

<b>CMS Manual System</b>	<b>Department of Health &amp; Human Services (DHHS)</b>
<b>Pub 100-06 Medicare Financial Management</b>	<b>Centers for Medicare &amp; Medicaid Services (CMS)</b>
<b>Transmittal 301</b>	<b>Date : March 19, 2018</b>
	<b>Change Request 10400</b>

**Transmittal 300, dated March 16, 2018, is being rescinded and replaced by Transmittal 301, dated, March 19, 2018, to correct the implementation date on the Business Requirements page and to add the excel attachment. All other information remains the same.**

**SUBJECT: The Fiscal Year 2018 Updates for the Centers for Medicare and Medicaid Services (CMS) Internet Only Manual (IOM) 100-06 The Medicare Financial Management Manual, Chapter 7 - Internal Control Requirements**

**I. SUMMARY OF CHANGES:** This Centers for Medicare & Medicaid Services (CMS) Enterprise Electronic Change Information Management Portal (ECHIMP) Change Request (CR) contains the upcoming Fiscal Year 2018 annual document updates, and provides clarification for the Office of Management & Budget (OMB) A-123 and Internal Controls over Financial Reporting.

**EFFECTIVE DATE: October 1, 2017**

*\*Unless otherwise specified, the effective date is the date of service.*

**IMPLEMENTATION DATE: June 19, 2018**

*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.

<b>R/N/D</b>	<b>CHAPTER / SECTION / SUBSECTION / TITLE</b>
R	7/Table of Contents
R	7/10/Introduction
R	7/10.1/Authority
R	7/10.1.1/Federal Managers' Financial Integrity Act of 1982 (FMFIA)
R	7/10.2.3.3/Control Activities
R	7/20/CMS Contractor Internal Control Review Process and Timeline
R	7/20.1/Risk Assessment
R	7/20.1.1/Risk Analysis Chart
R	7/20.2/Internal Control Objectives
R	7/20.2.1/CMS Contractor Control Objectives
R	7/20.3/Policies and Procedures
R	7/20.4/Testing Methods
R	7/20.5/Documentation and Working Papers
R	7/30.1/Certification Package for Internal Controls (CPIC) Requirements
R	7/30.1.1/OMB Circular A-123 Appendix A: Internal Controls Over Financial Reporting (ICOFR)
R	7/30.2/Certification Statement
R	7/30.4/CPIC- Report of Material Weaknesses
R	7/30.5/CPIC - Report of Internal Control Deficiencies
R	7/30.7/Material Weaknesses Identified During the Reporting Period
R	7/30.8/Statement on Standards for Attestation Engagements (SSAE) Number 18, (SSAE 18) Reporting on Controls at Service Providers
R	7/40.1/Submission, Review, and Approval of Corrective Action Plans
R	7/40.2/Corrective Action Plan (CAP) Reports
R	7/40.3/CMS Finding Numbers
R	7/40.4/Initial CAP Report
R	7/40.5/Quarterly CAP Report
R	7/40.6/CMS CAP Report Template
R	7/50/List of CMS Contractor Control Objectives
N	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: 301	Date: March 19, 2018	Change Request: 10400
-------------	------------------	----------------------	-----------------------

**Transmittal 300, dated March 16, 2018, is being rescinded and replaced by Transmittal 301, dated, March 19, 2018, to correct the implementation date on the Business Requirements page and to add the excel attachment. All other information remains the same.**

**SUBJECT: The Fiscal Year 2018 Updates for the Centers for Medicare and Medicaid Services (CMS) Internet Only Manual (IOM) 100-06 The Medicare Financial Management Manual, Chapter 7 - Internal Control Requirements**

**EFFECTIVE DATE: October 1, 2017**

*\*Unless otherwise specified, the effective date is the date of service.*

**IMPLEMENTATION DATE: June 19, 2018**

## I. 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 the Centers for Medicare and Medicaid Services (CMS) to meet requirements of FMFIA, Medicare contractors shall demonstrate that they comply with FMFIA.

**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 (MMA), 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.

## II. BUSINESS REQUIREMENTS TABLE

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

Number	Requirement	Responsibility									
		A/B MAC			D M E M A C	Shared- System Maintainers				Other	
		A	B	H H H		F I S S	M C S	V M S	C W F		
10400.1	All contractors shall be aware of the updates throughout Chapter 7 – Internal Control Requirements.  See IOM Pub. 100-06, Chapter 7	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.2	All contractors shall use the codes and abbreviations in the following tables as defined in Section 40.3 – CMS Finding Numbers:	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC

Number	Requirement	Responsibility								
		A/B MAC			D M E M A C	Shared- System Maintainers				Other
		A	B	H H H		F I S S	M C S	V M S	C W F	
	<p>Table 1 - Review/Audit Type</p> <p>Table 2 - Contractor Abbreviations</p> <p>Table 3 – Shared System Maintainer Abbreviations</p> <p>Table 4 – Data Center Abbreviations</p> <p>See IOM Pub. 100-06, Chapter 7, Section 40.3.</p>									
10400.3	<p>All contractors shall provide an Initial and Quarterly Corrective Action Plan (CAP) Report using the Fiscal Year 2018 Initial and Quarterly CAP Microsoft excel template located in Section 40.6. 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.</p> <p>See IOM Pub. 100-06, Chapter 7, Section 40.6.</p>	X	X	X	X				BCRC, CDS, CRC, RRB-SMAC, STC	
10400.4	<p>All contractors shall follow the listed controls for Control Objective A – Information Systems.</p> <p>See IOM Pub. 100-06, Chapter 7, Section 50.</p>	X	X	X	X				BCRC, CDS, CRC, RRB-SMAC, STC	
10400.5	<p>All contractors shall follow the listed controls for Control Objective B – Claims Processing.</p> <p>See IOM Pub. 100-06, Chapter 7, Section 50.</p>	X	X	X	X				BCRC, CDS, CRC, RRB-SMAC, STC	
10400.6	<p>All contractors shall follow the listed controls for Control Objective C – Appeals.</p> <p>See IOM Pub. 100-06, Chapter 7, Section 50.</p>	X	X	X	X				BCRC, CDS, CRC, RRB-SMAC, STC	
10400.7	<p>All contractors shall follow the listed controls for Control Objective D – Beneficiary/Provider Services.</p> <p>See IOM Pub. 100-06, Chapter 7, Section 50.</p>	X	X	X	X				BCRC, CDS, CRC, RRB-SMAC, STC	
10400.8	<p>All contractors shall follow the listed controls for Control Objective E – Complementary Credits.</p> <p>See IOM Pub. 100-06, Chapter 7, Section 50.</p>	X	X	X	X				BCRC, CDS, CRC, RRB-SMAC, STC	

Number	Requirement	Responsibility									
		A/B MAC			D M E M A C	Shared- System Maintainers				Other	
		A	B	H H H		F I S S	M C S	V M S	C W F		
10400.9	All contractors shall follow the listed controls for Control Objective F – Medical Review (MR).  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						
10400.10	All contractors shall follow the listed controls for Control Objective G – Medicare Secondary Payer (MSP).  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.11	All contractors shall follow the listed controls for Control Objective H – Administrative.  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.12	All contractors shall follow the listed controls for Control Objective I – Provider Audit.  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.13	All contractors shall follow the listed controls for Control Objective J – Financial.  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.14	All contractors shall follow the listed controls for Control Objective K – Debt Referral (MSP and Non-MSP).  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.15	All contractors shall follow the listed controls for Control Objective L – Non-MSP Debt Collection.  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.16	All contractors shall follow the listed controls for Control Objective M – Provider Enrollment.  See IOM Pub. 100-06, Chapter 7, Section 50.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC
10400.17	All contractors should be aware of the new List of Commonly Used Acronyms located in Section 70.  See IOM Pub. 100-06, Chapter 7, Section 70.	X	X	X	X						BCRC, CDS, CRC, RRB-SMAC, STC

### III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility				
		A/B MAC			D M E D I	C
		A	B	H H H	M A C	
	None					

### IV. 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**

### V. CONTACTS

**Pre-Implementation Contact(s):** Jonathan Wong, 410-786-0414 or jonathan.wong@cms.hhs.gov , Agbeko Kumordzie, 410-786-2100 or Agbeko.Kumordzie@cms.hhs.gov , Eleanor Sheain, 410-786-8120 or Eleanor.Sheain@cms.hhs.gov , Gernard Gray, 410-786-2285 or Gernard.Gray@cms.hhs.gov , Allison French, 410-786-1485 or allison.french@cms.hhs.gov , Karen Brownley, 410-786-5451 or karen.brownley@cms.hhs.gov , Floyd Epps, 410-786-1952 or Floyd.Epps@cms.hhs.gov

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

### VI. 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**

# Medicare Financial Management Manual

## Chapter 7 - Internal Control Requirements

### Table of Contents *(Rev. 301, 03-19-18)*

#### Transmittals for Chapter 7

#### 10 – Introduction

##### 10.1 – Authority

10.1.1 – Federal Managers' Financial Integrity Act of 1982 (FMFIA)

10.1.2 – FMFIA and the CMS Medicare Contractor Contract

10.1.3 – Chief Financial Officers Act of 1990 (CFO)

10.1.4 – OMB Circular A-123

10.1.5 – GAO Standards for Internal Controls in the Federal Government

##### 10.2 – GAO Standards in the Federal Government

10.2.1 – Definition and Objectives

10.2.2 – Fundamental Concepts

10.2.3 – Standards for Internal Control

10.2.3.1 – Control Environment

10.2.3.2 – Risk Assessment

10.2.3.3 – Control Activities

10.2.3.4 – Information and Communication

10.2.3.5 – Monitoring

#### 20 – CMS Contractor Internal Control Review Process and Timeline

##### 20.1 – Risk Assessment

20.1.1 – Risk Analysis Chart

##### 20.2 – Internal Control Objectives

20.2.1 – CMS Contractor Control Objectives

##### 20.3 – Policies and Procedures

##### 20.4 – Testing Methods

##### 20.5 – Documentation and Working Papers

#### 30 – Internal Control Reporting Requirements

##### 30.1 – Certification Package for Internal Controls (CPIC) Requirements

30.1.1 – OMB Circular A-123 Appendix A: Internal Control Over Financial Reporting (ICOFR)

30.1.2 – Identify and Document Key Controls at the Major Transaction Cycle, Sub-Cycle, or Account Level

##### 30.2 – Certification Statement

##### 30.3 – Executive Summary

##### 30.4 – CPIC - Report of Material Weaknesses

##### 30.5 – CPIC- Report of Internal Control Deficiencies

##### 30.6 – Definitions of Control Deficiency, Significant Deficiency, and Material Weaknesses

##### 30.7 – Material Weaknesses Identified During the Reporting Period

##### 30.8 – Statement on Standards for Attestation Engagements (SSAE) Number 18 (SSAE 18), Reporting on Controls at Service Providers

40 – Corrective Action Plans

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

40.2 – Corrective Action Plan (CAP) Reports

40.3 – CMS Finding Numbers

40.4 – Initial CAP Report

40.5 – Quarterly CAP Report

40.6 – CMS *Initial and Quarterly* CAP Report Template

50 – List of CMS Contractor Control Objectives

60 – CMS Contractor Cycle Memo

60.1 – CMS Contractor Cycle Memo Outline

*70 – List of Commonly Used Acronyms*

## 10 - Introduction

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

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 serves 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.

### 10.1 - Authority

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) establishes internal control requirements that shall be met by CMS. For CMS to meet the requirements of FMFIA, CMS contractors shall demonstrate that they *are in compliance* with the FMFIA guidelines.

#### 10.1.1 - Federal Managers' Financial Integrity Act of 1982 (FMFIA)

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The *FMFIA* requires that internal accounting and administrative controls of each executive agency be established in accordance with the standards prescribed by the Comptroller General. Under FMFIA, the Office of Management and Budget (OMB) establishes guidelines for agencies to evaluate their systems of internal accounting and administrative control to determine such systems' compliance with the standards established by the Comptroller General.

Under the prescribed standards of the FMFIA, agencies must provide reasonable assurance to the President and Congress on an annual basis that:

1. Obligations and costs are in compliance with applicable law;
2. Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and
3. Revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts, reliable financial and statistical reports, and to maintain accountability over the assets.

#### 10.2.3.3 - Control Activities

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the organization's control objectives.

Control activities are the written activities used to support policies and procedures that help ensure management directives are carried out. Also see Section 20.3, Policies and Procedures. They help ensure that necessary actions are taken to address potential risks that may affect the organization's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliation, performance reviews, security of assets, and segregation of duties. For examples of Non-Information Systems and Information Systems control activities, *please* see *the* GAO – Internal Control Management and Evaluation Tool at *the following hyperlink*:

**Hyperlink:** [The USGAO-ICS: Internal Control Management and Evaluation Tool of August 2001 \(GAO-01-1008G\)](http://www.usgaoinc.org/ICS/ICS%20-%20Internal%20Control%20Management%20and%20Evaluation%20Tool%20of%20August%202001%20(GAO-01-1008G).pdf) [[www.gao.gov/new.items/d011008g.pdf](http://www.gao.gov/new.items/d011008g.pdf)]

## 20 - CMS Contractor Internal Control Review Process and Timeline

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

**NOTE:** The CMS timeline is provided as a guide and is not considered absolute. Contractors may use the guideline as a reference.

### *Fiscal Year Calendar of Events and Activities*

<b>MONTH</b>	<b>ACTIVITY</b>
<b>OCTOBER</b>	<ul style="list-style-type: none"> <li>Release Certification Package for Internal Controls (CPIC) Update for period July – September</li> <li>Due: Within Five (5) business days after September 30, 20XX</li> <li>Review updated IOM to evaluate changes required to your system of operations</li> </ul>
<b>NOVEMBER</b>	<ul style="list-style-type: none"> <li>Update Standard Operating Procedures</li> <li>Incorporate updated IOM changes</li> </ul>
<b>DECEMBER</b>	<ul style="list-style-type: none"> <li>Conduct a risk assessment, see Section 20.1</li> <li>Prepare a Statement on Standards for Attestation Engagements Number 18 (SSAE 18) Statement of Work for the audit (MAC &amp; DME MAC)</li> </ul>
<b>JANUARY</b>	<ul style="list-style-type: none"> <li>Award SSAE 18 contract (MAC &amp; DME MAC)</li> <li>Update and submit A-123 cycle memos to CMS central office fifteen (15) business days after December 31. See Section 30.1.1.</li> </ul>
<b>FEBRUARY</b>	<ul style="list-style-type: none"> <li>Conduct A-123 Risk Assessment, Section 30.1.1</li> </ul>
<b>MARCH</b>	<ul style="list-style-type: none"> <li>Prepare for A-123 review or SSAE 18 audit onsite reviews</li> </ul>
<b>APRIL</b>	<ul style="list-style-type: none"> <li>Update CPIC Report of Internal Control Deficiencies, Section 30.5</li> </ul>
<b>MAY</b>	<ul style="list-style-type: none"> <li>Begin preparing CPIC for all geographical locations, Section 30.3</li> </ul>
<b>JUNE</b>	<ul style="list-style-type: none"> <li>Draft Assurance Statement; Prepare to submit CAP, Sections 30.2 &amp; 40</li> </ul>
<b>JULY</b>	<ul style="list-style-type: none"> <li>Submit CPIC for period October - June</li> </ul>
<b>AUGUST</b>	<ul style="list-style-type: none"> <li>Submit Corrective Action Plans CAPs, Section 40.1</li> <li>Due: 45 days after final A-123 and/or SSAE 18 Reports</li> </ul>
<b>SEPTEMBER</b>	<ul style="list-style-type: none"> <li>Determine if new material weaknesses were identified since the interim CPIC report in July</li> </ul>

### 20.1 - Risk Assessment

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

Risk assessment identifies areas that should be reviewed to determine which components of an organization's operation present the highest probability of waste, loss, or misappropriation. The risk assessment process is the identification, measurement, prioritization, and mitigation of risks. This process is intended to provide the contractors with:

- Direction for what areas should get priority attention from management due to the nature, sensitivity, and importance of the area's operations;
- A preliminary judgment from managers about the adequacy of existing internal control policies and procedures to minimize or detect problems; and
- An early indication of where potential internal control weaknesses exist that should be corrected.

The CMS requires contractors to perform an annual risk assessment, to identify the most critical areas and areas of greatest risk to be subjected to a review. Operational managers with knowledge and experience in their particular business area shall perform risk assessments. Outside sources can assist with this process, but should not be solely relied upon (e.g., Internal Audit departments, SSAE 18 audits, OMB Circular A-123 Appendix A reviews, etc.).

When performing your yearly risk assessment, you are to consider all results from final reports issued during the fiscal year from internal and external reviews including GAO, OIG, CFO audit, Contractor Performance Evaluation (CPE), CPIC, Contractor's Monthly Bank Reconciliation Worksheet (CMBRW) and 1522 reviews, A-123 Appendix A reviews and results of your own or CMS-sponsored SSAE 18 audits. Any of these findings could impact your risk assessment and preparation of your certification statement. Your risk assessment process shall provide sufficient documentation to fully explain the reasoning behind and the planned testing methodology for each selected area.

The contractor shall submit a description of the risk assessment process to CMS as an attachment with the annual CPIC and maintain sufficient documentation to support the risk assessment process. Examples of sufficient documentation are meeting agendas, meeting notes or minutes, and emails. The documentation should be readily available for CMS review.

Below are the elements to include in the description or methodology of your risk assessment process:

- Who - List who is involved and state their roles and responsibilities.
- Where - List the geographical location(s) for which the certification applies. For multi-site contractors, review and explain the roles for all sites, i.e., do they do their own risk assessment and control objective testing. Describe the certification process for geographical locations.
- What – Describe the risk factors and the risk assessment process.
- When - List when the risk assessment process was completed.
- Why – Prioritize control objectives based upon their level of risk while ensuring high risk areas are reviewed in accordance with the scoring criteria guidelines in [Section 20.1](#).

**NOTE:** The MAC and DME MAC Statements of Work may also include requirements regarding review of CMS control objectives.

- How – Describe the scoring methodology and provide a description and definition for each risk and exposure factor. Include specific value ranges used in your scoring methodology.

The contractor is encouraged to exceed the risk assessment approach provided below based on its unique operations. The risk assessment process shall at a minimum include the following and shall be submitted as part of the CPIC package:

#### Step 1 - Segment Operations

Segment the contractor's operation into common operational areas of activity that can be evaluated. List the primary components of the unit with consideration to the business purpose, objectives, or goals of the auditable unit. Limit the list to the primary activities designed to achieve the goals and objectives of the auditable unit. Include the CMS control objectives applicable to each auditable unit.

#### Step 2 - Prioritize Risk and Exposure Factors

Identify the primary risks and exposure factors that could jeopardize the achievement of the goals and objectives of the unit as well as the organization's ability to achieve the objectives of reliable financial

reporting, safeguarding of assets, and compliance with budget, laws, regulations and instructions. Risk and exposure factors can arise due to both internal and external circumstances. Document the definitions and methodology of the risk and exposure factors used in the risk assessment process.

### Step 3 – Create a Matrix to Illustrate the Prioritization of Risk and Exposure Factors

Create a matrix listing on the left axis by operational areas of activity (see Step 1 above). The top axis should list all the risk and exposure factors of concern and determine the weight each column should have. Some columns may weigh more than other columns. Develop a scoring methodology and provide a description and definitions of this methodology used for each risk or exposure factor. This methodology can use an absolute ranking or relative risk identification. Absolute ranking would assign predefined quantifiable measures such as dollars, volume, or some other factor in ranges that would equate to a ranking score such as high, medium or low. Relative risk ranking involves identifying the risk and exposure factors into natural clusters by definition and assigning values to these clusters. Include a legend with the score ranges representing high-risk, medium-risk, and low-risk on the risk matrix.

Assign a score to each cell based on the methodology predetermined. Retain notes to support scoring of key risk factors such as “prior audits” and factors that are scored very high or very low. This will assist CMS in evaluating the reasonableness of your risk assessment results. Total the scores for each line item (control objective). The higher scores for each line item will prioritize the risk areas for consideration to be reviewed to support the CPIC. If a high risk control objective is included in a current year Type II SSAE 18 audit, or A-123 Appendix A review, you may rely on the SSAE 18 audit, or A-123 Appendix A review testing and document this as the rationale for excluding it from testing.

The CMS considers system security to be a high risk area. Therefore, contractors shall include control objective A.1 in their CPIC each year. All contractors are required to certify their system security compliance. Contractors shall verify that a system's security plan meet CMS' Minimum Security Requirements as defined by the Business Partners Systems Security Manual (BPSSM). Contractors should write a few paragraphs to self-certify that their organization has successfully completed all required security activities including the security self-assessment of their Medicare IT systems and associated software in accordance with the terms of their Contract. *For more details, please see Section 3.3 of the BPSSM, which can be found at [the following hyperlink](#):*

***Hyperlink:*** [CMS IOM Publication #: 100-17, CMS Business Partners Systems Security Manual, Revision #: 12, Issued: 11/15/2013 \[https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/117\\_Systems\\_security.pdf\]](https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/117_Systems_security.pdf)

Also, include the results of the testing of A.1 in the Executive Summary. See Section 30.3.

## 20.1.1 - Risk Analysis Chart

(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)

Table 1 -- This chart is provided to assist contractors in selecting the high-risk activities within their organization. There are 3 columns that gives directions on how to rank operational areas for potential risk.

<u>HIGH RISK FACTORS</u> (1)	<u>MEDIUM RISK FACTORS</u> (2)	<u>LOW RISK FACTORS</u> (3)
<ul style="list-style-type: none"> <li>• Recent review or audit findings showing material weaknesses related to internal control processes.</li> <li>• Areas affected by significant changes in laws, regulations, special requirements or instructions.</li> <li>• Areas where policies and procedures regarding internal control over financial reporting are not well documented.</li> <li>• Areas of significant financial vulnerabilities (e. g., new accounting or regulatory guidelines).</li> <li>• Areas where guidelines have varied interpretations and/or areas being restructured.</li> <li>• Areas with new contract activities.</li> <li>• Areas where objectives of the corporate mission could be in jeopardy if not properly implemented.</li> <li>• Areas lacking performance measures or monitoring.</li> </ul>	<ul style="list-style-type: none"> <li>• Potential program weaknesses related to violation of privacy issues.</li> <li>• Areas with high visibility.</li> <li>• Areas where due dates are often not met or responses to correspondence are late.</li> <li>• Areas with consistent complaints or inquiry.</li> <li>• Areas where there are no written policies and procedures.</li> <li>• Areas where recent policy changes were implemented.</li> <li>• Areas with reorganization activities.</li> <li>• Areas where there is a breakdown in communication with corporate, regional, state or satellite offices, etc.</li> <li>• Areas with new or problematic performance measures.</li> </ul>	<ul style="list-style-type: none"> <li>• Areas where CAPs have already been implemented.</li> <li>• Areas with low visibility; routine program operations.</li> <li>• Areas where workers are meeting routine program operations and performance targets and attitudes and staff motivations are high.</li> <li>• Areas that undergo frequent financial audits/ reviews by external parties (e.g., CFO, SSAE 18, A-123 Appendix A, CPIC, etc.).</li> <li>• Areas that managers perform periodic reviews to ensure that work assignments are performed consistently, and accurately.</li> <li>• Work activities are being phased out.</li> <li>• Areas with established and validated performance measures.</li> </ul>

### Scoring Criteria Guidelines:

**High:** If an activity has two or more high risk rating factors, review annually.

**Medium:** If an activity has two or more medium risk factors, review biannually.

**Low:** Low activities can be reviewed within a *five (5)*-year timeframe or at manager's discretion that should be balanced with costs and resources.

## **20.2 - Internal Control Objectives**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

Internal control objectives are established to identify risk and vulnerabilities. Control objectives may be set for an entity as a whole, or be targeted to specific activities within the entity. Generally, objectives fall into three categories:

1. Operations - relating to effective and efficient use of the organization's resources.
2. Financial Reporting - relating to preparation of reliable financial statements.
3. Compliance - relating to the organization's compliance with applicable laws and regulations.

An acceptable internal control system can be expected to provide reasonable assurance of achieving objectives relating to the reliability of operations, financial reporting and compliance. Achievement of those objectives depends on how activities within the organization's control are performed.

Section 50 lists the minimum set of control objectives. The contractor may add to the CMS control objective list. For the respective operational areas selected for review in Step 2 of the Risk Assessment discussion, cross-reference the high risk operational areas to CMS' or the contractor's unique control objectives on a work sheet. Some control objectives will apply to more than one operational area selected for review. The control objectives identified in this step shall be validated by documentation of the control activities (see Section 10.2.3.3) used as well as testing (see Section 20.4) that supports the control objectives.

Reminder: Excessive control is costly and counterproductive. Too little control presents undue risk. There should be a conscious effort made to achieve an appropriate balance.

### **20.2.1 – CMS Contractor Control Objectives**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The complete list of control objectives is in Section 50. If you completed your risk assessment prior to issuance of the current year CMS control objectives, you should ensure that any new or revised control objectives are assessed and the risk matrix is updated. In addition, you should create or update the control activities supporting any new or revised control objectives as appropriate (see Section 10.2.3.3).

## **20.3 – Policies and Procedures**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

Policies and procedures are a set of established guidelines or rules for conducting the affairs of a business. Good policies:

- Are written in clear, concise, and simple language. They are updated as necessary, signed and dated.
- Address what the guideline or rule is; not how to implement the guideline or rule.
- Are readily available and properly communicated to staff.

Procedures are a set of steps in a plan intended to influence and determine decisions and actions. Good procedures are tied to policies and:

- Are written in clear, concise, and simple language.
- Are tied to the policy.

- Are developed and implemented with the user in mind.
- Are readily available and properly communicated to staff.

Contractors shall have written policies and procedures to achieve their control objectives. These policies and procedures shall be updated in a timely manner to reflect changes in CMS instructions or your internal operations.

Contractors shall demonstrate and document that its policies and procedures are actually being used as designed and are effectively and efficiently meeting the control objective, as described in Section 50. Evaluation and testing of the effectiveness of controls are important in determining if the major areas of risk have been properly mitigated.

An example of a policy is, “an agency shall establish physical control to secure and safeguard vulnerable assets”. The specific control activities, or procedures, which support this policy may include: all doors to the facility have locks, the locks only have one key, all keys are held by security guards, security guards are stationed at every door.

## 20.4 - Testing Methods

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

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 taking into account 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).

## **20.5 - Documentation and Working Papers**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The contractor shall document through its working papers, the process it employed to support its internal control certification. This documentation shall include working papers so that a CMS reviewer can conclude that the Risk Assessment process as described in Section 20.1 follows or exceeds these guidelines, and that the Control Activities (Section 10.2.3.3) identified to support the high risk control objectives selected for review are current and clearly stated. Finally, the CPIC documentation shall demonstrate how the Testing Methods employed comply with the general parameters as described in Section 20.4 for the purpose of Control Activity validation.

Working papers contain evidence accumulated throughout the review to support the work performed, the results of the review, including findings made, the judgment and/or conclusion of the reviewers. They are the records kept by the reviewer of the procedures applied, the tests performed, the information obtained, and the pertinent judgment and/or conclusions reached in the review process. Examples of working papers are review programs, analyses, memoranda, letters of confirmation and representation, abstracts of documents, and schedules or commentaries prepared or obtained by the reviewer. Working papers may be in the form of data stored on tapes, film, or other media.

General Content of Working Papers - Working papers should ordinarily include documentation showing that:

- The work has been adequately planned and supervised.
- The review evidence obtained, the reviewing procedures applied, and the testing performed has provided sufficient, competent evidential matter to support the reviewer's judgments and/or conclusions.

Format of Working Papers - Working paper requirements should ensure that the working papers follow certain standards. As a whole, a good set of working papers should contain the following:

- The objectives, scope, methodology, and the results of the review.
- Proper support for findings, judgments and/or conclusions, and to document the nature and scope of the work conducted.
- Sufficient information so that supplementary oral explanations are not required.
- Adequate indexing and cross-referencing, and summaries and lead schedules, as appropriate.
- Date and signature by the preparer and reviewer.
- Evidence of supervisory review of the work.
- Proper heading should be given to the basic content of the working papers.

## **30.1 – Certification Package for Internal Controls (CPIC) Requirements**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The contractor self-certification process provides CMS with assurance that contractors are in compliance with the FMFIA, OMB Circular A-123, and CFO Act of 1990 by incorporating internal control standards into their operations. The contractor self-certification process supports the audit of CMS' financial statements by the Office of Inspector General (OIG) and the CMS Administrator's FMFIA assurance statement.

This compliance is achieved by an annual self-certification statement and has been known as a CPIC. Through these self-certification statements, CMS has required each contractor to provide assurances that internal controls are in place and to identify and correct any areas of weakness in its operations. Contractors are expected to evaluate the effectiveness of their operations against CMS' control objectives discussed above. The control objectives represent the minimum expectations for contractor performance in the area of internal controls.

Contractors shall have written policies and procedures regarding their overall CPIC process and the preparation of the annual CPIC submission. They shall also have written policies and procedures that discuss the handling of potential internal control deficiencies identified by employees and managers in the course of their daily operations. This should include the process for reporting issues upward through the appropriate levels of management, tracking them to completion of any necessary corrective actions, and considering them for inclusion in the CPIC submission.

The CPIC represents a summary of your internal control environment for the period October 1 through June 30 (the CPIC period), as certified by your organization. It shall include an explicit conclusion as to whether the internal controls over financial reporting are effective (see Section 30.1.1). All material weaknesses that were identified during this period shall be included in the CPIC submission. You should consider the results of final reports issued from internal and external audits and reviews, such as GAO and OIG audits as well as CFO Act audits, consultant reviews, management control reviews, CPE reviews, SSAE 18 audits, A-123 Appendix A reviews and other similar activities. These findings should be classified as control deficiencies, significant deficiencies, or material weaknesses based upon the definitions provided in Section 30.6.

The contractor shall submit one CPIC report for each type of contract, i.e., Medicare Administrative Contractor (MAC) workload, Durable Medical Equipment (DME) MAC workload, Retiree Drug Subsidy (RDS), and Medicare Secondary Payer Recovery *Contractor* (MSPRC) workloads. The contractor shall follow these guidelines when submitting the CPIC for MACs and the DME MACs:

- Contractors with multiple MACs shall submit a CPIC for each MAC.
- DME MACs shall submit a CPIC for each DME MAC.
- Contractors that transitioned out of the program prior to June 30, and are not assuming additional workloads are not required to submit a CPIC.

Electronic CPIC reports shall be received by CMS within fifteen business days after June 30. The contractor is not required to submit a hard copy report if it has the capability to insert electronic signatures or if the CPIC is sent from the VP of Operations' email or the CFO's email. Where applicable, the CPIC hard copy report shall be post marked within fifteen business days after June 30, and mailed to the following address:

Centers for Medicare & Medicaid Services  
Office of Financial Management  
7500 Security Boulevard, Mailstop C3-13-08  
Baltimore, MD 21244-1850  
Attn: Internal Control Team

The CPIC shall include:

- A Certification Statement (including an assurance statement on the effectiveness of internal controls over financial reporting as of June 30, see Section 30.2);
- An Executive Summary;

- A description of your risk assessment process. This should include a matrix to illustrate the prioritization of risk and exposure factors and a narrative or flowchart that outlines the risk assessment process (see Section 20.1 for more details regarding the risk assessment), and
- A CPIC Report of Material Weaknesses.

Contractors shall submit an update for the period July 1 through September 30 to report subsequently identified material weaknesses. The update shall be no more than a one page summary of the material weakness(es) and the proposed corrective action. If no additional material weaknesses have been identified, submit the following: “No material weaknesses have been identified during the period July 1 through September 30; therefore no additional material weaknesses have been reported”. The submission of the update should follow the same guidelines as the initial CPIC. The CPIC update is due within five business days after September 30. A CAP shall be completed in accordance to the guidelines shown at Section 40.1.

An electronic version of all documents (including updates) submitted as part of your CPIC submission shall be sent to CMS at [internalcontrols@cms.hhs.gov](mailto:internalcontrols@cms.hhs.gov) as Microsoft Excel or Word files. Electronic copies shall also be sent as follows:

- MACs and DME MACs shall send to the ARA for Division of Financial Management and Fee for Service Operations, RO CFO Coordinator, and the Contracting Officer’s Representative (COR) of the MAC or DME MAC.
- RDS and MSPRC shall send to the CMS COR.

The file names for all electronic files submitted, as part of your CPIC package should begin with the three, four, or five letter abbreviation assigned to each contractor in Section 40.3. Additionally, in the subject line of your email submission, you shall include the corporate name of the entity submitting the CPIC.

Maintain the appropriate and necessary documents to support any assertions and conclusions made during the self-assessment process. In your working papers, you are required to document the respective policies and procedures for each control objective reviewed. These policies and procedures should be in writing, be updated to reflect any changes in operations, and be operating effectively and efficiently within your organization.

The supporting documentation and rationale for your certification statement, whether prepared internally or by an external organization, shall be available for review and copying by CMS and its authorized representatives.

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

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

CMS contractors, including MACs, DME 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 SSAE 16/18 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 16/18 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 16/18 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 16/18 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 16 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 16/18 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 MAC and the DME 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 30<sup>th</sup> will form the basis of the June 30<sup>th</sup> assurance statement. As testing continues into the fourth quarter, the results of that testing, along with any items corrected since the June 30<sup>th</sup> assurance statement will be considered in the September 30<sup>th</sup> 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 16/18 Reliance Examples

<b>Scenario</b>	<b>Prior Fiscal Year 2</b>	<b>Prior Fiscal Year 1</b>	<b>Current Fiscal Year</b>	<b>Additional Testing Required or Not Required*</b>
1	No SSAE 16/A-123 Appendix A Review	No SSAE 16/A-123 Appendix A Review	Unqualified	Not Required
2	No SSAE 16/A-123 Appendix A Review	Unqualified	No SSAE 18/A-123 Appendix A Review	Not Required
3	Unqualified	No SSAE 16/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 16/A-123 Appendix A Review	No SSAE 16/A-123 Appendix A Review	Qualified	Required
6	No SSAE 16/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 16/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

<b>Scenario</b>	<b>Prior Fiscal Year 2</b>	<b>Prior Fiscal Year 1</b>	<b>Current Fiscal Year</b>	<b>Additional Testing Required or Not Required*</b>
10	No SSAE 16/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
11	Qualified	No SSAE 16/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 16/18: No findings in Section I

A-123 Appendix A Internal Control Review: No material weaknesses were noted

Qualified Report

SSAE 16/18: 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 16/18 Section I findings.

#### 5) Report on Internal Controls

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 16/18 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.”

## **30.2 - Certification Statement**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

Provide a certification statement to CMS pertaining to your internal controls. Listed below is a generic certification statement. This statement should be included as part of your CPIC. The statement is to be signed jointly by your Medicare CFO and Vice President (VP) for Medicare, RDS or MSPRC or the equivalent Senior Executive responsible for Medicare, RDS or MSPRC. The CPIC is due within fifteen business days after June 30 and shall cover the period from October 1 through June 30. An updated assurance statement for the period July 1 through September 30 is due to CMS within five business days after September 30. Your certification statement should follow this outline:

Chief Financial Officer  
Office of Financial Management  
Attn: Accounting Management Group, **C3-13-08**  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard  
Baltimore, MD 21244-1850

Dear Chief Financial Officer:

As the (Chief Financial Officer and Vice President of (contractor name)), we are writing to provide certification of reasonable assurance for the period October 1 through June 30 that (contractor name) internal controls are in compliance with the Federal Managers'

Financial Integrity Act (FMFIA) and Chief Financial Officers (CFO) Act by incorporating internal control standards into our operations. We are also providing an unqualified [or qualified] statement of assurance that (contractor name) has effective internal controls over financial reporting in compliance with revised 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].

We are cognizant of the importance of internal controls. We have taken the necessary actions to assure that an evaluation of the system of internal controls and the inherent risks have been conducted and documented in a conscientious and thorough manner. Accordingly, we have included an assessment and testing of the programmatic, administrative, and financial controls for the (type of program) operations.

In the enclosures to this letter, we have provided an executive summary that identifies a list of the minimum requirements. (See Section 30.3 Executive Summary for the list of minimum requirements to be provided in your CPIC.)

If material weaknesses have been identified, use the following language: "Material weaknesses have been reported to you and the appropriate regional office, and/or COR. The respective Corrective Action Plans have been forwarded to your office." If no material weaknesses were identified, use the following language: "No material weaknesses have been identified during our review; therefore no material weaknesses have been reported."

We have included a description of our risk assessment analysis and our CPIC Report of Material Weaknesses. This letter and attachments summarize the results of our review. We also understand that officials from the Centers for Medicare & Medicaid Services, Office of Inspector General, Government Accountability Office, or any other appropriate Government agency have authority to request and review the working papers from our evaluation.

Sincerely,

(Chief Financial Officer Signature)

(Vice President for (type of program) Signature)

## **30.4 - CPIC- Report of Material Weaknesses**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The CPIC Report of Material Weaknesses (MW) shall include all initial MW identified during the CPIC period and not yet corrected and approved by a CAP closing letter. This report shall be updated as new findings are identified. It shall be prepared as a spreadsheet and include the following columns of information:

1. CMS Finding Number. The contractor shall use the CMS finding number assigned in the final audit report for all external findings. Assign a CMS finding number (see Section 40.3) to all internally-identified MWs. This shall be done as soon as the determination is made that the finding is a MW. Note: Information related to each MW should be on only one row of the spreadsheet; the "wrap text" function in Excel should be used.
2. Control Objective Impacted (see Section 50). Each MW shall have at least one control objective associated with it. However, a MW could have more than one control objective associated with it. If more than one control objective is impacted by the MW, the finding shall be listed only once with multiple control objectives listed with it. Prioritize the control objectives impacted by each finding and limit them to no more than five.
3. Summary of the material weakness.
4. Corrective action plan (CAP).
5. Date the MW was first identified at the contractor level.
6. Date initial CAP submitted to CMS.
7. CAP target completion date.
8. Actual completion date.
9. Original source of the finding. If the original source is a Contractor Performance Evaluation review, you shall include the report date and site location of the review. If the original source is an internal control review to support your CPIC certification, identify the MW either FMFIA or financial reporting (FR).

## EXAMPLE REPORT OF MATERIAL WEAKNESSES

### CMS Contractor XYZ

#### CPIC Report of Material Weaknesses

(1) CMS Finding Number	(2) Control Objective (s) Impacted	(3) Summary of the MW	(4) Corrective Action Plan (CAP)	(5) Date MW Identified at the contractor level	(6) Date Initial CAP Submitted to CMS	(7) CAP Target Completion Date	(8) Actual Completion Date	(9) Original Source of Finding
XYZ-XX-C-001	J.4	One individual opens Medicare checks and records them in the cash receipts log. This indicates inadequate separation of duties for this process.	Duties of opening mail and logging in cash receipts are being assigned to separate individuals.	02/03/20XX	02/27/20XX	03/15/20XX	03/15/20XX	Internal Review
XYZ-XX-C-002	J.3	There is no integrated general ledger accounting system to adequately track all Medicare financial data.	The services of a consulting firm have been obtained to develop an integrated general ledger system for reporting Medicare financial data.	02/20/20XX	02/27/20XX	04/30/20XX	To be determined	Internal Review
XYZ-XX-S-001	A.1	No Entity Wide Security Plan	Create an entity Wide Security Plan	03/01/20XX	03/10/20XX	6/30/20XX	To be determined	SSAE 18 Audit

**Reporting Period FY XXXX**

### **30.5 – CPIC - Report of Internal Control Deficiencies**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The CPIC Report of Internal Control Deficiencies is an internal report and it shall include control deficiencies, significant deficiencies, and SSAE 18 Section III/IV findings. The CPIC report of Internal Control Deficiencies shall not be submitted as part of the annual CPIC submission. However, you are required to report in the Executive Summary the number of control deficiencies and significant deficiencies identified during the period covered by the CPIC. The CPIC Report of Internal Control Deficiencies should be prepared as a spreadsheet and include the following columns of information:

1. The original source of the finding.
2. The type of control deficiency (control deficiency or significant deficiency).
3. Whether it is a design deficiency or operating deficiency.
4. The control objective numbers impacted (from **Section 50**).
5. The corrective action plan.
6. A summary of the control deficiency and significant deficiencies including when the condition was observed and if a corrective action plan was implemented (or the status if not corrected).

Each control deficiency and significant deficiency shall be listed, and the total number of control deficiencies and significant deficiencies shall be included in the report. The contractors are required to prepare and maintain this report internally and update this report as new control deficiencies are identified. It shall be available for review by CMS central and/or regional office staff. When CPIC control deficiencies are identified, evaluate internal corrective actions for each of the deficiencies and correct each problem. While you are required to document, track, and correct problems identified as control deficiencies, significant deficiencies and material weaknesses, CPIC CAPs are not required to be submitted to CMS for control deficiencies and significant deficiencies.

### **30.7 - Material Weaknesses Identified During the Reporting Period**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The evaluation of your internal control environment should be an ongoing process throughout the fiscal year. It should not be a once-a-year event, which occurs prior to submission of your annual CPIC. The identification and reporting of material weaknesses should not wait until the end of the CPIC reporting period. During the reporting period, if material weaknesses are identified, send an electronic Initial CAP report within 45 days of identifying the problem, via E-mail, to [CAPS@cms.hhs.gov](mailto:CAPS@cms.hhs.gov). (See **Section 40.4**). Within that same time frame MACs and DME MACs are required to provide written notification, to your Associate Regional Administrator for Financial

Management and Fee for Service Operations, RO CFO Coordinator, and the COR of the MAC or DME MAC, RDS and *MSPRC* shall send to the CMS COR.

**30.8 – Statement on Standards for Attestation Engagements (SSAE) Number 18, (SSAE 18) Reporting on Controls at Service Providers**  
*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

**NOTE:** This section would only be applicable to MACs and DME MACs.

In lieu of receiving an A-123 Appendix A review, MACs/DME MACs are required to undergo a SSAE 18 Type II audit. The MAC/DME MAC shall contract with an independent certified public accounting (CPA) firm to perform this audit in accordance with the requirements below. The MAC/DME MAC shall follow its respective internal procurement process for contracting with the independent CPA firm or contact CMS Office of Acquisition and Grants Management for assistance.

To maintain independence in the appointment, compensation, and oversight of the audit work of the CPA firm, the MAC/DME MAC shall utilize its internal audit function, a board of directors, an audit committee, or an area external to the CFO's responsibilities. This requirement is similar to the requirements under the Sarbanes Oxley Act of 2002, Title III - Corporate Responsibility, Public Law 107-204-July 30, 2002. The CPA firm must have experience in SSAE 16/18 Type II audits, Medicare operations and accounting and financial reporting. Key personnel shall have at least five years experience in Medicare operations with experience in American Institute of Certified Public Accountants (AICPA) consulting standards, and have a technical proficiency in internal controls and financial reporting. MACs shall ensure that SSAE 18 Type II audits are in compliance with the AICPA standards and state licensing regulations.

To ensure that the SSAE 18 Type II audit is complete and in compliance with AICPA Standards, MACs shall perform due diligence to obtain assurance and representations from the CPA firm that applicable state licensing regulations are followed and that relevant disclosures are provided. In addition, MACs shall complete the SSAE Checklist, which identifies the AICPA requirements of a SSAE 18 Type II audit report, including AICPA - SSAE 18, Reporting on Controls at a Service Organization, effective May 1, 2017, paragraph 7 - Complementary User Entity Controls. MACs shall submit the SSAE 18 Checklist along with the draft SSAE and Corrective Action Plan (CAP) Follow Up reports to the CMS Internal Control Team at [Internalcontrols@cms.hhs.gov](mailto:Internalcontrols@cms.hhs.gov) by June 15.

## SSAE 18 Type II Audit Report Checklist

<b>AB/DME MAC:</b>
--------------------

**The objective of this checklist is to evaluate whether the SSAE 18 Type II Audit is in compliance with AICPA Standards, state licensing regulations and in accordance with Internet Only Manual, Publication 100-06, Medicare Financial Management Manual, Chapter 7, Internal Control Requirements. The MAC shall review the SSAE 18 Type II Audit Report and check "yes" or "no" for each requirement. If the requirement is not met, the MAC shall follow-up with the CPA firm and indicate in the comment section the action(s) for meeting the requirement. The MAC shall ensure these requirements are reflected in the final report. If the MAC has any questions or comments, please contact your COR and copy the CMS Internal Control Team at [internalcontrols@cms.hhs.gov](mailto:internalcontrols@cms.hhs.gov).**

Type II Audit Requirements	Yes	No	Comments and Follow-up Action(s) as Required
<b>I. SSAE 18 Type II Audit Report</b>			
1. Does the title of the SSAE Report indicate it is for the period October 1, YYYY through March 31, YYYY?			
2. Is the Independent Service Auditor's Report (Section I) signed and dated by the CPA firm and include the City/State of the issuing office?			
3. Are there any deficiencies identified in the SSAE 18 Report Auditors' Opinion Section (Section I)?			
4. Did the CPA firm include a spreadsheet or table in Section I of the Report and include Finding Number, Description of the Finding, and Control Objective Number impacted?			
5. Were the appropriate control objectives tested? The initial audit for new MACs/DME MACs (which includes cases where outgoing MACs transition to a new MAC) must review all 12 or 13 applicable control objectives. Existing MACs/DME MACs must have the core 8 control objectives tested (see IOM Chapter 7, Section 30.8)			
6. Does the report include the following components? 1) Opinion, 2) Management's Assertion (placement may vary), 3) Description of System and Controls, 4) Control Objectives, Activities, Testing, and Results (including disclosure of sample sizes when exceptions are identified).			
7. Did the service auditor report on 3 elements of the system for the entire period covered by the report? 1) Fairness of presentation, 2) Suitability of design, and 3) Effectiveness of operation.			
<b>II. Corrective Action Plan Report</b>			
1. Is the Corrective Action Plan Report signed and dated by the CPA firm and include the City/State of the issuing office?			
2. Did the CPA firm include the specific procedures and testing performed to validate closure of each CAP reviewed?			
3. For each open CAP, did the CPA firm make a recommendation to close or to keep the CAP open?			
<b>III. AICPA Standards</b>			
1. Is the CPA firm in compliance with AICPA standards and state licensing regulations?			
2. Did the service auditor include Complementary User Entity Controls or CUECs in the final report? CUECs are controls that reside at the user organization (CMS). These controls are usually delineated in the SSAE 18 reports within their own report subsection and/or next to the control objectives they relate.			

<b>IV. Overall Comments/Observations</b>

<b>V. Supervisory Review and Approval</b>
---

This section is for Supervisory review, comment and approval.

<b>Review Performed By:</b> _____	<b>Date :</b> _____
<b>CFOSignature:</b> _____	<b>Date :</b> _____

The initial audit (for new MACs, which include cases where outgoing MACs transition to a new MAC) shall include all of the CMS Control Objective areas described in Section 50 of this IOM. In subsequent years, the control objectives for financial, MSP, non-MSP, information systems, debt referral, medical review, provider audit, and claims processing shall be audited. In addition, the contractor shall conduct a risk assessment regarding the remaining Control Objectives and have them audited if the risk assessment warrants such a conclusion. The scope of the audit begins October 1st of each fiscal year and ends no earlier than March 31 (6 months). Furthermore, subcontractors to the Contractor shall be included in the audit if the services they provide directly impact the financial statements of the MAC/DME MAC.

The MAC/DME MAC shall keep CMS informed of the progress of the SSAE 18 audit. This shall be performed as follows:

**Entrance Conference** - The CPA firm shall conduct an entrance conference with the MAC/DME MAC before the start of each engagement to discuss the scope, timeframe (including estimated fieldwork start and finish dates), and any other issues relating to the engagement. The MAC/DME MAC shall notify the individual Business Function Leads (BFLs), COR, and Technical Monitors (TMs) via email, as well as, the A-123 Technical Team (ATT) at [internalcontrols@cms.hhs.gov](mailto:internalcontrols@cms.hhs.gov) of the date and time of the entrance conference at least five days prior to its occurrence. The BFLs, COR, TMs and ATT reserve the right to participate in the entrance conference on-site or by teleconference.

**Status Meetings** - The CPA firm shall conduct status meetings, at least bi-weekly, with the MAC/DME MAC. The status meetings shall include discussion of the activities performed during the period prior to the status meeting (including CAP Follow Up Review activities, if applicable), significant findings/potential issues identified thus far, and any concerns that may affect the completion of the work. The MAC/DME MAC shall notify the BFLs, COR, TMs and ATT of the dates and times of the status meetings at least five days prior to their occurrence. The MAC/DME MAC shall provide a copy of the written status report outlining activities performed during the period prior to the status meeting (including CAP Follow Up activities, if applicable), any significant findings/potential issues identified thus far, and any concerns that may affect the completion of the work. The BFLs, COR, TMs, and ATT reserve the right to participate in the status meetings on-site or by teleconference.

**Exit Conference** – The CPA firm shall conduct an exit conference with the MAC/DME MAC after the release of the draft SSAE 18 report to provide a summary of the review areas and the estimated final report issuance date. The scheduling of the final exit conference shall provide adequate time for the MAC/DME MAC to review the draft report. The MAC/DME MAC shall notify the BFLs, COR, TMs and ATT of the date and time of the exit conference at least five days prior to its occurrence. The BFLs, COR, TMs and ATT reserve the right to participate in the exit conference on-site or by teleconference.

The CPA firm(s) shall deliver to the contractor a matrix in the form of a Microsoft Excel spreadsheet or Microsoft Word table to report all SSAE 18 findings in Sections I and III/IV of the report. The matrix must include:

- a. Finding Number (the CPA firm shall number the findings in accordance with Section 40.3)
- b. Description of the Finding
- c. Control Objective Number Impacted (limited to 5)

The CPA firm shall, if applicable, conduct Corrective Action Plan (CAP) Follow up Reviews for prior CAPs as part of the engagement. If or when the contractor has open prior year CAPs for the CPA firm to follow up on, the contractor may make recommendations to the CPA firm and/or check with CMS/OFM to verify what CAPs should be followed up on. Prior year CAPs are defined as any CAPs reported to CMS for any reviews/audits listed in Section 40. The CPA firm shall review the CAPs to ensure that corrective actions have been implemented and that the CAPs are operating effectively. The CPA firm shall make a recommendation to the Contractor whether or not to close the CAP or have it remain open. If testing is needed in addition to that performed for the required control objective areas, it shall be completed.

The CPA firm shall deliver a CAP Follow up Report to the Contractor. The report shall contain a Microsoft Excel spreadsheet or Microsoft Word table to report the status of all prior year CAPs. The matrix shall include:

- a. Finding Number
- b. Business Area
- c. Description of the Finding
- d. Corrective Action Plan
- e. Verification/Testing Methodology
- f. Correction Status
- g. Recommendation

Copies of the draft SSAE 18 and CAP Follow Up reports shall be issued and provided to CMS by June 15<sup>th</sup>. These documents shall be submitted electronically to the CMS Internal Control Team at [internalcontrols@cms.hhs.gov](mailto:internalcontrols@cms.hhs.gov), as well as to the BFLs, COR, and TMs. The target date for CMS comments back to the contractor is one week subsequent to issuance of the draft reports. Copies of the final SSAE 18 and CAP Follow Up reports shall be issued and provided to CMS by July 1<sup>st</sup>. These documents shall be submitted electronically to the e-mail address and noted parties above, as well as in hardcopy to:

Centers for Medicare & Medicaid Services  
Office of Financial Management  
7500 Security Boulevard, Mailstop C3-13-08  
Baltimore, MD 21244-1850  
Attn: Internal Control Team

Work papers and supporting documentation shall be made available upon request to any party designated by CMS. The CMS reserves the right to request and review work papers resulting from SSAE 18 audits and CAP Follow Up Reviews.

In addition to the SSAE 18 audit, MACs are required to submit a bridge letter attesting to the internal controls environment for the remaining fiscal year period (April 1 to September 30). This bridge letter is critically important to the maintenance and demonstration of a strong internal control environment that supports the CMS internal control objectives: effective and efficient operations, reliable reporting, and compliance with applicable laws and regulations. The bridge letter is due within five business days after September 30 and should be submitted via email to [InternalControls@cms.hhs.gov](mailto:InternalControls@cms.hhs.gov). The bridge letter shall be signed by the Chief Financial Officer (or designee).

MACs may use the attached sample language as the basis for their bridge letter or they may submit original language. At a minimum, the bridge letter shall have these key points addressed:

- **Name of CPA firm who prepared the latest SSAE 18 report;**
- **Date the SSAE 18 report was issued;**
- **Audit period covered by the most recent SSAE 18 report;**
  
- **The date the service organization is providing this assertion (through the date of the bridge letter or the as of date provided in the request for the bridge letter);**
- **Any material changes to the internal control environment (if applicable);**
- **Statement that the service organization is not aware of any material changes to the control environment;**
- **Statement that user entities are responsible for adhering to complementary user entity control from SSAE 18 report;**
- **Disclaimer that the bridge letter is not a substitute for the actual SSAE 18 report.**

The bridge letter will be reviewed by the CMS A-123 Technical Team (ATT) for compliance. If there are any questions regarding the letter, the ATT will contact the MAC point of contact, if necessary.

**Sample Bridge Letter - No Material Changes:**

[Current Date]

**Bridge Letter**

Centers for Medicare & Medicaid Services  
Office of Financial Management  
7500 Security Boulevard, Mailstop C3-13-08  
Baltimore, MD 21244-1850  
Attn: Internal Control Team

Dear CMS Internal Controls Team:

We have received your request for information regarding material changes in internal control related to the [list services here (A/B MAC or DME MAC)]. [CPA firm name] prepared the latest Type II SSAE 18 for these services and the report is dated [report date]. This report includes tests of operating effectiveness for the period ending [period end date].

[Name of MAC or DME MAC] recognizes the need to maintain an appropriate internal control environment and report upon the effectiveness, as well as material changes to its internal controls. As of [current date], I am not aware of any material changes in our control environment that would adversely affect the Auditor's Opinion reached in the [report end date (not the same as the report date)] report for the above named SSAE 18.

You should also be aware that [MAC or DME MAC name], as a normal part of its operations, continually updates its services and technology as appropriate. In addition, the controls for all of [MAC or DME MAC name] services were designed with certain responsibilities required of the system users (See Complimentary User Entity Control in the SSAE 18 report). [MAC or DME MAC name] controls must always be evaluated in conjunction with an assessment of the strength of these user controls.

Finally, in order to conclude upon the design and effectiveness of internal controls for [MAC or DME MAC name], you must read the current SSAE 18 report. This letter is not intended to be a substitute for the SSAE 18 report.

Sincerely,

[Name of Member of Management<sup>1</sup>]

[Title]

---

<sup>1</sup> Should be a signature from one of the same persons that signed the letter of representations.

**Sample Bridge Letter – Material Changes:**

[Current Date]

**Bridge Letter**

Centers for Medicare & Medicaid Services  
Office of Financial Management  
7500 Security Boulevard, Mailstop C3-13-08  
Baltimore, MD 21244-1850  
Attn: Internal Control Team

Dear CMS Internal Controls Team:

We have received your request for information regarding material changes in internal control related to the [list services here (MAC or DME MAC)]. [CPA firm name] prepared the latest Type II SSAE 18 for these services and the report is dated [report date]. This report includes tests of operating effectiveness for the period ending [period end date].

[MAC or DME MAC name] recognizes the need to maintain an appropriate internal control environment and report upon the effectiveness, as well as material changes to its internal controls. On [date or approximate date material change happened], [describe the control add/change/removal that was made. Two sentences is sufficient]. As of [current date], I am not aware of any other material changes in our control environment that would adversely affect the Auditor's Opinion reached in the [report end date (not the same as the report date)] report for the above named SSAE 18.

You should also be aware that [MAC or DME MAC name], as a normal part of its operations, continually updates its services and technology as appropriate. In addition, the controls for all of [MAC or DME MAC name] services were designed with certain responsibilities required of the system users (See Complimentary User Entity Control in the SSAE 18 report). [MAC or DME MAC name] controls must always be evaluated in conjunction with an assessment of the strength of these user controls.

Finally, in order to conclude upon the design and effectiveness of internal controls for [MAC or DME MAC name], you must read the current SSAE 18 report. This letter is not intended to be a substitute for the SSAE 18 report.

Sincerely,

[Name of Member of Management<sup>2</sup>]

[Title]

**40.1 - Submission, Review, and Approval of Corrective Action Plans**  
*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

---

<sup>2</sup> Should be a signature from one of the same person(s) that signed the letter of representations.

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. The Internal Control Team developed an excel format that is found in Section 40.6. The excel Initial CAP Report can be obtained *via email upon request* from [CAPS@cms.hhs.gov](mailto: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 newly identified and reported 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](mailto:CAPS@cms.hhs.gov). Contractors are required to furnish an electronic copy of the CAP reports to their CMS Associate Regional Administrator for Financial Management and Fee for Service Operations, and the designated Regional Office RO CFO coordinator. MACs and DME MACs shall submit initial and quarterly CAPs to the [CAPS@cms.hhs.gov](mailto: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](mailto:CAPS@cms.hhs.gov), and the central office 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.

## **40.2 - Corrective Action Plan (CAP) Reports**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The Initial or Quarterly CAP Report shall include the data explained below using the excel template located in Section 40.6; in addition to a Field Legend providing field completion instructions. Findings should be grouped by type of review (i.e. CFO, SSAE 18, A-123 Appendix A, CPIC, etc.). Definitions of CAP report data fields:

A. Contractor - The abbreviated name assigned to the Medicare Administrative Contractor (MAC), Shared System Maintainer (SSM), Data Center, RDS or MSPRC see tables 2, 3, and 4 in Section 40.3.

B. Fiscal Year (XX) – The last two digits of the fiscal year reviewed/audited (e.g., FY 2018 would be entered as 18).

C. Review/Audit Type – Refer to Section 40.3 Table 1 to identify the code for the review or audit type performed.

D. CAP No. – Sequential three digit number (starting with 001) issued by the auditor/reviewer (or assigned by the contractor if it is a CPIC material weakness) for each finding type.

E. Jurisdiction Identifier – Applicable to MACs only-refer to Section 40.3 Table 2 for jurisdiction code.

F. Repeat CAP – Indicate if original CAP has any repeat CAPs (“Yes”/”No”).

G. CAP Repeat Number – For Quarterly CAP reporting, if a finding is repeated or duplicated in subsequent years or reported in more than one type of review, provide all other CAP ID Nos. for that issue. Repeat finding numbers listed for a particular finding shall be an identical issue, not a related or similar issue and have been identified as a repeat by the auditors in their audit report.

Findings with a repeat finding number shall only be listed once on the CAP report. Repeat finding numbers shall only be reported in the “CAP ID Number” column in the Initial CAP Report for new repeat findings identified. For the Quarterly CAP Report, the “CAP ID Number” column will be populated with the primary (original) finding number only. The primary finding number is the finding number that was identified first. If in subsequent audit/review, the same finding is identified by the auditors, the auditors will assign a finding number applicable to the type of audit/review being conducted, and also note in the audit report that it is a repeat finding of a prior audit. The auditor should also note the primary (original) finding number so that the findings can be easily linked.

H. Control objective(s) impacted - Required only for SSAE 18 findings, A-123 Appendix A findings, and CPIC material weaknesses. This represents the control objective number(s) impacted by an identified finding. More than one control objective may be impacted for each finding but you need to prioritize and limit the control objectives impacted to no more than five. Note the CMSR number should not be reported in this field.

I. Deficiency Description - A detailed description of the finding as identified by the auditor/reviewer in their final report or the material weakness as reported in the CPIC.

J. Deficiency Classification – This column is reserved for use by the CMS internal control team.

1. CAP ID No. - This field represents the unique identification number assigned to each deficiency requiring a CAP (formula driven).
2. CAP Description – A description of the planned remediation strategy to eliminate or mitigate the deficiency identified. The CAP should address the root cause of the deficiency.
3. Progress Milestones – Sequentially numbered specific action-oriented steps that facilitates the CAP progress for each deficiency being remediated. Progress milestones shall not change once established. Any revision to an original progress milestone shall be documented in the “2. CAP Description” column and considered an amendment to the original progress milestone. Any changes to the original CAP shall be submitted to CMS for approval by the Business Owner. All steps (milestones) shall be included in one cell.
4. Original Target Completion Date – A target completion date must be assigned to every CAP and progress milestone within the CAP to include (MM/DD/YYYY). The target date shall not change once it is recorded.

5. Revised Target Completion Date – If the original target completion date is revised; the revised date should be included in this column and the reason for the revision should be documented in column “2. CAP Description” (MM/DD/YYYY). Note all changes in the original target completion date shall be submitted to CMS for approval by the Business owner.
6. Actual Completion Date – An actual completion date shall be recorded for every CAP and progress milestone within the CAP to include (MM/DD/YYYY) the remediation of the deficiency was validated as effective.
7. CAP Status – A status reflecting the disposition of the CAP must be assigned and updated as necessary for each deficiency being remediated. Status options for deficiencies assessment include:
  - i. **Open** – Remediation efforts are in progress and the target completion date has not passed;
  - ii. **Delayed** – Remediation efforts are in progress after the original target completion date has passed. Explanations/justifications for delayed status must be documented in the CAP;
  - iii. **Closed – Pending** – Verification and validation efforts have been completed and the CAP is awaiting closure by the issuing party (e.g., SSAE 18 Auditor, A-123 Assessor).
  - iv. **Closed** – Validation and verification procedures demonstrate remediation efforts were adequately addressed, proven effective, and remediation efforts have been closed by issuing party; and
  - v. **Cancelled** – Remediation efforts have ceased because the remediation was recorded inadvertently or erroneously, or it can be demonstrated that the remediation effort is no longer relevant. Explanations/justifications for cancelled statuses must be document in the CAP and approved by the Business Owner.
8. CAP Lead 1 - Individual responsible for managing corrective action efforts must be assigned and documented for each deficiency being remediated.
9. CAP Lead 2 – Not applicable to Medicare Contractors.
10. CAP Lead 3 – Not applicable to Medicare Contractors.
11. Executive Sponsor 1 – The senior executive official accountable for the deficiency and the associated CAP must be documented for each deficiency requiring a CAP.
12. Executive Sponsor 2 – Not applicable to Medicare Contractors.
13. Executive Sponsor 3 – Not applicable to Medicare Contractors.

14. Testing Document Reference – Not applicable to Medicare Contractors.
15. Sport/Prosight Identifier – Not applicable to Medicare Contractors.
16. Root Cause Analysis (RCA) Methodology – RCA is the examination process used to determine the underlying events(s) that cause the deficiency; the approach technique used to uncover causes of problems. Also, RCA can be seen as the process utilized to help identify what, how, and why an event occurred so that steps can be taken to prevent future occurrences. RCA documentation should be available upon request from the CAP Lead and include the decision process used to determine the RCA approach, and all supporting documentation (e.g. walk through documentation, meeting minutes, various dates analysis, emails, etc.).
17. Not for use by contractor
18. Progress Milestone Status – Each progress milestone must have an assigned status reflecting its disposition. Status options for deficiencies include:
  - i. **Open** – Remediation efforts are in progress and the target completion date has not passed;
  - ii. **Delayed** – Remediation efforts are in progress and after the original target completion date has passed. Explanations/justifications for delayed status must be documented in the CAP;
  - iii. **Closed – Pending** – Verification and validation efforts have been completed and the CAP is awaiting closure by the issuing party (e.g., SSAE 18 Auditor, A-123 Assessor).
  - iv. **Closed** – Validation and verification procedures demonstrate remediation efforts were adequately addressed, proven effective, and remediation efforts have been closed by issuing party; and
  - v. **Cancelled** – Remediation efforts have ceased because the remediation was recorded inadvertently or erroneously, or it can be demonstrated that the remediation effort is no longer relevant. Explanations/justifications for cancelled statuses must be document in the CAP and approved by the Business Owner.

### 40.3 - CMS Finding Numbers

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

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:

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

**Table 2 – *DME, MAC, AND SMAC CONTRACTOR ABBREVIATIONS***

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

**Table 3 – *CONTRACTOR ABBREVIATIONS***

Novitas Solutions, Inc. (Affordable Care Act <i>Exchange Oversight Contractor</i> )	<i>NOVA</i>
Group Health Inc. (GHI) Benefits Coordination and Recovery Center (BCRC) (MSPRC)	GHI
Noridian Healthcare Solutions, Pricing, Data Analysis, and Coding (PDAC)	NORP
<i>Performant</i> , Commercial Repayment Center (CRC) (MSPRC)	<i>PER</i>
<i>General Dynamics Information Technology</i> (GDIT) <i>Retiree Drug Subsidy</i> (Part D Contractor)	RDSV

**Table 4 – *SHARED SYSTEM MAINTAINER ABBREVIATIONS***

<i>DV United, LLC</i> (Common Working File)	CWF
Data Computer Corporation of America ( <i>Single Testing Contractor</i> )	DCCA
Enterprise Services Plano (Fiscal Intermediary Standard System)	FISS
Enterprise Services Plano (Multi-Carrier System)	MCS
General Dynamics Information Technology ( <i>Viable Medicare System / DME Claims Processing System</i> )	VMS

**Table 5 – *DATA CENTER ABBREVIATIONS***

Companion Data Services (CDS) <i>General Support System (GSS)</i> (VDC)	CDS
Data Computer Corporation of America (MBES)	MBES
<i>DXC Technology</i> – Tulsa, OK (VDC)	EDS
<i>Leidos – Culpepper, VA</i> (HIGLAS)	<i>LEI</i>
General Dynamics Information Technology / GHI (New York, NY)	GDIT

#### **40.4 – Initial CAP Report**

***(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)***

All initial CAPs shall be reported on the Initial CAP Report. After this initial submission, CAPs shall be merged onto the Quarterly CAP Report. All CAPs, for the reviews noted in Section 40, shall be consolidated onto one Quarterly CAP Report. However, if you have findings for an affiliated data center or system maintainer shown above, these findings shall also be reported using the CMS FISMA Controls Tracking System (CFACTS). A separate CAP report shall be submitted for each contractor, as listed in Section 40.3.

The contractor shall use the Initial CAP Report, as an Excel spreadsheet and add their data following the steps below. The format of the spreadsheet should not be altered; however, the column width and row height may be adjusted to accommodate data entry. Additionally, this electronic file should be labeled Initial CAP Report, should be identified using the contractor abbreviations found in Section 40.3, and should include the submission date. For example, Wisconsin Physicians Service Insurance Corporation (WPS) would name this file “WPS Initial CAP Report 10/30/XX.xls”.

The Initial CAP Report template can be found in Section 40.6.

## **40.5 – Quarterly CAP Report**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

The contractor shall use the Quarterly CAP Report, as an Excel spreadsheet and add their data accordingly, changes are only allowed to be made to the column width and row height to accommodate data entry. Additionally, this electronic file shall be labeled Quarterly CAP Report, should be identified using the contractor abbreviations found in Section 40.3, and shall include the submission date. For example, Wisconsin Physicians Service Insurance Corporation (WPS) would name this file “WPS Quarterly CAP Report 10/30/XX.xls”.

*The Quarterly CAP Report template can be found in Section 40.6.*

## **40.6 – CMS *Initial and Quarterly* CAP Report Template**

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

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](mailto:CAPS@cms.hhs.gov).*

*Additionally, any Initial and Quarterly CAPs questions and or concerns can be submitted to [CAPS@cms.hhs.gov](mailto:CAPS@cms.hhs.gov).*



## 50 – List of CMS Contractor Control Objectives

*(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)*

Control Number	Control Objectives
A – Control Number	Control Objective – Information Systems
<b><i>A.1 - A.11</i></b>	<b><i>Security Management: Controls provide reasonable assurance that security management is effective.</i></b>
A.1	<p><i>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:</i></p> <ul style="list-style-type: none"><li><i>• Is monitored and kept up-to-date in accordance with the current ARS requirements.</i></li><li><i>• Includes requirements to establish a security management structure that has appropriate independence, authority, expertise, and resources.</i></li><li><i>• Clearly assigns security responsibilities throughout the organization.</i></li><li><i>• Ensures that management implements, maintains, and updates the organization security policy and procedures in accordance with CMS guidance.</i></li></ul>
A.2	<p><i>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.</i></p>
A.3	<p><i>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.</i></p>

A – Control  
Number

Control Objective – Information Systems

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.*

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 – Control  
Number

Control Objective – Information Systems

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 – Control  
Number

Control Objective – Information Systems

- 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.*
- 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 – Control  
Number

Control Objective – Information Systems

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 by all employees, contractors, vendors, and/ or visitors, to Medicare facilities, data centers and system hardware is appropriately authorized, documented, and reviewed in accordance with the current CMS ARS, BPSSM, and other applicable policy.*

A.20

*Controls provide reasonable assurance that physical access protections to sensitive IT areas are implemented in accordance with the current CMS ARS, BPSSM, and other applicable policy.*

**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 eXpedited Life Cycle (XLC).*
- 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 – Control  
Number

Control Objective – Information Systems

- 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.*
- 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 – Control  
Number

Control Objective – Information Systems

*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.*

B – Control  
Number

Control Objective – Claims Processing

**B.1** The Medicare claims processing system tracks each claim from receipt to final resolution.

*B.2 Controls provide reasonable assurance that fee-for-service information system edits and/or validations are configured in accordance with CMS guidelines including:*

- Management maintains a current baseline of edit configurations in accordance with CMS guidelines.*
- Management assesses the current configuration of edits against the baseline periodically.*
- For misconfigured edits Management remediates the configuration in a timely fashion.*
- Management reports results of reconciliations / reviews to CMS periodically.*

**(Maintainer Only)**

B – Control Number	Control Objective – Claims Processing
B.3	The system generates an audit trail with respect to each claim, adjustment, or other related transaction. Such audit trail shall include the results of each applicable claim edit. (Maintainer Only)
B.4	Each claim is adjudicated in accordance with CMS instructions.
B.5	Claims are reopened in accordance with CMS guidelines and readjudicated in accordance with CMS instructions.
B.6	<i>Claim payment amounts are calculated in accordance with CMS instruction. Fee schedules are properly received, logged, and changed in the system and monitored, and applied in accordance with CMS instructions.</i>
B.7	The system shall identify and deny duplicate claims in accordance with CMS instructions. (Maintainer Only)
B.8	Claims are properly aged from the actual receipt date to the actual date of payment in compliance with CMS instructions.
B.9	The system shall detect apparent fraudulent or abusive practices in accordance with CMS instructions. Personnel are trained to detect fraudulent and abusive practices and, in accordance with CMS instructions, to deter such practices. Any such apparent fraudulent or abusive practices as are identified are documented and reported in accordance with CMS instructions.
C – Control Number	Control Objective – Appeals
C.1	Medicare Part A and Part B redeterminations processed by MACs are processed based on CMS instructions, appropriately logged and completed within legislatively mandated time frames and tracked to meet CMS guidelines. (Does not pertain to MSPRC. Refer to C.3 for MSPRC control objective.)
C.2	Medicare Part B redeterminations processed by MACs are processed based on CMS instructions, appropriately logged and completed within legislatively mandated time frames and tracked to meet CMS guidelines. (Does not pertain to MSPRC. Refer to C.3 for MSPRC control objective.)
C.3	Redeterminations processed by the MSPRC are processed based on CMS instructions, appropriately logged and completed within legislatively mandated time frames and tracked to meet CMS guidelines.

C – Control Number	Control Objective – Appeals
C.4	Qualified Independent Contractor (QIC) request for case files are handled in compliance with CMS time frames.
C.5	Effectuations are processed as directed by CMS guidelines.
C.6	Contractor communications are clear and in compliance with CMS’ instructions to include specific communications such as acknowledgement letters, decision letters, and information on additional appeal rights, etc.
D – Control Number	Control Objective – Beneficiary/Provider Services
D.1	Personally identifiable health information, which is used and disclosed in accordance with the Privacy Act, is handled properly. (Internet Only Manual (IOM) Chapter 2-20.1.8-Beneficiary Customer Service; IOM Pub. 100-09, Chapter 6-Provider Customer Service Program).
D.2	Beneficiary and Provider written inquiries are retained and handled accurately, appropriately, and in a timely manner. (IOM Chapter 2-20.2 – Written Inquiries; IOM Pub. 100-9, Chapter 6-Provider Customer Service Program).
D.3	Telephone inquiries are answered timely, accurately, and appropriately. (IOM Chapter 2-20.1 Telephone Inquiries; IOM Pub. 100-09, Chapter 6-Provider Customer Service Program).
E – Control Number	Control Objective – Complementary Credits
E.1	Contractors shall report cash received from the BCRC for COBA crossover claims as the cash is received in the CMS Analytical, Reporting, & Tracking system (CMS ART).
<i>E.2</i>	<i>Control number E.2 reserved. Control not in use as of IOM revision number 228.</i>

F – Control  
Number

Control Objective – Medical Review (MR)

- F.1 Contractor shall use the Program Integrity Manual (PIM) guidelines, data analysis (prior year and most current) and Medical Review (MR) results including Strategy Analysis Report (SAR), and Comprehensive Error Rate Testing (CERT) results to develop and update the Improper Payment Reduction Strategy (IPRS). The problem-focused outcome-based IPRS report shall address provider specific problems, and service-specific problems only in the rare circumstance it is approved by CMS. The IPRS shall focus its medical review activities toward the goal of reducing the claims improper payment rate. All work performed by the MR unit shall be identified in the IPRS and targeted based on the contractor's prioritized problem list or as directed by CMS.*
- F.2 Contractor shall budget and perform the MR workloads throughout the year as established in the IPRS. MACs shall report workload volume, and costs associated with MR activities in CMS *Analysis, Reporting, and Tracking (ART) systems* or as directed by the COR. MACs shall explain any significant fluctuations in workload or costs in the Monthly Status Report and SAR.
- F.3 Contractor shall perform data analysis continuously to identify potential problems such as aberrant billing practices, potential of over-utilization areas, and changes in patterns of care to target medical review activities to reduce the claims improper payment rate. Data from a variety of sources must be used for data analysis. At a minimum, sources include: contractor internal data; CMS program vulnerability alerts such as Quarterly Vulnerability Technical Direction Letters that require corrective action reporting, FATHOM/PEPPER and other comparative billing reports; results from medical review studies performed by specialty MR or Program Integrity contractors; and other national or regional sources such as Office of Inspector General (OIG) reports, Government Accountability Office (GAO) reports, enrollment data, and fraud alerts.
- F.4 Contractor shall ensure that effective MR edits are developed and implemented as a result of data analysis findings and policies. The effectiveness of each MR edit shall be analyzed and measured by tracking the denial rate, appeals reversal rate, basis of the appeals reversal, and the dollar return on the cost of operationalizing the edit (savings), and success of edit towards billing behavior correction. MR edits shall be modified, deleted, or deactivated when they are determined to no longer be effective.

F – Control Number	Control Objective – Medical Review (MR)
F.5	Contractor shall utilize the Progressive Corrective Action (PCA) process, in accordance with the Pub. 100-08 and CMS instructions, to drive MR activity (i.e., data analysis, claims review, medical review education).
F.6	Contractor shall be capable of identifying the status of each claim subjected to medical review at any time (and all claims must be processed timely for closure in accordance with Pub. 100-08 instructions).
F.7	<i>Control number F.7 reserved. Control not in use as of IOM revision number 278.</i>
F.8	The MR unit shall effectively collaborate with Provider Outreach and Education (POE) by referring educational needs that will address existing program vulnerabilities and emerging problems identified during the MR process conducted throughout the fiscal year.
F.9	Contractor shall implement and utilize a Provider Tracking System (PTS) to track all informational provider contacts made by medical review and all educational referrals submitted to POE and external organizations.
F.10	<i>Contractor shall ensure that there is adequate internal networking and sharing of information, and appropriate collaborative actions are taken as a result, between MR and other business functions such as Appeals, Audits, POE, and inquiries and external organizations such as the Zone Program Integrity Contractors (ZPIC), Unified Program Integrity Contractors (UPIC), Recovery Auditors, and Quality Improvement Organizations (QIOs).</i>
F.11	Contractor shall apply quality assurance processes to all elements of the MR Strategy and to all aspects of program management, data analysis, edit effectiveness, problem identification, and claim adjudication.
F.12	Contractor shall effectively comply with all of the MR requirements of the Joint Operating Agreement (JOA) with the PSCs/ZPICs and Recovery Auditors, and other entities as directed by CMS.
<i>F.13</i>	Contractor shall institute a corrective action reporting process for claims-specific errors and vulnerabilities in accordance with PIM 3.7.5. For each issue, MACs shall report interim actions, final actions, and action dates.

G – Control  
Number

Control Objective – Medicare Secondary Payer (MSP)

G.1

*Medicare Administrative Contractor internal quality controls are established and maintained that ensure timely and accurate processing of secondary claims submitted, including paper MSP claims, with a primary payer's explanation of benefits (EOB) or remittance advice (RA). This includes utilization of the MSPPAY module, resolving all MSP edits (including 6800 codes\*), creation of "I" records and resolving suspended claims in accordance with CMS instructions at Publication 100-05 Chapter 5 and 6. Contractor internal systems used to process MSP claims are updated via the Common Working File (CWF) automatic notice in an automated fashion. Suspended claims that require manual intervention are corrected and reviewed by the appropriate suspense staff.*

*This control objective does not pertain to BCRC or the CRC contractors.*

G.2

*Audit trails for MSP receivables are created and maintained. An audit trail should include details of the source of the receivable, correspondence in date order, reasons for adjustments, referral to treasury, collection of the debt, and any information regarding the establishing, reconciling and resolving a receivable for an outstanding debt. All applicable systems (e.g. HIGLAS) should be updated accurately and timely, and be accessible to the appropriate individuals.*

*This control objective pertains to MACs, BCRC, and CRC Contractors.*

G.3.1

*Contractors ensure compliance with all CMS instructions and directives relating to MSP Investigations by the Benefit Coordination & Recovery Center (BCRC). This includes transmitting appropriate, timely and complete Electronic Correspondence Referral System (ECRS) submissions in accordance with Publication 100-05, CWF Assistance Requests and ECRS MSP inquiries to the BCRC as a result of the receipt of a phone call, correspondence, claim or unsolicited check/voluntary refund. All references must be maintained in an area accessible to MSP staff and must be available for CMS review.*

*\*The ECRS user guide is located at: Publication # 100-05 The Electronic Correspondence Referral System on the Web (ECRS Web) User Guide.*

*This control objective does not pertain to the CRC Contractor*

G – Control  
Number

Control Objective – Medicare Secondary Payer (MSP)

G.3.2

*The Commercial Repayment Center (CRC) and the Benefits Coordination and Recovery Center (BCRC) must transmit appropriate, timely and complete ECRS submissions and CWF Assistance Request as a result of a phone call, inquiry or correspondence received to ensure debtor information is accurate.*

*This control objective pertains to the CRC and the BCRC.*

G.4

*Contractors identify and track all incoming correspondence to ensure timely acknowledgement, response, and priority compliance with the Statement of Work (SOW) for MACs and other Medicare Contractors. These tracking mechanisms should include the ability to track ECRS submissions when awaiting response/status from the BCRC, or further actions such as claims adjustments after the BCRC has completed their investigation.*

*This control objective pertains to MACs, BCRC, and CRC Contractors.*

G.5

*Contractors shall have quality assurance measures in place to ensure the accuracy of the implementation of any CMS directive or any required work process/deliverable expressed in the SOW. Contractors shall also provide evidence that the results from quality assurance checks are documented to identify errors and that training venues are implemented to prevent the reoccurrence of these errors.*

*This control objective pertains to MACs, BCRC, and CRC Contractors.*

H – Control  
Number

Control Objective – Administrative

H.1

For contracts expected to exceed \$5.5 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 – Control Number	Control Objective – Administrative
H.2	Procurements are awarded and administered in accordance with CMS regulations, CMS general instructions and the Federal Acquisition Regulation.
H.3	<i>Control number H.3 reserved. Control not in use as of IOM revision number 278.</i>
H.4	CMS management structure provides for efficient contract performance.
H.5	Records shall be maintained/retained according to the <a href="#">National Archives and Records Administration</a> (NARA) guidelines, CMS implementing guidelines and other requirements, FAR guidelines and other Federal requirements, as may be identified.
<i>H.6</i>	<i>Contractor's</i> 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.
I – Control Number	Control Objective – Provider Audit
I.1	Interim, tentative and PIP payments to Medicare providers are established, monitored and adjusted, if necessary, in a timely and accurate manner in accordance with CMS general instructions and provider payment files are updated in a timely and accurate manner. Adjustments to interim payments shall be made to ensure that payments approximate final program liability within established ranges. Payment records are adequately protected. <i>All applicable CMS systems are properly updated.</i>
I.2	Information received by the contractor from CMS or obtained from other sources regarding new providers, change of ownership for an existing provider, termination of a provider, or a change of <i>Medicare Administrative Contractor (MAC)</i> are identified, recorded, and processed in System Tracking for Audit and Reimbursement (STAR) in a timely and accurate manner and reflected in subsequent audit activities.

I – Control Number	Control Objective – Provider Audit
1.3	Provider Cost Reports are properly submitted and accepted in accordance with CMS’ regulations, policies, and instructions. Appropriate program policies and instructions are followed in situations where the provider did not file a cost report. Cost report submission information is timely and properly forwarded to the proper CMS Systems.
I.4	Desk review procedures and work performed are documented and are sufficient to obtain an accurate review of the submitted cost report <i>and are in accordance with the Uniform Desk Review (UDR) Program</i> . Documentation is established and maintained to identify situations requiring a limited desk review or a full desk review.
I.5	Notices of Program Reimbursement (NPR) are issued accurately and timely to providers and include all related documentation (e.g. an audit adjustment report, copy of the final settled cost report).
I.6	Inputs to mandated systems regarding provider audit, settlement, <i>reopening, appeals</i> , and reimbursement performance (STAR) are complete, accurate and in compliance with program instructions. Documentation supporting reports and inputs shall be maintained.
I.7	The contractor’s cost report reopening process is conducted in accordance with CMS regulations and program policy.
I.8	Provider appeals (including both the Provider Reimbursement Review Board (PRRB) and <i>Contractor Appeals</i> ) are handled appropriately. Jurisdictional questions are addressed and PRRB timeframes for submission are observed.
I.9	<i>Control number I.9 reserved. Control not in use as of IOM revision number 278.</i>
I.10	An internal quality control process has been established and is functioning in accordance with CMS instructions to ensure that audit work performed on providers’ cost reports is accurate, meets CMS quality standards, and results in program payments to providers which are in accordance with Medicare law, regulations and program instructions.
I.11	Cost reports are scoped and selected for audit or settled without audit. <i>Audit plans are approved by the Audit &amp; Reimbursement (A&amp;R) Business Function Lead and adhere to CMS guidelines and instructions.</i>

I – Control Number	Control Objective – Provider Audit
I.12	The contractor’s audit process is conducted in accordance with CMS manual instructions and timelines, i.e., timeframes for issuance of the engagement letter, documentation requests, pre-exit and exit conferences, and settlement of the audited cost report.
I.13	Communications of audit programs, desk review programs, CMS audit and reimbursement policies, and other audit related instructions are timely and accurately communicated to all appropriate audit staff.
I.14	The contractor’s audit staff maintains its necessary knowledge and skills by completing continuing education and training (CET) required by CMS instructions, and documentation is maintained to support compliance by each staff member.
I.15	Supervisory reviews of the audit and settlement process are conducted and the policies and procedures for these reviews are communicated to all supervisors in accordance with CMS program instructions.
I.16	All cost reports where fraud <i>and abuse</i> is suspected shall be referred to the <i>Zone Program Integrity Contractor (ZPIC)</i> in accordance with CMS and contractor instructions.
I.17	The contractor has processes and procedures in place to document that supervisory reviews by provider audit department management were completed on all provider audit <i>Corrective Action Plans (CAPs)</i> from the establishment of the CAPs to the implementation and validation of the CAPs.
<i>I.18</i>	HITECH incentive payments for Medicare subsection (d) and critical access hospitals are calculated properly, in accordance with CMS’ regulations, policies, and instructions. Data is properly entered into the FISS screens in order for the HITECH system to generate the incentive payments.
<i>I.19</i>	Notices of CAP Determination Letter are issued accurately and timely to Hospices and include all related documentation.

## **J Controls – *Financial Reporting Review Requirements***

Transactions for Medicare accounts receivable, payables, expenses shall be recorded and reported timely and accurately, and financial reporting shall be completed in accordance with CMS standards, Federal Acquisition Regulation (FAR), Financial Accounting Standards Advisory Board, Cost Accounting Standards, and Generally Accepted Accounting Principles (GAAP). For the following control objectives, the review shall focus on the following areas:

- Cost Report Settlement Process;
- Contractor Financial Reports:
  - Statement of Financial Position (CMS-H750A/B),
  - Status of Accounts Receivable (CMS-751A/B),
  - Status of Debt – Currently Not Collectible (CNC) (CMS –C751 A/B),
  - Status of Medicare Secondary Payer Accounts Receivable (CMS-M751A/B),
  - Status of Medicare Secondary Payer Debt-Currently Not Collectible (CMS-MC751A/B),
  - HIGLAS-CMS Balance Sheets and Income Statements,
  - HIGLAS-CMS Treasury Report on Receivables (TROR),
  - HIGLAS-CMS CNC Eligibility,
  - HIGLAS-CMS MSP Recovery GHP/Non-GHP Receivables,
  - Reconcile the HIGLAS accounts receivable balance and activity to the following reports/registers:
    - CMS Beginning Balance Report,
    - CMS Transaction Register,
    - CMS Applied Collection Register,
    - CMS Adjustment Register,
    - CMS AR Overpayments Report,
    - CMS Interest and Late Charges,
    - CMS AR Balance Detail,
    - CMS Written-Off/CNC,
- Monthly Contractor Financial Report (CMS 1522) and Contractor Draws on Letter of Credit (CMS 1521),
- Reconciliation of Cash Balances and Cash Receipts.
- HIGLAS-CMS Trial Balance and General Ledger,
- HIGLAS-CMS Cash Management Reports,
- HIGLAS-CMS Accounts Payable Reports:
  - AP Detail Schedule of Entitlement Payables Due & Payable-Refunds Payable (216006),
  - AP Detail Schedule of Entitlement Payables Due & Payable-Top Offsets (216097),
  - AP Detail Schedule of Entitlement Payables Due & Payable-Settlement Matching (216098),
  - AP Detail Schedule of Entitlement Payables Due & Payable-Third Party Payer (216099),
- HIGLAS-Contractor’s Monthly Bank Reconciliation Worksheet.

J – Control Number	Control Objective – Financial
J.1	Financial statements and reports should include all authorized transactions that occurred for the period reported.
J.2	<i>Valid</i> financial transactions are <i>prepared</i> and approved by authorized personnel in accordance with management and CMS’ policies.
J.3	Recorded and processed transactions are correctly classified, maintained, summarized and reconciled. In addition, transactions shall be properly supported.
J.4	Segregation of duties exists <i>and are implemented</i> within the <i>area of financial reporting</i> (i.e., there shall be separate authorization, record keeping, and custody).
J.5	All assets <i>and liabilities</i> exist, <i>are</i> properly valued, and <i>are correctly recorded in the books/records of the contractor</i> .
J.6	<i>Accounts receivable and accounts payable balances be properly valued and aged appropriately in accordance with CMS policies.</i>
J.7	Contractor Financial Reports are accurate, signed/certified by authorized individuals and presented timely to CMS in accordance with Publication (Pub) 100-06 of the Medicare Financial Management Manual, Chapter 5, Financial Reporting, Section 230 and/or the HIGLAS Certification Statement.
J.8	Banking information relevant to Medicare processing is accurately stated and conforms to the tripartite agreement.
K – Control Number	Control Objective – Debt Referral (MSP and Non-MSP)
K.1	Procedures are documented and followed to identify a debt eligible for referral to Treasury for cross servicing and Treasury Offset Program (TOP) prior to the debt becoming 120 days delinquent. These procedures are written and available for review. Debts eligible for referral and debts ineligible for referral are properly reported on the appropriate CMS Forms 751, Contractor Financial Reports, Status of Accounts Receivable, or the Treasury Report on Receivables and Debt Collection Activities Report. For MSP debt, see Internet Only Manual (IOM), Pub 100-05, MSP Manual, Chapter 7, Section 60 and Chapter 4, Debt Collections.

K – Control Number	Control Objective – Debt Referral (MSP and Non-MSP)
K.2	Intent to Refer <i>Letters</i> (IRLs) for eligible debt are sent in a timely manner in accordance with CMS instructions. <i>Timeframes for each type of debt can be found in the IOM, Chapter 4, Debt Collections.</i>
K.3	Responses to the IRL letter are handled timely according to CMS instructions. Appropriate systems are updated to reflect any changes to the eligibility status of the debt and these statuses are properly reported on the financial reporting forms outlined in K.1. Procedures are in place to handle undeliverable letters. <i>Refer to the IOM, Chapter 4, Debt Collections.</i>
K.4	<i>Non-HIGLAS contractors ensure that eligible delinquent debts are input to the Debt Collection System (DCS) timely and accurately, including debt type, in accordance with CMS instructions. HIGLAS contractors review the AutoSys generated DCIA report and update HIGLAS accordingly to ensure appropriate debts are referred to Treasury.</i>
K.5	<i>When there is a change to a debt that has been referred for cross servicing, non-HIGLAS contractor initiated recalls, collections, and adjustments are entered timely and accurately to DCS in accordance with CMS instructions. Procedures to update these debts in DCS are in place and are being followed. . HIGLAS contractor initiated recalls, collections, and adjustments are entered timely and accurately into HIGLAS including the ‘Debt Referral Reason Code’ Descriptive FlexField. Procedures to update these debts from the HIGLAS Debt Management Module training guide are followed.</i>
K.6	<i>Non-HIGLAS contractors ensure that the Collection/Refund Spreadsheets are completed in accordance with CMS instructions, and the appropriate systems are updated. HIGLAS contractors ensure the Debt Management Module is updated with refund/adjustment information as needed.</i>
K.7	Treasury Cross-Servicing Dispute Resolution forms are researched, resolved, and responded to Treasury timely in accordance with CMS instructions. <i>Procedures are in place and are being followed to respond to these disputes/inquiries, update the appropriate system, and properly report the status and balance of the debt in the financial reporting forms.</i>

K – Control  
Number

Control Objective – Debt Referral (MSP and Non-MSP)

K.8

*Non-HIGLAS contractors ensure Returned to Agency (RTA) Spreadsheets are completed in accordance with CMS instructions and debts listed on the spreadsheet are properly reported on the financial reporting forms and the DCS in accordance with CMS instructions. HIGLAS contractors follow the RTA Interface and Report instructions in the HIGLAS Debt Management Module training guide.*

K.9

*Contractors ensure that debts have the correct status when the debt is referred to Treasury and retains this correct status while at Treasury.*

L – Control  
Number

Control Objective – Non-MSP Debt Collection

L.1

*All overpayments that meet the applicable threshold should be demanded.* Demand letters initiate the collection of a provider debt as well as inform the provider of the existence of the debt, their appeal rights with respect to the debt, and the ramifications if the debt is not paid or an agreement is not reached within a specified time period *in accordance with CMS instructions. The content of manually created demand letters are reviewed and approved according to CMS guidelines.* The demand letter shall be issued, printed mailed timely, *and maintained*, in accordance with CMS instructions at Pub 100-06, chapters 3 and 4.

L.2

Extended Repayment Schedules (ERSs) shall be analyzed for approval or denial *by a supervisor in accordance with CMS instructions. The supervisor's review includes monitoring all approved ERSs, the complete financial analysis of the provider's application, compliance with the ERS,* and the referral to CMS when necessary in accordance with CMS instructions at Pub 100-06, Chapters 3 and 4.

L.3

Interest is *calculated and* applied correctly and timely in accordance with CMS instructions *at Publication 100-06, Chapters 3 and 4. The interest rate is updated in accordance with the notice of the new interest rate for Medicare Overpayments and Underpayments notification. Interest changes are updated in all applicable systems.*

L – Control  
Number

Control Objective – Non-MSP Debt Collection

- L.4 Bankruptcy cases are handled in accordance with CMS instructions and instructions given by the Office of General Counsel (OGC). An audit trail of the overpayment shall exist before and after the bankruptcy filing to ensure that Medicare's best interest can be represented by OGC. *Contractors shall maintain, track, and update the status of a bankruptcy in accordance with CMS instructions at Pub 100-06, Chapters 3 and 4.*
- L.5 Provider debt is collected timely, completely, and accurately with an appropriate audit trail of all collection activity and attempts of collection activity *in accordance with CMS instructions at Pub 100-06, Chapters 3 and 4.*
- L.6 *Control number L.6 reserved. Control not in use as of IOM revision number 214.*
- L.7 Timely review and processing of all 838 Credit Balance Reports. Ensure that all reported credit balances are collected and properly processed in accordance with CMS instructions in accordance with CMS instructions at Pub 100-06, Chapter 12.
- L.8 *Control number L.8 reserved. Control not in use as of this IOM revision.*
- L.9 *For overpayments subject to the limitation on recoupment of the Medicare Modernization Act (MMA), recoupment is stopped when, a timely and (redetermination, or reconsideration request is received.*
- Once both levels of appeal are completed and CMS prevails, collection activities, including revised demand letters and internal recoupment may resume within the timeframes set forth. Contractors will calculate the interest on the principal amount paid if the provider at the ALJ or subsequent levels. Contractors shall update, track, and maintain appeal status in the applicable systems. This does not apply certain overpayments in accordance with CMS instructions at Publication 100-06 Chapter 3, Section 200.*

M – Control  
Number

Control Objective – Provider Enrollment

M.1

Review the Medicare enrollment applications (paper CMS-855 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 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 15, Section 15.5.20, of the PIM.

M.3

*Control number M.3 reserved. Control not in use as of this IOM revision.*

## **70 – List of Commonly Used Acronyms**

**(Rev. 301, Issued: 03-19-18, Effective: 10-01-17, Implementation: 06-19-18)**

<i>Acronym</i>	<i>Definition</i>
AO	<i>Authorizing Official</i>
AP	<i>Account Payable</i>
A&R	<i>Audit &amp; Reimbursement</i>
AR	<i>Account Receivable</i>
ARA	<i>Associate Regional Administrator</i>
ARS	<i>Acceptable Risk Safeguards</i>
BCRC	<i>Benefit Coordination &amp; Recovery Center</i>
BPSSM	<i>Business Partners Systems Security Manual</i>
CAP	<i>Corrective Action Plan</i>
CET	<i>Continuing Education and Training</i>
CFACTS	<i>CMS FISMA Controls Tracking System</i>
CFO	<i>Chief Financial Officers Act of 1990</i>
CMBRW	<i>Contractor’s Monthly Bank Reconciliation Worksheet</i>
CMS	<i>Centers for Medicare and Medicaid Services</i>
CNC	<i>Currently Not Collectible</i>
COR	<i>Contracting Officer Representative</i>
CPE	<i>Contractor Performance Evaluation</i>
CPIC	<i>Certification Package for Internal Controls</i>
CRC	<i>Commercial Repayment Center</i>
CWF	<i>Common Working File</i>
DCS	<i>Debt Collection System</i>
DME	<i>Durable Medical Equipment</i>
DPP	<i>Duplicate Primary Payment</i>
ECRS	<i>Electronic Correspondence Referral System</i>
EOB	<i>Explanation of Benefits</i>
ERM	<i>Enterprise Risk Management</i>
ERS	<i>Extended Repayment Schedule</i>
FAR	<i>Federal Acquisition Regulation</i>
FISMA	<i>Federal Information Security Management</i>
FISS	<i>Fiscal Intermediary Standard System</i>
FMFIA	<i>Federal Managers’ Financial Integrity Act of 1982</i>
FR	<i>Financial Reporting</i>
FY	<i>Fiscal Year</i>
GAAP	<i>Generally Accepted Accounting Principles</i>
GAO	<i>Government Accountability Office</i>
GHP	<i>Group Health Plan(s)</i>
GSS	<i>General Support System</i>
HHS	<i>The US Department of Health and Human Services</i>
HIGLAS	<i>Healthcare Integrated General Ledger Accounting System</i>
HITECH	<i>Health Information Technology for Economic and Clinical Health</i>
ICOFR	<i>Internal Controls Over Financial Reporting</i>
ICS	<i>Internal Control Standards</i>
IOM	<i>Internet Only Manual</i>
IRL	<i>Intent to Refer Letters</i>
IT	<i>Information Technology</i>
JOA	<i>Joint Operating Agreement</i>
MAC	<i>Medicare Administrative Contractor</i>
MCS	<i>Multi-Carrier System</i>

<i>Acronym</i>	<i>Definition</i>
<i>MMA</i>	<i>Medicare Prescription Drug, Improvement, and Modernization Act of 2003</i>
<i>MW</i>	<i>Material Weakness</i>
<i>MSP</i>	<i>Medicare Secondary Payer</i>
<i>MSPRC</i>	<i>Medicare Secondary Payer Recovery</i>
<i>NARA</i>	<i>National Archives and Records Administration</i>
<i>NPR</i>	<i>Notices of Program Reimbursement</i>
<i>NVA/ST</i>	<i>Network Vulnerability Assessment / Security Testing</i>
<i>OGC</i>	<i>Office of General Counsel</i>
<i>OIG</i>	<i>Office of Inspector General</i>
<i>OMB</i>	<i>Office of Management and Budget</i>
<i>PIM</i>	<i>Program Integrity Manual</i>
<i>POA&amp;M</i>	<i>Plan of Action and Milestone</i>
<i>POE</i>	<i>Provider Outreach and Education</i>
<i>PRRB</i>	<i>Provider Reimbursement Review Board</i>
<i>PTS</i>	<i>Provider Tracking System</i>
<i>Pub</i>	<i>Publication</i>
<i>QIO</i>	<i>Quality Improvement Organization</i>
<i>RA</i>	<i>Remittance Advice</i>
<i>RDS</i>	<i>Retiree Drug Subsidy</i>
<i>RMH</i>	<i>Risk Management Handbook</i>
<i>RO</i>	<i>Regional Office</i>
<i>RTA</i>	<i>Returned to Agency</i>
<i>SA&amp;A</i>	<i>Security Assessment and Authorization</i>
<i>SD</i>	<i>Significant Deficiency</i>
<i>SDLC</i>	<i>System Development Life Cycle</i>
<i>SOW</i>	<i>Statement of Work</i>
<i>SMAC</i>	<i>Specialty Medicare Administrative Contractor</i>
<i>SSAE 18</i>	<i>Statement on Standards for Attestation Engagements Number 18</i>
<i>SSP</i>	<i>System Security Plan</i>
<i>STAR</i>	<i>System Tracking for Audit and Reimbursement</i>
<i>STC</i>	<i>Single Testing Contractor</i>
<i>TDL</i>	<i>Technical Direction Letter</i>
<i>TOP</i>	<i>Treasury Offset Program</i>
<i>TROR</i>	<i>Treasury Report on Receivables</i>
<i>UDR</i>	<i>Uniform Desk Review</i>
<i>UPIC</i>	<i>Unified Program Integrity Contractors</i>
<i>USGAO</i>	<i>United States General Accounting Office</i>
<i>VDC</i>	<i>Virtual Data Center</i>
<i>VMS</i>	<i>Viable Medicare System</i>
<i>XLC</i>	<i>eXpedited Life Cycle</i>
<i>ZPIC</i>	<i>Zone Program Integrity Contractor</i>





**Field Legend:**

FIELD	INSTRUCTIONS
A	Select from Drop-down box Contractor abbreviated name (see Internet Only Manual (IOM), Chapter 7, Section 40.3).
B	Enter last two digits of fiscal year audited (YY).
C	Select from Drop-down box Review/Audit Type (see IOM, Chapter 7, Section 40.3).
D	Enter sequential three digit CAP number, as a label, starting with "001".
E	Select from Drop-down box Medicare Administrative Contractor jurisdiction identifier, if applicable (e.g., JX).
F	Select from Drop-down Box if Cap is a Repeat CAP "Yes" or "No".
G	If CAP is a Repeat list repeat CAP number(s) starting with oldest CAP number.
H	Enter Control Objective(s) impacted, no more than three control objectives (see IOM, Chapter 7, Section 50)
I	Enter a description of the deficiency or the condition which resulted in the deficiency. The <i>condition</i> is a situation that exists and is not in compliance with appropriate criteria.
J	CMS A-123 Technical Team (ATT) will populate this field.
1.	CAP ID No. - Automatically populated
2.	Document the corrective action plan to remediate the root cause of the deficiency. See Field 22 for Root Cause Analysis Instructions.
3.	Document measurable progress milestones actions to facilitate the progress of remediating the root cause of the deficiency. Each contractor must provide a detailed summary of the progress milestone, state whether the progress milestone is critical, the planned start date, the actual start date, the target completion date, dependencies, performance measures and metrics, and the actual completion date (when applicable). The progress milestones must be reviewed and approved by the CAP Lead(s) and CMS Business Process Owner(s). <b>Note all information provided shall be restricted to one cell.</b>
4.	Enter the projected target completion date (MM/DD/YYYY) in which the deficiency will be fully remediated by the CAP.
5.	If the original CAP date of completion (Field 4) will not be met, enter the revised target completion date (MM/DD/YYYY).
6.	Enter the date that the planned corrective action(s) were actually completed to fully resolve the deficiency (MM/DD/YYYY).
7.	From the drop-down menu, select whether the CAP is Open, Delayed, Closed, Closed-Pending or Cancelled. See IOM, Chapter 7, Section 40.2 for definitions of status options.
8.	
9.	Enter the name of the individual(s) (e.g., First Name, Last Name) responsible for leading the actions to correct the deficiency. CAP Leads must be individuals who have direct knowledge of the deficiency and in a position to facilitate progress milestone actions.
10.	
11.	
12.	Enter the name of the senior official(s) (e.g., First Name, Last Name) accountable for corrective action. The Executive Sponsor is the Senior level official accountable for the weakness and the associated remediation plans.
13.	
14.	Enter all workpaper references, which are internal to the Contractor, that support the corrective action efforts to close this CAP.
15.	Enter the remediation identifier for all IT Security deficiencies. Enter N/A if not applicable.
16.	Document the methodology used and the steps taken to identify the root cause(s) of a deficiency, as well as the identified root cause(s). A single deficiency can have multiple root causes. The identified root cause(s) must be reviewed and approved by the CAP Lead(s) and Executive Sponsor(s). This analysis must be completed before developing the CAP (Field 2) and Progress Milestones (Field 3).
17.	Not for use by Contractor.
18.	Provide a detailed summary of the corrective actions taken associated with the progress milestones, related outcomes, related deliverables (if applicable), percent complete, whether the progress milestone is scheduled to meet the target completion date, and progress inhibitors. <b>Note all information provided shall be restricted to one cell.</b>