

# ***CMS* Information Security (IS) Acceptable Risk Safeguards (ARS)**

***(Rev. 2, Issued: 03-07-14)***

## **Table of Contents**

10.0	Introduction
20.0	Purpose
30.0	SCOPE
40.0	How To Use The Appendices
40.1	CMSR Appendices
40.2	Authentication <i>and E-Authentication</i>
50.0	CMSR Structure
50.1	CMSR Family Numbering and Description
50.2	Control Requirements
50.2.1	Baseline Control
50.2.2	<i>Enhancements</i>
50.2.3	Implementation Standard
50.2.4	Guidance
50.2.5	<i>References</i>
50.2.6	Related Control Requirements
50.2.7	<i>Priority</i>
50.2.8	<i>Assurance</i>
50.3	Assessment Procedures
50.3.1	Assessment Objective
50.3.2	Assessment Methods and Objects
60.0	References

## **List of Tables**

---

Table 50-1. CMSR Security Control Family Descriptions

Table 50-2. Example Implementation Standards for CMSR AC-20

## **Appendices**

---

Appendix A CMS Minimum Security Requirements for High Impact Level Data

Appendix B CMS Minimum Security Requirements for Moderate Impact Level Data

Appendix C CMS Minimum Security Requirements for Low Impact Level Data

Appendix D e-Authentication Standard

## 10.0 Introduction

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The Centers for Medicare & Medicaid Services (CMS) Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR) contain a broad set of required security standards based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security *and Privacy* Controls for Federal Information Systems *and Organizations*, dated *April 2013*, and the *HHS-OCIO Policy for Information Systems Security and Privacy*, dated *July 7, 2011*, and *HHS-OCIO Policy for Information Systems Security and Privacy Handbook*, dated *July 7, 2011*, as well as additional standards based on CMS policies, procedures, and guidance, other federal and non-federal guidance resources and industry leading security practices. This document provides guidance to CMS and its contractors as to the minimum level of required security controls that must be implemented to protect CMS' information and information systems.

Incorporating controls cataloged in this document will ensure that all CMS systems meet a minimum level of *information security and privacy assurance*. However, many CMS systems, particularly those that are mission-critical, or that are available to Internet users, will require additional *technical* security protections as part of CMS' implementation requirements such as the CMS *Technical Reference Architecture (TRA) or any applicable TRA Supplements*. *These documents describe* architecture standards that must be in place for *CMS* systems. Business Owners should refer to <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html> to ensure that all CMS information system development *architecture, design, and lifecycle* requirements are met.

A system may be required to meet additional, higher-level or more rigorous, information protection requirements as mandated by specific federal, legal, program, or accounting sources. For example, the CMSR control "Audit and Accountability" (AU) AU-11 Audit Retention, states that for all systems "the audit records will be retained for ninety (90) days and then archived for one (1) year." However, the National Archives and Records Administration (NARA) has determined that "*Documents relating to periodic audits of teaching facilities nationwide by carriers to recover overpayment*" (NC1-440-78-1, Item B) be retained for four (4) years after completion of an audit. Therefore, if these logs were utilized as part of *such* an audit, the NARA requirements would take precedence. The CMS system must be developed to meet these higher-level standards where applicable. **The ARS shall not be construed to relieve or waive these other standards.**

It is *also* important to note that the ARS does not address specific business-process requirements that ensure business requirements are fulfilled. The goal of the CMSRs is to provide a baseline of *minimal* internal/ *external information security and privacy assurance* controls. It is the responsibility of the Business Owner of CMS systems, with direction provided by the Office of Information Services (OIS), to ensure that all applicable internal/ *external information security and privacy assurance* controls are incorporated into CMS systems. Business Owners must

document and certify the incorporated controls in their respective *security plan* and identify any risks in the corresponding *risk assessment* for their system.

## 20.0 Purpose

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

Protecting and ensuring the confidentiality, integrity, and availability (CIA) for all of CMS' information and information systems is the primary purpose of the *information security and privacy assurance* program. The ARS complies with the CMS Policy for the Information Security and Privacy and the *CMS Policy for the Information Security and Privacy Program*<sup>1</sup> by providing a defense-in-depth security structure along with a least-privilege, need-to-know basis for all information access.

The CMSRs within the ARS are not intended to be an all-inclusive list of security controls nor are they intended to replace a Business Owner's due diligence to incorporate additional controls to mitigate risk. The CMSRs are the minimum security requirements to be considered and employed where applicable throughout the risk management process and the CMS *eXpedited Life Cycle (XLC)*.

## 30.0 SCOPE

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions and performing work on behalf of CMS shall observe the baseline policy statements described in the *CMS Policy for the Information Security and Privacy Program* and the complementary controls defined in the ARS as the minimum security requirements for all CMS information and information systems.

The Business Owner, assisted by the System Developer/Maintainer, has primary responsibility for evaluating the ARS and determining the appropriateness of the CMSRs for their system and ensuring their proper implementation.

A Business Owner may choose to strengthen the control beyond its system security level requirement to provide the best possible protection of CMS' information and information systems. In some cases, a Business Owner may not need to directly implement some specific controls as long as they can adequately demonstrate (and document) that the requirement is satisfied by a parent system.

---

<sup>1</sup> The *CMS Policy for the Information Security and Privacy Program* can be found at <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>.

Sometimes security controls cannot be implemented even at the minimum level due to resource issues such as funding restrictions, personnel constraints or hardware/software limitations. Alternative or compensating controls *may* be implemented to reduce the risk to CMS: its information, information systems, assets and reputation. This must be considered as part of risk management process though the CMS *security assessment and authorization (SA&A)* program. The alternative or compensating controls must be documented in the *security plan*, any remaining risk must be *documented in accordance with current risk assessment procedure*, and approved by the Chief Information Officer (CIO) or his/her designated representative, *using appropriate policy waiver mechanisms*.

## 40.0 How To Use The Appendices

*((Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work))*

The CMSRs provided in Appendices A, B, and C is a detailed resource for understanding all aspects of the CMS defined security controls.

### 40.1 CMSR Appendices

*((Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work))*

Each CMSR Appendix is a set of security controls based on a CMS System Security Level (i.e., High, Moderate, and Low) as established by Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. Each Business Owner is required to determine their system's security level according to *Risk Management Handbook (RMH), Volume II, Procedure 2.3, Categorizing an Information System*, and use that designation to select the appropriate CMSR appendix for defining their minimum set of required security controls. The CMSRs Appendices are:

- Appendix A: CMS Minimum Security Requirements for High Impact Level Data
- Appendix B: CMS Minimum Security Requirements for Moderate Impact Level Data
- Appendix C: CMS Minimum Security Requirements for Low Impact Level Data

Each Appendix includes baseline and enhancement controls, and associated amplifying information, for the indicated security level. The CMSRs include:

- Control text (Baseline and Enhancement Controls)
- Additional CMS or data-type specific standards (e.g., CMS defined variables) to which the control must meet (Implementation Standards)
- Additional guidance for clarifying the control (Guidance)

- The specific laws, standards, or mandates from which the control originated (Reference)
- Related controls (Related Control Requirements)
- Recommended objects and methodologies for assessing compliance with each control. (Assessment Procedure)

While each CMSR contains a significant amount of associated information, it should be noted that this information is provided to the user in order to maximize understanding of, not only the controls, but also the expectations for reaching compliance and the methodologies that will be used to verify compliance.

## **40.2 Authentication *and E-Authentication***

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

CMSR IA-2 is the baseline control for *organizational user authentication requirements*. *IA-8 is the baseline for non-organizational user authentication requirements (i.e., “e-Authentication”).* Included with the baseline are the enhancements establishing the minimum *authentication* control requirements. The specific implementation of local and remote *authentication and e-Authentication* controls are described in *RMH, Volume III, Standard 3.1*, and CMS Authentication *Standards*.

## **50.0 CMSR Structure**

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

### **50.1 CMSR Family Numbering and Description**

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The security controls have a well-defined organization and structure. They are organized into 18 control families for ease of use in the security control selection and specification process. The families are established by NIST SP 800-53, and are in alignment with the 18 security-related

areas specified in FIPS 200<sup>2</sup>, Minimum Security Requirements for Federal Information and Information Systems, and 8 privacy families listed in Appendix J<sup>3</sup> of the NIST SP 800-53.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each of the 18 security control families and 8 privacy control families. Table 1 summarizes the 26 security control families and the applicable two-character identifier used in the CMSRs.

**Table 50-1. CMSR Security Control Family Descriptions**

Family (and Identifier)	Description
Access Control (AC)	The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
Awareness and Training (AT)	The standards listed in this section focus on how the organization shall: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.
Audit and Accountability (AU)	The standards listed in this section focus on how the organization shall: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Security Assessment and Authorization (CA)	The standards listed in this section focus on how the organization shall: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

<sup>2</sup> Of the eighteen security control families in NIST Special Publication 800-53, seventeen families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS Publication 200. One additional family (Program Management [PM] family) provides controls for information security programs required by FISMA. This family, while not specifically referenced in FIPS Publication 200, provides security controls at the organization level rather than the information system level.

<sup>3</sup> Privacy controls listed in Appendix J, have an organization and structure similar to security controls, including the use of two-character identifiers for the eight privacy families.

---

CMS Information Security (IS) Acceptable Risk Safeguards (ARS)

---

Family (and Identifier)	Description
Configuration Management (CM)	The standards listed in this section focus on how the organization shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
Contingency Planning (CP)	The standards listed in this section focus on how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Incident Response (IR)	The standards listed in this section focus on how the organization shall: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
Maintenance (MA)	The standards listed in this section focus on how the organization shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	The standards listed in this section focus on how the organization shall: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
Physical and Environmental Protection (PE)	The standards listed in this section focus on how the organization shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
Planning (PL)	The standards listed in this section focus on how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.



CMS Information Security (IS) Acceptable Risk Safeguards (ARS)

Family (and Identifier)	Description
Personnel Security (PS)	The standards listed in this section focus on how the organization shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Risk Assessment (RA)	The standards listed in this section focus on how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
System and Services Acquisition (SA)	The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate <i>information security and privacy assurance</i> considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection (SC)	The standards listed in this section focus on how the organization shall: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective <i>information security and privacy assurance</i> within organizational information systems.
System and Information Integrity (SI)	The standards listed in this section focus on how the organization shall: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.
<i>Program Management (PM)</i>	<i>The PM family provides controls for information security programs required by Federal Information Security Management Act (FISMA). This family, while not specifically referenced in FIPS Publication 200, provides security controls at the organization level rather than the information system level.</i>
<i>Authority and Purpose (AP)</i>	<i>This family furthers compliance with the Privacy Act by ensuring that organizations: (i) identify the legal bases that authorize a particular Personally Identifiable Information (PII) collection or activity that impacts privacy; and (ii) specify the purpose(s) for which they collect PII in their notices.</i>
<i>Accountability, Audit, and Risk Management (AR)</i>	<i>This family is intended to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that an organization is complying with all applicable privacy protection requirements and minimizing its overall privacy risk.</i>

Family (and Identifier)	Description
<i>Data Quality and Integrity (DI)</i>	<i>This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the public notice.</i>
<i>Data Minimization and Retention (DM)</i>	<i>This family assists organizations in implementing the data minimization and retention elements of the Privacy Act, which requires organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a NARA-approved record retention schedule.</i>
<i>Individual Participation and Redress (IP)</i>	<i>This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.</i>
<i>Security (SE)</i>	<i>This family supplements the security controls in Appendix F to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with Office of Management and Budget (OMB) policies and guidance. The controls in this family are implemented in coordination with information security personnel using the existing NIST Risk Management Framework.</i>
<i>Transparency (TR)</i>	<i>This family implements Sections 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization's information practices and the privacy impact of government programs and activities.</i>
<i>Use Limitation (UL)</i>	<i>This family is intended to assist organizations in complying with the Privacy Act, which prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the Controls in this Family will ensure that the scope of PII use is limited accordingly.</i>

*Some Controls, Enhancements, Implementation Standards and Guidance, or portions thereof, only pertain to narrowly-defined types of data, such as Protected Health Information (PHI), PII or Federal Tax Information (FTI). Additionally, some requirements may only apply within specific implementation scenarios. The approved migration of data into a Federal Risk and Authorization Management Program (FedRAMP)-approved Cloud Service Provider (CSP) for instance, may require the unique application of specific Controls, Enhancements, Implementation Standards or Guidance that are only applicable in this specific scenario. These specialized requirements will be indicated with a “(For XXX only)” in the text immediately preceding the applicable section within the ARS—where “XXX” will serve as an acronym or short description to indicate the type of data or scenario where that portion of the applicable text uniquely applies.*

*All other text, where no “(For XXX only)” is indicated, are CMS-wide control elements that shall be implemented at the designated system security level for all CMS information, information systems, and scenarios.*

## 50.2 Control Requirements

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The CMS security control structure consists of the Baseline or Enhancement section, Guidance section, References section, Related Requirements section and Assessment Procedures section. In addition, the baseline *and enhancements controls may* have a sub-section for Implementation Standards *that* will be associated with that baseline *or enhancement*.

The CMS-tailored security controls serve as the starting point for organizations in determining the appropriate controls and countermeasures necessary to protect their information systems.

### 50.2.1 Baseline Control

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The Baseline control is the concise statement specifying the capability needed to protect a particular aspect of the CMS information or information system at *the applicable* system security level.

Baseline *ARS* controls are identified by security control Family ID and convey CMS policy, which are based on *minimum Federal requirements, and:*

*Employ, and correlate directly to, NIST 800-53*

- Numbering (e.g., AC-1, AC-2, AC-3...)
- Use CMS designators *for additional requirements* where a direct NIST correlation *is* not made (e.g., AC-CMS-1.)
- Ordered such that the CMS designators always follow the complete set of NIST designators and always restart the numbering of the CMS designator at 1 (e.g. AC-1, AC-2, AC-3, AC-4, AC-5 ...AC-CMS-1.)

The baseline section includes the following:

- Control Requirement
- Implementation Standards (may not exist for all Baseline controls)
- Guidance (may not exist for all Baseline controls)

- References
- Related Control Requirements
- Assessment Procedure
  - Assessment Objectives
  - Assessment Methods and Objects

### **50.2.2    *Enhancements***

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

*Enhancements* supplement baseline controls to achieve the overall required level of protection in accordance with the system security level. Enhancements may only be required for higher system security level baselines, but may be used to strengthen the level of protection provided in lower system security level systems if deemed appropriate by the Business Owner.

The enhancement controls are structured the same as the baseline controls. Each enhancement section is as follows:

- Control Requirement
- *Implementation Standards* (may not exist for all Enhancements)
- Guidance (may not exist for all Enhancements)
- References
- Related Control Requirements
- Assessment Procedure
  - Assessment Objectives
  - Assessment Methods and Objects

### **50.2.3    Implementation Standard**

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

When an implementation standard is indicated, it is associated with a baseline control *or enhancement*. The purpose of the implementation standard is to provide CMS tailored controls for implementation of the associated baseline.

Some standards may contain specific CMS definitions or event values (such as “90 days”) to be implemented as the compliance standard for a given control. Other implementation standards are based on specific types of data such as Protected Health Information (PHI), Personally Identifiable Information (PII), or Federal Tax Information (FTI).

For example, AC-20’s second implementation standard, at the High system security level states:

“(For PII only) only organization owned computers and software can be used to process, access, transmit, and store PII.”

This particular implementation standard is used by organizations responsible for PII information.

Similar implementation standards exist and apply for organizations responsible for PHI or FTI data, *or for scenarios where FedRAMP-approved CSPs are used*. All other implementation standards, where no “(For XXX only)” is indicated, are CMS implementation controls that shall be implemented at the designated system security level for all CMS information and information systems.

0 shows an example of *a possible* implementation standard associated with CMSR AC-20. Implementation Standard item 1<sup>4</sup> is a CMS-specified control *that* applies to all CMS information and information systems. Item 2 is specifically designated for those organizations responsible for PII and must be followed for implementation, assessment, and audit.

**Table 50-2. *Example* Implementation Standards for CMSR AC-20**

Implementation Standard(s) <i>[Example]</i>
<ol style="list-style-type: none"> <li>1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.</li> <li>2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII.</li> </ol>

*The RMH, Volume III, Standard 7.1, Incident Handling*, provides definitions for PII, PHI and FTI. Organizations responsible for these types of information must provide *the* additional safeguards as defined in the *applicable* implementation standards.

## 50.2.4 Guidance

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The CMSRs may include additional Guidance to explain the intent of the control. In some cases, these include specific CMS desires or recommendations, or may refer to other CMS or NIST publications for further guidance. It is a *recommended* security practice to refer to the guidance

<sup>4</sup> When referenced outside of the context of the specific CMSR, implementation standards may be referred to (more specifically) as AC-20.Std.1, AC-20.Std.2, etc.

and procedures for additional information to *have a clearer and more detailed understanding of specifics of the requirement to assist* the organization meeting the CMS security requirements.

## 50.2.5 References

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The references section identifies the source documents and section or paragraph designations that are the basis or source for the applicable CMSR. For example, an *Internal Revenue Service (IRS)* reference *may* look like *this*: IRS-1075: 5.6.3.2#1. From this example:

- The IRS-1075 is the publication.
- The 5.6.3.2#1 portion is the section with sub-paragraphs leading to the applicable reference used for the control requirement—*where the numbers before the “#” represent the actual numbered Section within the reference document, and the number after the “#” represents the unnumbered paragraph within the referenced Section.*

## 50.2.6 Related Control Requirements

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

Many, but not all, CMSRs may be related to one or more other CMSRs. When addressing some CMSRs, it may be important that their *implementation documentation* during an assessment or audit be consistent with one or more related CMSRs. At the very least, organizations shall take care to ensure that related CMSR *implementations* do not conflict. While every effort was made to identify related CMSRs, other unidentified relationships may exist that are unique to a particular system, contract type, or organization.

## 50.2.7 Priority

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

*The priority value listed on the right side of the Control or Enhancement title provides the recommended priority codes used for sequencing decisions during security control implementation. Organizations can use the priority code designation associated with each security control to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control, a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the security control is not selected (or has been withdrawn) for any baseline). This recommended sequencing prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of*



*security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all of the security controls in the security plan have been implemented. The priority codes are intended only for implementation sequencing, not for making security control selection decisions.*

### **50.2.8-Assurance**

***(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)***

*Two fundamental components affecting the trustworthiness of information systems are security functionality and security assurance. Security functionality is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system—thus possessing the capability to accurately mediate and enforce established security policies. Security controls address both security functionality and security assurance. Some controls focus primarily on security functionality (e.g., PE-3, Physical Access Control; IA-2, Identification and Authentication; SC-13, Cryptographic Protection; AC-2, Account Management). Other controls focus primarily on security assurance (e.g., CA-2, Security Assessment; SA-17, Developer Security Architecture and Design; CM-3, Configuration Change Control). Finally, certain security controls can support security functionality and assurance (e.g., RA-5, Vulnerability Scanning; SC-3, Security Function Isolation; AC-25, Reference Monitor). Security controls related to functionality are combined to develop a security capability with the assurance-related controls implemented to provide a degree of confidence in the capability within the organizational risk tolerance.*

*The CMSRs specify assurance-related controls with an “A” in the controls header to identify the security controls that have assurance-related characteristics or properties (i.e., assurance-related controls). Assurance-related controls are discussed in greater detail in NIST SP 800-53 (as amended), Appendix E, Assurance and Trustworthiness, to include the allocation of such controls to security control baselines. There is no summary table provided in the NIST SP 800-53 Appendix E for the Program Management (PM) family or the Privacy families since PM and Privacy controls are not associated with any particular security control baseline.*

## **50.3 Assessment Procedures**

***(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)***

The Assessment Procedures, including Assessment Objectives, and Assessment Methods and Objects, help determine if the security *control implementations* in the information system are effective (i.e., implemented correctly, operating as intended, and producing the desired outcome). They provide a foundation to support the security *assessment and authorization* process. The Assessment Procedure consists of a set of procedural steps that are designated to achieve one or more objectives by applying methods to assessment objects.

### **50.3.1 Assessment Objective**

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The Assessment Objectives include a set of determination statements (“Determine if...”) related to the particular security control under assessment. The determination statements are closely linked to the content of the security control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

Assessment Objectives establish the expectations for security control assessments based on the assurance requirements defined in the security control. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Each of the Assessment Objective determination statements is either traceable to requirements *within* the baseline or enhancement security control. This ensures that all aspects of the security control are *fully* assessed and that any weaknesses or deficiencies in the control can be identified, and *corrective* actions taken *(usually in the form of a Plan of Actions and Milestones [POA&M])*.

### **50.3.2 Assessment Methods and Objects**

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The assessment methods define the nature of the assessor’s actions and include Examine, Interview, and Test. The assessment object identifies the specific item being assessed including specifications, mechanism, activities, and individuals. The application of an assessment procedure to a security control produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the control.

## **60.0 References**

*(Rev.2, Issued: 03-07-14, Effective: 04-07-14, Implementation: 03-09-15, October 6, 2014-VMS to Implement the Client Letter Work)*

The CMS *information security and privacy assurance* program and ARS were developed in accordance with Federal mandates and CMS requirements for the handling and processing of CMS’ information and information systems. A list of applicable laws across the program *is* provided below:

- Public Law 74-271, Social Security Act, as amended  
[http://www.ssa.gov/OP\\_Home/ssact/ssact.htm](http://www.ssa.gov/OP_Home/ssact/ssact.htm).
- Public Law 93-579, The Privacy Act of 1974, as amended  
<http://www.justice.gov/opcl/privstat.htm>



- Public Law 104-13, Paperwork Reduction Act of 1995, as amended  
<http://www.fws.gov/policy/library/rgpl104-13.pdf>
- Public Law 108–173, Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), SEC. 912: Requirements for Information Security for Medicare Administrative Contractors  
<http://www.gpo.gov/fdsys/pkg/BILLS-108hr1enr/pdf/BILLS-108hr1enr.pdf>
- Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability,  
<http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=5:2.0.1.1.7&idno=5>
- United States Code Title 44 Chapter 33—Disposal of Records  
<http://www.archives.gov/about/laws/disposal-of-records.html>
- GAO-09-232G, Federal Information System Controls Audit Manual (FISCAM), February 2, 2009  
<http://www.gao.gov/new.items/d09232g.pdf>
- OMB Circulars can be found at the CMS web site or at:  
<http://www.whitehouse.gov/omb/circulars/index.html>
- Homeland Security Presidential Directives can be found at:  
<http://www.dhs.gov/xabout/laws/>.
- Executive Orders can be found at:  
<http://www.archives.gov/federal-register/executive-orders/disposition.html>
- A list of NIST special publications and FIPS publications can be found at:  
<http://csrc.nist.gov/publications/>
- The most recent Internal Revenue Service publication 1075 can be found at:  
<http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- *HHS-OCIO Policy for Information Systems Security and Privacy, dated July 7, 2011*  
<http://www.hhs.gov/ocio/policy/index.html#Security>
- *HHS-OCIO Policy for Information Systems Security and Privacy Handbook, dated July 7, 2011 (available upon request via <mailto:ciso@cms.hhs.gov>)*

Additional CMS documents were used as references in the development of this manual. The CMS *information security* web site at <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/> provides a list of applicable CMS documents across the *information assurance* program.