VOLUME 1, CHAPTER 3: "FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT COMPLIANCE"

SUMMARY OF MAJOR CHANGES

Changes are identified in this table and also denoted by blue font.

Substantive revisions are denoted by an asterisk (*) symbol preceding the section, paragraph, table, or figure that includes the revision.

Unless otherwise noted, chapters referenced are contained in this volume.

Hyperlinks are denoted by ***bold, italic, blue, and underlined font*.**

The previous version dated September 2023 is archived.

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
All	Streamlined chapter to remove instructional language.	Revision
1.1	Added interdependencies between Federal Financial Management Improvement Act (FFMIA) and other compliance requirements.	Addition
1.3	Added the following to the Authoritative Guidance section: Title 10, United States Code, Section 2222; Government Accountability Office, Financial Audit Manual, Volumes 1, 2, and 3; and the Department of Defense (DoD) Instruction 5000.75.	Addition
2.0	Added and revised definitions.	Revision
3.0	Added and revised FFMIA compliance requirements.	Revision
4.0	Added and revised responsible entities.	Revision
Table 4-1	Added table for the DoD Information Technology Investment Portal (DITIP) DoD Auditability Requirements Compliance assertion criteria.	Addition

Table of Contents

CHAPTER 3

FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT COMPLIANCE

1.0 GENERAL

*1.1 Overview

1.1.1. The Federal Financial Management Improvement Act of 1996 (***FFMIA)*** is intended to ensure Federal financial systems provide reliable, consistent, and uniform disclosure of financial data using accounting standards. FFMIA requires the Department of Defense (DoD) to implement and maintain financial management (FM) systems that substantially comply with Federal Financial Management System Requirements (FFMSR), applicable Federal accounting standards, and the United States Standard General Ledger (USSGL) at the transaction level. FFMIA requires DoD management to annually assess and document the Department's compliance with FFMIA and report the results to the Office of Management and Budget (OMB), accomplished through the annual Statement of Assurance (SOA) processes. Generally Accepted Government Auditing Standards (GAGAS), the Financial Audit Manual (FAM), and OMB Bulletin 24-02 require the Department's financial statement auditors to evaluate and report on whether the agency's financial management systems comply with FFMIA requirements, accomplished through the Agency Financial Report (AFR) process. Financial statement auditors use the results of DoD management's internal control assessments, including FFMIA and other compliance assessments, to inform the scope and rigor of their testing. The results of management's own assessment and the auditors' independent evaluation determine whether the Department's financial management systems substantially comply with FFMIA. If not, management is responsible for developing and implementing remediation and risk management plans as applicable.

1.1.2. While FFMIA compliance centers on these three requirements, it is not limited to them. Other relevant standards and requirements include the Federal Managers' Financial Integrity Act, the Agency Chief Financial Officers Act, the Federal Information Security Management Act of 2002 (FISMA), and OMB Circular A-123 requirements.

1.2 Purpose

This chapter prescribes the Department's policy for achieving substantial compliance with FFMIA. It provides the basis for the implementation of FFMIA for the Department to generate timely, accurate, and useful financial information with which the Department leadership can make informed decisions and ensure accountability on an ongoing basis.

*1.3 Authoritative Guidance

The requirements prescribed by this chapter are in accordance with the applicable provisions of:

1.3.1. Title 10, United States Code, section 2222 ***(10 U.S.C. § 2222)***, "Defense business systems: business process reengineering; enterprise architecture; management."

1.3.2. ***10 U.S.C. § 2223 (a) & (b)***, "Information technology: additional responsibilities of Chief Information Officers."

1.3.3. ***31 U.S.C. § 1115***, "Federal Government and agency performance plans."

1.3.4. ***31 U.S.C. § 3512,*** "Executive agency accounting and other financial management reports and plans"; with emphasis on sections 801 – 807 (FFMIA)."

1.3.5. ***31 U.S.C. Chapter 9***, "Agency Chief Financial Officers."

1.3.6. ***44 U.S.C. Chapter 35, Subchapter III***, "Confidential Information Protection and Statistical Efficiency."

1.3.7. ***44 U.S.C. § 3601,*** "Definition."

1.3.8. ***OMB Bulletin No. 24-02***, "Audit Requirements for Federal Financial Statements."

1.3.9. ***OMB Circular A-123, Memorandum M-23-06, Appendix D,*** "Management of Financial Management Systems – Risk and Compliance."

1.3.10. ***OMB Circular A-130, Appendix I,*** "Responsibilities for Protecting and Managing Federal Information Resources."

1.3.11. Statement on Standards for Attestation Engagements No. 18, ***(SSAE No. 18 Examinations, AT-C Section 320)***, "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting."

1.3.12. National Institute of Standards and Technology ***(NIST) Special Publication 800-53,*** Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

1.3.13. U.S. Department of Treasury Financial Manual (TFM), Volume 1, Part 6, Chapter 9500 ***(1 TFM 6-9500)***, "Fiscal Year 2024 Revised Federal Financial Management System Requirements for Fiscal Reporting."

1.3.14. Government Accountability Office (GAO), Financial Audit Manual (FAM), Volume 1 (***GAO-24-107278***), "Audit Methodology", Section 350 and 360."

1.3.15. GAO, FAM, Volume 2 (***GAO-24-107279***), "Detailed Implementation Guidance", Section 701 – 710."

1.3.16. GAO, FAM, Volume 3 (***GAO-24-107280***), "Federal Financial Reporting Checklist."

1.3.17. GAO, Federal Information System Controls Audit Manual (FISCAM), (***GAO-24-107026***)

1.3.18. ***DoD Instruction (DoDI) 5000.75,*** "Business Systems Requirements And Acquisition."

1.3.19. ***DoDI 5010.40***, "DoD Enterprise Risk Management and Risk Management and Internal Control Program"

1.3.20. ***DoDI 8510.01,***"Risk Management Framework (RMF) for DoD Systems."

1.3.21. DoD Internal Control Over Reporting - Financial Reporting and Financial Systems (***ICOR-FR & FS***).

1.3.22. DoD Statement of Assurance Executive Handbook (***SOA Executive Handbook***)

*2.0 DEFINITIONS

The definitions outlined in this section cover both the Federal and DoD vernaculars. Paragraphs 2.1 through 2.3 are the Federal vernacular contained in OMB Circular A-123, Memorandum M-23-06, Appendix D, while paragraphs 2.4 through 2.6 conform to the vernacular the Department uses to categorize DoD-owned financial management systems based on the functions the system supports. DoD Components should utilize the definitions in 2.4 through 2.6 to meet the requirements of paragraph 4.4.2.1 of this chapter.

2.1 Financial Management Systems

FM systems include the core financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data hardware, software, and support personnel dedicated to the operation and maintenance of system functions. Both financial systems and mixed systems may directly or indirectly trigger a financial event within the system itself or in another system and may be required to comply with some or all FFMIA requirements. The ICOR-FR & FS systems recorded in the FIAR Systems Database (FSD) will be used to identify DoD FM Systems that are subject to FFMIA requirements and compliance reviews.

2.2 Core Financial Systems

2.2.1. Core financial systems and financial systems are synonymous terms and consist of six functional areas: general ledger management, funds management, payment management, receivable management, cost management, and financial reporting.

2.2.2. Core financial systems are comprised of one or more software programs (commonly referred to as applications), that are used for:

2.2.2.1. Collecting, processing, maintaining, transmitting, or reporting data about financial events;

2.2.2.2. Supporting financial planning or budgeting activities;

2.2.2.3. Accumulating and reporting costs information; or

2.2.2.4. Supporting the preparation of financial statements.

2.3 Mixed Systems

Mixed systems are information systems that support both financial and nonfinancial functions of the federal government or components thereof. FFMIA requirements apply only to the financial portion of mixed systems.

2.4 Accounting Systems

Accounting systems are core financial systems configured to post transactions to an internal USSGL-compliant subsidiary or general ledger. Depending on the functions performed, accounting systems may be required to comply with some or all FFMIA requirements.

2.5 Financial Business Feeder Systems

Financial business feeder systems may be core financial or mixed systems. Financial business feeder systems create or process transactions with financial or accounting impacts and exchange financial/accounting data with another business feeder system(s) and/or accounting system(s). The term financial business feeder system is synonymous with feeder systems. Depending on the functions performed, financial feeder systems may be required to comply with some or all FFMIA requirements.

2.6 No (Neither) Systems

No (Neither) systems are FM systems that do not fit into the accounting system or financial business feeder system categories. These systems do not directly handle financial transactions but play significant roles in supporting the overall system functionalities and user interactions. They serve purposes such as access and identity management or data visualizations. Advanced Analytics (ADVANA) is an example of a no (neither) system.

2.7 Service Providers

Service Providers refer to external parties that perform the operational process(es) for an entity. Service Providers providing services to user entities that are likely to be relevant to those user entities' internal control over reporting – financial reporting and financial systems may undergo an SSAE No. 18 Examination covering systems used and common controls performed uniformly for user entities. The results of the examination are captured in a System and Organization Control (SOC 1) Report. The SOC 1 Report is specifically intended to meet the needs of entities that use service organizations (user entities) and the independent public accountants (IPAs) that audit the user entities' financial statements (user auditors). It assists them in understanding the control environment and evaluating the effectiveness of the controls at the service organization and their impact on the user entities' financial statements.

2.8 Hosting Organization

Hosting Organizations provide application hosting services for systems owned by DoD. Examples of hosting organizations include the Defense Information Systems Agency (DISA) and commercial Cloud Service Providers.

*3.0 FFMIA COMPLIANCE REQUIREMENTS

3.1 FFMIA Compliance

3.1.1. In determining whether the Department's financial management systems substantially comply with FFMIA, management and auditors must consider the degree to which a system's performance prevents the Department from meeting the specific requirements of FFMIA as listed in paragraph 1.1.

3.1.1.1. DoD management may use OMB Circular A-123, Appendix D, Attachment 1, "FFMIA Compliance Determination Framework", to determine whether a system is substantially compliant with FFMIA.

3.1.1.2. Financial statement auditors apply OMB Bulletin 24-02 or the latest version and the GAO FAM Volumes 2 and 3 in combination with the results of their own independent testing and documentation provided by DoD management to determine DoD management's overall compliance with FFMIA.

3.1.2. The DoD strategy for FFMIA compliance is integrated with related efforts to achieve auditability and maintain effective Internal Control over Reporting (ICOR) including ICOR-FR & FS systems. Documentation that supports these related requirements also supports FFMIA compliance and may be used to avoid duplication of efforts.

3.1.3. The DoD ICOR-FR & FS Guide serves as a standard reference for users involved in financial reporting internal control activities within the DoD. This includes the annual requirements prescribed in the OMB Circular A-123, the FFMIA, and other applicable laws, regulations, and guidance. A system is subject to FFMIA if it is determined to be ICOR-FR & FS relevant as defined in the DoD ICOR-FR & FS Guide and performs any business functions with FFMIA compliance controls.

3.1.4. The DoD ICOR-FR & FS Guide identifies the Federal Information System Controls Audit Manual (FISCAM) as the methodology to be used for performing IT control assessments and audits. It groups IT controls into two categories, General Controls (GC) and Business Process Controls (BP). See section 3.5 for additional details.

3.1.5. The selection of applicable FISCAM controls is governed by the application of the FM Overlay developed by OUSD(C). All DoD Components are required to implement the FM Overlay for each system that is relevant to ICOR-FR & FS. Compliance is enforced in the controls selection phase of assessment and authorization processes in the Enterprise Mission Assurance Support Service (eMASS) system or other software/tools implemented for this purpose. Components must consider the results of control assessments, regardless of who performs them, when evaluating federal financial systems' compliance with laws and regulations, such as FFMIA and FISMA.

3.1.6. The Defense Business Systems (DBS) annual Certification Guidance memorandum identifies the annual FFMIA requirements as DoD Auditability Requirements consistent with 10 U.S.C. § 2222(g) and requires DoD Components with priority or covered ICOR-FR & FS DBS to comply or plan to comply with applicable requirements, to include FFMIA controls in financially relevant business events (operational activities) within the DoD business enterprise architecture (BEA). The ***ADVANA FM Functions – Requirements Matrix*** (requires ADVANA Qlik access) provides the financially relevant business events associated with BEA operational activities.

3.1.7. The GAO FAM Volumes 1 and 2 and OMB Bulletin 24-02 provide guidance to auditors for the assessment of FFMIA compliance and state the requirements for auditors to report whether an agency's financial management systems comply substantially with FFMIA requirements. The auditor's report should include the nature and extent of the noncompliance, including areas in which there is substantial but not full compliance; the primary reason or cause of noncompliance; the entity or organization responsible for the noncompliance, any relevant comments from any responsible officer or employee, and a statement with respect to the recommended remedial actions and the time frames for implementing those actions.

3.2 USSGL at the Transaction Level

3.2.1. The Department's financial management systems must maintain accounting data at the transaction level. Financial management systems include both financial and mixed systems. Every DoD financial event (budgetary and proprietary) must be recorded by applying the requirements of the USSGL guidance in the TFM, and DoD USSGL transaction library (See Chapters 4 and 7 for additional guidance).

3.2.2. Every financial relevant business event that results in an automated or manual transaction in a core financial system must generate accurate and compliant postings to all relevant budgetary and proprietary general ledger accounts according to the rules defined in the DoD USSGL transaction library guidance and website. The GAO FAM provides procedural guidance for testing compliance with USSGL.

3.3 Federal Accounting Standards

DoD financial events (budgetary and proprietary) must be recorded by applying the requirements of the Federal accounting standards governed by the Federal Accounting Standards Advisory Board. (See Chapter 2 for additional guidance). Applicable Standard Federal Financial Accounting Standard (SFFAS) requirements have been integrated into the DoD BEA operational activities. The GAO FAM provides procedural guidance for testing compliance with federal accounting standards.

3.4 Federal Financial Management System Requirements

3.4.1. The FFMSRs were originally developed to support the adoption of uniform financial systems, standards, and reporting required by the FFMIA. Subsequently, the FFMSRs were incorporated into the Federal Financial Management (FFM) Federal Integrated Business Framework (FIBF) Business Capabilities and their use was expanded beyond compliance with FFMIA.

3.4.2. The FFM FIBF Business Capabilities are a component of the Financial Management Capability Framework, which provides a common set of standards and capabilities that are the foundation for all offerings in the Financial Management Quality Service Management Office Marketplace. The FFMSRs are maintained by the U.S. Department of the Treasury in the TFM, Volume 1, Part 6, Chapter 9500. The GAO FAM provides procedural guidance for testing compliance with FFMSRs.

3.5 Information System Controls

3.5.1. GC are policies, procedures, and controls that apply to all or large segments of an entity's information systems and to individual systems and applications. General control categories include security management, access control, segregation of duties, configuration management, and contingency planning. The Financial Management Overlay leverages the audit methodology and criteria found in the GAO FISCAM and NIST SP 800-53 respectively to provide

the NIST-to-FISCAM control mapping used during controls selection and hybrid assessment procedures that help to ensure that controls are tested to the same rigor as is used by auditors.

3.5.1.1. Security Management provides the foundation of a security-control structure and reflects senior management's commitment to addressing security and privacy risks and provides a framework and continuous cycle of activity for managing risk, developing and implementing effective security policies, assigning and communicating responsibilities, and monitoring the adequacy of the entity's IS controls over the infrastructure, data processing environment and applications.

3.5.1.2. Access Control limits access or detects inappropriate logical access to information resources (e.g., data, systems, files, and other resources), thereby protecting these resources against unauthorized modification, loss, and disclosure, and restricting physical access to information resources and facilities.

3.5.1.3. Segregation of Duties relates to the policies, procedures, and organizational structure for managing who can control key aspects of computer-related operations and thereby prevent unauthorized actions or unauthorized access to assets or records.

3.5.1.4. Configuration Management relates to identifying and managing security features for information technology (e.g., hardware, software, firmware, equipment, media, and services) at a given point and systematically controlling changes to that configuration during the system's life cycle.

3.5.1.5. Contingency Planning provides for the continuation of critical or essential mission and business functions in the event of a system disruption, compromise, or failure and the restoration of the information system following a system disruption.

3.5.2. Business Process Controls include the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions; activities across business processes; and events between business process applications, their components, and other systems. They relate to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. The Financial Management Overlay leverages the audit methodology and criteria found in the GAO FISCAM and NIST SP 800-53 respectively to provide the NIST-to-FISCAM control mapping used during controls selection and hybrid assessment procedures that help to ensure that controls are tested to the same rigor as is used by auditors. Specific control areas of business process controls are:

3.5.2.1. Input: relates to controls over data that is entered into the application (e.g., data validation and edit checks).

3.5.2.2. Processing: relates to controls over data integrity within the application (e.g., review of transaction processing logs).

3.5.2.3. Output: relates to controls over data output and distribution (e.g., output reconciliation and review).

3.5.2.4. Master Data Setup and Maintenance relates to controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendor file).

3.6 Compliance Determination Framework

The FFMIA Compliance Determination Framework (Framework) assists in determining whether the Section 803(c) requirements of FFMIA are followed. The Framework is a risk and evidence-based assessment model that leverages existing audit tests, evaluations, and reviews that auditors, agency management, and others already perform. This work may include the external audit report and internal reports prepared by the agency in providing any assurances over the financial statements. Consistent with OMB Circular A-123, Appendix D, Attachment 1, the Department has developed an auditor perspective within the FM Systems – FFMIA Scorecard within ADVANA to identify systems associated with internal and external auditor evaluations and other findings.

*4.0 RESPONSIBILITIES

The responsibilities identified in this section are limited to those specific to FFMIA compliance and are not meant to be an exhaustive list of all the responsibilities of these entities. This includes the authorities and framework that the Department employs to monitor, analyze, validate, integrate, and control FFMIA compliance requirements.

4.1 Office of the Under Secretary of Defense (Comptroller)

4.1.1. The Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) is supported by the Deputy Comptroller for Enterprise Financial Transformation (EFT) and Deputy Chief Financial Officer (DCFO), through its subordinate organizations (the Financial Improvement and Audit Remediation (FIAR) Directorate and the Financial Management Policy and Reporting (FMPR) Directorate). OUSD(C) is responsible for providing Department-wide oversight of substantial compliance with the FFMIA requirements.

4.1.1.1. If the DoD Component's financial management systems do not substantially comply with the requirements of Section 803(c), the FFMIA requires that a remediation plan be developed, in consultation with OMB that describes the resources, remedies, and milestones for achieving substantial compliance, and/or a risk management plan to meet management assurance requirements.

4.1.1.2. OUSD(C) must annually report to OMB the progress made towards resolving identified deficiencies and such progress must be discussed in the DoD Components remediation plan, capital planning and investment control plans, risk management plan, and other

planning documents, when applicable. The findings or analysis of noncompliance must be included with a discussion of ongoing remediation activities. Progress towards resolving the deficiencies must not be construed as substantial compliance with FFMIA.

4.1.1.3. Remediation plans are expected to bring the Department's financial management systems into substantial compliance no later than three years after the date a noncompliance determination is made by OUSD(C) or its auditors. However, if OUSD(C), with the concurrence of OMB, determines that the Department's financial management systems cannot be brought into substantial compliance within three years, the DoD Component (in consultation with OUSD(C)) may specify a longer period. In either case, the DoD Component must designate a DoD Component official responsible for bringing the DoD Component's financial management systems into substantial compliance by the date specified in the DoD Information Technology Portfolio Repository (DITPR) and for reporting progress to EFT (acting on behalf of the Defense Business Council) on a scheduled basis.

4.1.2. The EFT governs the enterprise FFMIA oversight program. Annually, EFT will publish the oversight schedule and other FFMIA substantially compliance details, consistent with OMB Circular 123, Appendix D, and the DoD SOA Execution Handbook. for DoD Components to execute in support of FFMIA compliance. EFT utilizes the ICOR-FR & FS system inventory established by the FIAR Directorate to identify systems that are required to comply with FFMIA. EFT uses transaction-level data from ICOR-FR & FS systems ingested into ADVANA to support oversight of FFMIA compliance. EFT develops and utilizes ADVANA tools to enable governance and oversight of the DoD-owned financial management system environment. These tools and governance capabilities inform the Department's annual business system investment decisions and other management actions. EFT is responsible for reporting the progress of the DoD financial management information technology roadmap and overall FFMIA compliance progress within the SOA section of the DoD AFR.

4.1.3. The Office of the DCFO (ODCFO) is responsible for developing and implementing financial improvement audit strategies, monitoring auditors' findings, and providing internal control training to improve the quality and security of financial information. Additionally, the ODCFO develops and interprets DoD-wide accounting and finance policies, ensuring consistency with laws and regulations, and oversees financial integrity initiatives such as the Standard Financial Information Structure (SFIS) USSGL program. Ultimately, both FIAR and FMPR Directorates work to support the DoD's financial management and audit requirements, with the goal of achieving accurate and reliable financial information and unmodified audit opinions.

4.1.3.1. FIAR Directorate. The FIAR Directorate develops, publishes, and issues detailed financial improvement audit strategies, methodologies, and implementation guidance. The FIAR Directorate establishes the ICOR-FR & FS systems inventory subject to FFMIA compliance reporting, monitors auditors' findings and recommendations around FFMIA compliance, provides internal control training to reporting entities on improving the design and operating effectiveness of IT controls, publishes the results of the Department's SOA for FFMIA within the DoD AFR. As a result, the FIAR Directorate, improves the quality and security of the financial information, with an unmodified audit opinion as the desired outcome.

4.1.3.2. FMPR Directorate. The FMPR Directorate develops, publishes, implements, and interprets DoD-wide accounting and finance policies and ensures the DoD Financial Management Regulation (DoD 7000.14-R) is consistent with laws and other applicable guidance. The FMPR Directorate leads and oversees DoD financial integrity to include the DoD SFIS USSGL program. As a result, FMPR develops, publishes, and interprets DoD-wide financial management improvements and guidance that supports statutory requirements for the Department to audit its full set of financial statements.

4.2 DoD Chief Information Officer

4.2.1. The DoD Chief Information Officer (CIO) executes and governs information technology oversight.

4.2.2. Deputy CIO for Information Enterprise (IE) establishes information technology policy and guidance for the infrastructure components of the DoD IE to include networks, computers, and software. The IE directorate also maintains the DoD BEA and oversees DBS compliance with all applicable laws, including Federal accounting, financial management, and reporting requirements. See 10 U.S.C. § 2222 for additional guidance.

4.2.3. Deputy CIO for Cybersecurity (CS) is responsible for providing expert policy, technical, program, and Defense-wide oversight on all aspects and matters related to DoD CS. The CS Directorate oversees the risk management framework for DoD systems. See DoDI 8501.01 for additional guidance.

4.2.4. Deputy CIO for Resources and Analysis provides guidance on the information technology/cyberspace activities budget submission. See Volume 2B, Chapter 18 for additional guidance.

4.3 Director of Administration and Management

The Director of Administration and Management (DA&M) is the principal management office for the Secretary of Defense responsible for optimizing the business environment across the DoD enterprise. DA&M executes the DoD Enterprise Risk Management and Internal Controls Over Reporting - Operations programs, providing resources and assistance with evaluating and managing risk associated with systems non-compliance with applicable FFMIA requirements. The DA&M delivers program management, oversight, security services, and support functions that enable uninterrupted operations of the Department Headquarters.

4.4 DoD Components

4.4.1. DoD Components must establish and maintain financial management systems that substantially comply with FFMIA Section 803(c) requirements. DoD-owned ICOR-FR & FS relevant systems must be developed and maintained to generate reliable, timely, and consistent information necessary for the Department to comply with FFMIA requirements and enable the

preparation of accurate, reliable, and timely financial statements and other required financial and budget reports using information generated by the financial management systems. DoD Component management must annually test and report financial management systems for FFMIA compliance.

4.4.2. DoD Components must maintain records of systems and transactional data that substantially comply with applicable FFMIA requirements. Applicable FM systems (see definitions section) must annually assess/test compliance to maintain complete and accurate data in:

4.4.2.1. DoD Information Technology Portfolio Repository (DITPR). DoD Components must ensure their financial system portfolio is accurately reported in DITPR. DoD financial systems must review, report, and update appropriately all applicable DITPR FFMIA reporting requirements and DoD business enterprise architecture operational activity aligned to federal financial management functions (see the FM Functions – Requirements Matrix) on an annual basis in accordance with 10 U.S.C. § 2222(g). DoD Components must ensure their FM systems align to applicable financial events represented in the DoD BEA as operational activities, end-to-end processes, and capabilities; and ensure the system complies with the controls associated with the DoD BEA operational activity. DoD Component FFMIA oversight officials and system owners must ensure their FM system's current level of compliance with each of the applicable FFMIA requirements is recorded in DITPR and consistent with their Annual SOA reporting.

4.4.2.2. FSD. DoD Components must utilize FSD to identify, capture, and report on the universe of financially relevant systems to support internal controls, financial audits, executive leadership, and Congressional reporting requirements. DoD Component FFMIA oversight officials and system owners must ensure their FM system's current overall compliance with FFMIA is recorded in the FSD and asserted in their Annual SOA reporting.

4.4.2.3. ADVANA. DoD Components must provide budgetary and proprietary transactional data to ADVANA from FM systems and ensure their ADVANA common data models remain complete and accurate. See Chapter 10 for additional guidance.

4.4.2.4. DoD Information Technology Investment Portal (DITIP). DoD Components must report compliance with the DoD Auditability Requirements in the investment certification module of DITIP as required by 10 U.S.C. § 2222 and consistent with the DBS Annual Certification Guidance memorandum. For ICOR-FR & FS DBS, Table 4-1 provides the applicable reporting criteria.

4.4.2.5. Notice of Findings and Recommendations (NFR) Database. DoD Components must ensure complete, accurate, and timely CAPs are established and recorded in the NFR Database. This includes IT and non-IT NFRs from stand-alone financial statement audits and SSAE No. 18 Examinations. Intelligence community DoD Components with stand-alone financial statement audits are exempted from this requirement. DoD Component officials must ensure their IT budget reflects the funding needed to complete all milestones identified in the CAP to address/close potential vulnerabilities identified by the open IT NFRs.

4.4.2.6. eMASS and FM Overlay. eMASS is a comprehensive solution used to support FISMA compliance and cybersecurity oversight and management. Features include dashboard reporting, control scorecard measurement, and the generation of a system security authorization package to support system authorization decisions. The FM Overlay helps DoD Components to efficiently and consistently meet the RMF and controls-based financial statement audit expectations for ICOR-FR & FS-relevant systems. DoD Components that use eMASS are required to apply the FM Overlay to all ICOR-FR & FS systems eMASS records. DoD Components that use other software or tools to support FISMA compliance and cybersecurity oversight and management are likewise required to implement and apply the reporting requirements of the FM Overlay to all ICOR-FR & FS relevant systems.

4.4.3. DoD Components must ensure the applicable FFMIA requirements are included in their pre-acquisition requirements documentation, and applicable FFMIA requirements are implemented with the deployment of new financial management solutions (manual or automated) as well as included in acquisition strategies for commercial off-the-shelf and software-as-a-service solutions consistent with DoDI 5000.75.

4.4.4. DoD Component must ensure the system portfolio and remediation plans are consistent with modernization priorities identified in 44 U.S.C. §3601.

4.4.5. DoD Components are required to perform an assessment to identify all Service Providers that are relevant to their internal control over financial reporting and obtain copies of the applicable SOC 1 Reports. DoD Components are also required to design, document, and implement effective controls to address the applicable Complementary User Entity Controls and when relevant, the applicable Complementary Subservice Organization Controls in the applicable SOC 1 Reports. This includes reviewing the Service Providers' and Hosting Organizations' FFMIA assessment results and addressing any deficiencies identified by the Service Providers / Hosting Organizations that may impact the DoD Component's internal controls.

4.4.6. DoD Component oversight officials must ensure all DBS, both priority/non-priority and covered/non-covered that are not substantially compliant with FFMIA are conditioned and remediated consistent with 10 U.S.C. § 2222, and/or have substantiated compensating controls for areas of non-compliance.

4.5 Service Providers

Service Providers must develop and maintain FFMIA compliance assessment and remediation plans in coordination with using DoD Components (user entities). For each financial system and mixed system managed by a Service Provider, a Memorandum of Agreement (MOA) or other suitable agreement, must be established with each using DoD Component. As part of the MOA, compliance testing must be conducted to support DoD Component (user entity) end-to-end business process testing. For systems covered by an SSAE No. 18 Examinations, Service Providers must provide DoD Components (user entities) with a Report on Controls at a Service

Providers Relevant to User Entity's ICOR-FR & FS also known as a Service SOC 1 Report. The SOC 1 Report documents management's description of the control environment and the design and operating effectiveness of the controls in place at the service organization and/or subservice organizations. It describes the user entities' responsibilities for certain controls, known as Complementary User Entity Controls and Complementary Subservice Organization Controls.

4.6 Hosting Organizations

Hosting Organizations, internal to DoD (e.g., DISA) and external to DoD (e.g., commercial Cloud Service Providers), provide application hosting services for systems owned by DoD. As a result, hosting organizations are responsible for most of the ITGC over the computing environment in which many financial, personnel, and logistics applications reside and often provide a SOC 1 Report. For Service Providers and DoD Components to rely on automated controls and documentation within these applications, controls must be appropriately and effectively designed and operated effectively.

4.7 Inspector General

4.7.1. The Office of the Inspector General (IG) performs FFMIA compliance evaluations as part of financial statement audits and/or oversees evaluations performed by IPA firms during financial statement audits. This includes identifying in writing the nature and extent of non-compliance when appropriate. The IG reports to Congress instances and reasons when the Department has not met the intermediate target dates established in the remediation plan required under FFMIA Section 803(c).

4.7.2. The IG oversees many of the DoD's financial statement audits performed by the IPAs. Oversight includes monitoring the IPAs' adherence to the FAM requirements, GAGAS, and OMB Bulletin 24-02.

*Table 4-1 DITIP DoD Auditability Requirements Compliance Reporting Criteria for DoD ICOR-FR & FS systems

Assertion Category	Assertion Criteria
Y-Assessed Compliant	The system does not have open IT NFRs, and the system is substantially compliant with applicable FFMIA requirements: -Applicable SFIS business rules, FFMSR, and/or SFFAS (accounting and feeder systems) -Chart of Accounts; Posting Logic and Trial Balance requirements (accounting systems)
P-Assessed Planned Compliant	DoD Component has reported planned compliance dates for each applicable FFMIA requirement that is not substantially compliant in DITPR and/or validate corrective action plan (CAP) with milestone dates for each open IT and system-impacting BP NFR.
N-Assessed Not Compliant	Non-reporting of levels of compliance and planned compliance dates and/or compliance levels below published substantial compliance thresholds for any of the FFMIA requirements in DITPR and/or system has open GC and BP-impacting NFRs in the NFR Database without a validate CAP.
X-Assessment Not Completed	Not applicable for enduring ICOR-FR & FS systems. All ICOR-FR & FS systems must be assessed and reported annually.
Z-Not Applicable	Not applicable for enduring ICOR-FR & FS systems