CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-06 Medicare Financial Management	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 13001	**Date: December 13, 2024**
	Change Request 13731

SUBJECT: The Fiscal Year 2025 Updates for the CMS Internet Only Manual (IOM) Publication (Pub.) 100-06, Medicare Financial Management Manual, Chapter 7 - Internal Control Requirements

I. SUMMARY OF CHANGES: The purpose of this Change Request (CR) is to provide updated Internal Controls over Financial Reporting Guidance with respect to the following:

1. Office of Management & Budget (OMB) A-123 Reviews,

2. Certification Package of Internal Controls (CPIC) Reporting,

3. American Institute of Certified Public Accountants (AICPA) SSAE 18 Reporting, &

4. Corrective Action Plan (CAP) Initial & Quarterly Reporting for IOM Pub 100-06, Chapter 7 for the upcoming Fiscal Year 2025.

EFFECTIVE DATE: October 1, 2024
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: January 15, 2025

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	7/10/Introduction
R	7/10.2.2/Fundamental Concepts
R	7/20.2.1/CMS Contractor Control Objectives
R	7/20.4/Testing Methods
R	7/30.1.1/OMB Circular A-123, Appendix A: Internal Controls Over Financial Reporting (ICOFR)
R	7/30.9.1/A CUECs – Information Systems
R	7/30.9.8/L CUECs – Non-MSP Debt Collection
R	7/40.1/Submission, Review, and Approval of Corrective Action Plans
R	7/40.3/CMS Finding Numbers
R	7/40.6/CMS Initial and Quarterly CAP Report Template
R	7/50.1/A Controls – Information Systems
R	7/50.8/H Controls – Administrative
R	7/ 50.13/M Controls – Provider Enrollment
R	7/70/List of Commonly Used Acronyms

III. FUNDING:

For Medicare Administrative Contractors (MACs):

The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

Attachment - Business Requirements

Pub. 100-06	Transmittal: 13001	Date: December 13, 2024	Change Request: 13731

SUBJECT: The Fiscal Year 2025 Updates for the CMS Internet Only Manual (IOM) Publication (Pub.) 100-06, Medicare Financial Management Manual, Chapter 7 - Internal Control Requirements

EFFECTIVE DATE: October 1, 2024
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: January 15, 2024

I. SUMMARY OF CHANGES: The purpose of this Change Request (CR) is to provide updated Internal Controls over Financial Reporting Guidance with respect to the following:

1. Office of Management & Budget (OMB) A-123 Reviews,

2. Certification Package of Internal Controls (CPIC) Reporting,

3. American Institute of Certified Public Accountants (AICPA) SSAE 18 Reporting, &

4. Corrective Action Plan (CAP) Initial & Quarterly Reporting for IOM Pub 100-06, Chapter 7 for the upcoming Fiscal Year 2025.

II. GENERAL INFORMATION

A. Background: The Federal Managers' Financial Integrity Act of 1982 (FMFIA) established internal control requirements that shall be met by federal agencies. For CMS to meet requirements of FMFIA, Medicare contractors shall demonstrate that they comply with FMFIA.

The purpose of this Change Request (CR) is to provide updated Internal Controls over Financial Reporting Guidance with respect to the following:

1. Office of Management & Budget (OMB) A-123 Reviews,

2. Certification Package of Internal Controls (CPIC) Reporting,

3. American Institute of Certified Public Accountants (AICPA) SSAE 18 Reporting, &

4. Corrective Action Plan (CAP) Initial & Quarterly Reporting for IOM Pub 100-06, Chapter 7 for the upcoming Fiscal Year 2025.

B. Policy: The CMS contract with Medicare contractors includes an article titled FMFIA. In this article, the Medicare contractor agrees to cooperate with CMS in the development of procedures permitting CMS to comply with FMFIA, and other related standards prescribed by the Comptroller General of the United States. Under various provisions of the Social Security Act and the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Medicare contractors are to be evaluated by CMS on administrative service performance. CMS evaluates Medicare contractor's performance by various internal and external audits and reviews.

III. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
13731.1	All contractors shall be aware and comply with the Fiscal Year 2025 updates throughout Chapter 7 – Internal Control Requirements.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC
13731.2	All contractors shall comply with the updated Section 10 – Introduction.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC
13731.3	All contractors shall comply with the updated Section 10.2.2 - Fundamental Concepts.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC
13731.4	All contractors shall comply with the updated Section 20.2.1 – CMS Contractor Control Objectives.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC
13731.5	All contractors shall comply with the updated Section 20.4 - Testing Methods.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC
13731.6	All contractors shall comply with the updated Section 30.1.1 - OMB Circular A-123, Appendix A: Internal Controls Over Financial Reporting (ICOFR).	X	X	X	X	X	X	X	X	BCRC, CRC, SMRC
13731.7	All contractors shall be aware that the CUEC for Control Number A.21 under Section 30.9.1 – A CUECs – Information Systems terminology has been updated with “eXpedited Life Cycle”	X	X	X	X					BCRC, CRC, RRB-SMAC, STC

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
	revised to "Target Life Cycle": A.21: CMS maintains, updates, and makes available the current CMS Target Life Cycle (TLC) and other applicable policy to provide the MACs requirements and guidance for the establishment of change management and SDLC processes.									
13731.8	All contractors shall be aware that the CUEC for Control Number L.2 under Section 30.9.8 – L CUECs – Non-MSP Debt Collection terminology has been updated: L.2: CMS ensures the Contractor and Regional Office (if needed) reviews and determines eligibility for Extended Repayment Schedules (ERS) not to exceed 60 months.	X	X	X	X		X			BCRC, CMS, CRC, RRB-SMAC
13731.9	All contractors shall comply with the updated Section 40.1 - Submission, Review, and Approval of Corrective Action Plans.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC
13731.10	All contractors shall comply with the updated Section 40.3 - CMS Finding Numbers.	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC, STC
13731.11	All contractors shall comply and use the updated Initial and Quarterly CAP	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
	Microsoft Excel template located in Section 40.6 - CMS Initial and Quarterly CAP Report Template and accompanying this CR. Additionally, a Field Legend sheet providing field completion instructions, and Example Initial and Quarterly CAP sheets shall be used for CAP creation and formatting guidance.									SMAC, STC
13731.12	All contractors shall comply with the updates to Control Number A.21 under Section 50.1 – A Controls – Information Systems: Terminology Update: eXpedited Life Cycle revised to Target Life Cycle. A.21: Controls provide reasonable assurance that configuration management policies, plans, and procedures are established, documented, kept up-to-date, and approved in accordance with the current CMS ARS, BPSSM, and other applicable policy including the following: • A System Development Life Cycle (SDLC) methodology is documented and in use and aligns with the CMS Target Life Cycle (TLC).	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC, STC

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
	• Change management policies and procedures that have been developed, documented, and implemented include documented testing and approval of changes for regular and emergency changes.									
13731.13	All contractors shall comply with the updates to the listed controls under Section 50.8 – H Controls – Administrative: Amount Update: $5.5 Million revised to $6 Million. H.1: For contracts expected to exceed $6 Million in value and the performance period is 120 days or more, Contractors shall have a written Contractor Code of Business Ethics and Conduct as required by the Federal Acquisition Regulation (FAR) 3.1004 and FAR 52.203-13. To promote compliance with such code of business ethics and conduct and to ensure that all employees comply with applicable laws and regulations, contractors shall assign oversight responsibility to a member at a sufficiently high level.	X	X	X	X					BCRC, CRC, RRB-SMAC, STC
13731.14	All contractors shall comply with the updates to the listed controls under Section 50.13 – M	X	X	X	X					BCRC, CRC, RRB-SMAC

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
	Controls – Provider Enrollment. Chapter Reference Removed: [and 15]. Brackets denote removal. M.1: Review the Medicare enrollment applications (paper CMS-855 and CMS-20134 or Internet-based Provider Enrollment Chain and Ownership System enrollment application) and take appropriate action in accordance with CMS guidelines in the Publication 100-08, Chapter 10 [and 15] of the Program Integrity Manual (PIM). M.2: Reassignments of benefits are made in accordance with Publication 100-04, Chapter 1, Section 30.2 of the Medicare Claims Processing Manual and Publication 100-08, Chapter 10 [and 15] of the PIM.									
13731.14.1	All National Provider Enrollment (NPE) Contractors (e.g. NPEAST, NPWEST, & PECOS) shall submit their Control Objective M update impacts Level of Effort (LOE) via email to your assigned CMS COR due to being newly added to ECHIMP and limited in reply options.									NPEAST, NPWEST, PECOS

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
13731.15	All contractors should be aware of the updated List of Commonly Used Acronyms located in Section 70. Added: MIST & TLC Removed: XLC	X	X	X	X	X	X	X	X	BCRC, CRC, RRB-SMAC, STC

IV. PROVIDER EDUCATION

None

Impacted Contractors: None

V. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A

"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information:N/A

VI. CONTACTS

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VII. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 1

10 – Introduction

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

Chapter 7: Internal Control Requirements provides guidelines and policies to the CMS contractors in enabling them to strengthen their internal controls procedures. The CMS contracts with companies to administer the Medicare program under the Social Security Act and the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA). The contractors shall administer the Medicare program efficiently and economically in order to achieve the program objectives. Internal controls are an essential part of managing an organization. Additionally, internal controls also *serve* as the first line of defense in safeguarding assets and preventing and detecting errors and or fraud. In summary, internal controls assists government program managers in achieving desired results through effective stewardship of public resources.

End Section 10 – Introduction: Back to Table of Contents

10.2.2 - Fundamental Concepts

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

Three fundamental concepts provide the underlying framework for designing and applying the internal control standards.

A. A continuous built-in component of operations

Internal control includes measures and practices that are used to mitigate risks and exposures that could potentially prevent an organization from achieving its goals and objectives. Internal control is not one event or circumstance, but a series of actions that permeate an organization's activities. These actions are pervasive and are inherent in the way management runs the organization. Internal controls involve an organization-wide commitment that defines and implements a continuous process of assessing, monitoring, and tracking activities and risks, through an integrated and effective communication mechanism.

B. Are *affected* by people

An organization's management directs internal control, which is carried out by the people within that organization. Management's commitment to establish strong internal control affects the organization's practices. Management sets goals and policies, provides resources, and monitors and evaluates the performance of the organization. The organization's internal control environment is established by these policies and is controlled by available resources. Although internal control begins with this established environment, the employees make it work and must be adequately trained. It is the manner in which the entire organization embraces the internal control that affects their accountability and operational results.

C. Provide reasonable assurance, not absolute assurance

Reasonable assurance indicates that an internal control system, no matter how well conceived and operated, can provide only reasonable, not absolute, assurance regarding achievement of an entity's objectives, and further indicates that the likelihood of achievement of these objectives is affected by limitations inherent in all internal control systems.

Examples of limitations are:

a. Judgment - the effectiveness of controls will be limited by decisions made by human judgment under pressures to conduct business based on information at hand;

b. Breakdowns - even well designed internal controls can break down. Employees sometimes misunderstand instructions or simply make mistakes. Errors may also result from new technology and the complexity of computerized information systems;

c. Management Override - high-level personnel may be able to override prescribed policies and procedures for personal gain or advantage. This should not be confused with management intervention, which represents management actions to depart from prescribed policies and procedures for legitimate purposes;

d. Collusion - control systems can be circumvented by employee collusion. Individuals acting collectively can alter financial data or other management information in a manner that cannot be identified by control systems.

End Section 10.2.2 – Fundamental Concepts: Back to Table of Contents

20.2.1 – CMS Contractor Control Objectives

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

CMS issues broad control objectives for which contractors shall develop control activities to ensure the objectives are met. The complete list of control objectives **is** in Section 50. If your risk assessment was completed prior to issuance of the current year CMS control objectives, ensure that any new or revised control objectives are assessed and the risk matrix is updated. In addition, control activities should be created or updated to support any new or revised control objectives as appropriate (see Section 10.2.3.3). Contractors shall also include in their risk assessment any significant or material areas not covered by a CMS control objective.

End Section 20.2.1 – CMS Contractor Control Objectives: Back to Table of Contents

20.4 - Testing Methods

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

Testing the policies and procedures involves ensuring that the documented policies and procedures are actually being used as designed and are effective to meet a control objective. Evaluating and testing the effectiveness of policies and procedures is important to determine if the major areas of risks have been properly mitigated and provide reasonable assurance that the control objective is met.

Testing and evaluating the policies and procedures consists of five (5) steps:

Step 1: Select the policies or procedures to be tested

It is both impractical and unnecessary to test all policies and procedures. The policies and procedures to be tested are those that primarily contribute to the achievement of the control objectives. A policy or procedure may be eliminated from testing when it does not meet the control objective to be tested due to being poorly designed, unnecessary or duplicative, or not performed in a timely manner. However, if this justification is invoked, other policies and procedures should be tested to validate meeting the control objective. Another justification for testing elimination is due to the cost of testing the policy or procedure exceeds the value of

the control objective to be tested. If a policy or procedure is eliminated from testing, the reasoning should be documented.

Step 2: Select test methods

Once the policies and procedures to be tested are determined, test methods shall be determined. A combination of tests can be used depending on risk or type of activity. The following would be considered acceptable tests:

1. Inquiry: Asking responsible personnel if certain controls are functioning as intended (e.g., "Do you reconcile your activity or do you review a certain report each month?").

2. Inspection: Analyzing evidence of a given control procedure (e.g., searching for signatures of a reviewing official or reviewing past reconciliations).

3. Observation: Observing actual controls in operation (e.g., observing a physical inventory or watching a reconciliation occur).

4. Re-performance: Conducting a given control procedure more than once (e.g., recalculating an estimate or re-performing a reconciliation).

Observation and inquiry are less persuasive forms of evidence than inspection and re-performance.

Step 3: Determine how much testing is needed

The next sub-step is to determine the extent of the testing efforts. In most cases, it is unrealistic to observe each policy and procedure or to review 100 percent of all records. Instead, policies and procedures are tested by observing a selected number of controls performed or by reviewing a portion of the existing records. This selection process is called sampling. A representative sample provides confidence that the findings are not by chance by **considering** the factors of breadth and size.

1. Breadth: Breadth of the sample assures that the testing covers all bases and is a representative cross section of the universe being tested. This will provide confidence that the sample will lead to a conclusion about the situation as a whole.

2. Size: Size is the number of items sampled. The size should be large enough to allow a conclusion that the findings have not happened by chance and provide confidence in the conclusion. The size of the sample should not be so large that testing becomes too costly. When selecting the size of the sample consider:

    a. Experience: Reducing the size of the sample when controls have operated satisfactorily in the past and no major changes have occurred.

    b. Margin of Error: Increase the size of the sample when only a small margin of error is acceptable.

    c. Importance: Increase the size of the sample when an important resource is at stake.

    d. Type: Increase the size of the sample when the control to be tested requires judgment calls. Decrease the size of the sample when the control is routine.

Step 4: Plan data collection

The sampling plan gives an idea of the "who, where, what, when, why, and how" (see Section 20.1) aspect of the tests to be conducted. A data collection plan can be used to determine how the test results will be recorded. The accurate recording of test results is an extremely important part of the test documentation.

Planning data collection prior to beginning the testing can be very helpful to ensure the information collected will provide conclusive data from which to evaluate the controls.

Step 5: Conduct the tests

The final step of testing and evaluating controls consists of actually effectuating the testing protocol and documenting the results.

At the conclusion of the testing, the results are analyzed and evaluated. Evaluating involves reviewing the information collected and making an overall judgment on the adequacy of the internal control system as a whole. Deficient areas are to be categorized into Control Deficiencies, Significant Deficiencies, and Material Weaknesses and should be considered for inclusion in the CPIC submission (see Section 30.6).
End Section 20.4 – Testing Methods: Back to Table of Contents

30.1.1 - OMB Circular A-123, Appendix A: Internal Controls Over Financial Reporting (ICOFR)

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

CMS contractors, including A/B, DME, and Specialty MACs, MSPRC and RDS, shall use the five steps below to assess the effectiveness of its internal control over financial reporting. Documentation shall occur within each of the basic steps, whether documenting the assessment methodology during the planning phase or documenting key processes and test results during the evaluation and testing steps.

1) Plan and Scope the Evaluation

During this phase, the CMS contractor shall leverage existing internal and external audits/reviews performed (Such as SSAE 18 audits, A-123 Appendix A Internal Control Reviews, CPIC, 912 Evaluations, Federal Information Security Management (FISMA), Contractor Performance Evaluations (CPE), etc.) when conducting its assessment of internal control over financial reporting. Management shall consider the results of these audits/reviews in order to identify gaps between current control activities and the documentation of them. The control objectives of A, B, F, G, I, J, K, and L shall be considered, if applicable.

If a CMS contractor had an SSAE 18 audit, or an A-123 Appendix A Internal Control Review in the current or past two fiscal years, it shall be used as a basis for the statement of assurance combined with other audits and reviews as appropriate. The contractor shall conduct additional testing for Circular A-123 as deemed necessary (see A-123 Appendix A Internal Control Review/SSAE 18 Reliance Examples chart). For example, if the A-123 Appendix A assurance statement was unqualified, then the contractor is not required to conduct additional testing. Similarly, if the SSAE 18 audit report was unqualified (no findings in Section I (Opinion Letter)), then the contractor is not required to conduct additional testing. However, if the previous year's A-123 Appendix A assurance statement is qualified, then the contractor shall conduct additional testing on the control deficiencies identified. Similarly, if Section I of the prior year's SSAE 18 audit report is qualified (one or more findings that have not been corrected and validated), then the contractor shall conduct additional testing on the findings identified in Section I and the exceptions identified in Section III (See A-123 Appendix A Internal Control Review Reliance Examples chart). If other audits and reviews contradict the SSAE 18 audit or A-123 Appendix A Internal Control Review, then that contradiction shall be addressed via testing if the issue has not already been corrected and validated.

2) Document Controls and Evaluate Design of Controls

This step begins with the documentation and evaluation of entity-level controls. Consideration must be given to the five standards of internal control (control environment, risk assessment, control activities, information and communication, and monitoring) (see Section 10.2.3 – Standards for Internal Control) that can have a pervasive effect on the risk of error or fraud, and will aid in determining the nature and extent of internal control testing that may be required at the transaction or process level. The GAO issued an internal

control evaluation tool (The GAO Internal Control Management and Evaluation Tool) to assess the effectiveness of internal control and identify important aspects of control in need of improvement. This tool shall be used in conducting your assessment.

Contractors shall prepare cycle memos for financial reporting, accounts receivable, accounts payable, and claims expense (Note: Contractors may combine related cycles (e.g., accounts payable and claims expense). These major transaction cycles relate to significant line items on the financial reports. Cycle memos should identify the key control activities that are relied upon to assure the relevant financial statement assertions are met:

- **Existence and Occurrence:** All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date. Recorded transactions represent economic events that actually occurred during a stated period of time.

- **Rights and Obligations:** The entity legally owns all its assets collectively and all liabilities are legal obligations of the entity. Assets and liabilities reported on the Balance Sheet are bona fide rights and obligations of the entity as of that point in time.

- **Completeness:** All assets, liabilities, and transactions that should be reported have been included, and no unauthorized transactions or balances are included. All transactions during a specific period should have been recorded in that period. No unrecorded assets, liabilities, transactions or omitted disclosures.

- **Valuation or Allocation:** Assets, liabilities, revenue, and expenses have been included in the financial statements at appropriate amounts. Where applicable, all costs have been properly allocated. Assets and liabilities are recorded at appropriate amounts in accordance with relevant accounting principles and policies.

- **Presentation and Disclosure:** The financial report is presented in the proper form and any required disclosures are present. Financial statement items are properly described, classified and fairly presented.

Not all assertions will be significant to all accounts. A single key control will often not cover all assertions; which may necessitate several key controls to support the selected assertions for each line item. However, each assertion is applicable to every major transaction cycle and all associated assertions must be covered to avoid any control gaps.

Documenting transaction flows accurately is one of the most important steps in the assessment process, as it provides a foundation for the A-123 assessment. Thorough, well-written documents and flowcharts can facilitate the review of key controls. The documentation should reflect an understanding, from beginning to end, of the underlying processes and document flows involved in each major transaction cycle. This would include the procedures for initiating, authorizing, recording, processing, and reporting accounts and transactions that affect the financial reports. The cycle memo shall include Information Technology (IT) key control activities pertinent to the transaction cycle.

The documentation should start with the collection and review of documentation that already exists. The following are examples of existing documentation that could be used:

- Existing policy and procedure manuals;
- Existing forms and documents;
- Documentation from independent auditors and the OIG;
- Risk assessments;
- Accounting manuals;
- Memoranda;
- Flowcharts;

- Job descriptions;
- Decision tables;
- Procedural write-ups; and/or
- Self-assessment reports.

Interviews should be conducted with personnel who have knowledge of the relevant operations to validate that manuals, policies, forms, and documents are accurate and being applied.

A major transaction cycle narrative is a written summary of the transaction process. For each major transaction cycle, the narrative describes:

- The initiation point;
- The processing type (e.g., automated versus manual, preventative versus detective);
- The completion point;
- Other data characteristics, such as source; receipt; processing; and transmission;
- Key activities/class of transactions within the process;
- Controls in place to mitigate the risk of financial statement errors;
- Supervisor/manager review; process and calculations performed in preparation of financial reporting; and process outputs;
- Use of computer application controls and controls over spreadsheets used in the preparation of financial reporting;
- Identification of errors; types of errors found; reporting errors; and resolving errors; and
- Ability of personnel to override the process or controls.

Within the cycle memo, the key controls should be clearly identified by highlighting, bolding, or underlining. Contractors are responsible for reviewing and updating cycle memos to keep them current.

Control activities are the specific policies, procedures, and activities that are established to manage or mitigate risks. Key controls are those controls designed to meet the control objectives and support management's financial statement assertions. In other words, they are the controls that management relies upon to prevent and detect material errors and misstatements. For each key control activity, state: (a) the frequency of performance; (b) the specific steps performed; (c) how exceptions are resolved; and (d) how the performance of the control activity and related results/disposition are documented.

Examples of control activities that may be identified include:

- Top-level reviews of actual performance;
    - Compare major achievements to plans, goals, and objectives
- Reviews by management at the functional or actual level;
    - Compare actual performance to planned or expected results
- Management of human capital;
    - Match skills to organizational goals
    - Manage staff to ensure internal control objectives are achieved
- Controls over information processing;
    - Edit checks of data
    - Control totals on data files
    - Access controls
    - Review of audit logs
    - Change controls
    - Disaster recovery
- Physical controls over vulnerable assets;
    - Access controls to equipment or other assets
    - Periodic inventory of assets and reconciliation to control records
        - Establishment and review of performance measures and indicators;

    - Relationship monitoring of data
- Segregation of duties;
- Proper execution of transactions and events
    - Communicating names of authorizing officials
    - Proper signatures and authorizations
- Accurate and timely recording of transactions and events
    - Interfaces to record transactions
    - Regular review of financial reports
- Access restrictions to and accountability for resources and records; and
    - Periodic reviews of resources and job functions
- Appropriate documentation of transactions and internal control.
    - Clear documentation
    - Readily available for examination
    - Documentation should be included in management directives, policies, or operating manuals

To document management's understanding of major transaction cycles, management should use a combination of the following:

- Narratives;
- Flowcharts; and
- Control matrices.

To illustrate this process, we have provided cycle memo guidelines in Section 60. Updated cycle memos shall be submitted to the CMS Internal Controls mailbox within fifteen business days after December 31.

Note: The cycle memos must be 508 compliant when released to the Internal Controls mailbox. For information on 508 compliance, please visit the website at the following hyperlink:

Hyperlink: The US Department of Health and Human Services (HHS) Section 508 Compliance Information

In addition, the A/B, DME, and Specialty MAC contractors shall provide updated cycle memos to the SSAE 18 auditors.

3) Test Operating Effectiveness

Testing of the operation of key controls shall be performed and documented (refer to "Plan and Scope the Evaluation" (above) as well as the chart below with regard to testing applicability), to determine whether the control is operating effectively, partially effectively, or not effectively. Testing shall address both manual and automated controls. Ideally, testing should be performed throughout the year. The results of testing completed prior to June 30th will form the basis of the June 30th assurance statement. As testing continues into the fourth quarter, the results of that testing, along with any items corrected since the June 30th assurance statement will be considered in the September 30th assurance statement update. The chart below is provided to assist contractors in determining when to conduct testing.

A-123 Appendix A Internal Control Review/SSAE 18 Reliance Examples

Scenario	Prior Fiscal Year 2	Prior Fiscal Year 1	Current Fiscal Year	Additional Testing Required or Not Required*
1	No SSAE 18/A-123 Appendix A Review	No SSAE 18/A-123 Appendix A Review	Unqualified	Not Required
2	No SSAE 18/A-123 Appendix A Review	Unqualified	No SSAE 18/A-123 Appendix A Review	Not Required
3	Unqualified	No SSAE 18/A-123 Appendix A Review	No SSAE 18/A-123 Appendix A Review	Not Required
4	Qualified	Unqualified	No SSAE 18/A-123 Appendix A Review	Not Required
5	No SSAE 18/A-123 Appendix A Review	No SSAE 18/A-123 Appendix A Review	Qualified	Required
6	No SSAE 18/A-123 Appendix A Review	Qualified	No SSAE 18/A-123 Appendix A Review and the Findings are Corrected and Validated by CMS (CAP Closure Letter Received)	Not Required
7	Unqualified	Qualified	No SSAE 18/A-123 Appendix A Review and the Findings are Corrected and Validated by CMS (CAP Closure Letter Received)	Not Required
8	Qualified	No SSAE 18/A-123 Appendix A Review and the Findings are Corrected and Validated by CMS (CAP Closure Letter Received)	No SSAE 18/A-123 Appendix A Review	Not Required
9	Unqualified	Qualified	No SSAE 18/A-123 Appendix A Review and the Findings are NOT Corrected or Validated by CMS (No CAP Closure Letter)	Required
10	No SSAE 18/A-123 Appendix A Review	Qualified	No SSAE 18/A-123 Appendix A Review and the Findings are NOT Corrected or Validated by CMS (No CAP Closure Letter)	Required

Scenario	Prior Fiscal Year 2	Prior Fiscal Year 1	Current Fiscal Year	Additional Testing Required or Not Required*
11	Qualified	No SSAE 18/A-123 Appendix A Review and the Findings are NOT Corrected or Validated by CMS (No CAP Closure Letter)	No SSAE 18/A-123 Appendix A Review and the Findings are NOT Corrected or Validated by CMS (No CAP Closure Letter)	Required

Unqualified Report
SSAE 18: No findings in Section I
A-123 Appendix A Internal Control Review: No material weaknesses were noted

Qualified Report
SSAE 18: 1 or More Findings in Section I
A-123 Appendix A Internal Control Review: Material weaknesses were noted, but were not pervasive

*Note:
Assumes other subsequent audits and reviews do not contradict the SSAE 18/A-123 Appendix A Review or contradictions have been corrected and validated.

4) Identify and Correct Deficiencies

If design or operating deficiencies are noted, the potential impact of control gaps or deficiencies on financial reporting shall be discussed with management. The magnitude or significance of the deficiency will determine if it should be categorized as a control deficiency, a significant deficiency, or a material weakness (see Section 30.6).

Corrective action plans (CAPs) shall be created and implemented to remediate identified deficiencies (see Section 40). The contractor shall submit corrective action plans for all deficiencies (control deficiencies, significant deficiencies, and material weaknesses) identified as a result of A-123 Appendix A reviews and SSAE 18 Section I findings.

5) Report on Internal Controls / **Certification Statement**

The culmination of the contractor's assessment will be the assurance statement regarding its internal control over financial reporting. The statement will be one of three types:

1) Unqualified Statement of Assurance

Each contractor shall submit, as part of the CPIC report, an assurance statement for internal controls over financial reporting (ICOFR) stating:

"… (Contractor) has effective internal controls over financial reporting (ICOFR) in compliance with OMB Circular A-123, Appendix A."

NOTE: The contractor's statement of assurance should be unqualified if this is consistent with the A-123 Appendix A Internal Control Review statement per the CPA firm report (augmented by internal reviews, if necessary). Similarly, if the SSAE 18 audit (augmented by internal reviews, if necessary) did not result in any Section I findings or the contractor has not classified any findings as material weaknesses, then an unqualified statement of assurance would be applicable.

2) Qualified Statement of Assurance

Each contractor shall submit, as part of the CPIC report, an assurance statement for internal controls over financial reporting stating:

"…(Contractor) has effective internal controls over financial reporting in compliance with OMB Circular A-123, Appendix A, except for the SSAE 18 Section I finding(s) and/or material weakness(es) identified in the attached Report of Material Weaknesses."

Note: The contractor's statement of assurance should be qualified if this is consistent with the A-123 Appendix A Internal Control Review statement per the CPA firm report (augmented by internal reviews, if necessary). Similarly, if a SSAE 18 audit disclosed at least one Section I finding and/or internal reviews in the current year disclosed a material weakness, then a qualified statement of assurance (see above) or a statement of no assurance (see below) would be issued, depending on the pervasiveness of the Section I findings or material weakness. The results of work performed in other control-related activities may also be used to support your assertion as to the effectiveness of internal controls.

3) Statement of No Assurance

Each contractor shall submit, as part of the CPIC report, an assurance statement for internal controls over financial reporting stating:

"…(Contractor) is unable to provide assurance that its internal control over financial reporting was operating effectively due to the material weakness(es) identified in the attached Report of Material Weaknesses."

or

"…(Contractor) did not fully implement the requirements included in OMB Circular A-123, Appendix A and therefore cannot provide assurance that its internal control over financial reporting was operating effectively."

End Section 30.1.1 – OMB Circular A-123, Appendix A: Internal Controls Over Financial Reporting (ICOFR): Back to Table of Contents

30.9.1 – A CUECs – Information Systems

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

A – Control Objective Number	**A – CUEC Description**
A.1	CMS maintains, updates, and makes available current CMS Acceptable Risk Safeguards (ARS), Business Partners Systems Security Manual (BPSSM), and other applicable policy to provide Medicare Administrative Contractors (MACs) requirements and guidance for the establishment of an entity-wide security program.
A.3	CMS, as the Authorizing Official (AO), reviews and approves the Information System Security Categorization through the Authority to Operate (ATO) process.
A.7	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors update and / or remove user logical access accounts and system permissions as requested and approved by the MAC for transferred personnel in a timely fashion. In addition, CMS or its contractors remove logical access accounts and system permissions as requested and approved by the MAC for separated personnel in a timely fashion.
A.9	CMS, as the Authorizing Official (AO), authorizes the information system for processing prior to commencing operations and periodically thereafter. In addition, the Information Security and Privacy Group (ISPG) of CMS inputs, in a timely manner, POA&Ms into the CMS FISMA Controls Tracking System (CFACTS).
A.12	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors: • Create MAC and non-MAC user accounts (including remote access accounts, temporary, emergency, and privileged accounts if applicable) as requested and approved by the MAC. • If emergency and / or temporary accounts are utilized they are automatically removed as required by CMS standards and/or based on request by the MAC. • CMS or its contractors update information system accounts in a timely fashion based on periodic reviews conducted by the MACs.
A.13	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors remove logical access accounts and system permissions as requested and approved by the MAC for separated personnel in a timely fashion. Further, CMS or its contractors automatically disable inactive accounts as required by CMS.

A – Control Objective Number	A – CUEC Description
A.15	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors configure password based authentication for major applications / information systems in accordance with current CMS ARS, BPSSM, and other applicable policies.
A.17	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors produce and distribute security audit logs to the MACs for investigation as needed.
A.18	CMS collaborates with the MAC to analyze, respond, and report security incidents.
A.21	CMS maintains, updates, and makes available the current CMS **Target** Life Cycle (**T**LC) and other applicable policy to provide the MACs requirements and guidance for the establishment of change management and SDLC processes.
A.22	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors are responsible for software development and maintenance processes including authorization of changes, documentation, testing, and approvals in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.23	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors are responsible for properly restricting and controlling the movement of code between libraries.
A.27	For shared systems, outside of the MAC's ATO boundary, CMS or its contractors have implemented system backup and recovery procedures including contingency plans, disaster recovery plans, testing of plans, and corrective action based on lessons learned in accordance with the current CMS ARS, BPSSM, and other applicable policy.

End Section 30.9.1 – A CUECs – Information Systems: Back to Table of Contents

30.9.8 – L CUECs – Non-MSP Debt Collection

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

L – Control Objective Number	L – CUEC Description
L.1, L.3 and L.5	The initial demand letter is either manually created or systematically created in HIGLAS. The content of the initial demand letters and Intent to Refer (ITR) letters are consistent with CMS instructions.
L.1, L.3 and L.5	As under tolerance overpayments reach the threshold, HIGLAS automatically aggregates and demands the debt.
L.1, L.3 and L.5	CMS ensures the Contractor has the ability in HIGLAS to make adjustments and generate various HIGLAS reports on an as-needed basis for debt management.
L.2	*CMS Regional Office (RO) review ERS requests (only) when contractors request additional guidance. CMS Central Office will evaluate ERS requests as needed or requested by the RO.*

L – Control Objective Number	L – CUEC Description
L.3	CMS provides quarterly interest rate updates, and interest is automatically calculated by the system on the overpayment.
L.4	CMS provides guidance to the Contractor upon receipt of a notification of bankruptcy of a debtor.
L.5	CMS reviews and approves the Write-Off Reports.
L.8	CMS Systems are configured to stop collection activity once overpayment cases are updated with certain appeal statuses.
ALL	CMS accurately and timely communicates mandated regulatory requirement changes and internal policy changes.
No Corresponding Control Number	CMS establishes systematic controls to ensure recoupment of Medicare overpayments and Federal tax and non-tax debts in accordance with the Federal Payment Levy Program (FPLP), which is managed by the Internal Revenue Service (IRS).

End Sections 30.9.8 – L CUECs – Non-MSP Debt Collection and 30 – Internal Control Reporting Requirements: Back to Table of Contents

40.1 - Submission, Review, and Approval of Corrective Action Plans

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

Upon completion of any of the audits/reviews noted in Section 40, with the exception of the CPIC, the contractor will receive a final report from the auditors/reviewers noting all findings identified during their audit/review. Within 45 calendar days of the date of electronic receipt of the final report, the contractor is required to submit an Initial CAP Report, using the excel Initial CAP Report that is found in Section 40.6. The excel Initial CAP Report can be obtained via email upon request from CAPS@cms.hhs.gov. For SSAE 18, CFO, and A-123 Appendix A reviews, initial CAPS are due within 45 calendar days of the electronic receipt date of the final report. When submitting the Initial CAP Report, the email subject line shall denote the following information: Initial CAP Report, IOM entity abbreviated name (see Section 40.3, Table I), jurisdiction code, and reporting due date.

The Initial CAP Report shall address new findings that have been assigned a finding number either by the auditor/reviewer (e.g., SSAE 18 audit or A-123 Appendix A review) or by the contractor (i.e., CPIC). All entities shall submit an Initial CAP Report even if the entity has no new findings. If there are no findings, this should be annotated on the Initial CAP Report. The CAP shall summarize the procedures that have been or will be implemented to correct the finding. Upon receipt of the Initial CAP Reports, the Internal Control Team will send the reports to the appropriate CMS business owner for review of the CAP. Business owners may either approve the CAP as submitted, or may request additional information to be included in the CAP. All business owner comments shall be provided to the contractors before the due date of the next Quarterly CAP Report. Responses to the CMS business owner comments on the initial CAPs shall be included in the next Quarterly CAP Report due after the date of receipt of the comments.

After an initial CAP has been submitted, the CAP shall be merged onto the Quarterly CAP report. This report will contain all findings and CAPs that have not been closed through an official CMS CAP closure letter and provide updates to the actions taken to resolve the findings. All entities shall submit a Quarterly CAP Report even if the entity has no CAPs. If there are no open CAPs, this must be annotated on the

Quarterly CAP Report. Only one Quarterly CAP Report shall be submitted for each jurisdiction that shall include all FYs and review types, i.e., SSAE 18 audits, A-123 reviews, CFO audits, etc.

The quarterly updates will also be reviewed; however, CMS will not respond to the quarterly updates unless the CAP indicates that the contractor is not making adequate progress on implementing the CAP or has made significant changes to target completion dates.

The Quarterly CAP Report is due within 30 days following the end of each quarter. Therefore, all electronic and hardcopy CAP reports should be received by CMS on or before January 30, April 30, July 30, and October 30 annually. When submitting the Quarterly CAP report, the email subject line shall denote the following information: Quarterly CAP Report, IOM entity abbreviated name (see Section 40.3, Table I), jurisdiction code, and reporting due date. The Quarterly CAP Report shall address all open findings, as well as continue to report information on all findings reported as closed by the contractors until CMS sends the contractor a closeout letter indicating which findings are officially closed. After the contractor receives the closeout letter, the CAP shall be removed from the Quarterly CAP Report.

Submit Initial and Quarterly CAP Reports electronically to: CAPS@cms.hhs.gov. Contractors are required to furnish an electronic copy of the CAP reports to their CMS Associate IFM Administrator for Financial Management and Fee for Service Operations, and the designated IFM CFO coordinator. MACs and DME MACs shall submit initial and quarterly CAPs to the CAPS@cms.hhs.gov mail box, and the MAC COR. RDS and MSPRC shall submit initial and quarterly CAPs to the CAPS@cms.hhs.gov, and the **C**entral **O**ffice COR.

NOTE: If the electronic copy of the Initial and Quarterly CAP Reports has the Vice President (VP) of Operations electronic signature or is sent from the VP of Medicare Operations email or the CFO's email, then a hardcopy is not required to be sent to CMS. Otherwise, a hardcopy is required.

Contractors shall maintain and have available for review backup documentation to support implementation of each CAP. This will facilitate the validation of CAPS by CMS or its agents.

End Section 40.1 – Submission, Review, and Approval of Corrective Action Plans: Back to Table of Contents

40.3 - CMS Finding Numbers

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

Finding Numbers should be assigned using the following instructions. Each section of digits should be separated by a dash.

A. The first three, four, or five digits are letters, which identify the name of the contractor. Each contractor is assigned a unique set of letters listed below. Finding numbers ending with D & J are defined as follows:
   - End letter "D" represents a DME MAC (e.g. ZZZD or ZZZZD)
   - End letter "J" represents a A/B MAC (e.g. ZZZJ or ZZZZJ)

B. The second two digits are the last two numbers of the year of the review.
C. The next one digit is a letter to identify the review/audit type.
D. The last three digits are three numbers assigned sequentially to each finding type beginning with 001.

Table 1 – REVIEW/AUDIT TYPE

Findings resulting from the following types of audits or reviews should be reported using the Initial and Quarterly CAP Reports. Choose one from the following list:

Review / Audit Letter	Review / Audit Description
A	A-123 Appendix A Non-IT
C	CPIC (Your Annual Self Certification Package)
E	CFO EDP Audit
F	CFO Financial Audit
G	GAO Review (Financial Reviews)
I	A-123 Appendix A IT
M	CMS' CPIC Reviews
O	OIG Review HHS / OIG / IT Controls Assessment
P	CMS' 1522 and CMBRW Reviews
S	SSAE 18 Audit
V	CFO Related NVA / ST
W	IFM Review

Table 2 – A/B, DME, AND SPECIALTY MAC CONTRACTOR ABBREVIATIONS

A/B, DME, and Specialty MAC Contractor Name and Jurisdiction	A/B / DME / SMAC Abbreviation
Noridian Healthcare Solutions, LLC, Durable Medical Equipment (DME) MAC JA & JD	NORD
CGS Administrators, LLC, DME MAC, JB & JC	CGSD
Wisconsin Physicians Service Insurance Corporation, A/B MAC, J5 & J8	WPSJ
National Government Services, Inc., A/B MAC, J6 & JK	NGSJ
CGS Administrators, LLC, A/B MAC, J15	CGSJ
Noridian Healthcare Solutions, LLC, A/B MAC, JE & JF	NORJ
Novitas Solutions, Inc., A/B MAC, JH & JL	NOVJ
Palmetto GBA, LLC, A/B MAC, JJ & JM	PGBAJ
First Coast Service Options, Inc., A/B MAC, JN	FCSOJ
Palmetto GBA, LLC, Railroad Retirement Board (RRB) Specialty MAC (SMAC)	PGBAR

Table 3 – CONTRACTOR ABBREVIATIONS

Contractor Name and Area	Contractor Abbreviation
Novitas Solutions, Inc., Affordable Care Act Exchange Oversight Contractor	NOVA
General Dynamics Information Technology (GDIT), Benefits Coordination and Recovery Center (BCRC), Medicare Secondary Payer Recovery Contractor (MSPRC)	*BCRC*
Palmetto GBA, LLC, Pricing, Data Analysis, and Coding (PDAC)	*PDAC*
Performant, Commercial Repayment Center (CRC), MSPRC	*CRC*

Contractor Name and Area	Contractor Abbreviation
General Dynamics Information Technology (GDIT), Retiree Drug Subsidy (Part D Contractor)	*RDS*
National Government Services Financial Solutions, Innovation Payment Contractors (IPC)	*IPC*

Table 4 – SHARED SYSTEM MAINTAINER ABBREVIATIONS

Shared System Maintainer Name and Area	SSM Abbreviation
Common Working File *Maintainer* (CWF)	CWF
Fiscal Intermediary Standard System (FISS)	FISS
Multi-Carrier System (MCS)	MCS
Viable *Information Processing Systems (ViPS)* Medicare System (VMS), DME Claims Processing System	*VMS*

Table 5 – DATA CENTER ABBREVIATIONS

Data Center Name and Area	DC Abbreviation
Amazon Web Services (AWS)	*AWS*
Companion Data Services (CDS), Virtual Data Center (VDC)	CDS
Disaster Recovery as a Service (DRaaS) General Support System (GSS)	*DRaaS*
Leidos *Managed Data Center (LMDC)* – Culpepper, VA, Healthcare Integrated General Ledger Accounting System (HIGLAS)	L*MDC*
Workload A (Managed by CDS)	*WKLDA*
Workload B (Managed by CDS)	*WKLDB*

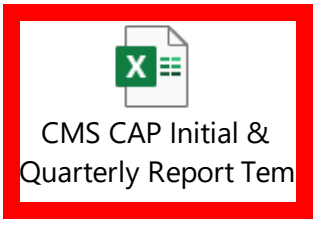
End Section 40.3 – CMS Finding Numbers: Back to Table of Contents

40.6 - CMS Initial and Quarterly CAP Report Template

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

The contractor shall use the CMS Initial and Quarterly CAP Microsoft Excel Report Template for CAP reporting. This template supersedes all prior templates issued, and can also be obtained via email upon request from: CAPS@cms.hhs.gov.

Additionally, any Initial and Quarterly CAPs questions and or concerns can be submitted to CAPS@cms.hhs.gov.



End Sections 40.6 – CMS Initial and Quarterly CAP Report Template and 40 – Corrective Action Plans: Back to Table of Contents

50.1 – A Controls – Information Systems

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

	Control Objective – Information Systems
A.1 - A.11	**Security Management:** Controls provide reasonable assurance that security management is effective.
A.1	Controls provide reasonable assurance that management has established, documented, and approved an entity-wide security program in accordance with the current CMS Acceptable Risk Safeguards (ARS), Business Partners Systems Security Manual (BPSSM), and other applicable policy including that the security program: • Is monitored and kept up-to-date in accordance with the current ARS requirements. • Includes requirements to establish a security management structure that has appropriate independence, authority, expertise, and resources. • Clearly assigns security responsibilities throughout the organization. • Ensures that management implements, maintains, and updates the organization security policy and procedures in accordance with CMS guidance.
A.2	Controls provide reasonable assurance that security risks are periodically assessed and appropriately mitigated in accordance with the current CMS ARS, BPSSM, and other applicable policy. A risk assessment and supporting activities of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated periodically based on ARS and Federal requirements. The assessment includes, but may not be limited to, identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.
A.3	Controls provide reasonable assurance that information systems and resources are categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets or individuals in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.4	Controls provide reasonable assurance that a system security plan(s) (SSP) has been documented, approved, and reviewed by management in accordance with the current CMS ARS, BPSSM, and other applicable policy. The SSP covers all major facilities and operations supporting the CMS Medicare program and is updated and maintained within CFACTS in accordance with the ARS and current version of the CMS Risk Management Handbook (RMH).
A.5	Controls provide reasonable assurance that management develops and maintains a current inventory of hardware, software, platforms, information systems, and other tools / devices that support the Medicare program in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.6	Controls provide reasonable assurance that security related personnel-policies are implemented that include performance of background investigations (initial and / or periodic) in accordance with the current CMS ARS, BPSSM, and other applicable policy.

	Control Objective – Information Systems
A.7	Controls provide reasonable assurance that security related personnel-policies are implemented that include transfer and separation procedures which require: • Review and appropriate update, if necessary, of logical and physical access rights for transferred personnel. • Exit interviews, return of property, such as keys and ID cards, timely notification to security management of separations, removal of physical and logical access to systems and escorting of separated personnel out of the facility. Performance of transfer and separation processes are in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.8	Controls provide reasonable assurance that personnel including employees, contractors, and vendors, are aware of security policies and procedures. Initial security awareness training, ongoing security awareness training, and role specific training for individuals with significant security responsibilities is documented, completed, and monitored by management. The security training program and content of training are in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.9	Controls provide reasonable assurance that management has implemented appropriate risk management and security assessment and authorization (SA&A) processes in accordance with the current CMS ARS, BPSSM, and other applicable policy including the following: • SA&A policies and procedures are documented, kept up-to-date, maintained and approved by management. • Security Assessments are planned and conducted • A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial action addressing findings noted from all security audits and reviews of IT systems, components, and operations. Plan of Action and Milestones (POA&Ms) and corrective action plans are developed and monitored to address weaknesses. • Authorizing Official (AO) authorizes the information system for processing prior to commencing any operations and periodically thereafter.
A.10	Controls provide reasonable assurance that management continuously monitors the effectiveness of the security program including security operations and completion of vulnerability assessments in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.11	Controls provide reasonable assurance that external third party activities of sub-service organizations (i.e. sub-contractors) are secure, documented, and monitored in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.12 - A.20	**Access Controls and Segregation of Duties:** Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals and that incompatible duties are effectively segregated.
A.12	Controls provide reasonable assurance that access, including remote access, to significant computerized applications (such as claims processing), accounting systems, systems software, and Medicare data are appropriately authorized, documented, reviewed, and monitored and includes approval by resource owners, procedures to control emergency and temporary access and procedures to share and properly dispose of data. Procedures are performed timely and in accordance with the current CMS ARS, BPSSM, and other applicable policy.

	Control Objective – Information Systems
A.13	Controls provide reasonable assurance that inactive logical access accounts and accounts for separated individuals are disabled and / or removed in a manner that satisfies the current CMS ARS, BPSSM, and other applicable policies.
A.14	Controls provide reasonable assurance that multifactor authentication is implemented in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.15	Controls provide reasonable assurance that password based authentication is configured in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.16	Controls provide reasonable assurance that access to sensitive system resources and privileged accounts / functions are restricted to individuals with a need-to-know and activities are appropriately logged and monitored. Additionally, Management segregates incompatible duties between various system and Medicare operations functionality which is supported by appropriate documentation, approvals, and monitoring.
A.17	Controls provide reasonable assurance that management identifies system functions, events, and access permissions that require audit logging and implements an effective audit log monitoring capability in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.18	Controls provide reasonable assurance that management has documented, implemented, and approved an effective security operations and incident response program which includes processes to: a) identify and log suspicious activity, sensitive and privileged functions, and potential security events / incidents, b) monitor systems and networks audit logs, unusual activity, and / or intrusion attempts, c) correlate log data, d) analyze potential incidents, and e) report on security events, incidents, and intrusions in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.19	Controls provide reasonable assurance that physical access to sensitive IT areas (such as Medicare facilities, data centers and system hardware) by all employees, contractors, vendors, and/ or visitors is appropriately authorized, documented, and reviewed in accordance with the current CMS MAC ARS, BPSSM, and other applicable policy.
A.20	Control number A.20 reserved. Control not in use as of this IOM revision.
A.21 - A.26	**Configuration Management:** Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended.
A.21	Controls provide reasonable assurance that configuration management policies, plans, and procedures are established, documented, kept up-to-date, and approved in accordance with the current CMS ARS, BPSSM, and other applicable policy including the following: • A System Development Life Cycle (SDLC) methodology is documented and in use and aligns with the CMS *Target* Life Cycle (*T*LC). • Change management policies and procedures that have been developed, documented, and implemented include documented testing and approval of changes for regular and emergency changes.
A.22	Controls provide reasonable assurance that Medicare application and related systems software development and maintenance activities (e.g. quarterly releases, off-quarterly releases, and emergency changes) are authorized, documented, tested, and approved in accordance with the current CMS ARS, BPSSM, and other applicable policy.

	Control Objective – Information Systems
A.23	Controls provide reasonable assurance that access to program libraries is properly restricted and movement of programs among libraries is controlled.
A.24	Controls provide reasonable assurance that management has established and consistently monitors information security related configuration for information technology in accordance with the current CMS ARS, BPSSM, and other applicable Federal standards and best practices including the following: • Develops and maintains a security configuration baseline for information technology that aligns with CMS requirements and industry standards. • Reviews the IT environment against the baseline. • Remediates misconfigurations in a timely fashion. • For misconfigurations that cannot be remediated timely, a plan of action and milestones (POA&M) or other corrective action plan is created, documented, and approved. • Deviations from CMS or other standards are analyzed and approved. • Results of periodic assessments are reported to CMS.
A.25	Controls provide reasonable assurance that management has established a vulnerability management program in accordance with the current CMS ARS, BPSSM, and other applicable policy that includes: • Scanning to identify vulnerabilities and unauthorized and unsupported software. • Disabling / removing unauthorized and unsupported software in a timely manner. • Remediation of vulnerabilities in a timely manner. • Creation of corrective action plans or POA&Ms if vulnerabilities cannot be remediated timely. Further, software is updated (patched) in a timely fashion to protect against vulnerabilities in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.26	Controls provide reasonable assurance that an effective virus, spam and spyware protection process is documented, approved, and implemented in accordance with the current CMS ARS, BPSSM, and other applicable policy.
A.27 - A.28	**Contingency Planning:** Controls provide reasonable assurance that contingency planning: (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur.
A.27	Controls provide reasonable assurance that information system backup and recovery procedures have been implemented in accordance with the current CMS ARS, BPSSM, and other applicable policy including: • Development, approval and maintenance of an up-to-date contingency plan and / or disaster recovery plan. • Periodic testing of contingency and / or disaster recovery plans. • Updating plans based on lessons learned.
A.28	Controls provide reasonable assurance that appropriate environment protections for sensitive areas such as data centers are implemented in accordance with the current CMS ARS, BPSSM, and other applicable policy.

End Section 50.1 – A Controls – Information Systems: Back to Table of Contents

50.8 – H Controls – Administrative

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

H – Control Number	Control Objective – Administrative
H.1	For contracts expected to exceed $*6* Million in value and the performance period is 120 days or more, Contractors shall have a written Contractor Code of Business Ethics and Conduct as required by the Federal Acquisition Regulation (FAR) 3.1004 and FAR 52.203-13. To promote compliance with such code of business ethics and conduct and to ensure that all employees comply with applicable laws and regulations, contractors shall assign oversight responsibility to a member at a sufficiently high level.
H.2	Procurements are awarded and administered in accordance with CMS regulations, CMS general instructions and the Federal Acquisition Regulation.
H.3	Control number H.3 reserved. Control not in use as of IOM revision number 278.
H.4	CMS management structure provides for efficient contract performance.
H.5	Records shall be maintained/retained according to the National Archives and Records Administration (NARA) guidelines, CMS implementing guidelines and other requirements, FAR guidelines and other Federal requirements, as may be identified.
H.6	Contractor's internal controls provide reasonable assurance that certain regularly scheduled processes required to support the CMS contractor's continuity of operations in the event of a catastrophic loss of relevant, distinguishable Medicare business unit facilities are performed as scheduled.

End Section 50.8 – H Controls – Administrative: Back to Table of Contents

50.13 – M Controls – Provider Enrollment

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

M – Control Number	Control Objective – Provider Enrollment
M.1	Review the Medicare enrollment applications (paper CMS-855 *and CMS-20134* or Internet-based Provider Enrollment Chain and Ownership System enrollment application) and take appropriate action in accordance with CMS guidelines in the Publication 100-08, Chapters 10 of the Program Integrity Manual (PIM).
M.2	Reassignments of benefits are made in accordance with Publication 100-04, Chapter 1, Section 30.2 of the Medicare Claims Processing Manual and Publication 100-08, Chapter 10 of the PIM.
M.3	Control number M.3 reserved. Control not in use as of this IOM revision.

End Sections 50.13 – M Controls – Provider Enrollment and 50 – List of CMS Contractor Control Objectives: Back to Table of Contents

70 – List of Commonly Used Acronyms

(Rev. 13001, Issued: 12-13-24, Effective: 10-01-24, Implementation: 01-15-25)

Acronym	Definition
A/B	Medicare Part A / B
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
AP	Account Payable
A&R	Audit & Reimbursement
AR	Account Receivable
ARS	Acceptable Risk Safeguards
ATO	Authority to Operate
BCRC	Benefit Coordination & Recovery Center
BDS	Beneficiary Data Streamlining
BPSSM	Business Partners Systems Security Manual
CAP	Corrective Action Plan
CERT	Comprehensive Error Rate Testing
CET	Continuing Education and Training
CFACTS	CMS FISMA Controls Tracking System
CFO	Chief Financial Officers Act of 1990
CMBRW	Contractor's Monthly Bank Reconciliation Worksheet
CMD	Contractor Medical Directors
CMS	Centers for Medicare and Medicaid Services
CNC	Currently Not Collectible
COR	Contracting Officer Representative
CPA	Certified Public Accountant
CPE	Contractor Performance Evaluation
CPIC	Certification Package for Internal Controls
CR	Change Request
CRAF	Collection Reconciliation Acknowledgement Forms
CRC	Commercial Repayment Center
CUECs	Complementary User Entity Controls
CWF	Common Working File
DD	Day/Date Number (01 – 31)
DME	Durable Medical Equipment
DPNA	Denial of Payment for New Admissions
ECRS	Electronic Correspondence Referral System
EDC	Enterprise Data Center
EOB	Explanation of Benefits
ERM	Enterprise Risk Management
ERS	Extended Repayment Schedule
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management
FISS	Fiscal Intermediary Standard System
FM	Financial Management
FMFIA	Federal Managers' Financial Integrity Act of 1982
FPLP	Federal Payment Levy Program
FR	Financial Reporting
FY	Fiscal Year
GAAP	Generally Accepted Accounting Principles
GAO	Government Accountability Office
GHP	Group Health Plan(s)

Acronym	Definition
GSS	General Support System
HHS	The US Department of Health and Human Services
HIGLAS	Healthcare Integrated General Ledger Accounting System
HITECH	Health Information Technology for Economic and Clinical Health
ICOFR	Internal Controls Over Financial Reporting
ICS	Internal Control Standards
ID	Identifier
IFM	Innovation & Financial Management Group
IOM	Internet Only Manual
IPRS	Improper Payment Reduction Strategy
IRL	Intent to Refer Letters
IRS	Internal Revenue Service
ISPG	Information Security and Privacy Group
IT	Information Technology
ITR	Intent to Refer
IUR	Informational Unsolicited Response
JOA	Joint Operating Agreement
MAC	Medicare Administrative Contractor
MBES	Medicaid Budget and Expenditure System
MCS	Multi-Carrier System
MD	Maryland
MM	Month Number (01 – 12)
MMA	Medicare Prescription Drug, Improvement, and Modernization Act of 2003
MR	Medical Review
MW	Material Weakness
MSP	Medicare Secondary Payer
MSPPAY	Medicare Secondary Payer Payment Module
MSPRC	Medicare Secondary Payer Recovery Contractor
MSR	Monthly Status Report
NARA	National Archives and Records Administration
NPR	Notices of Program Reimbursement
NVA/ST	Network Vulnerability Assessment / Security Testing
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDAC	Pricing, Data Analysis, and Coding
PIM	Program Integrity Manual
POA&M	Plan of Action and Milestone
POC	Point of Contact
POE	Provider Outreach and Education
PRRB	Provider Reimbursement Review Board
PTS	Provider Tracking System
Pub	Publication
QIO	Quality Improvement Organization
RA	Remittance Advice
RO	Regional Office
RAC	Recovery Audit Contractor
RCA	Root Cause Analysis
RDS	Retiree Drug Subsidy
RMH	Risk Management Handbook
RRB	Railroad Retirement Board

Acronym	Definition
RTA	Returned to Agency
SA&A	Security Assessment and Authorization
SAR	Strategy Analysis Report
SD	Significant Deficiency
SDLC	System Development Life Cycle
SMAC	Specialty Medicare Administrative Contractor
SOW	Statements of Work
SSAE 18	Statement on Standards for Attestation Engagements Number 18
SSM	Shared System Maintainer
SSP	System Security Plan
STAR	System Tracking for Audit and Reimbursement
STC	Single Testing Contractor
TDL	Technical Direction Letter
TLC	*Target Life Cycle*
TOP	Treasury Offset Program
TROR	Treasury Report on Receivables
UDR	Uniform Desk Review
UPIC	Unified Program Integrity Contractor(s)
USGAO	United States General Accounting Office
VDC	Virtual Data Center
ViPS	*Viable Information Processing Systems*
VMS	*ViPS Medicare System*
VP	Vice President
20YY	Year Number (e.g. 2019, 2020, 2021, etc.)
ZPIC	Zone Program Integrity Contractor(s)

End Section 70 – List of Commonly Used Acronyms: Back to Table of Contents