Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Workbook:

Test Scripts for System Security Assessments

FINAL
Version 1.0
August 31, 2010

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *TEST SCRIPTS FOR SYSTEM SECURITY ASSESSMENT*S, VERSION 1.0

1) Publication revised to version 1.0 to synchronize with *CMS Acceptable Risk Safeguards* manual version change due to incorporation ito CMS Internet Only Manual inventory.

SUMMARY OF CHANGES IN *TEST SCRIPTS FOR SYSTEM SECURITY ASSESSMENT*S, VERSION 4.0

1) Initial publication started at version 4.0 to synchronize with *CMS Acceptable Risk Safeguards* manual.

(This Page Intentionally Blank)

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health & Human Services (DHHS) have prepared a set of security assessment scripts based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*.

The Test Scripts for System Security Assessments are based on the required security controls from NIST SP 800-53A, the *CMS Policy for the Information Security Program (PISP)*, and the *CMS Minimum Security Requirements*. Additional references to the *Government Accountability Office (GAO) Federal Information Systems Controls Audit Manual (FISCAM)* are included to ensure that GAO standards are identified as part of the evaluation criteria. The scripts also reference other legislative mandates such as the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, the *Internal Revenue Service (IRS) Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies*, and other reference materials. This document establishes the minimum testing criteria baseline for each security control to be utilized by CMS and its security assessment contractors.

All federal systems must conduct Certification and Accreditation (C&A) of their information systems and incorporate information security controls to protect federal information assets in accordance with the *Federal Information Security Management Act of 2002 (FISMA).* Also, the Office of Management and Budget (OMB) through Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires executive agencies within the federal government to plan for security; ensure that appropriate officials are assigned security responsibility; review the security controls in their information systems; and authorize system processing prior to operations and periodically thereafter. CMS defines its C&A process in the *CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedures*. The security assessment, which will leverage the scripts to determine compliance with the applicable information security controls, is part of the CMS IS C&A Program.

2 PURPOSE

The purpose of the scripts is to ensure that the defined IS minimum requirements for CMS systems are tested uniformly based on its system security level by CMS and its contractors. The scripts are not intended to be an all-inclusive list and will be subject to regular updates to reflect the changing technological and regulatory environment. The scripts are not intended to replace a Business Owner’s due diligence to incorporate additional controls in order to mitigate any identified risk.

Each CMS system has an assigned system security level based on its confidentiality, integrity and availability requirements. Each set of scripts to be used for a system is based on its system security level. The assessment levels provide assessors with reference points as to what results are acceptable for the determination of security control effectiveness based on its system security level. The system security level of the scripts reflects the minimum thresholds for information security controls.

3 HOW TO USE THIS DOCUMENT

The scripts have a well-defined organization and structure which has been based on the security controls as presented within the NIST SP 800-53A. In addition, the format is designed to afford the tester a vehicle to record the results of their assessment. The scripts have been divided into the seventeen (17) security service family categories. A unique two-character identifier is assigned to each family. For example, the 2-character identifier for the Risk Assessment family is “RA”.

Table 1 summarizes the security service families and the associated identifiers.

Table 1 Family Identifier

SECURITY SERVICE FAMILY	IDENTIFIER
Access Control	AC
Awareness and Training	AT
Audit and Accountability	AU
Certification, Accreditation, and Security Assessments	CA
Configuration Management	CM
Contingency Planning	CP
Identification and Authentication	IA
Incident Response	IR
Maintenance	MA
Media Protection	MP
Physical and Environmental Protection	PE
Planning	PL
Personnel Security	PS
Risk Assessment	RA
System and Services Acquisition	SA
Systems and Communication	SC
System and Information Integrity	SI

Each of the seventeen (17) security service families has been classified further into sub-categories or security controls related to the security function of the family. To identify each control, a unique numeric identifier is appended to the family identifier to indicate the number of the control within the control family. For example, CP-9 is the ninth control in the Contingency Planning family.

Each security control has a control baseline which is the minimum security control defined for a low-impact, moderate-impact, or high-impact information system. Each of the security control baselines may have additional Security Control Enhancements which are statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

The Security Control Enhancements are derived from statements made in NIST 800-53A, CMSRs, other CMS specific controls and FISMA controls. These are all documented within the enhancement control section.

For ease of use, the scripts have been organized into a table format. The table has also been designed with appropriate columns to record notes and findings when an assessment is performed. Each security service family starts on a new page in order to separate the controls for a particular test. The tester should record test activities, such as documents reviewed or persons interviewed, directly on the script template whenever possible. When used properly the test script pages will become a significant part of the "Working Papers" section of the assessment report.

The script table has the following items:

3.1 CONTROL REQUIREMENTS

To uniquely identify each control requirement, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family. For example, PS-2 is the second security requirement in the Personnel Security family. If you are looking at the first security requirement in Appendix A, this would be AC-1 – Access Control Policy and Procedures (High) or the first security requirement in the Access Control family. Included is the specific control requirement title and at what level. As indicated on the first page of Appendix A, AC-1 is: **Access Control Policy and Procedures (High).**

The security control requirement structure consists of the security requirement section (baseline for ease of use), guidance section, applicability section, reference section and related controls section. An important sub-section of the baseline security requirement section is the implementation standards. Additional information for the security requirement is included in the enhancement security requirement section. The enhancement security requirement contains the same sub-sections as the baseline control requirement, but without any implementation standards included for each. The implementation standards will only be found in the baseline security requirement.

The baseline security requirements contain the following sections and sub-sections:

- Control Requirement
- Implementation Standard
- Guidance (optional)
- Applicability
- References
- Related Control Requirements
- Assessment Procedures

3.1.1 BASELINE CONTROL REQUIREMENTS

The control requirement, as applied or implemented, is the CMS concise statement specifying the capability needed to protect the CMS particular aspect of the CMS data or system at that sensitivity level.

There are two types of CMS security controls; one being the baseline control requirement and the other is the enhancement security control requirement. Additionally, CMS has more definitively specified extraordinary situations. For example, PS-CMS-1 is an added baseline control requirement which meets specific needs for CMS data protection.

3.1.2 IMPLEMENTATION STANDARD

When an implementation standard is indicated, it is associated with a baseline security requirement. The purpose of the implementation standard is to provide a tailored CMS definition or event with a value, such as 90 days, to be implemented and/or audited. An example of a list of implementation standards can be found in Appendix A under security control requirement AC-2.

Some 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 has two implementation standards. The second implementation standard 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 having PII data. The same applies when an organization has PHI or FTI data. Note: All other implementation standards are ‘CMS’ implementation standards and shall be implemented at the designated impact level.

In table 4, the AU-11, implementation standard item 1 is a specific CMS standard. Items 2 through 4, inclusive, are specifically designated for those organizations which hold PII. That is these implementation standards must be followed for implementation, assessment or audit.

Table 2 Implementation Standards

Implementation Standard(s)
1) Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year.
2) (For PII only) Employ mechanisms to facilitate the review of PII disclosure/access records and retain the records for five (5) years or the applicable records control schedule, whichever is longer.
3) (For PII only) To support the audit of activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever PII is stored.
4) (For PII only) Inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

Table 5, handling of special information, provides definitions for the use of organizations holding, storing and transmitting PII, PHI and FTI. Organizations holding these types of information must provide additional safeguards and follow more specific security requirements. The designated implementation standards apply for these organizations.

Table 3 Handling of Special Information

Term	Definition
Personally Identifiable Information (PII)	Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.
Protected Health Information (PHI) or Individually Identifiable Health Information	Individually identifiable health information that is: • transmitted by electronic media, • maintained in electronic media, or • transmitted or maintained in any other form or medium. (HIPAA) **NOTE:** PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.
Federal Tax Information (FTI)	Generally, Federal Tax Returns and return information are confidential, as required by IRC Section 6103. The information is used by the IRS to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality.

3.2 GUIDANCE

For, most but not all, security control requirements there is a section pertaining to guidance which provides additional information such as NIST SP 800-92 for computer security log management. It is good security practice to refer to the guidance for additional information and procedures to allow the organization to meet the CMS baseline security requirements. In some cases, enhancement security requirements may have a guidance section.

3.3 APPLICABILITY

All CMSRs in a selected control requirement set apply UNLESS a specific contract/entity type is specified as an exception or optional in the applicability section. Because CMS may add new contract types and/or systems that use the CMSR, due diligence requires that all security control requirements be met unless a control requirement is deemed optional for a specific contract/entity type. Refer to the bulleted list below for the current CMS contract types with predefined exceptions.

- ABMAC – A/B Medicare Administrative Contractor
- COB – Coordination of Benefits
- CWF – Common Working File [Host]
- DC – Data Center

- DMEMAC – Durable Medical Equipment Medicare Administrative Contractor
- EDC – Enterprise Data Center
- PartA – Part A Fiscal Intermediary
- PartB – Part B Carrier
- PSC – Program Safeguard Contractor
- QIC – Quality Integrity Contractor
- RAC – Recovery Audit Contractor
- SS – Standard System [Maintainer]
- ZPIC – Zone Program Integrity Contractor

3.4 REFERENCES

The references section identifies the source documents and section or paragraph designations that are the basis or source for the applicable CMSR security control requirement. For example an IRS reference would look like: 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.

3.5 RELATED CONTROL REQUIREMENTS

Many, but not all, CMSRs may be related to one or more other CMSR security control requirements. When addressing some CMSRs, it may be important that their responses 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 responses 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.

3.6 ENHANCEMENT CONTROL REQUIREMENTS

The enhancement control requirements are laid out the same at the baseline control requirements but at this time do not contain any implementation standards. Each enhancement section is as follows:

- Control Requirement
- Guidance (optional)
- Applicability

- References
- Related Control Requirements
- Assessment Procedures

The implementation standard for the baseline control requirement may be sufficient to determine if the organization is in compliance with the control requirement. However, even without implementation standards for the enhancement control requirement, there are assessment procedures for each that can assist in determination of the organization's control requirement compliance.

3.7 ASSESSMENT PROCEDURES

The assessment procedures section (i.e., Assessment Objectives, and Assessment Methods and Objects) in the CMSRs directly support the validation of individual control effectiveness. The primary objective of the assessment procedures is to help determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system). The security assessment procedures defined in the CMSRs provide a foundational level of assessment to support the security certification process. The "Assessment Procedures" are identified using their applicable control identifier (e.g., AC-1, AC-2(1), etc.) followed by a numerical decimal identifier (e.g., AC-1.1, AC-2(1).1, etc.).

3.7.1 ASSESSMENT OBJECTIVE

The "Assessment Procedure" consists of a set of procedural steps that are designed to achieve one or more assessment objectives by applying assessment methods to assessment objects.

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 in the baseline or enhancement security control, or the guidance. This ensures that all aspects of the security control are assessed and that any weaknesses or deficiencies in the control can be identified and remediation actions taken.

NIST SP 800-53A (as amended), Appendix E, Assessment Expectations, provides an explanation of the expectations of security assessments by impact level. These 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. Organizations are expected to review and use the NIST SP 800-53A assessment expectations as guidance during their assessments.

Table 4 summarizes the assessment expectations for Low-impact, Moderate-impact, and High-impact information systems.

Table 4 Assessment Expectations by Information System Impact Level

Assessment Expectations	Impact Level Low	Impact Level Moderate	Impact Level High
Security controls are in place with no obvious errors.	X	X	X
Increased grounds for confidence that the security controls are implemented correctly and operating as intended.	-	X	X
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	-	-	X

The decision to reduce the level of effort for the assessment of security controls in Low-impact and Moderate-impact information systems does not affect the basic requirements in the control as stated in the CMSRs. The decision to employ optional determination statements and assessment methods should be a decision guided by an organizational assessment of risk with input from key organizational officials with a vested interest in the assessment and with responsibility for carrying out or supporting CMS missions and business functions.

3.7.2 ASSESSMENT METHODS AND OBJECTS

The Assessment Procedure consists of a set of procedural steps that are created to achieve one or more Assessment Objectives by applying assessment methods to assessment objects. As stated in the previous section, the assessment objectives include a set of determination statements related to the particular security control under assessment. The application of assessment procedures to a security requirement produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the security requirement.

The three (3) assessment methods defined in the processing component of the framework include Examine, Interview, and Test. NIST SP 800-53A (as amended), Appendix D, Assessment Method Descriptions, provides a detailed explanation of these three (3) assessment methods. Organizations are expected to review and use the NIST SP 800-53A assessment method explanations as guidance during their assessments.

Table 5 summarizes the hierarchal order of the three (3) assessment methods and their definition.

Table 5 Assessment Method Hierarchy and Definitions

Assessment Method	Definition
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.
Interview	The process of conducting focused discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.
Test	The process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of the security control effectiveness.

Each of the assessment methods (Examine, Interview, and Test) includes a set of attributes: Depth and Coverage. NIST SP 800-53A (as amended), Appendix D, Assessment Method Descriptions, provides detailed explanations of the assessment method Depth and Coverage attribute values. Organizations are expected to review and use the NIST SP 800-53A assessment method depth and coverage attribute value explanations as guidance during their assessments.

Table 6 summarizes the assessment method attributes values by information system impact level.

Table 6 Assessment Method Attributes and Attribute Values by Impact Level

Assessment Methods Examine, Interview, Test	Information System Impact Level		
Attribute	Low	Moderate	High
Depth	Generalized	Focused	Detailed
Coverage	Representative	Specific	Comprehensive

The attribute values for the assessment methods (which describe the rigor and level of detail associated with the assessment) are hierarchical in nature. For the Depth attribute, the Focused attribute value includes and builds upon the assessment rigor and level of detail defined for the Generalized attribute value; the Detailed attribute value includes and builds upon the assessment rigor and level of detail defined for the Focused attribute value. For the Coverage attribute, the Specific attribute value includes and builds upon the number and type of assessment objects defined for the Representative attribute value; the Comprehensive attribute value includes and builds upon the number and type of assessment objects defined for the specific attribute value.

NIST SP 800-53A (as amended), Appendix E, Assessment Expectations, provides detailed explanations of the assessment objects. Organizations are expected to review and use the NIST SP 800-53A assessment object explanations as guidance during their assessments.

Table 7 summarizes the assessment objects and their definitions.

Table 7 Assessment Objects and Definitions

Assessment Object	Definition
Specifications	The document-based artifacts (e.g., policies, plans, procedures, system requirements, designs) associated with an information system.
Mechanisms	The specific hardware, software, or firmware safeguards and countermeasures employed within an information system. These also include physical protection devices associated with an information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes).
Activities	The specific protection-related pursuits or actions supporting an information system that involve people (e.g., system operations, administration, and management; exercises).
Individuals	The people or groups of people applying the specifications, mechanisms, or activities described above.

Recognizing that organizations can specify, organize, document, and configure their information systems in a variety of ways, the assessment objects identified in the CMSRs that are provided in conjunction with the Interview, Examine, and Test assessment methods should be considered suggested objects where information/evidence may be found. As such, assessors are expected to use their judgment in applying the designated assessment methods to the associated set of assessment objects. Each assessment method listed in a procedural step should be applied to a sufficient number of assessment objects to produce the information necessary to make the determination in the determination statement and to satisfy the assessment objective. It may not always be necessary (or possible) to apply each assessment method to every assessment object in the CMSR list.

4 FINDINGS

The findings are the deficiencies resulting from applying the methods to the objects when assessing if the implemented control(s) meet the objective.

4.1 REQUIREMENTS MET?

This column enables the assessor/tester to incorporate their overall results.

- Mark “Y” for a “yes” when the requirement has been fully met and initial for each basement objective being met. Include references to the documentation, work papers or test results that demonstrate compliance with the requirement in the “Comments and Documentation References” section.

- Mark “N” for a “no” if the requirement is partially met or not met and initial each assessment objective that is not met. Include references to the documentation, work papers or test results that demonstrate partial compliance with the requirement in the “Comments and Documentation References” section.

4.2 COMMENTS AND DOCUMENTATION REFERENCES

This row is for recording the status of the reference materials being reviewed; the type of settings being observed, the relevant policies and procedures, the type of testing being performed; the persons that were interviewed; etc. for each security control being evaluated.

All boxes that apply must be checked and a brief explanation must be documented under "explain why" to justify the decision for "Requirements Met or Not Met". Include any other notations or comments germane to the evaluation.

This row also includes a gray colored cell for recording the "Document Request List Number" from the file that is provided during the initial period to the Business Owner by the Evaluator. This number tracking will act as a cross check of documents reviewed to enable an auditor to track back to the document being referenced.

5 COMPLETING THIS DOCUMENT

The document will be considered complete when all of the answer fields contain an appropriate Yes or No. The assessment team should collaborate to ensure that all sections have been answered. Assessors/testers should initial each page to denote their completion of the items on the page. This will also assist future review of the script information by identifying the assessor/tester for any given section.

NOTE: As soon as the template begins to be populated with testing results, the document becomes sensitive information and requires special handling as defined in the CMS IS ARS.

6 APPROVED

Charles
R. Brewer

Digitally signed by Charles R.
Brewer
DN: c=US, o=U.S. Government,
ou=HHS, ou=CMS, ou=People,
cn=Charles R. Brewer,
0.9.2342.19200300.100.1.1=2000
389294
Date: 2010.08.26 12:11:30 -04'00'

August 31, 2010

C. Ryan Brewer
CMS Chief Information Security Officer and
Director, Office of the Chief Information Security Officer

Date of Issuance

(This Page Intentionally Blank)