. Avoid any reference of ambiguous or future planned initiatives.

The next succeeding tables provide consideration for word usage and formatting.

Table 20: Management Priority Narrative Word Usage

Item #	Topic	Word Usage Considerations
1	Active Voice	Use ***ACTIVE*** voice. **Correct:** "DOE implemented controls to restrict access to the accounting system by unauthorized personnel." **Incorrect:** "DOE has implemented controls that will restrict access to the accounting system by unauthorized personnel."
2	Bulleted Lists	Do not begin a bullet with "the". Begin with an action verb when possible. (Particularly for describing the initiatives taken). Strive for a consistent tone in the opening sentence of each bullet under a particular key challenge/initiative: • "Improved X by…" • "Completed X to…" • "Developed X to…" ***OR*** • "Improving X by…" • "Completing X to…" • "Developing X to…"
3	Buzz Words	***Avoid*** buzz words, such as: • Allow • Cultivate • Driver • Engage • Ensure • Stakeholders • Utilize
4	Other Words	Other words to ***avoid*** include: • Additional, additionally, in addition • Amplify • Any • As follows, following (when referencing a location within document) • Customer • Enable • Etc. • Everything • Few • Furthermore • Great • However • Invaluable • Many • Rigorous • Required (Use "needed," where applicable) • Robust • Should (when unnecessary, delete) • Show, showed • Some • Soon • That (when unnecessary, delete) • Therefore • Their • Whether
5	Acronyms	• Consider using if term is referenced multiple times throughout section (two or more times) • Consider writing out if only used once.
6	Pronouns	***Avoid*** using pronouns, such as: I, you, she/he, it, and this.
7	Titles	Use titles instead of actual names.

Table 21: Management Priorities Formatting Considerations

Item #	Topic	Formatting Considerations
1	Spacing	Double space after periods and colons.
2	Bullets	Do not begin a bullet with “the”.
3	Bullets	Spacing for bulleted lists: • First level indent is 0.00” (depicted by a black dot) ○ Second level indent is 0.25” (depicted by a hollow dot)
4	Bullets	No comma after “and”. Example: • Completed removal of the Livermore Pool Reactor from within Building 280 and awarded an inter-agency agreement to demolish Building 280; • Completed demolition of Building 175; **and** • Commenced demolition of Building 251.
5	List	Where there is a list, use number list with open and close parenthesis. Example: Currently, DOE is tracking towards completing three high-priority initiatives: **1)** example; **2)** example; and **3)** example.
6	Publications	Italicize publications.
7	Quotations	Only use quotation marks around direct quotes.
8	Numbering	Spell out numbers less than 10 (one, two, three, …nine, 10, 11, 12…)
9	Fiscal Year Reference	Formatting should be FY XXXX (Example: FY 2024).
10	Commonly Used Acronyms	DoD (lower caps “o” – Department of Defense EO (without periods) – Executive Order U.S. (with periods) – United States
11	Non-Breaking Space	Use non-breaking space for any form of measurement, date references, and fiscal year reference. (Example: $65 million, 90 tons, FY 2024, December 2024).
12	Font	Font Style: Cambria Font Size: 10
13	Percent	**Percent** should be spelled out.
14	Hyperlink	Confirm hyperlinks are working before inserting into the document. Ensure that the links contain accurate information.
15	Sentence Tense	The AFR is released every year on the 15th of November. Earmark certain passages or paragraphs where the tense needs to be corrected at year-end.

7.4 Management Priorities Due Dates

Table 22 provides a summary of the Management Priorities key dates and deliverables for FY 2024. Management Priority owners and lead coordinating offices should contact the Internal Controls Fraud Risk and Management Division (e-mail: CFO-ICFRMD@hq.doe.gov) if there are any issues in meeting the below deadlines.

Table 22: Management Priorities Key Dates

FY 2024 Key Dates	Deliverables
May 14	OCFO provides the lead coordinating offices with Management Priorities in the required templates for FY 2024 update. **Note:** *Applicable to Management Priority Lead Coordinating Offices Only.*
June 18	Lead coordinating offices provide OCFO with mid-year updates on Management Priorities using provided templates based on FY 2024 planned and performed enterprise activities. **Note:** *Applicable to Management Priority Lead Coordinating Offices Only.*
September 5	Lead coordinating offices provide OCFO with Management Priorities year-end updates. **Note:** *Applicable to Management Priority Lead Coordinating Offices Only.*
October – TBD	OCFO will provide Management Priorities updates to the DICARC in early October for review. Be prepared to provide responses for potential OMB comments. **Note:** *Applicable to Management Priorities Lead Coordinating Offices Only. Per DICARC recommendation, the final Management priorities are incorporated into the AFR and process through Exec Sec Concurrence Process.*

Appendix A: Glossary of Terms

AMERICA An application that automates and streamlines the Department's management, reporting, and analysis of risks and controls in compliance with OMB Circular A-123.

Assurance Memorandum Annual statement of assurance provided by reporting organizations that expresses the overall adequacy and effectiveness of the system of internal controls. For the required Assurance Memorandum content, see Appendix D, *Assurance Memorandum Templates*.

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

The Basis of Evaluation should be a documented activity. Examples include reports, bi-annual workforce planning survey results, other reports, memos, reviews, assessments, evaluations, plans, emails, meeting minutes, certificates, and documented signatures.

Bid-rigging Agency officials or contractors bidding on a contract conspire to influence the purchase of goods or services to avoid competitive bidding controls. Bid-rigging typically involves contractors agreeing to artificially increase the prices of goods or services offered in bids to the government or bidding in such a way to guarantee a specific contractor wins the contract.

Billing Schemes Contractors obtaining payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

Budget to Close (B2C) The cycle comprises financial and/or accounting processes used to manage financial data and resources such as: General Ledger Management; Funds Management; Fund Balance with Treasury; Cost Management; Grants Administration; and Loan Administration. Specific areas involved in the cycle are budgeting, journal entries, costing reconciliations, financial reporting and closing activities at month, quarter, and year-end.

Combined Risk Assessment The residual risk considering the control environment and a measure of the end risk to DOE. In the FMA Module, the combined risk is a calculated field based on exposure risk and control risk. If an organization has not performed control testing, the combined risk rating defaults to the exposure risk rating. Once control testing is conducted and recorded, the combined risk will automatically calculate.

H – High risk, ineffective risk mitigation;
M – Moderate risk; and
L – Low risk, effective risk mitigation.

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

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

Conflicts of Interest

Agency officials or government contractors inappropriately awarding business to vendors in which they have an unreported direct or indirect interest, potentially resulting in higher contract costs or purchases of goods or services not needed. Conflicts of interest can arise at the individual or organizational level. Organizational conflict of interest can occur when a contractor has a preexisting relationship with a potential subcontractor or vendor that results in in appropriate award of subcontracts at higher cost to the government.

Contract Progress Schemes

Contractors inappropriately obtaining payments by purposefully misrepresenting the extent of project completion.

Control Deficiency

A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing the assigned functions, to achieve control objectives and address related risks. There are three types of control deficiencies:

Design Deficiency – A deficiency in design exists when (1) a control necessary to meet a control objective is missing or (2) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met.

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

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

Control Execution

A **rating** resulting from individual control testing. Control Execution ratings are defined in the FMA Module as:

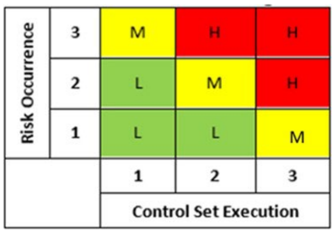
1 – Passed with no failures.
2 – Passed with failures within acceptable threshold.
3 – Failed.

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 and the goal to be achieved to minimize, manage, or mitigate risks. Each objective considers the nature of the activity, the organization's mission, and the cost and benefits of each control in determining desired control objectives.

Control Risk Assessment

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



Risk Occurrence				
	3	M	H	H
	2	L	M	H
	1	L	L	M
		1	2	3
		Control Set Execution		

Control Set Execution: Rating based on an assessment of the 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 through observation during normal business operations. Ask, did the risk occur during normal business operations 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 Module to facilitate the FMA Evaluation. The FMA Module also allows each organization to add local risks.

Corrective Action Plan (CAP)

A plan to correct a control deficiency. A CAP must be prepared and tracked for all significant control deficiencies identified during the internal control evaluations process. A CAP Summary for significant deficiencies and material weaknesses identified in the Assurance Memorandum must be provided with the memorandum.

Data Analytics

Process of examining data sets in order to find trends and draw conclusions about the information.

Departmental Element Refers to DOE Headquarters Offices, Power Marketing Administrations, Field, and/or Operations Offices.

Entity Refers to DOE reporting organizations and includes DOE Headquarters Offices, Field Offices, Site Offices, Power Marking Administrations, Operations Offices, and Major/Integrated Contractors.

Entity Assessment (EA) Module The central location for documenting and reporting the results of evaluations of the entity's internal controls and objectives as well as financial management system evaluations.

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 and FFMIA.

Entity Level Controls Controls that have a pervasive effect on an entity's internal control system and pertains to multiple components.

Enterprise Risk Management (ERM) An agency-wide approach to addressing the full spectrum of DOE external and internal risks by understanding the combined impact of all organization risks as an interrelated portfolio, rather than addressing risks in individual programs.

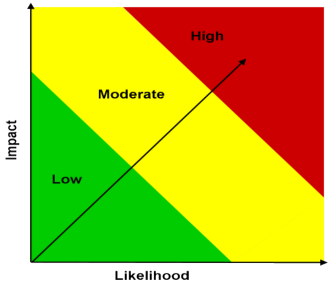
Evaluation Summary Presents the key information or activities leveraged/performed to provide reliable support for assurances that the control objectives and considerations have been addressed.

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).

In the FMA Module, this is a professional judgment rating of High, Moderate, Low, or Not Relevant (NR). The NR rating is for corporately defined risks that may not impact all organizations. No assessment is required with a rating of NR, although a short rationale will need to be provided.

General environment: Environment assumes no mitigating controls 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)

Federal Act that requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency (including DOE). 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 significant issues up through the chain of command to the President and Congress. To support Departmental reporting, Heads of organizations, including the National Nuclear Security Administration (NNSA), are required to report on the status of the organization’s internal controls, including reportable issues identified and progress made in correcting prior reportable issues.

FMFIA provides for:

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

Federal Financial Management Improvement Act (FFMIA)

Federal Act that requires each agency to implement and maintain financial management systems that comply substantially with the:

- Federal financial management systems requirements;
- Applicable Federal accounting standards; and
- United States Government Standard General Ledger (USSGL) at the transaction level.

Financial Management Assessment (FMA) Evaluation

An evaluation of internal controls over reporting that tests an entity’s controls in order to provide assurance on the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Financial Management Assessment (FMA) Module

The central location for documenting the evaluation of the relevant financial business processes, sub processes, and risks facing each reporting entity, as well as the key controls and testing information for each process that are relied upon to mitigate the risks.

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, including hardware, applications and system software, personnel, procedures, data, and reporting functions. The financial management system may fully integrate with other management information systems (i.e., mixed systems) where transactions automatically flow into an accounting general ledger. The financial management system could also include manual processes to post transactions from other management systems into the accounting general ledger."

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 the 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, entity owners of a financial management system included in the Department's FMS Inventory, and users of an FMS, are required to conduct an FMS Evaluation as part of the annual internal controls evaluation process.

Focus Area

Specific areas of emphasis which require additional assessment in the FMA Module.

Improper Payment

When the payment funds go to the wrong recipient, the recipient receives the incorrect amount of funds, or the recipient uses the funds in an improper manner resulting in unintentional payment errors or intentional fraud and abuse.

Interim Internal Controls Status (IICS) Assessment

A questionnaire that provides a mid-year update confirming that annual non-financial and financial risk assessments are being performed, risk exposure ratings updated, corrective actions are being taken on any significant issues identified in the current or prior year assessments, and whether any issues have been identified that would rise to the level of a significant deficiency or material weakness.

Internal Control

An integrated component of management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations;
- Reliability of reporting; and
- Compliance with applicable laws and regulations.

Inherent Risk The exposure arising from a risk before any action is taken to manage it.

Inquiry Inspection A detailed discussion with knowledgeable personnel to determine if controls are in place and functioning.

Key Control Scrutiny of specific business processes and documents through consideration and analysis for approval authorities that indicate the effectiveness of controls.

A control or set of controls that address the relevant assertions for a material activity or significant risk. When management is ready to test controls, and in order to focus test work, management must identify the key controls in place.

Kickbacks and Gratuities Contractors making undisclosed payments to agency officials or government contractors or giving something of value to reward a business decision.

Local Risk A risk in the FMA that is added by a reporting organization because the risk is applicable to that organization and the risk is not captured in a corporate risk.

Material Non-conformance Exists when *financial systems* do not substantially comply with federal financial management system requirements or where control deficiencies impact financial systems' ability to comply. The EA Module defines the conformance criteria and captures identified non-conformances.

Material Weakness A significant deficiency that the Entity Head determines to be significant enough to report outside of the Entity as a material weakness. Four types:

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

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

Material Weakness in Internal Control Over Reporting – A significant deficiency, in which the Entity's Head determines significant enough to impact internal or external decision-making and reports outside of the Entity as a material weakness.

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

Material Weakness in Internal Control Over Compliance – A condition where management lacks a process that reasonably assures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving Entity objectives.

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

Misrepresentation of Eligibility
Contractors purposefully reporting incorrect information in bid proposal to falsely claim eligibility to perform the work, such as status as a small business.

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

All controls in all business processes and sub-processes must be on a three- year testing cycle, including processes with a Low exposure rating and no control risk rating. If an organization has not tested a control in the past two years, the control will receive testing in the current year.

Mitigate
To put controls in place that would reduce the probability or impact of a given risk from being realized.

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

Non-Conformance
Exists when the Entity has identified potentially significant deficiencies in the scope of the internal controls’ evaluations conducted, which would warrant disclosure to assure limitations are understood.

OMB Circular A-123
Prescribes guidance for internal control and risk management requirements.

Observation
The viewing of a specific business process in action, and in particular the control activities associated with the process, to test the effectiveness of an internal control.

Payment Integrity Information Act (PIIA)
Federal act requiring agency leaders to assess and identify high-risk or otherwise significant programs and activities and share these findings in an annual publication.

Payroll Schemes Contractors obtaining payment through submission of false claims for compensation, such as misrepresenting employee labor in order to charge for more work hours and increase profit.

Procure to Pay (P2P) The cycle comprises the purchasing and payment processes including Acquisition Management; Inventory Management; Payables Management; and Travel Administration. Specific areas involved in this cycle are approving requisitions, issuing RFP's, maintaining, and selecting vendors, awarding contracts, maintaining obligations, receiving and managing goods or services, approving and paying invoices, tracking funds, monitoring continuing resolutions, and managing travel and purchase cards.

Product Quality Contractors purposefully conducting work in a way that results in the delivery of goods of a lesser quality than required by the contract.

Projects to Assets (P2A) The cycle comprises processes related to the oversight of projects resulting in an asset and the management of project costs and property. Processes included in this cycle are Project Cost Management, and Property Management. Specific areas that fall within this process cycle are managing large projects including capturing all costs and managing to budget; capturing costs for reimbursable expenses; creating and monitoring assets; monitoring depreciation; and controlling property.

Quote to Cash (Q2C) The cycle comprises processes related to working capital management and capturing revenue as a receivable to be managed and collected. The cycle consists of Revenue Management and Receivable Management processes. Specific areas that fall within this process cycle include invoicing for reimbursable expenses, along with other expected revenues through to managing accounts receivable and receiving cash.

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 control deficiency identified through an internal controls assessment.

Re-performance An objective execution of procedures or controls performed as part of a test of the effectiveness of the entity's internal control.

Residual Risk The amount of risk that remains after action has been taken to manage it

Risk Assessment A systematic process of evaluating the potential risks that may impact the ability of an organization to achieve objectives or goals.

Risk Factor

Identification of changes that may affect the exposure risk or effectiveness of existing controls in mitigating the risk. Risk factors include system, process, organization, or other changes (e.g., Inspector General (IG) or GAO audits).

Risk Profile

A prioritized inventory of the most significant risks identified that the Agency faces toward achieving its strategic objectives arising from its activities and operations and identifies appropriate options for addressing significant risks.

Risk Register Risk Response

An inventory of potential risks the Agency may face when striving to achieve its strategic objectives.

A determination by management on how a risk should be managed, considering the potential impact of the risk and the likelihood of occurrence, as well as the cost associated with mitigating the risk.

Types of risk responses:
Acceptance Take no action to respond to the risk based on insignificance of risk, requirement to complete the work, or benefits and opportunities exceed the risk.

Avoidance – Action is taken to stop the operational process, or the part of the operational process causing the risk.

Reduce – Action is taken to reduce the likelihood or impact of the risk.

Share – Action is taken to share the risks with another entity within the organization or with one or more external parties.

Transfer – Action to transfer the responsibility for ownership and handling the risk to an organization other than the current entity that owns the risk.

Risk Tolerance

The level of variation in performance that management is willing to accept, relative to achieving objectives. Management should establish its risk tolerance level before the placement of controls.

Sabotage

The intentional and deliberate destruction of property or the obstruction of an activity.

Sampling

Used to select the appropriate number of transactions to test for each control. Sampling methods for consideration are:

- **Random**- A method of selecting a sample whereby each item in the population of transactions is given an equal chance of selection regardless of the population size.
- **Judgmental**- A method of sample selection whereby the sampled items are selected based on a deliberate choice based on the profile of the population of transactions. This method provides validation that high-risk or other items of interest are included in the selected sample and reviewed as part of testing the control.

- **Systematic**- A method of sample selection whereby a uniform interval is selected throughout the population. The appropriate interval is determined by dividing the number of items in the population by the sample size.

Scope Limitation Exists when the entity has identified potentially significant deficiencies in the scope of the internal control evaluations conducted, which would warrant disclosure to assure limitations are understood. Scope limitations may be determined by the entity or may be required by the Office of the Chief Financial Officer (OCFO) in certain circumstances.

Significant Deficiency A deficiency or a combination of deficiencies in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

Special Purpose (SPC) The cycle comprises processes which are unique and cannot be categorized under other process cycles. These processes require significant attention due to the impact on the financial statements and scope of responsibility. The cycle consists of the Environmental Management (EM) Liability process.

Standard Process A business process that is pre-populated in the FMA Module.

Standard Sub-process A sub-component of a standard process, also pre-populated in the FMA Module.

Statement of Assurance Annual statement required by FMFIA and included in the DOE Agency Financial Report (AFR) that represents the Secretary's informed judgment as to the overall adequacy and effectiveness of DOE internal controls. The AFR reports the results of evaluations made on DOE entity, financial, and financial management systems controls, including identified material weaknesses or material non-conformances and corrective action progress made on existing material weaknesses and material non-conformances.

Testing Activity Theft Vandalism Procedure to determine if internal control systems work in accordance with internal control objectives.

Contractors stealing or misappropriating government resources, such as cash or other assets.

The mindless and malicious harm and injury to another's property.

Appendix B: Data Analytics Survey Template

Please refer to the attached spreadsheet for the Data Analytics Survey Template.

FY 2024 DAWG Survey
12-28-2023.xlsm